Cisco Secure Firewall Management Center Device Configuration Guide, 7.3 [英語]

最終更新：2026 年 1 月 27 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2023 Cisco Systems, Inc. All rights reserved.

目 次

第 I 部 : デバイス設定のスタートアップガイド 85

第 1 章 デバイス管理 1

デバイス管理について 1

Firewall Management Center およびデバイス管理について 1

Secure Firewall Management Center で管理できるデバイス 2

管理接続について 3

ポリシーとイベント以外の機能 4

デバイス管理インターフェイスについて 4

Firewall Threat Defense の管理インターフェイスとイベントインターフェイス 4

管理のための Firewall Threat Defense データインターフェイスの使用について 5

デバイスモデルごとの管理インターフェイスのサポート 6

管理インターフェイス上のネットワークルート 7

NAT 環境 8

管理およびイベント トラフィック チャネルの例 10

デバイス管理の要件と前提条件 11

デバイスのコマンド ライン インターフェイス（CLI）へのログイン 12

Firewall Threat Defense 初期設定の完了 14

Firewall Device Manager を使用した Firewall Threat Defense の初期設定の完了 14

CLI を使用した Firewall Threat Defense 初期設定の実行の完了 21

イベントインターフェイスの設定 29

デバイスの管理 32

デバイス グループの追加 33

Management Center への登録 34

デバイスの追加 34
新しい Management Center への登録 38
Firewall Management Center からのデバイスの削除（登録解除） 39
デバイスのシャットダウンまたは再起動 41
マネージャの切り替え 42
Firewall Device Manager から Firewall Management Center への切り替え 42
Firewall Management Center から Firewall Device Manager への切り替え 48
Cisco Secure Firewall 3100 での SSD のホットスワップ 49
デバイス管理の履歴 52

第 2 章 デバイス設定 55
全般設定の編集 55
別のデバイスへの構成のコピー 57
デバイス設定のエクスポートとインポート 59
ライセンス設定の編集 63
システム情報の表示 64
デバイス インベントリの表示 65
検査エンジンの表示 65
正常性設定の編集 66
管理設定の編集 66
冗長マネージャアクセス用データインターフェイスの設定 66
マネージャ アクセス インターフェイス設定の変更 72
デバイス IP アドレスを変更する 72
Firewall Management Center IP アドレスの変更 86
Firewall Management Center と Threat Defense の両方の IP アドレスの変更 87
マネージャ アクセス インターフェイスの変更 91
管理接続のトラブルシューティング 104
Firewall Management Center の接続が失われた場合の構成の手動ロールバック 104
データインターフェイスでの管理接続のトラブルシューティング 106
インベントリ詳細の表示 111
適用されたポリシーの編集 111

詳細設定の編集 113
自動アプリケーションバイパスの設定 115
オブジェクトグループ検索の構成 116
インターフェイス オブジェクトの最適化の設定 117
展開設定の編集 118
クラスタのヘルスモニター設定の編集 121
デバイス設定の履歴 127

第 3 章 ユーザー 131
ユーザについて 131
内部および外部ユーザ 131
CLI アクセス 132
CLI ユーザー ロール 132
デバイスのユーザーアカウントの要件と前提条件 133
デバイスのユーザーアカウントの注意事項と制約事項 133
CLI での内部ユーザーの追加 134
FTD の外部認証の設定 136
Firewall Threat Defense の外部認証について 136
LDAP について 137
RADIUS について 137
Firewall Threat Defense 用の LDAP 外部認証オブジェクトの追加 138
Firewall Threat Defense 用の RADIUS 外部認証オブジェクトの追加 144
FTD デバイスのユーザーに対する外部認証の有効化 150
LDAP 認証接続のトラブルシューティング 150
ユーザーの履歴 152

第 4 章 設定の展開 155
設定の展開について 155
展開が必要な設定変更 155
展開のプレビュー 156
選択的ポリシーの展開 158

システムユーザー名 161
アプリケーションディテクタの自動有効化 162
ネットワーク検出ポリシーの変更によるアセットの再検出 162
Snort 再起動のシナリオ 162
デバイスの再起動の警告 163
ポリシー適用中のトラフィックの検査 164
Snort の再起動によるトラフィックの動作 165
展開またはアクティブ化された際に Snort プロセスを再起動する設定 167
変更により Snort プロセスがただちに再起動する場合 169
ポリシー管理の要件と前提条件 170
設定変更を展開するためのベストプラクティス 170
設定の展開 172
設定変更の展開 172
デバイスへの既存の設定の再展開 179
展開の管理 180
展開ステータスの表示 180
展開履歴の表示 180
展開のロールバック 185
ロールバックの実行 188
展開ロールバック トランスクリプトの表示 190
ポリシーの比較 190
現在のポリシーレポートの生成 192
設定の展開の履歴 193

第 II 部 : デバイスの操作 197

第 5 章 トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード 199
ファイアウォール モードについて 200
ルーテッド ファイアウォール モードについて 200
トランスペアレント ファイアウォール モードについて 200
ネットワークでのトランスペアレント ファイアウォールの使用 200

ルーテッド モード機能のためのトラフィックの通過 201
ブリッジグループについて 201
ブリッジ仮想インターフェイス（BVI） 202
トランスペアレント ファイアウォール モードのブリッジグループ 202
ルーテッド ファイアウォール モードのブリッジグループ 203
レイヤ 3 トラフィックの許可 204
許可される MAC アドレス 204
BPDU 処理 205
MAC アドレスとルート ルックアップ 205
トランスペアレント モードのブリッジ グループのサポートされていない機能 206
ルーテッド モードのブリッジ グループのサポートされていない機能 207
デフォルト設定 208
ファイアウォール モードのガイドライン 209
ファイアウォール モードの設定 210

第 6 章 **Firepower 4100/9300 の論理デバイス 213**
インターフェイスについて 213
シャーシ管理インターフェイス 214
インターフェイス タイプ 214
FXOS インターフェイスとアプリケーション インターフェイス 217
共有インターフェイスの拡張性 219
共有インターフェイスのベスト プラクティス 220
共有インターフェイスの使用状況の例 222
共有インターフェイス リソースの表示 230
Firewall Threat Defense のインライン セット リンク ステート伝達サポート 231
論理デバイスについて 231
スタンドアロン論理デバイスとクラスタ化論理デバイス 232
論理デバイスのアプリケーション インスタンス：コンテナとネイティブ 232
コンテナ インスタンス インターフェイス 233
シャーシがパケットを分類する方法 233
分類例 234

コンテナ インスタンスのカスケード 237
一般的な複数インスタンス展開 238
コンテナ インスタンス インターフェイスの自動 MAC アドレス 239
コンテナ インスタンスのリソース管理 240
マルチインスタンス機能のパフォーマンス スケーリング係数 240
コンテナ インスタンスおよびハイ アベイラビリティ 240
コンテナインスタンスおよびクラスタリング 241
コンテナ インスタンスのライセンス 241
論理デバイスの要件と前提条件 242
のハードウェアとソフトウェアの要件と前提条件 242
コンテナ インスタンスの要件と前提条件 244
ハイアベイラビリティの要件と前提条件 245
クラスタリングの要件と前提条件 246
論理デバイスに関する注意事項と制約事項 250
インターフェイスに関する注意事項と制限事項 250
一般的なガイドラインと制限事項 253
インターフェイスの設定 254
インターフェイスの有効化または無効化 254
物理インターフェイスの設定 254
EtherChannel（ポート チャネル）の追加 256
コンテナ インスタンスの VLAN サブインターフェイスの追加 258
論理デバイスの設定 260
コンテナインスタンスにリソースプロファイルを追加 260
スタンドアロン Firewall Threat Defense の追加 262
ハイ アベイラビリティ ペアの追加 268
Firewall Threat Defense 論理デバイスのインターフェイスの変更 269
アプリケーションのコンソールへの接続 272
論理デバイスの履歴 274

第 7 章 高可用性 283
Secure Firewall Threat Defense のハイ アベイラビリティについて 283

高可用性 のシステム要件 284
ハードウェア要件 284
ソフトウェア要件 285
高可用性ペアでの Firewall Threat Defense デバイスのライセンス要件 285
フェールオーバー リンクとステートフル フェールオーバー リンク 285
フェールオーバー リンク 286
ステートフル フェールオーバー リンク 288
フェールオーバーの中断の回避とデータ リンク 288
高可用性 の MAC アドレスと IP アドレス 289
ステートフル フェールオーバー 291
サポートされる機能 291
サポートされない機能 293
ハイ アベイラビリティのためのブリッジ グループの要件 294
フェールオーバーのヘルス モニタリング 295
装置のヘルス モニターリング 295
インターフェイス モニタリング 295
フェールオーバー トリガーおよび検出タイミング 297
アクティブ/スタンバイ フェールオーバーについて 299
プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス 299
起動時のアクティブ装置の判別 299
フェールオーバー イベント 299
設定同期の最適化 301
ハイアベイラビリティの要件と前提条件 302
高可用性 のガイドライン 302
ハイ アベイラビリティ ペアの追加 305
オプションの高可用性パラメータの設定 308
スタンバイ IP アドレスとインターフェイス モニタリングの設定 308
ハイ アベイラビリティ フェールオーバー条件の編集 309
仮想 MAC アドレスを設定します。 310
高可用性 の管理 311
Firewall Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替え 311

単一の Firewall Threat Defense 高可用性ペアのノードステータスの更新 312
ハイ アベイラビリティの中断と再開 312
Firewall Threat Defense ハイアベイラビリティペアでのユニット交換 313
バックアップなしでのプライマリ Firewall Threat Defense HA ユニットの交換 314
バックアップなしでのセカンダリ Firewall Threat Defense HA ユニットの交換 315
高可用性ペアの解除 315
削除（登録解除）高可用性ペアのと新しい Firewall Management Center への登録 317
高可用性のモニタリング 318
フェールオーバー履歴の表示 318
ステートフル フェールオーバーの統計情報の表示 319
高可用性の履歴 319

第 8 章 における Firewall Threat Defense のクラスタの展開Cisco Secure Firewall 3100 のクラスタリング 323
Cisco Secure Firewall 3100 のクラスタリングについて 323
クラスタをネットワークに適合させる方法 324
制御ノードとデータノードの役割 324
クラスタ インターフェイス 324
クラスタ制御リンク 325
コンフィギュレーションの複製 325
管理ネットワーク 325
クラスタリングのライセンス 325
クラスタリングの要件と前提条件 325
クラスタリングに関するガイドライン 326
クラスタリングの設定 331
クラスタ インターフェイスについて 331
クラスタ制御リンク 331
スパンド EtherChannel 334
Firewall Management Center へのデバイスのケーブル接続と追加 336
クラスタの作成 338
インターフェイスの設定 347

クラスタのヘルスモニターの設定 349
クラスタノードの管理 354
新しいクラスタノードの追加 355
ノードの除外 357
クラスタの解除 358
クラスタリングを無効にする 359
クラスタへの再参加 359
制御ノードの変更 360
クラスタ設定の編集 361
クラスタノードの照合 363
クラスタまたはノードの削除（登録解除）と新しい Firewall Management Center への登録 364
クラスタのモニタリング 366
クラスタ ヘルス モニター ダッシュボード 368
クラスタ ヘルスの表示 369
クラスタメトリック 371
クラスタリングの例 372
スティック上のファイアウォール 372
トラフィックの分離 373
クラスタリングの参考資料 373
Firewall Threat Defense の機能とクラスタリング 374
クラスタリングでサポートされない機能 374
クラスタリングの中央集中型機能 374
接続設定とクラスタリング 375
FTP とクラスタリング 375
個別インターフェイス モードでのマルチキャスト ルーティング 376
NAT とクラスタリング 376
でのダイナミック ルーティング 378
SIP インスペクションとクラスタリング 378
SNMP とクラスタリング 379
syslog とクラスタリング 379

Cisco TrustSec とクラスタリング 379
VPN とクラスタリング 379
パフォーマンス スケーリング係数 380
制御ノードの選定 380
クラスタ内のハイ アベイラビリティ 381
ノードヘルスモニタリング 381
インターフェイス モニタリング 381
障害後のステータス 382
クラスタへの再参加 382
データ パス接続状態の複製 383
クラスタが接続を管理する方法 383
接続のロール 383
新しい接続の所有権 385
TCP のサンプルデータフロー 385
ICMP および UDP のサンプルデータフロー 386
クラスタリングの履歴 388

第 9 章 **プライベートクラウドでの Threat Defense Virtual のクラスタリング 389**
プライベートクラウドでの Threat Defense Virtual のクラスタリングについて 389
クラスタをネットワークに適合させる方法 390
制御ノードとデータノードの役割 390
個々のインターフェイス 391
ポリシーベース ルーティング 391
等コスト マルチパス ルーティング 392
クラスタ制御リンク 392
クラスタ制御リンク トラフィックの概要 393
コンフィギュレーションの複製 393
管理ネットワーク 394
Threat Defense Virtual クラスタリングのライセンス 394
Threat Defense Virtual クラスタリングの要件および前提条件 394
Threat Defense Virtual クラスタリングのガイドライン 396

Threat Defense Virtual クラスタリングの設定 397
Management Center へのデバイスの追加 397
クラスタの作成 398
インターフェイスの設定 406
クラスタのヘルスモニターの設定 407
クラスタノードの管理 412
新しいクラスタノードの追加 413
ノードの除外 414
クラスタの解除 415
クラスタリングを無効にする 416
クラスタへの再参加 417
制御ノードの変更 418
クラスタ設定の編集 419
クラスタノードの照合 420
クラスタまたはノードの削除（登録解除）と新しい Firewall Management Center への登録 421
クラスタのモニタリング 423
クラスタ ヘルス モニター ダッシュボード 425
クラスタ ヘルスの表示 426
クラスタメトリック 428
クラスタリングの参考資料 429
Threat Defense の機能とクラスタリング 429
サポートされていない機能とクラスタリング 429
クラスタリングの中央集中型機能 430
接続設定とクラスタリング 431
ダイナミック ルーティングおよびクラスタリング 431
FTP とクラスタリング 432
NAT とクラスタリング 432
SIP インスペクションとクラスタリング 434
SNMP とクラスタリング 434
syslog とクラスタリング 434

Cisco TrustSec とクラスタリング 434
VPN とクラスタリング 435
パフォーマンス スケーリング係数 435
制御ノードの選定 435
クラスタ内のハイアベイラビリティ 436
ノードヘルスモニタリング 436
インターフェイス モニタリング 436
障害後のステータス 437
クラスタへの再参加 437
データ パス接続状態の複製 438
クラスタが接続を管理する方法 438
接続のロール 438
新しい接続の所有権 440
TCP のサンプルデータフロー 440
ICMP および UDP のサンプルデータフロー 441
プライベートクラウドでの Threat Defense Virtual のクラスタリング履歴 443

第 10 章 **パブリッククラウドでの Threat Defense Virtual のクラスタリング 445**
パブリッククラウドにおける Threat Defense Virtual クラスタリングについて 446
クラスタをネットワークに適合させる方法 446
個々のインターフェイス 447
制御ノードとデータノードの役割 447
クラスタ制御リンク 447
クラスタ制御リンク トラフィックの概要 448
コンフィギュレーションの複製 449
管理ネットワーク 449
Threat Defense Virtual クラスタリングのライセンス 449
Threat Defense Virtual クラスタリングの要件および前提条件 449
Threat Defense Virtual クラスタリングのガイドライン 451
AWS でクラスタを展開する 453
AWS ゲートウェイロードバランサおよび Geneve シングルアームプロキシ 453

トポロジの例 454
AWS で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス 455
テンプレート 457
CloudFormation テンプレートを使用した AWS へのスタックの展開 458
AWS でのクラスタの手動展開 472
AWS 向け Day 0 構成の作成 472
クラスタノードの展開 473
Azure でクラスタを展開する 474
GWLB ベースのクラスタ展開のサンプルトポロジ 474
Azure ゲートウェイロードバランサおよびペアプロキシ 475
GWLB を使用して Azure で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス 476
テンプレート 478
前提条件 478
Azure Resource Manager テンプレートを使用した Azure と GWLB でのクラスタの展開 479
NLB ベースのクラスタ展開のサンプルトポロジ 482
NLB を使用して Azure で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス 482
テンプレート 484
前提条件 484
Azure Resource Manager テンプレートを使用した Azure と NLB でのクラスタの展開 485
Azure でのクラスタの手動展開 487
Azure 向け Day 0 構成の作成 487
クラスタノードの手動展開：GWLB ベースの展開 492
クラスタノードの手動展開：NLB ベースの展開 492
Azure でのトラブルシューティング クラスタ展開 493
GCP でのクラスタの展開 494
トポロジの例 495
GCP で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス 495
テンプレート 497
インスタンステンプレートを使用した GCP でのインスタンスグループの展開 498

GCP でのクラスタの手動展開 499
GCP 向け Day 0 構成の作成 499
クラスタノードの手動展開 502
GCP ネットワークロードバランサのヘルスチェックの許可 502
Management Center へのクラスタの追加（手動展開） 504
クラスタのヘルスモニターの設定 511
クラスタノードの管理 517
クラスタリングを無効にする 517
クラスタへの再参加 518
クラスタノードの照合 518
クラスタまたはノードの削除（登録解除）と新しい Firewall Management Center への登録 519
クラスタのモニタリング 520
クラスタ ヘルス モニター ダッシュボード 523
クラスタ ヘルスの表示 524
クラスタメトリック 526
クラスタのアップグレード 526
クラスタリングの参考資料 527
Threat Defense の機能とクラスタリング 528
サポートされていない機能とクラスタリング 528
クラスタリングの中央集中型機能 528
Cisco TrustSec とクラスタリング 529
接続設定とクラスタリング 529
ダイナミック ルーティングおよびクラスタリング 529
FTP とクラスタリング 530
NAT とクラスタリング 531
SIP インスペクションとクラスタリング 533
SNMP とクラスタリング 533
syslog とクラスタリング 533
VPN とクラスタリング 533
パフォーマンス スケーリング係数 534

制御ノードの選定 534
クラスタ内のハイアベイラビリティ 535
ノードヘルスモニタリング 535
インターフェイス モニタリング 535
障害後のステータス 535
クラスタへの再参加 536
データ パス接続状態の複製 536
クラスタが接続を管理する方法 537
接続のロール 537
新しい接続の所有権 539
TCP のサンプルデータフロー 539
ICMP および UDP のサンプルデータフロー 540
パブリッククラウドの Threat Defense Virtual クラスタリングの履歴 541

第 11 章 **Firepower 4100/9300 のクラスタリング 543**
Firepower 4100/9300 シャーシのクラスタリングについて 543
ブートストラップ設定 544
クラスタ メンバー 544
クラスタ制御リンク 545
クラスタ制御リンクのサイジング 545
クラスタ制御リンクの冗長性 546
シャーシ間クラスタリングのクラスタ制御リンクの信頼性 546
クラスタ制御リンク ネットワーク 546
管理ネットワーク 547
管理インターフェイス 547
クラスタ インターフェイス 547
スパンド EtherChannel 548
冗長スイッチシステムへの接続 548
コンフィギュレーションの複製 549
クラスタリングのライセンス 549
クラスタリングの要件と前提条件 549

クラスタリング ガイドラインと制限事項 553
クラスタリングの設定 557
FXOS：Firewall Threat Defense クラスタの追加 557
Firewall Threat Defense クラスタの作成 558
クラスタノードの追加 569
Firewall Management Center：クラスタの追加 574
Firewall Management Center：クラスタ、データ、および診断インターフェイスの設定 580
Firewall Management Center：クラスタのヘルスモニターの設定 583
FXOS：クラスタノードの削除 588
FMC：クラスタメンバーの管理 590
新規クラスタ メンバーの追加 590
クラスタ メンバーの置換 591
メンバーの非アクティブ化 593
クラスタへの再参加 594
データノードの削除（登録解除） 595
制御ユニットの変更 596
クラスタ メンバーの照合 597
Firewall Management Center：クラスタのモニタリング 597
クラスタ ヘルス モニター ダッシュボード 599
クラスタ ヘルスの表示 600
クラスタメトリック 602
クラスタリングの例 603
スティック上のファイアウォール 604
トラフィックの分離 605
クラスタリングの参考資料 605
Firewall Threat Defense の機能とクラスタリング 605
クラスタリングでサポートされない機能 606
クラスタリングの中央集中型機能 606
接続設定 607
ダイナミック ルーティングおよびクラスタリング 607
FTP とクラスタリング 608

マルチキャスト ルーティングとクラスタリング 608
NAT とクラスタリング 609
SIP インスペクションとクラスタリング 610
SNMP とクラスタリング 611
syslog とクラスタリング 611
TLS/SSL 接続とクラスタリング 611
Cisco TrustSec とクラスタリング 611
VPN とクラスタリング 611
パフォーマンス スケーリング係数 612
制御ユニットの選定 612
クラスタ内のハイ アベイラビリティ 613
シャーシ アプリケーションのモニターリング 613
装置のヘルス モニターリング 613
インターフェイス モニタリング 613
デコレータ アプリケーションのモニタリング 614
障害後のステータス 614
クラスタへの再参加 615
データ パス接続状態の複製 615
クラスタが接続を管理する方法 616
接続のロール 616
新しい接続の所有権 618
TCP のサンプルデータフロー 618
ICMP および UDP のサンプルデータフロー 619
クラスタリングの履歴 620

第 III 部 : インターフェイスとデバイスの設定 627

第 12 章 インターフェースの概要 629
管理/診断インターフェイス 629
管理インターフェイス 629
診断インターフェイス（レガシー） 630

インターフェイス モードとタイプ 630
セキュリティ ゾーンとインターフェイス グループ 631
Auto-MDI/MDIX 機能 633
冗長インターフェイス（廃止） 633
インターフェイスのデフォルト設定 633
セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成 634
物理インターフェイスの有効化およびイーサネット設定の構成 635
EtherChannel インターフェイスの設定 638
EtherChannel インターフェイスについて 639
EtherChannel について 639
EtherChannel インターフェイスのガイドライン 642
EtherChannel の設定 644
Firewall Management Center とのインターフェイスの変更の同期 648
Cisco Secure Firewall 3100 のネットワークモジュールの管理 652
ブレークアウトポートの設定 653
ネットワークモジュールの追加 657
ネットワークモジュールの交換方法 659
ネットワークモジュールを別のタイプに交換する 662
ネットワーク モジュールの取り外し 666
インターフェイスの履歴 669

第 13 章 通常のファイアウォール インターフェイス 673
通常のファイアウォール インターフェイスの要件と前提条件 673
Firepower 1010 のスイッチポートの設定 674
スイッチ ポートについて 674
スイッチポートおよびインターフェイスについて 674
Auto-MDI/MDIX 機能 675
スイッチポートの注意事項および制約事項 675
スイッチ ポートと Power Over Ethernet の設定 677
スイッチ ポート モードの有効化または無効化 677
VLAN インターフェイスの設定 678

スイッチ ポートのアクセス ポートとしての設定 680
スイッチ ポートのトランク ポートとしての設定 682
Power over Ethernet の設定 685
ループバック インターフェイスの設定 686
ループバック インターフェイスについて 686
ループバック インターフェイスのガイドラインと制限事項 687
ループバック インターフェイスの設定 687
ループバック インターフェイスへのトラフィックのレート制限 688
VLAN サブインターフェイスと 802.1Q トランキングの設定 692
VLAN サブインターフェイスのガイドラインと制限事項 693
デバイス モデルによる VLAN サブインターフェイスの最大数 694
サブインターフェイスの追加 694
VXLAN インターフェイスの設定 697
VXLAN インターフェイスについて 697
カプセル化 697
VXLAN トンネル エンドポイント 697
VTEP 送信元インターフェイス 698
VNI インターフェイス 699
VXLAN パケット処理 699
ピア VTEP 700
VXLAN 使用例 701
VXLAN インターフェイスの要件と前提条件 705
VXLAN インターフェイスのガイドライン 706
VXLAN または Geneve インターフェイスの設定 707
VXLAN インターフェイスの設定 707
Geneve インターフェイスの設定 710
ゲートウェイロードバランサのヘルスチェックの許可 712
ルーテッド モードとトランス ペアレント モードのインターフェイスの設定 713
ルーテッドモードインターフェイスとトランスペアレントモードインターフェイスについて 713
デュアル IP スタック（IPv4 および IPv6） 714

31 ビット サブネット マスク 714
ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項 715
ルーテッド モードのインターフェイスの設定 717
ブリッジ グループ インターフェイスの設定 724
ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定 724
ブリッジ仮想インターフェイス（BVI）の設定 726
IPv6 アドレスの設定 728
IPv6 について 728
IPv6 プレフィックス委任クライアントの設定 729
グローバル IPv6 アドレスの設定 734
IPv6 ネイバー探索の設定 738
高度なインターフェイスの設定 741
インターフェイスの詳細設定について 741
MAC アドレスについて 742
MTU について 743
TCP MSS について 744
ブリッジグループ トラフィックの ARP インスペクション 746
MAC アドレス テーブル 746
デフォルト設定 747
ARP インスペクションと MAC アドレス テーブルのガイドライン 747
MTU の設定 747
MAC アドレスの設定 749
スタティック ARP エントリの追加 750
静的 MAC アドレスの追加とブリッジグループの MAC 学習の無効化 751
セキュリティの設定パラメータの設定 752
通常のファイアウォール インターフェイスの履歴 755

第 14 章 インラインセットとパッシブインターフェイス 763
IPS インターフェイスについて 763
インライン セット 764

複数のインライン ペアと非同期ルーティング 764
パッシブ インターフェイス 765
インライン セットのハードウェア バイパスについて 766
ハードウェア バイパス トリガー 766
ハードウェア バイパスのスイッチオーバー 767
Snort フェール オープンと ハードウェア バイパス 767
ハードウェア バイパス Status 767
インラインセットの要件と前提条件 767
インライン セットとパッシブ インターフェイスのガイドライン 769
パッシブ インターフェイスの設定 771
インライン セットを設定します。 773
インラインセットとパッシブインターフェイスの履歴 778

第 15 章 **DHCP および DDNS 781**
DHCP サービスと DDNS サービスについて 781
DHCPv4 サーバについて 781
DHCP オプション 781
DHCPv6 ステートレス サーバーについて 782
DHCP リレー エージェントについて 783
DHCP および DDNS の要件と前提条件 783
DHCP サービスと DDNS サービスのガイドライン 783
DHCPv4 サーバーの設定 785
DHCPv6 ステートレス サーバーの設定 788
DHCP IPv6 プールの作成 788
DHCPv6 ステートレスサーバーの有効化 791
DHCP リレー エージェントの設定 792
ダイナミック DNS の設定 794
DHCP および DDNS の履歴 801

第 16 章 **Firepower 1000/2100 の SNMP 803**
Firepower 1000/2100 の SNMP について 803

Firepower 1000/2100 の SNMP の有効化と SNMP プロパティの設定 804
Firepower 1000/2100 の SNMP トラップの作成 806
Firepower 1000/2100 の SNMP ユーザーの作成 807

第 17 章 QoS 809
QoS の概要 809
QoS ポリシーについて 810
QoS の要件と前提条件 810
QoS ポリシーによるレート制限 811
QoS ポリシーの作成 812
QoS ポリシーのターゲット デバイスの設定 813
QoS ルールの設定 813
QoS ルール コンポーネント 814
QoS ルール条件 816
インターフェイスルール条件 816
ネットワークルール条件 816
ユーザールール条件 817
アプリケーションルール条件 817
ポートルールの条件 819
URL ルール条件 821
カスタム SGT ルール条件 821
ISE SGT とカスタム SGT ルール条件との比較 821
カスタム セキュリティ グループ タグ（SGT）から ISE セキュリティ グループ タグ（SGT）への自動遷移 822
QoS の履歴 822

第 18 章 プラットフォーム設定 823
プラットフォーム設定の概要 824
プラットフォーム設定ポリシーの要件と前提条件 824
プラットフォーム設定ポリシーの管理 824
ARP インスペクション 826

バナー 827
DNS 828
外部認証 832
フラグメント設定 838
HTTP 840
ICMP 841
Shellの確保 843
SMTP サーバー 845
SNMP 846
SNMP について 848
SNMP の用語 848
MIB およびトラップ 849
MIB でサポートされるテーブルおよびオブジェクト 850
SNMPv3 ユーザーの追加 854
SNMP ホストの追加 857
SNMP トラップの設定 859
SSL の設定 862
SSL 設定について 863
Syslog 867
Syslog について 867
重要度レベル 869
syslog メッセージ フィルタリング 869
syslog メッセージ クラス 870
ロギングのガイドライン 873
Firewall Threat Defense デバイスの syslog ロギングの設定 875
セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 876
ロギングの有効化および基本設定の構成 876
ロギング接続先の有効化 879
電子メール アドレスへの syslog メッセージの送信 880
カスタム イベント リストの作成 881
syslog メッセージの生成レートの制限 882

Syslog 設定 883
Syslog サーバーの設定 885
タイムアウト 888
時刻の同期 890
タイムゾーン 892
UCAPL/CC コンプライアンス 892
パフォーマンス プロファイル 893
プラットフォーム設定の履歴 895

第 19 章 ネットワーク アドレス変換 901
NAT を使用する理由 901
NAT の基礎 902
NAT の用語 902
NAT タイプ 903
ルーテッド モードとトランスペアレント モードの NAT 903
ルーテッド モードの NAT 903
トランスペアレント モードまたはブリッジ グループ内の NAT 904
自動 NAT および 手動 NAT 906
自動 NAT 906
手動 NAT 906
自動 NAT と 手動 NAT の比較 907
NAT ルールの順序 907
NAT インターフェイス 910
NAT 用のルーティングの設定 911
マッピング インターフェイスと同じネットワーク上のアドレス 911
固有のネットワーク上のアドレス 911
実際のアドレスと同じアドレス（アイデンティティ NAT） 912
NAT ポリシーの要件と前提条件 912
NAT のガイドライン 913
NAT のファイアウォール モードのガイドライン 913
IPv6 NAT ガイドライン 913

IPv6 NAT のベスト プラクティス 914
検査対象プロトコルの NAT サポート 915
FQDN 宛先のガイドライン 917
NAT のガイドラインの補足 918
NAT ポリシーの管理 921
NAT ポリシーの作成 922
NAT ポリシーの対象の設定 922
脅威に対する防御のための NAT の設定 923
複数のデバイスの NAT ルールのカスタマイズ 925
NAT ルールテーブルの検索とフィルタリング 928
複数ルールの有効化、無効化、または削除 930
ダイナミック NAT 931
ダイナミック NAT について 931
ダイナミック NAT の欠点と利点 932
ダイナミック自動 NAT の設定 932
ダイナミック手動 NAT の設定 934
ダイナミック PAT 937
ダイナミック PAT について 937
ダイナミック PAT の欠点と利点 938
PAT プール オブジェクトの注意事項 938
ダイナミック自動 PAT の設定 940
ダイナミック手動 PAT の設定 943
ポート ブロック割り当てによる PAT の設定 947
スタティック NAT 950
スタティック NAT について 950
スタティック自動 NAT の設定 955
スタティック手動 NAT の設定 957
アイデンティティ NAT 961
アイデンティティ自動 NAT の設定 962
アイデンティティ手動 NAT の設定 964
Firewall Threat Defense の NAT ルールのプロパティ 967

インターフェイス オブジェクト：NAT のプロパティ 968
自動 NAT の変換プロパティ 968
手動 NAT の変換プロパティ 970
PAT プールの NAT プロパティ 972
詳細 NAT プロパティ 973
IPv6 ネットワークの変換 975
NAT64/46：IPv6 から IPv4 へのアドレス変換 975
NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット 976
NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク 978
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換 983
NAT66 の例：ネットワーク間のスタティック変換 983
NAT66 の例：シンプル IPv6 インターフェイス PAT 986
NAT のモニタリング 989
NAT の例 990
内部 Web サーバへのアクセスの提供（スタティック自動 NAT） 990
内部ホストのダイナミック自動 NAT および外部 Web サーバーのスタティック NAT 993
複数のマッピング アドレス（スタティック自動 NAT、1 対多）を持つ内部ロード バランサ 1000
FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック自動 NAT） 1004
宛先に応じて異なる変換（ダイナミック手動 PAT） 1013
宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT） 1020
NAT およびサイトツーサイト VPN 1027
NAT を使用した DNS クエリと応答の書き換え 1033
DNS64 応答修正 1034
DNS 応答修正、外部の DNS サーバ 1041
DNS 応答修正、ホスト ネットワーク上の DNS サーバ 1045
Firewall Threat Defense NAT の履歴 1049

第 20 章 **Cisco ISA 3000 のアラーム** 1053
アラームについて 1053

アラーム入力インターフェイス 1054
アラーム出力インターフェイス 1054
Syslog アラーム 1055
SNMP アラーム 1055
アラームのデフォルト設定 1056
アラームの要件と前提条件 1056
ISA 3000 のアラームの設定 1057
アラーム入力コンタクトの設定 1057
電源装置アラームの設定 1060
温度アラームの設定 1063
アラームのモニタリング 1066
アラーム ステータスのモニタリング 1066
アラームに関する Syslog メッセージのモニタリング 1066
外部アラームをオフにする 1067
アラームの履歴 1067

第 IV 部 : ルーティング 1069

第 21 章 スタティック ルートとデフォルト ルート 1071
スタティック ルートとデフォルト ルートについて 1071
デフォルトルート 1071
スタティック ルート 1072
不要なトラフィックをドロップするための null0 インターフェイスへのルート 1072
ルートのプライオリティ 1073
トランスペアレント ファイアウォール モードおよびブリッジ グループのルート 1073
スタティック ルート トラッキング 1073
スタティックルートの要件と前提条件 1074
スタティック ルートとデフォルト ルートのガイドライン 1075
スタティック ルートの追加 1075
ルーティングのリファレンス 1077
パスの決定 1077

サポートされるルート タイプ 1078
スタティックとダイナミックの比較 1078
シングルパスとマルチパスの比較 1079
フラットと階層型の比較 1079
リンクステートと距離ベクトル型の比較 1079
ルーティングでサポートされるインターネット プロトコル 1080
ルーティングテーブル 1080
ルーティング テーブルへの入力方法 1080
転送の決定方法 1083
ダイナミック ルーティングおよび高可用性 1084
クラスタリングでのダイナミック ルーティング 1084
個別インターフェイス モードでのダイナミック ルーティング 1085
管理トラフィック用ルーティングテーブル 1087
Equal-Cost Multipath（ECMP）ルーティング 1088
ルート マップについて 1088
permit 句と deny 句 1089
match 句と set 句の値 1089

第 22 章 仮想ルータ 1091
仮想ルータと Virtual Route Forwarding（VRF）について 1091
仮想ルータの適用 1092
グローバルおよびユーザー定義の仮想ルータ 1092
仮想ルーター対応ポリシーの設定 1094
仮想ルータの相互接続 1094
IP アドレスのオーバーラップ 1097
ユーザー定義の仮想ルータでの SNMP の設定 1098
デバイス モデルごとの仮想ルータの最大数 1098
仮想ルータの要件と前提条件 1099
仮想ルータに関する注意事項と制限事項 1100
Firewall Management Center Web インターフェイスの変更：[ルーティング（Routing）] ページ 1102

仮想ルータの管理 1103
仮想ルータの作成 1103
仮想ルータの設定 1104
仮想ルータの変更 1106
仮想ルータの削除 1107
仮想ルータのモニタリング 1107
仮想ルータの設定例 1108
仮想ルータを介して遠隔サーバにルーティングする方法 1108
重複するアドレス空間を使用してインターネットアクセスを提供する方法 1113
仮想ルーティングで内部ネットワークへの RA VPN アクセスを許可する方法 1123
サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法 1125
仮想ルーティングにおいて 2 つの重複するネットワークホスト間でトラフィックをルーティングする方法 1129
BVI インターフェイスを使用したルーテッド ファイアウォール モードでの重複セグメントの管理方法 1132
重複するネットワークを使用したユーザー認証の設定方法 1136
BGP を使用して仮想ルータを相互接続する方法 1143
仮想ルータの履歴 1150

第 23 章 ECMP 1153
ECMP について 1153
ECMP の注意事項と制限事項 1153
ECMP の管理ページ 1154
ECMP ゾーンの作成 1155
等コストスタティックルートの設定 1156
ECMP ゾーンの変更 1157
ECMP ゾーンの削除 1158
ECMP の設定例 1158
Secure Firewall Threat Defense の ECMP の履歴 1162

第 24 章 双方向フォワーディング検出ルーティング 1163

BFD ルーティングについて 1163
BFD ルーティングのガイドライン 1163
BFD の設定 1165
BFD ポリシーの設定 1165
シングルホップ BFD ポリシーの設定 1166
マルチホップ BFD ポリシーの設定 1167
BFD ルーティングの履歴 1168

第 25 章 **Open Shortest Path First（OSPF） 1169**
Open Shortest Path First（OSPF） 1169
OSPF について 1169
fast hello パケットに対する OSPF のサポート 1171
Fast Hello パケットに対する OSPF サポートの前提条件 1171
OSPF Hello インターバルと dead 間隔 1171
OSPF fast hello パケット 1172
OSPF Fast Hello パケットの利点 1172
OSPFv2 および OSPFv3 間の実装の差異 1172
OSPF の要件と前提条件 1173
OSPF のガイドライン 1173
OSPFv2 の設定 1176
OSPF エリア、範囲、仮想リンクの設定 1176
OSPF 再配布の設定 1180
OSPF エリア間フィルタリングの設定 1181
OSPF フィルタルールの設定 1183
OSPF サマリーアドレスの設定 1184
OSPF インターフェイスとネイバーの設定 1185
OSPF 詳細プロパティの設定 1188
OSPFv3 の設定 1192
OSPFv3 エリア、ルート集約、および仮想リンクの設定 1192
OSPFv3 再配布の設定 1195
OSPFv3 サマリー プレフィックスの設定 1196

OSPFv3 インターフェイス、認証、およびネイバーの設定 1197
OSPFv3 詳細プロパティの設定 1201
OSPF の履歴 1204

第 26 章 EIGRP 1205
EIGRP ルーティングについて 1205
EIGRP の要件と前提条件 1206
EIGRP ルーティングのガイドラインと制限事項 1207
EIGRP の設定 1208
EIGRP の設定 1209
EIGRP ネイバー設定の設定 1210
EIGRP のフィルタルールの設定 1210
EIGRP 再配布の設定 1211
EIGRP サマリーアドレスの設定 1213
EIGRP インターフェイス設定の指定 1213
EIGRP の高度な設定の指定 1214
EIGRP の履歴 1217

第 27 章 BGP 1219
BGPについて 1219
ルーティング テーブルの変更 1219
BGP を使用する状況 1221
BGP パスの選択 1221
BGP マルチパス 1222
BGP の要件と前提条件 1223
BGP のガイドライン 1223
BGP の設定 1224
BGP 基本設定 1225
BGP 一般設定 1228
BGP ネイバーの設定 1230
BGP 集約アドレス設定の設定 1234

BGPv4 フィルタリング設定 1236
BGP ネットワーク設定 1236
BGP 再配布設定 1237
BGP ルート注入の設定 1238
BGP ルートのインポート/エクスポート設定の設定 1239
BGP の履歴 1242

第 28 章 RIP 1243
RIP について 1243
ルーティング アップデート プロセス 1244
RIP のルーティング メトリック 1244
RIP 安定性機能 1244
RIP タイマー 1244
RIP の要件と前提条件 1245
RIP のガイドライン 1246
RIP の設定 1246

第 29 章 マルチキャスト 1251
マルチキャスト ルーティングについて 1251
IGMP プロトコル 1252
スタブ マルチキャスト ルーティング 1252
PIM マルチキャスト ルーティング 1253
PIM Source Specific Multicast のサポート 1253
マルチキャスト双方向 PIM 1254
PIM ブートストラップ ルータ（BSR） 1254
PIM ブートストラップ ルータ（BSR）の用語 1254
マルチキャスト グループの概念 1255
マルチキャスト アドレス 1256
クラスタ 1256
マルチキャストルーティングの要件と前提条件 1256
マルチキャスト ルーティングのガイドライン 1256

IGMP 機能の設定 1258
マルチキャスト ルーティングの有効化 1258
IGMP プロトコルの設定 1259
IGMP アクセスグループの設定 1261
IGMP スタティック グループの設定 1262
IGMP 参加グループの設定 1263
PIM 機能の設定 1264
PIM プロトコルの設定 1264
PIM ネイバー フィルタの設定 1265
PIM 双方向ネイバー フィルタの設定 1266
PIM ランデブー ポイントの設定 1268
PIM ルート ツリーの設定 1269
PIM リクエスト フィルタの設定 1270
Secure Firewall Threat Defense デバイスのブートストラップ ルータ設定 1271
マルチキャスト ルートの設定 1272
マルチキャスト境界フィルタの設定 1273

第 30 章 ポリシーベースルーティング 1275
ポリシーベース ルーティングについて 1275
ポリシーベースルーティングに関する注意事項と制約事項 1277
パスモニタリング 1279
パスモニタリングの設定 1280
ポリシーベース ルーティング ポリシーの設定 1281
パス監視ダッシュボードの追加 1285
ポリシーベースルーティングの設定例 1285
パスモニタリングを使用した PBR の設定例 1292
ポリシーベース ルーティングの履歴 1294

第 V 部 : オブジェクトと証明書 1297

第 31 章 オブジェクト管理 1299

オブジェクトの概要 1300
オブジェクト マネージャ 1303
オブジェクトのインポート 1303
オブジェクトの編集 1306
オブジェクトとその使用状況の表示 1307
オブジェクトまたはオブジェクト グループのフィルタリング 1308
オブジェクト グループ 1308
再利用可能オブジェクトのグループ化 1309
オブジェクトのオーバーライド 1310
オブジェクト オーバーライドの管理 1311
オブジェクトのオーバーライドの許可 1312
オブジェクトのオーバーライドの追加 1312
オブジェクト オーバーライドの編集 1313
AAAサーバ 1313
RADIUS サーバーグループの追加 1314
RADIUS サーバー グループのオプション 1314
RADIUS サーバー オプション 1316
シングルサインオンサーバーの追加 1317
アクセスリスト 1319
拡張 ACL オブジェクトの設定 1320
標準 ACL オブジェクトの設定 1322
アドレス プール 1323
アプリケーション フィルタ 1325
ASパス 1325
BFD テンプレート 1326
暗号スイート リスト 1327
暗号スイート リストの作成 1328
コミュニティ リスト 1328
拡張コミュニティ 1330
DHCP IPv6 プール 1332
識別名 1332

識別名オブジェクトの作成 1334
DNS サーバ グループ 1335
DNS サーバー グループ オブジェクトの作成 1335
外部属性 1336
API で作成したダイナミックオブジェクトについて 1336
API で作成したダイナミックオブジェクトの追加または編集 1336
セキュリティグループタグ 1337
セキュリティ グループ タグ オブジェクトの作成 1338
ファイル リスト 1338
ファイル リストのソース ファイル 1339
ファイル リスト別の SHA-256 値の追加 1340
ファイル リストへの個々のファイルのアップロード 1341
ファイル リストへのソース ファイルのアップロード 1342
ファイル リストの SHA-256 値の編集 1343
ファイル リストからソース ファイルをダウンロードする 1343
FlexConfig 1344
位置情報 1345
地理位置情報オブジェクトの作成 1345
インターフェイス（Interface） 1346
Key Chain 1346
キー チェーンのオブジェクトの作成 1347
ネットワーク 1349
ネットワーク ワイルドカード マスク 1350
ネットワーク オブジェクトの作成 1351
ネットワークオブジェクトのインポート 1352
PKI 1352
内部認証局オブジェクト 1354
CA 証明書と秘密キーのインポート 1354
CA 証明書および秘密キーのインポート 1355
新しい CA 証明書と秘密キーの生成 1355
新しい署名付き証明書 1356

未署名の CA 証明書と CSR の作成 1356
CSR への応答として発行された署名付き証明書のアップロード 1357
CA 証明書および秘密キーのダウンロード 1357
CA 証明書および秘密キーのダウンロード 1358
信頼できる認証局オブジェクト 1358
信頼できる CA オブジェクト 1359
信頼できる CA オブジェクトの追加 1359
信頼できる CA オブジェクトの証明書失効リスト 1360
信頼できる CA オブジェクトへの証明書失効リストの追加 1360
外部証明書オブジェクト 1361
外部証明書オブジェクトの追加 1361
内部証明書オブジェクト 1362
内部証明書オブジェクトの追加 1362
証明書の登録オブジェクト 1363
証明書の登録オブジェクトの追加 1365
証明書の登録オブジェクト EST オプション 1367
証明書の登録オブジェクト SCEP オプション 1368
証明書の登録オブジェクト 証明書のパラメータ 1369
証明書の登録オブジェクト の主要なオプション 1370
証明書の登録オブジェクト 失効オプション 1373
ポリシー リスト 1373
ポート 1376
ポート オブジェクトの作成 1377
ポートオブジェクトのインポート 1377
プレフィックス リスト 1377
IPv6 プレフィックス リストの設定 1378
IPv4 プレフィックス リストの設定 1379
ルート マップ 1380
セキュリティ インテリジェンス 1384
セキュリティ インテリジェンス オブジェクトの変更方法 1386
グローバルおよびドメインのセキュリティインテリジェンスリスト 1387

セキュリティ インテリジェンス リストとマルチテナンシー 1387
グローバル セキュリティ インテリジェンス リストへのエントリの追加 1389
グローバル セキュリティ インテリジェンス リストからのエントリを削除する 1390
セキュリティ インテリジェンスのリストとフィードの更新 1391
セキュリティ インテリジェンス フィードの更新頻度の変更 1391
カスタム セキュリティ インテリジェンスのリストとフィード 1392
カスタムリストとカスタムフィード：要件 1392
URL リストとフィード：URL 構文と一致基準 1392
カスタム セキュリティ インテリジェンス フィード 1394
カスタム セキュリティ インテリジェンス リスト 1396
シンクホール 1398
シンクホール オブジェクトの作成 1399
SLA モニタ 1399
時間範囲 1401
時間範囲オブジェクトの作成 1401
タイムゾーン 1403
トンネル ゾーン 1404
URL 1404
URL オブジェクトの作成 1405
変数セット 1406
侵入ポリシー内の変数セット 1407
変数 1408
定義済みデフォルト変数 1409
ネットワーク変数 1411
ポート変数 1413
拡張変数 1414
変数のリセット 1415
セットに変数を追加する 1416
変数のネスト 1417
変数セットの管理 1419
変数セットの作成 1420

変数の管理 1421
変数の追加 1422
変数の編集 1423
VLAN タグ 1424
VLAN タグ オブジェクトの作成 1424
VPN 1425
証明書マップオブジェクト 1425
セキュアクライアント カスタム属性オブジェクト 1427
セキュアクライアントのカスタム属性オブジェクトの追加 1427
グループポリシーへのカスタム属性の追加 1429
Firewall Threat Defense グループ ポリシー オブジェクト 1430
グループ ポリシー オブジェクトの設定 1430
グループ ポリシー一般オプション 1431
グループポリシーの セキュアクライアントオプション 1434
グループ ポリシーの詳細オプション 1438
Firewall Threat Defense IPsec プロポーザル 1439
IKEv1 IPsec プロポーザル オブジェクトの設定 1440
IKEv2 IPsec プロポーザル オブジェクトの設定 1441
Firewall Threat Defense IKE ポリシー 1442
IKEv1 ポリシー オブジェクトの設定 1442
IKEv2 ポリシー オブジェクトの設定 1444
ファイルオブジェクト 1446
オブジェクト管理の履歴 1449

第 32 章 **証明書** 1455
証明書の要件と前提条件 1455
Secure Firewall Threat Defense VPN 証明書の注意事項と制約事項 1455
Firewall Threat Defense 証明書の管理 1456
CA バンドルの自動更新 1458
自己署名登録を使用した証明書のインストール 1460
EST 登録を使用した証明書のインストール 1461

SCEP の登録を使用した証明書のインストール 1462
手動登録を使用した証明書のインストール 1463
PKCS12 ファイルを使用した証明書のインストール 1464
Firewall Threat Defense 証明書のトラブルシューティング 1465
証明書の履歴 1466

第 VI 部： VPN 1467

第 33 章 VPN の概要 1469
VPN タイプ 1469
VPN の基本 1470
Internet Key Exchange（IKE） 1471
IPsec 1472
VPN パケット フロー 1473
IPsec フローのオフロード 1473
VPN ライセンス 1474
VPN 接続をセキュアにする方法 1475
セキュリティ証明書要件の遵守 1475
使用する暗号化アルゴリズムの決定 1475
使用するハッシュ アルゴリズムの決定 1476
使用する Diffie-Hellman 係数グループの決定 1477
使用する認証方式の決定 1478
事前共有キー 1478
PKI インフラストラクチャとデジタル証明書 1479
削除または廃止されたハッシュアルゴリズム、暗号化アルゴリズム、および Diffie-Hellman モジュラスグループ 1480
VPN トポロジ オプション 1481
ポイントツーポイントの VPN トポロジ 1481
ハブ アンド スポーク VPN トポロジ 1482
フル メッシュ VPN トポロジ 1483
暗黙的トポロジ 1484

第 34 章 サイト間 VPN 1485

サイト間 VPN について 1485

Secure Firewall Threat Defense サイト間 VPN ガイドラインと制約事項 1487

サイト間 VPN トポロジのタイプ 1488

サイト間 VPN の要件と前提条件 1489

サイト間 VPN の管理 1489

ポリシーベースのサイト間 VPN の設定 1491

Firewall Threat Defense VPN エンドポイント オプション 1492

Firewall Threat Defense VPN IKE オプション 1497

Firewall Threat Defense VPN IPsec オプション 1500

Firewall Threat Defense のサイト間 VPN 展開の詳細オプション 1503

Firewall Threat Defense VPN の IKE 詳細オプション 1503

Firewall Threat Defense VPN の IPsec 詳細オプション 1505

Firewall Threat Defense のサイト間 VPN トンネルの詳細オプション 1506

仮想トンネル インターフェイスについて 1507

スタティック VTI 1508

Dynamic VTI 1510

仮想トンネルインターフェイスのガイドラインと制限事項 1512

VTI インターフェイスの追加 1516

ルートベースのサイト間 VPN の作成 1518

ポイントツーポイント トポロジのエンドポイントの設定 1519

ルートベース VPN のポイントツーポイント トポロジの詳細設定 1522

ハブアンドスポークトポロジのエンドポイントの設定 1522

ルートベースの VPN のハブアンドスポークに対する詳細設定 1526

ルートベースの VPN での複数ハブの設定 1527

ルートベース VPN での複数ハブのルーティングの設定 1530

ルートベースの VPN での複数ハブ構成の確認 1531

バックアップ VTI トンネルを介したトラフィックのルーティング 1532

ルートベースのサイト間 VPN のダイナミック VTI の設定 1534

VTI のルーティングおよび AC ポリシーの設定 1534

Umbrella に SASE トンネルを展開する 1538
Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項 1540
Cisco Umbrella に SASE トンネルを展開する方法 1541
Cisco Umbrella SASE トンネルを設定するための前提条件 1541
Management Center の Umbrella パラメータと Cisco Umbrella の API キーのマッピング 1542
Cisco Umbrella 用の SASE トンネルの設定 1544
SASE トンネルステータスの表示 1546
サイト間 VPN のモニタリング 1547
サイト間 VPN の履歴 1553

第 35 章 リモート アクセス VPN 1557
リモート アクセス VPN の概要 1557
リモート アクセス VPN の機能 1558
Secure Client のコンポーネント 1560
リモート アクセス VPN 認証 1561
権限および属性のポリシー実施の概要 1563
AAA サーバー接続の概要 1563
リモートアクセス VPN のライセンス要件 1565
リモートアクセス VPN の要件と前提条件 1565
リモート アクセス VPN の注意事項と制限事項 1566
新規リモート アクセス VPN 接続の設定 1570
リモート アクセス VPN を設定するための前提条件 1571
新規リモート アクセス VPN ポリシーの作成 1572
Secure Firewall Threat Defense デバイスのアクセス コントロール ポリシーの更新 1575
（任意）NAT 免除の設定 1576
DNS の設定 1578
Secure Client プロファイル XML ファイルの追加 1578
（任意）スプリット トンネリングの設定 1579
（任意）ダイナミック スプリット トンネリングの設定 1580
ダイナミック スプリット トンネリング設定の確認 1582
設定の確認 1582

既存のリモートアクセス VPN ポリシーのコピーの作成 1583
リモートアクセス VPN ポリシーのターゲットデバイスの設定 1583
ローカルレルムとリモートアクセス VPN ポリシーの関連付け 1584
その他のリモートアクセス VPN の設定 1585
接続プロファイルの設定 1585
VPN クライアントの IP アドレスの設定 1585
リモートアクセス VPN の AAA 設定 1588
接続プロファイルのエイリアスの作成または更新 1607
リモートアクセス VPN のアクセス インターフェイスの設定 1608
リモートアクセス VPN の高度なオプションの設定 1611
Cisco Secure Client イメージ 1611
リモート アクセス VPN のアドレス割り当てポリシー 1614
証明書から接続プロファイルへのマッピングの設定 1615
グループ ポリシーの設定 1616
LDAP 属性マッピングの設定 1617
VPN ロード バランシングの設定 1619
IPsec の設定 1623
Secure Client 管理 VPN トンネルの設定 1630
Secure Client 管理 VPN トンネルの要件と前提条件 1631
Secure Client 管理 VPN トンネルの制限事項 1631
Firewall Threat Defense での Secure Client 管理 VPN トンネルの設定 1632
複数証明書認証 1634
複数証明書認証のガイドラインと制限事項 1635
複数証明書認証の設定 1635
リモート アクセス VPN の AAA の設定のカスタマイズ 1637
クライアント証明書を使用した VPN ユーザーの認証 1637
クライアント証明書と AAA サーバー経由での VPN ユーザー認証の設定 1639
VPN セッションでのパスワード変更の管理 1641
RADIUS サーバーへのアカウンティング レコードの送信 1641
認証サーバーへのグループ ポリシーの選択の委任 1642
許可サーバーによるグループ ポリシーまたはその他の属性の選択のオーバーライド 1643

ユーザー グループへの VPN アクセスの拒否 1644
ユーザー グループに対する接続プロファイルの選択の制限 1645
リモートアクセス VPN クライアントの セキュアクライアント プロファイルの更新 1646
RADIUS ダイナミック認証 1647
RADIUS ダイナミック認証の設定 1648
二要素認証 1649
RSA 二要素認証の設定 1650
Duo 二要素認証の設定 1651
セカンダリ認証 1653
リモートアクセス VPN のセカンダリ認証の設定 1654
SAML 2.0 シングルサインオン認証 1657
SAML 2.0 に関する注意事項と制約事項 1657
SAML シングルサインオン認証の設定 1659
SAML 認証の設定 1660
拡張 セキュアクライアント 設定 1662
Firewall Threat Defense での セキュアクライアント モジュールの設定 1662
セキュアクライアント モジュールのタイプ 1663
セキュアクライアント モジュールの設定の前提条件 1664
セキュアクライアント モジュールの設定に関するガイドライン 1665
Firewall Threat Defense を使用した セキュアクライアント モジュールの取り付け 1666
セキュアクライアント モジュールのリモートアクセス VPN グループポリシーの設定 1667
セキュアクライアント モジュール設定の確認 1668
モバイルデバイスでのアプリケーションベース（アプリケーションごとのVPN）のリモートアクセス VPN の設定 1669
Per App VPN トンネルの設定の前提条件とライセンス 1669
モバイルアプリケーションのアプリケーション ID の決定 1670
アプリケーションベースの VPN トンネルの設定 1671
アプリケーションごとの設定の確認 1673
リモート アクセス VPN の例 1673
ユーザーあたりの Secure Client 帯域幅を制限する方法 1673

ユーザー ID ベースのアクセスコントロールルールに VPN アイデンティティを使用する方法 1674
Firewall Threat Defense 複数証明書認証の設定 1675
リモートアクセス VPN の履歴 1679

第 36 章 ダイナミック アクセス ポリシー 1683
Secure Firewall Threat Defense ダイナミック アクセス ポリシーについて 1683
Firewall Threat Defense での権限および属性のポリシー適用階層 1684
ダイナミック アクセス ポリシーの前提条件 1685
ダイナミック アクセス ポリシーに関する注意事項と制限事項 1685
ダイナミック アクセス ポリシー（DAP）の設定 1686
ダイナミック アクセス ポリシーの作成 1686
ダイナミック アクセス ポリシー レコードの作成 1686
DAP の AAA 基準設定を構成する 1687
DAP のエンドポイント属性選択基準の設定 1688
DAP へのマルウェア対策エンドポイント属性の追加 1689
DAP へのデバイス エンドポイント属性の追加 1690
DAP への Secure Client エンドポイント属性の追加 1691
DAP への NAC エンドポイント属性の追加 1691
DAP へのアプリケーション属性の追加 1692
DAP へのパーソナル ファイアウォール エンドポイント属性の追加 1692
DAP へのオペレーティング システム エンドポイント属性の追加 1693
DAP へのプロセス エンドポイント属性の追加 1693
DAP へのレジストリ エンドポイント属性の追加 1693
DAP へのファイル エンドポイント属性の追加 1694
DAP への証明書認証属性の追加 1695
DAP の詳細設定の設定 1695
ダイナミック アクセス ポリシーとリモートアクセス VPN の関連付け 1696
ダイナミック アクセス ポリシーの履歴 1697

第 37 章 VPN のモニタリングとトラブルシューティング 1699

VPN サマリ ダッシュボード 1699
リモートアクセス VPN ダッシュボード 1699
VPN セッションとユーザー情報 1701
リモート アクセス VPN アクティブ セッションの表示 1701
リモート アクセス VPN ユーザー アクティビティの表示 1702
VPN ヘルス イベント 1702
VPN ヘルス イベントの表示 1702
VPN のトラブルシューティング 1703
システムメッセージ 1703
VPN システム ログ 1703
debug コマンド 1704
debug aaa 1706
debug crypto 1706
debug ldap 1710
debug ssl 1710
debug webvpn 1711

第 VII 部： アクセス制御 1715

第 38 章 アクセス制御の概要 1717
アクセス制御の概要 1717
ルールの概要 1718
デバイス別のフィルタリング ルール 1719
ルールとその他のポリシーの警告 1720
アクセス コントロール ポリシーのデフォルト アクション 1721
ファイルポリシーと侵入ポリシーを使用したディープインスペクション 1723
侵入ポリシーとファイルポリシーを使用したアクセス制御トラフィック処理 1724
ファイル インスペクションおよび侵入インスペクションの順序 1726
アクセス コントロール ポリシーの継承 1728
アプリケーション制御のベストプラクティス 1729
アプリケーション制御に関する推奨事項 1729
アプリケーション制御の設定のベストプラクティス 1732

アプリケーションの特性 1734
用途別の注意事項と制限事項 1735
アクセス制御ルールのベストプラクティス 1736
アクセス制御の一般的なベストプラクティス 1736
順序付けルールのベストプラクティス 1738
ルールのプリエンプション 1738
ルールのアクションとルールの順序 1740
アプリケーション ルールの順序 1741
URL ルールの順序 1741
ルールの簡素化および絞り込みのベストプラクティス 1742
アクセス制御ルールと侵入ポリシーの最大数 1743

第 39 章 アクセス制御ポリシー 1745
アクセス コントロール ポリシーのコンポーネント 1745
システム作成のアクセス コントロール ポリシー 1746
アクセス コントロール ポリシーの要件と前提条件 1747
アクセス コントロール ポリシーの管理 1747
基本的なアクセス コントロール ポリシーの作成 1748
アクセス コントロール ポリシーの編集 1749
アクセス コントロール ポリシーのロック 1752
アクセス コントロール ポリシーの継承の管理 1753
基本アクセス コントロール ポリシーの選択 1754
基本ポリシーからアクセス コントロール ポリシー設定を継承する 1755
子孫アクセス コントロール ポリシーでの設定のロック 1755
ドメインでのアクセス コントロール ポリシーの強制 1756
アクセス コントロール ポリシーのターゲット デバイスの設定 1757
アクセス コントロール ポリシーのロギング設定 1757
アクセス コントロール ポリシーの詳細設定 1759
アクセス制御への他のポリシーの関連付け 1765
ルールヒットカウントの表示 1767
ルールの競合および警告の分析 1769

ルールの検索 1771
アクセス コントロール ポリシーの履歴 1772

第 40 章 アクセス コントロール ルール 1775
アクセス コントロール ルールの概要 1775
アクセス コントロール ルールの管理 1777
アクセス コントロール ルールのコンポーネント 1778
アクセス コントロール ルールの順序 1780
アクセス コントロール ルールのアクション 1781
アクセス コントロール ルールのモニター アクション 1781
アクセス コントロール ルールの信頼アクション 1782
アクセス コントロール ルールのブロック アクション 1783
アクセス コントロール ルール インタラクティブ ブロック アクション 1784
アクセス コントロール ルールの許可アクション 1784
アクセスコントロールルールの要件と前提条件 1785
アクセス制御ルールのガイドラインと制限事項 1786
アクセスコントロールルールの管理 1787
アクセス制御ルール カテゴリの追加 1787
アクセスコントロールルールの作成および編集 1788
アクセスコントロールルール条件 1790
アクセス コントロール ルールの有効化と無効化 1801
アクセス コントロール ポリシー間でのアクセス コントロール ルールのコピー 1801
アクセスコントロールルールのプレフィルタポリシーへの移動 1802
アクセス コントロール ルールの配置 1805
アクセス制御ルールへのコメントの追加 1806
アクセスコントロールルールの例 1806
セキュリティゾーンを使用したアクセスの制御方法 1806
アプリケーションの使用を制御する方法 1807
脅威のブロック方法 1809
アクセス制御ルールの履歴 1812

第 41 章

URL フィルタリング 1815
URL フィルタリングの概要 1815
カテゴリおよびレピュテーションによる URL のフィルタリングについて 1816
URL カテゴリとレピュテーションの説明 1817
Cisco Cloud からの URL フィルタリングのデータ 1817
URL フィルタリングのベスト プラクティス 1818
HTTPS トラフィックのフィルタリング 1822
URL フィルタリングでのカテゴリの使用 1823
URL フィルタリングのライセンス要件 1824
URL フィルタリングの要件と前提条件 1825
カテゴリとレピュテーションを使用した URL フィルタリングの設定方法 1825
カテゴリとレピュテーションを使用した URL フィルタリングの有効化 1827
URL フィルタリング オプション 1827
URL 条件の設定 1829
URL 条件を伴うルール 1831
URL ルールの順序 1831
DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別（ベータ版） 1832
ドメインルックアップ中に URL を識別するための DNS フィルタリングの有効化 1832
DNS フィルタリングの制限事項 1833
DNS フィルタリングとイベント 1833
手動 URL フィルタリング 1833
手動 URL フィルタリングオプション 1834
カテゴリおよびレピュテーションベースの URL フィルタリングの補完または選択的オーバーライド 1835
HTTP 応答ページの設定 1836
HTTP 応答ページの制限 1836
HTTP 応答ページの要件と前提条件 1837
HTTP 応答ページの選択 1838
HTTP 応答ページでのインタラクティブ ブロッキングの設定 1839

インタラクティブ ブロッキングの設定 1839
ブロックされた Web サイトのユーザー バイパス タイムアウトの設定 1840
URL フィルタリングのヘルス モニターの設定 1841
URL カテゴリとレピュテーションの異議申し立て 1841
URL カテゴリセットが変更された場合、アクションを実行 1842
URL カテゴリとレピュテーションの変更：イベントへの影響 1844
URL フィルタリングのトラブルシューティング 1844
URL フィルタリングの履歴 1848

第 42 章 セキュリティ インテリジェンス 1851
セキュリティ インテリジェンスについて 1851
セキュリティ インテリジェンスのベストプラクティス 1852
セキュリティ インテリジェンスのためのライセンス要件 1853
セキュリティ インテリジェンスの要件と前提条件 1853
セキュリティ インテリジェンス送信元 1854
セキュリティ インテリジェンスの設定 1855
セキュリティ インテリジェンス オプション 1857
セキュリティ インテリジェンス カテゴリ 1859
ブロックリストのアイコン 1861
設定例：セキュリティインテリジェンスブロック 1862
セキュリティ インテリジェンス モニタリング 1863
セキュリティ インテリジェンス ブロッキングのオーバーライド 1864
セキュリティ インテリジェンスのトラブルシューティング 1865
セキュリティ インテリジェンスのカテゴリが使用可能なオプションのリストに表示されない 1865
セキュリティ インテリジェンス ブロック リストへの登録の履歴 1866

第 43 章 DNS ポリシー 1867
DNS ポリシーの概要 1867
Cisco Umbrella DNS ポリシー 1868
DNS ポリシーの構成要素 1869

DNS ポリシーのライセンス要件 1870
DNS ポリシーの要件と前提条件 1870
DNS および Cisco Umbrella DNS ポリシーの管理 1871
基本的な DNS ポリシーの作成 1871
DNS ポリシーの編集 1872
DNS ルール 1873
DNS ルールの作成と編集 1874
DNS ルールの管理 1874
DNS ルールの有効化と無効化 1874
DNS ルールの評価順序 1875
DNS ルールのアクション 1876
DNS ルールの条件 1877
セキュリティゾーンルール条件 1877
ネットワークルール条件 1878
VLAN タグルール条件 1879
DNS ポリシー ルールの条件 1879
DNS ルールの作成方法 1879
DNS およびセキュリティ ゾーンに基づくトラフィックの制御 1880
DNS およびネットワークに基づくトラフィックの制御 1880
DNS および VLAN に基づくトラフィックの制御 1881
DNS リストまたはフィードに基づくトラフィックの制御 1882
DNS ポリシーの導入 1883
Cisco Umbrella DNS ポリシー 1883
DNS 要求を Cisco Umbrella にリダイレクトする方法 1884
Cisco Umbrella DNS コネクタを設定するための前提条件 1884
Cisco Umbrella の接続設定の設定 1885
Cisco Umbrella DNS ポリシーを作成する 1887
Cisco Umbrella DNS ポリシーとルールの編集 1887
Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付ける 1888

第 44 章 プレフィルタリングおよびプレフィルタ ポリシー 1891

プレフィルタリングについて 1891
プレフィルタ ポリシーについて 1892
トンネルとプレフィルタのルール 1893
プレフィルタリングとアクセス コントロール 1894
パススルー トンネルとアクセス制御 1896
Fastpath プレフィルタリングのベストプラクティス 1897
カプセル化されたトラフィックの処理のベストプラクティス 1898
プレフィルタポリシーの要件と前提条件 1899
プレフィルタリングの設定 1900
トンネルとプレフィルタ ルールのコンポーネント 1902
プレフィルタルール条件 1904
インターフェイスルール条件 1904
ネットワークルール条件 1905
VLAN タグルール条件 1905
プレフィルタルールのポートルール条件 1906
時間と日のルール条件 1906
トンネルルール条件 1907
カプセル化ルールの条件 1907
トンネル ゾーンおよびプレフィルタリング 1907
トンネル ゾーンの使用 1908
トンネル ゾーンの作成 1911
プレフィルタルールのアクセス コントロール ポリシーへの移動 1912
プレフィルタ ポリシーのヒット カウント 1914
大規模フローのオフロード 1914
フロー オフロードの制限事項 1916
プレフィルタリングの履歴 1918

第 45 章 サービスポリシー 1919
Firepower Threat Defense のサービス ポリシーについて 1919
FlexConfig とその他の機能にサービス ポリシーを関連付ける方法 1920
接続設定に関する情報 1921

サービスポリシーの要件と前提条件 1922
サービス ポリシーのガイドラインと制限事項 1922
Threat Defense サービスポリシーの設定 1923
サービス ポリシー ルールの設定 1924
非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス） 1928
非対称ルーティングの問題 1928
TCP ステート バイパスのガイドラインと制限事項 1929
TCP ステート バイパスの設定 1930
TCP シーケンスのランダム化のディセーブル 1932
サービス ポリシーのルールの例 1934
SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信） 1934
Firewall Threat Defense デバイスをトレースルートに表示する 1938
サービス ポリシーのモニタリング 1940
Threat Defense サービスポリシーの履歴 1941

第 46 章 脅威の検出 1943
ポートスキャンの検出と防止 1943
ポートスキャン検出の事前定義された感度レベル 1943
ポートスキャン防止のベストプラクティス 1945
脅威検出の要件と前提条件 1946
脅威検出のガイドラインと制限事項 1946
ポートスキャンの検出と防止の設定 1947
脅威検出のモニタリング 1950
ポートスキャンアラートの表示 1950
ファイアウォールでのポートスキャンのモニタリング 1951
ホストのブロック解除 1952
脅威検出の履歴 1952

第 47 章 エレファントフローの検出 1953
エレファントフローの検出と修復について 1953

インテリジェント アプリケーション バイパスからのエレファントフローのアップグレード 1954
エレファントフローの設定 1954

第 48 章 インテリジェント アプリケーション バイパス 1959
IAB の概要 1959
IAB オプション 1960
インテリジェント アプリケーション バイパスの要件と前提条件 1962
インテリジェント アプリケーション バイパスの設定 1962
IAB のロギングと分析 1964

第 49 章 コンテンツ規制 1969
コンテンツ制限について 1969
コンテンツ制限の要件と前提条件 1971
コンテンツ制限のガイドラインと制限事項 1971
アクセス コントロール ルールを使用したコンテンツ制限の実施 1971
アクセス制御ルールのセーフサーチ オプション 1973
DNS シンクホールを使用したコンテンツ制限の実施 1973

第 VIII 部： 侵入検知と防御 1977

第 50 章 ネットワーク分析ポリシーと侵入ポリシーの概要 1979
ネットワーク分析ポリシーと侵入ポリシーの基本 1979
ポリシーがトラフィックで侵入を検査する方法 1981
復号、正規化、前処理：ネットワーク分析ポリシー 1982
アクセス コントロール ルール：侵入ポリシーの選択 1983
侵入インスペクション：侵入ポリシー、ルール、変数セット 1984
侵入イベントの生成 1986
システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー 1987
システム提供のネットワーク分析ポリシーと侵入ポリシー 1988
カスタムネットワーク分析ポリシーと侵入ポリシーの利点 1989

カスタム ネットワーク分析ポリシーの利点 1990
カスタム侵入ポリシーの利点 1991
カスタム ポリシーの制限 1992
ネットワーク分析ポリシーと侵入ポリシーのライセンス要件 1995
ネットワーク分析と侵入ポリシーの要件と前提条件 1995
ネットワーク分析ポリシーと侵入ポリシーに関するガイドラインと制限事項 1995
ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー 1996
競合と変更：ネットワーク分析ポリシーと侵入ポリシー 1998
ネットワーク分析または侵入ポリシーの終了 1999

第 51 章 侵入ポリシーの使用を開始するには 2001
侵入ポリシーの基本 2001
侵入ポリシーのためのライセンス要件 2003
侵入ポリシーの要件と前提条件 2003
侵入ポリシーの管理 2003
カスタム侵入ポリシーの作成 2005
カスタム Snort 2 検査ポリシーの作成 2005
Snort 2 侵入ポリシーの編集 2006
侵入ポリシーの変更 2007
侵入防御を実行するためのアクセスコントロールルール設定 2007
アクセス コントロール ルール設定と侵入ポリシー 2008
侵入防御を実行するアクセス コントロール ルールの設定 2008
インライン展開でのドロップ動作 2009
インライン展開でのドロップ動作の設定 2010
デュアル システム展開でのドロップ動作 2010
侵入ポリシーの詳細設定 2011
侵入検知と防御のパフォーマンス最適化 2012

第 52 章 ルールを使用した侵入ポリシーの調整 2013
侵入ルールの調整の基本 2013
侵入ルールのタイプ 2014

侵入ルールのライセンス要件 2015
侵入ルールの要件と前提条件 2015
侵入ポリシー内の侵入ルールの表示 2015
[侵入ルール（Intrusion Rules）] ページの列 2016
侵入ルールの詳細 2017
侵入ルール詳細の表示 2018
侵入ルールのしきい値の設定 2019
侵入ルールの抑制の設定 2020
[ルール詳細（Rule Details）] ページからの動的ルール状態の設定 2020
侵入ルールの SNMP アラートの設定 2021
侵入ルールへのコメントの追加 2022
侵入ポリシー内の侵入ルール フィルタ 2022
侵入ルール フィルタの注意事項 2023
侵入ポリシー ルール フィルタ構築のガイドライン 2023
侵入ルール構成フィルタ 2026
侵入ルール コンテンツ フィルタ 2027
侵入ルール カテゴリ 2028
侵入ルールのフィルタ コンポーネント 2028
侵入ルール フィルタの使用 2030
侵入ポリシー内のルール フィルタの設定 2030
侵入ルールの状態 2031
侵入ルールの状態オプション 2031
侵入ルール状態の設定 2032
侵入ポリシーの侵入イベント通知フィルタ 2033
侵入イベントしきい値 2033
侵入イベントしきい値の設定 2033
侵入イベントしきい値の追加と変更 2035
侵入イベントしきい値の表示と削除 2036
侵入ポリシー抑制の設定 2037
侵入ポリシー抑制タイプ 2037
特定のルールの侵入イベントの抑制 2038

抑制条件の表示と削除 2039
動的侵入ルール状態 2040
ダイナミックな侵入ルール状態の設定 2041
[ルール（Rule）] ページからの動的ルール状態の設定 2042
侵入ルールコメントの追加 2043

第 53 章 カスタム侵入ルール 2045
カスタム侵入ルールの概要 2045
侵入ルールエディタのライセンス要件 2046
侵入ルールエディタの要件と前提条件 2046
ルールの詳細 2047
侵入ルール ヘッダー 2047
侵入ルール ヘッダー アクション 2048
侵入ルール ヘッダー プロトコル 2049
侵入ルール ヘッダーの方向 2050
侵入ルール ヘッダーの送信元と宛先の IP アドレス 2050
侵入ルール ヘッダーの送信元および宛先ポート 2053
侵入イベント詳細 2054
カスタム分類の追加 2058
イベント優先順位の定義 2059
イベント参照の定義 2059
カスタム ルールの作成 2060
新規ルールの作成 2061
既存のルールの変更 2062
ルール ドキュメンテーションの表示 2063
侵入ルールへのコメントの追加 2064
カスタム ルールの削除 2065
ルールの検索 2066
侵入ルールの検索条件 2067
侵入ルール エディタ ページでのルールのフィルタリング 2068
フィルタリング ガイドライン 2068

キーワード フィルタリング 2069
文字列フィルタリング 2070
キーワードと文字列の組み合わせによるフィルタリング 2070
フィルタリング ルール 2071
侵入ルールのキーワードと引数 2072
content キーワードと protected_content キーワード 2072
基本コンテンツおよび protected_content キーワードの引数 2074
コンテンツ（content）および保護コンテンツ（protected_content）キーワード検索位置 2075
概要：HTTP content および protected_content キーワードの引数 2078
概要：content キーワードによる高速パターン マッチ機能 2082
replace キーワード 2086
byte_jump キーワード 2087
byte_test キーワード 2090
byte_extract キーワード 2092
byte_math キーワード 2095
概要：pcre キーワード 2098
PCRE の構文 2099
PCRE 修飾子のオプション 2101
PCRE のキーワード値の例 2105
metadata キーワード 2107
サービス メタデータ 2108
メタデータ検索のガイドライン 2114
IP ヘッダー値 2115
ICMP ヘッダー値 2118
TCP ヘッダー値とストリーム サイズ 2119
stream_reassembly キーワード 2124
SSL キーワード 2125
appid キーワード 2127
アプリケーション層プロトコル値 2128
RPC キーワード 2128

ASN.1 キーワード 2128
urilen キーワード 2129
DCE/RPC キーワード 2131
SIP キーワード 2134
GTP キーワード 2137
SCADA キーワード 2150
Modbus キーワード 2150
DNP3 キーワード 2151
CIP および ENIP のキーワード 2154
S7Commplus キーワード 2155
パケット特性 2156
アクティブ応答のキーワード 2158
resp キーワード 2159
react キーワード 2160
detection_filter キーワード 2161
tag キーワード 2162
flowbits キーワード 2164
flowbits キーワードのオプション 2164
flowbits キーワードの使用に関するガイドライン 2166
flowbits キーワードの例 2166
http_encode キーワード 2171
http_encode キーワードの構文 2172
http_encode キーワードの例：2 つの http_endcode キーワードを使用した 2 つのエンコーディングの検索 2173
概要：file_type および file_group キーワード 2173
file_type キーワードと file_group キーワード 2174
file_data キーワード 2175
pkt_data キーワード 2176
base64_decode キーワードと base64_data キーワード 2176

第 54 章 侵入ポリシーとネットワーク分析ポリシーのレイヤ 2179

レイヤの基本 2179
ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤのライセンス要件 2180
ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤの要件と前提条件 2180
レイヤ スタック 2180
基本レイヤ 2181
システム提供の基本ポリシー 2181
カスタム基本ポリシー 2182
基本ポリシーに対するルール更新の影響 2182
基本ポリシーの変更 2183
Cisco 推奨レイヤ 2184
レイヤ管理 2185
共有レイヤ 2186
レイヤの管理 2187
レイヤ間のナビゲーション 2188
レイヤでの侵入ルール 2189
レイヤでの侵入ルールの設定 2191
複数のレイヤからのルール設定の削除 2191
カスタム基本ポリシーからのルール変更の受け入れ 2193
レイヤでのプリプロセッサと詳細設定 2194
層のプリプロセッサと詳細の設定 2195

第 55 章 ネットワーク資産に応じた侵入防御の調整 2197
シスコ推奨ルールについて 2197
Cisco 推奨のデフォルト設定 2198
Cisco 推奨事項の詳細設定 2200
Cisco 推奨事項の生成と適用 2201
スクリプト検出 2202

第 56 章 機密データの検出 2203
機密データ検出の基本 2203
グローバル センシティブ データ検出オプション 2205

個別のセンシティブ データ タイプのオプション 2205
システム提供のセンシティブ データのタイプ 2206
機密データの検出のライセンス要件 2207
機密データの検出の要件と前提条件 2208
センシティブ データ検出の設定 2208
監視対象のアプリケーション プロトコルおよび機密データ 2210
モニター対象のアプリケーション プロトコルの選択 2210
特別なケース：FTP トラフィックでのセンシティブ データの検出 2212
カスタム 機密データ タイプ 2213
カスタム機密データ タイプのデータ パターン 2213
カスタム センシティブ データ タイプの設定 2215
カスタムセンシティブ データ タイプの編集 2216

第 57 章 侵入イベントロギングのグローバル制限 2219
グローバル ルールのしきい値の基本 2219
グローバル ルールしきい値オプション 2220
グローバルなしきい値のライセンス要件 2222
グローバルしきい値の要件と前提条件 2222
グローバルなしきい値の設定 2223
グローバルしきい値の無効化 2224

第 58 章 侵入防御のパフォーマンスの調整 2225
侵入防御のパフォーマンス チューニングについて 2225
侵入防御パフォーマンスの調整のライセンス要件 2226
侵入防御パフォーマンスの調整の要件と前提条件 2226
侵入に関するパターン一致の制限 2227
正規表現による侵入ルールのオーバーライドの制限 2228
侵入ルールの正規表現制限のオーバーライド 2229
パケットごとの侵入イベント生成の制限 2230
パケットごとに生成される侵入イベントの制限 2231
パケットおよび侵入ルールの遅延しきい値構成 2231

遅延ベースのパフォーマンス設定 2232
パケット遅延しきい値構成 2232
パケット遅延しきい値構成の注意事項 2233
パケット遅延しきい値の有効化 2234
パケット遅延しきい値の設定 2234
ルール遅延しきい値構成 2235
ルール遅延しきい値構成の注記 2237
ルール遅延しきい値の設定 2237
侵入パフォーマンス統計情報のロギング設定 2239
侵入パフォーマンス統計情報のロギングの設定 2240

第 IX 部 : ネットワークマルウェア防御とファイルポリシー 2241

第 59 章 ネットワークマルウェア防御とファイルポリシー 2243
ネットワークにおけるマルウェア防御とファイルポリシーについて 2243
ファイル ポリシー 2244
ファイルポリシーの要件と前提条件 2245
ファイルおよびマルウェア ポリシーのライセンス要件 2245
ファイルポリシーとマルウェア検出のベストプラクティス 2246
ファイルルールのベストプラクティス 2246
ファイル検出のベストプラクティス 2247
ファイルブロッキングのベストプラクティス 2247
ファイルポリシーのベストプラクティス 2249
マルウェア防御の設定方法 2249
マルウェア防御の計画と準備 2250
ファイル ポリシーの設定 2252
アクセス コントロール設定へのファイル ポリシーの追加 2252
マルウェア保護のためのアクセス コントロール ルールの設定 2253
マルウェア防御のメンテナンスとモニタリングの設定 2255
マルウェア防御のためのクラウド接続 2255
AMP クラウド接続の設定 2257

AMP クラウド接続の要件とベストプラクティス 2257
AMP クラウドの選択 2257
Cisco AMP プライベート クラウド 2258
AMP クラウドへの接続の管理（パブリックまたはプライベート） 2260
AMP オプションの変更 2261
動的分析接続 2262
動的分析の要件 2262
デフォルト動的分析接続の表示 2262
オンプレミスアプライアンスの動的分析（Cisco Secure Malware Analytics） 2263
パブリック クラウドでの動的分析の結果へのアクセスの有効化 2265
システムの保守：動的分析の対象となるファイル タイプの更新 2266
ファイル ポリシーとファイル ルール 2266
ファイルポリシーの作成または編集 2266
高度およびアーカイブ ファイル インスペクション オプション 2267
ファイル ポリシーの管理 2271
ファイル ルール 2273
ファイル ルールのコンポーネント 2273
ファイル ルール アクション 2275
ファイル ルールの作成 2284
マルウェア防御のためのアクセス制御ルールのロギング 2286
レトロスペクティブな性質の変更 2286
ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション 2286
ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整 2289
（オプション）Secure Endpoint を使用したマルウェア防御 2290
マルウェア防御の比較：Firepower と Secure Endpoint 2291
Firepower と Secure Endpoint の統合について 2292
Firepower と Secure Endpoint の統合の利点 2292
Secure Endpoint と AMP プライベート クラウド 2292
Firepower と Secure Endpoint の統合 2293
ネットワークマルウェア防御とファイルポリシーの履歴 2295

第 X 部： 暗号化トラフィックの処理 2297

第 60 章 トラフィックの復号の概要 2299

トラフィック復号の説明 2299

TLS/SSL ハンドシェイク処理 2301

ClientHello メッセージ処理 2301

ServerHello とサーバー証明書メッセージの処理 2305

復号 ルールとポリシーの基本 2307

復号のケース 2308

トラフィックを復号する場合としない場合 2308

復号と再署名（発信トラフィック） 2310

既知のキーでの復号（着信トラフィック） 2311

その他の 復号ルール アクション 2311

復号ルール のコンポーネント 2311

復号ルールの評価の順序 2313

複数ルールの例 2314

TLS 暗号化アクセラレーション 2316

TLS 暗号化アクセラレーション の注意事項と制限事項 2317

TLS 暗号アクセラレーションのステータスの表示 2319

復号ポリシー とルールの設定方法 2319

復号ポリシー の履歴 2322

第 61 章 復号ポリシー 2327

復号ポリシーについて 2327

復号ポリシー の要件と前提条件 2328

復号ポリシーの作成 2328

アウトバウンド接続保護を使用した復号ポリシーの作成 2329

インバウンド接続保護を使用した復号ポリシーの作成 2330

復号ポリシーの除外 2333

アウトバウンド保護のための内部 CA の生成 2337

アウトバウンド保護のための内部 CA のアップロード 2339
アウトバウンド保護のための内部証明書のアップロード 2339
他のルールアクションを使用した復号ポリシーの作成 2340
復号ポリシー のデフォルトアクション 2341
復号できないトラフィックのデフォルト処理オプション 2342
復号できないトラフィックのデフォルト処理を設定する 2344
復号ポリシーの詳細オプション 2345
TLS 1.3 復号のベストプラクティス 2347

第 62 章 復号ルール 2349
復号ルールの概要 2349
復号ルール の要件と前提条件 2350
復号ルール の注意事項と制限事項 2350
TLS/SSL 復号の使用上のガイドライン 2351
復号ルール サポートされていない機能 2352
TLS/SSL 復号禁止のガイドライン 2352
TLS/SSL 復号：再署名のガイドライン 2354
TLS/SSL 復号：既知のキーのガイドライン 2357
TLS/SSL ブロックのガイドライン 2358
TLS/SSL 証明書のピン留めのガイドライン 2358
TLS/SSL ハートビートのガイドライン 2358
TLS/SSL 匿名の暗号スイートの制限事項 2359
TLS/SSL 正規化のガイドライン 2359
その他の 復号ルール ガイドライン 2359
復号ルールトラフィック処理 2360
暗号化トラフィック インスペクションの設定 2362
復号ルールの評価の順序 2363
復号ルール 条件 2365
セキュリティゾーンルール条件 2366
セキュリティ ゾーン条件とマルチテナンシー 2367
ネットワークルール条件 2367

VLAN タグルール条件 2367
ユーザールール条件 2368
アプリケーションルール条件 2368
ポートルールの条件 2370
カテゴリルール条件 2371
サーバー証明書ベースの 復号ルール条件 2371
証明書の 復号ルール条件 2372
識別名（DN）のルール条件 2373
外部認証局の信頼 2378
証明書ステータスの 復号ルール条件 2379
暗号スイートの 復号ルール 条件 2382
暗号化プロトコルバージョンの復号ルール条件 2385
復号ルール アクション 2386
復号ルール モニターアクション 2386
復号ルール [復号しない（Do Not Decrypt）] アクション 2386
復号ルールのブロックアクション 2388
復号ルールの復号アクション 2388
TLS/SSL ハードウェア アクセラレーションのモニター 2389
情報カウンタ 2389
アラート カウンタ 2389
エラー カウンタ 2390
重大カウンタ 2390
復号ルール のトラブルシューティング 2391
TLS/SSL オーバーサブスクリプションについて 2391
TLS/SSL オーバーサブスクリプションのトラブルシューティング 2391
TLS ハートビートについて 2394
TLS ハートビートのトラブルシューティング 2394
TLS/SSL のピニングについて 2395
TLS/SSL ピニングのトラブルシューティング 2396
不明または不正な証明書または認証局のトラブルシュート 2398
TLS/SSL 暗号スイートの確認 2400

第 63 章 復号ルールとポリシーの例 2403
復号ルール ベスト プラクティス 2403
プレフィルタとフローオフロードによる検査のバイパス 2404
[復号しない（Do Not Decrypt）] のベストプラクティス 2405
[復号-再署名（Decrypt - Resign）] と [復号-既知のキー（Decrypt - Known Key）] のベストプラクティス 2406
最初に配置する 復号ルール 2407
最後に配置する 復号ルール 2407
推奨ポリシーとルールの設定 2407
推奨ポリシーとルールの設定 2408
復号ポリシー の設定 2409
アクセス コントロール ポリシーの設定 2411
復号ポリシーのウォークスルー 2412
推奨ポリシーとルールの設定 2413
復号ポリシー の設定 2414
アクセス コントロール ポリシーの設定 2416
復号ルール 例 2417
プレフィルタするトラフィック 2418
2418
：特定のトラフィックを復号する 2418
低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない 2419
カテゴリの [復号-再署名（Decrypt - Resign）] ルールの作成 2420
復号ルール：証明書とプロトコルバージョンをブロックまたは監視する 2421
復号ルール の設定 2427

第 XI 部 : ユーザー ID 2429

第 64 章 ユーザーアイデンティティの概要 2431
ユーザー アイデンティティについて 2431
アイデンティティの用語 2432

ユーザー アイデンティティ ソースについて 2433
ユーザーアイデンティティのベストプラクティス 2434
アイデンティティ導入 2437
アイデンティティ ポリシーの設定方法 2438
ユーザー アクティビティ データベース 2442
ユーザ データベース 2442
Firepower システムのホストとユーザーの制限 2443
ホスト制限（Host Limit） 2444
Microsoft Active Directory のユーザー制限 2445
アイデンティティ レルムの制限 2447
Microsoft Azure Active Directory レルムのユーザー制限 2447

第 65 章 [Realms] 2451
レルムのライセンス要件 2451
レルムの要件と前提条件 2451
LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 2452
レルムとレルムシーケンスについて 2455
レルムおよび信頼できるドメイン 2458
レルムがサポートされているサーバー 2461
サポートされているサーバー オブジェクト クラスと属性名 2462
Kerberos 認証の前提条件 2463
レルム フィールド 2464
[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド 2468
Active Directory または LDAP に安全に接続する 2471
Active Directory サーバーの名前の検索 2472
Active Directory サーバーのルート証明書のエクスポート 2473
ユーザーとグループの同期 2475
レルムシーケンスの作成 2476
クロスドメイン信頼のために Firewall Management Center を設定する：セットアップ 2477
クロスドメイン信頼のために Secure Firewall Management Center を設定する。ステップ 1：レルムとディレクトリの設定 2478

クロスドメイン信頼のための Secure Firewall Management Center の設定。ステップ 2：ユーザーとグループの同期 2483
クロスドメイン信頼のための Secure Firewall Management Center の設定。ステップ 3：問題の解決 2484
レルムの管理 2486
レルムの比較 2486
レルムとユーザーのダウンロードのトラブルシュート 2487
レルムまたはユーザーの不一致の検出 2491
クロスドメイン信頼のトラブルシュート 2492
レルムの履歴 2496

第 66 章 ISE/ISE-PIC によるユーザーの制御 2497
ISE/ISE-PIC アイデンティティ ソース 2497
送信元および宛先セキュリティグループタグ（SGT）の照合 2498
ISE/ISE-PIC のライセンス要件 2500
ISE/ISE-PIC の要件と前提条件 2500
ISE/ISE-PIC の注意事項と制限事項 2500
ユーザー制御用 ISE/ISE-PIC の設定方法 2503
レルムを使用しない ISE/ISE-PIC の設定方法 2503
レルムを使用したユーザー制御用 ISE/ISE-PIC の設定方法 2505
ISE/ISE-PIC の設定 2507
ISE でのセキュリティグループと SXP パブリッシングの設定 2508
Firewall Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート 2510
システム証明書のエクスポート 2511
自己署名証明書の生成 2512
ISE/ISE-PIC 証明書のインポート 2513
ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング 2514
ISE/ISE-PIC の履歴 2516

第 67 章 キャプティブポータルによるユーザーの制御 2519
キャプティブ ポータルのアイデンティティ ソース 2519

ホスト名のリダイレクトについて 2520
キャプティブポータルのライセンス要件 2520
キャプティブポータルの要件と前提条件 2520
キャプティブ ポータルのガイドラインと制約事項 2521
ユーザー制御のためのキャプティブ ポータルの設定方法 2524
キャプティブポータルの設定パート 1：ネットワークオブジェクトの作成 2526
キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成 2528
キャプティブポータルの設定パート 3：TCP ポートアクセス コントロール ルールの作成 2530
キャプティブポータルの設定パート 4：ユーザー アクセス コントロール ルールの作成 2532
キャプティブポータルの例：アウトバウンドルールを使用した復号ポリシーの作成 2533
キャプティブポータルの設定パート 6：アクセス コントロール ポリシーへのアイデンティティと 復号ポリシー の関連付け 2535
キャプティブ ポータル フィールド 2536
キャプティブ ポータルからのアプリケーションの除外 2537
キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング 2539
キャプティブ ポータルの履歴 2541

第 68 章 **リモートアクセス VPN によるユーザーの制御 2543**
リモート アクセス VPN アイデンティティ ソース 2543
ユーザー制御用 RA VPN の設定 2544
リモート アクセス VPN アイデンティティ ソースのトラブルシューティング 2545
VPN 統計の設定が正しくない 2546
RA VPN の履歴 2548

第 69 章 **TS エージェントによるユーザーの制御 2549**
ターミナル サービス（TS）エージェントのアイデンティティ ソース 2549
TS エージェントのガイドライン 2550
TS エージェントによるユーザーの制御 2550
TS エージェント アイデンティティ ソースのトラブルシューティング 2551
TS エージェントの履歴 2552

第 70 章 ユーザー アイデンティティ ポリシー 2553
アイデンティティ ポリシーについて 2553
アイデンティティポリシーのライセンス要件 2554
アイデンティティポリシーの要件と前提条件 2555
アイデンティティ ポリシーの作成 2555
アイデンティティ マッピング フィルタの作成 2557
アイデンティティルールの条件 2558
セキュリティゾーンルール条件 2558
セキュリティ ゾーン条件とマルチテナンシー 2559
ネットワークルール条件 2559
ホスト名ネットワークルール条件にリダイレクト 2559
VLAN タグルール条件 2560
ポートルールの条件 2560
ポート、プロトコル、および ICMP コードルールの条件 2561
レルムと設定のルール条件 2562
アイデンティティ ルールの作成 2565
アイデンティティ ルール フィールド 2567
アイデンティティ ポリシーの管理 2568
アイデンティティ ルールの管理 2569
ユーザー制御のトラブルシューティング 2569

第 XII 部 : ネットワーク検出 2573

第 71 章 ネットワーク検出の概要 2575
ホスト、アプリケーション、およびユーザーのデータの検出について 2575
ホストおよびアプリケーション検出の基礎 2576
オペレーティング システムおよびホスト データのパッシブ検出 2576
オペレーティング システムおよびホスト データのアクティブ検出 2577
アプリケーションおよびオペレーティング システムの現在の ID 2578
現在のユーザー ID 2579

アプリケーションおよびオペレーティング システムの ID の競合 2579
NetFlow データ 2580
NetFlow データを使用するための要件 2581
NetFlow データと管理対象デバイス データの違い 2582

第 72 章 ホスト アイデンティティ ソース 2585
概要：ホストのデータ収集 2585
ホスト アイデンティティ ソースの要件と前提条件 2586
システムが検出できるホスト オペレーティング システムの判別 2586
ホスト オペレーティング システムの識別 2587
カスタムフィンガープリント 2587
フィンガープリントの管理 2588
フィンガープリントのアクティブおよび非アクティブの設定 2589
アクティブなフィンガープリントの編集 2590
非アクティブなフィンガープリントの編集 2590
クライアント用のカスタム フィンガープリントの作成 2591
サーバー用のカスタム フィンガープリントの作成 2594
ホスト入力データ 2598
サードパーティのデータを使用するための要件 2598
サードパーティ製品のマッピング 2599
サードパーティの製品のマッピング 2599
サード パーティ製品の修正のマッピング 2601
サードパーティの脆弱性のマッピング 2602
カスタム製品マッピング 2603
カスタム製品マッピングの作成 2603
カスタム製品マッピング リストの編集 2605
カスタム製品マッピングのアクティブ化と非アクティブ化 2605
ホスト入力クライアントの設定 2606
Nmap スキャン 2607
Nmap 修復オプション 2608
Nmap スキャンのガイドライン 2613

例：Nmap を使用した不明なオペレーティング システムの解決 2615
例：Nmap を使用した新しいホストへの応答 2616
Nmap スキャンの管理 2618
Nmap スキャン インスタンスの追加 2619
Nmap スキャン インスタンスの編集 2620
Nmap スキャン ターゲットの追加 2621
Nmap スキャン ターゲットの編集 2622
Nmap 修復の作成 2623
Nmap 修復の編集 2625
オンデマンド Nmap スキャンの実行 2626
Nmap スキャンの結果 2627
Nmap スキャン結果の表示 2627
Nmap スキャン結果のフィールド 2628
Nmap スキャン結果のインポート 2629
ホスト アイデンティティ ソースの履歴 2630

第 73 章 アプリケーションの検出 2631
概要：アプリケーション検出 2631
アプリケーション ディテクタの基本 2633
Web インターフェイスでのアプリケーション プロトコルの識別 2634
クライアント検出からの暗黙的アプリケーション プロトコル検出 2635
ホスト制限と検出イベント ロギング 2636
アプリケーション検出に関する特別な考慮事項 2636
Snort 3 でのアプリケーション検出 2638
アプリケーション検出の要件と前提条件 2639
カスタム アプリケーション ディテクタ 2639
カスタム アプリケーション ディテクタおよびユーザー定義アプリケーション フィールド 2640
カスタム アプリケーション ディテクタの設定 2643
ユーザー定義アプリケーションを作成する 2645
基本ディテクタでの検出パターンの指定 2646

高度なディテクタでの検出条件の指定 2647
EVE のプロセス割り当ての指定 2648
カスタム アプリケーション プロトコル ディテクタのテスト 2649
ディテクタ詳細情報の表示またはダウンロード 2650
ディテクタ リストのソート 2651
ディテクタ リストのフィルタリング 2651
ディテクタ リストのフィルタ グループ 2652
他のディテクタ ページへの移動 2653
ディテクタのアクティブおよび非アクティブの設定 2653
カスタム アプリケーション ディテクタの編集 2654
ディテクタの削除 2655

第 74 章 ネットワーク検出ポリシー 2657
概要：ネットワーク検出ポリシー 2657
ネットワーク検出ポリシーの要件と前提条件 2658
ネットワーク検出のカスタマイズ 2658
ネットワーク検出ポリシーの設定 2659
ネットワーク検出ルール 2660
ネットワーク検出ルールの設定 2661
アクションと検出されるアセット 2662
モニター対象ネットワーク 2663
ポート除外 2665
ネットワーク検出ルールのゾーン 2667
トラフィック ベース検出のアイデンティティ ソース 2668
高度なネットワーク検出オプションの設定 2671
ネットワーク検出の一般設定 2672
ネットワーク検出の一般設定を行う 2672
ネットワーク検出アイデンティティ競合の設定 2673
ネットワーク検出アイデンティティ競合の解決の設定 2674
ネットワーク検出の脆弱性の影響の評価オプション 2674
ネットワーク検出の脆弱性影響評価の有効化 2675

侵害の兆候 2675
侵害の兆候ルールの有効化 2676
NetFlow エクスポータのネットワーク検出ポリシーへの追加 2677
ネットワーク検出のデータ ストレージ設定 2677
ネットワーク検出データ ストレージの設定 2679
ネットワーク検出イベント ロギングの設定 2679
ネットワーク検出 OS およびサーバー アイデンティティ ソースの追加 2680
ネットワーク検出戦略のトラブルシューティング 2681

第 XIII 部 : FlexConfig ポリシー 2685

第 75 章 FlexConfig ポリシー 2687
FlexConfig ポリシーの概要 2687
FlexConfig ポリシーの推奨される使用法 2688
FlexConfig オブジェクトの CLI コマンド 2689
ASA ソフトウェア バージョンと現在の CLI 設定の決定 2689
禁止された CLI コマンド 2690
テンプレート スクリプト 2692
FlexConfig 変数 2693
変数の処理方法 2694
変数がデバイスに関して返す内容を表示する方法 2697
FlexConfig ポリシー オブジェクト変数 2698
FlexConfig システム変数 2699
定義済みの FlexConfig オブジェクト 2701
定義済みのテキスト オブジェクト 2707
FlexConfig ポリシーの要件と前提条件 2711
FlexConfig の注意事項と制約事項 2712
FlexConfig ポリシーによるデバイス設定のカスタマイズ 2712
FlexConfig オブジェクトの設定 2714
FlexConfig オブジェクトへのポリシーオブジェクト変数の追加 2718
秘密キーの設定 2719

FlexConfig テキスト オブジェクトの設定 2720
FlexConfig ポリシーの設定 2722
FlexConfig ポリシーのターゲット デバイスの設定 2723
FlexConfig ポリシーのプレビュー 2724
展開された構成の確認 2725
FlexConfig を使用した設定済み機能の削除 2727
FlexConfig から管理対象機能への変換 2728
FlexConfig の例 2729
高精度時間プロトコルの設定方法（ISA 3000） 2729
停電時の自動ハードウェアバイパスの設定方法（ISA 3000） 2734
FlexConfig ポリシーの移行 2737
FlexConfig の履歴 2739

第 XIV 部： 高度なネットワーク分析と前処理 2743

第 76 章 ネットワーク分析ポリシーと侵入ポリシーに対するアクセス コントロールの詳細設定 2745
ネットワーク分析および侵入ポリシーのアクセス コントロールの詳細設定について 2745
ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定の要件と前提条件 2745
トラフィック識別の前に通過するパケットのインスペクション 2746
トラフィック識別の前に通過するパケットを処理するためのベストプラクティス 2746
トラフィック識別の前に通過するパケットを処理するためのポリシーの指定 2747
ネットワーク分析プロファイルの詳細設定 2748
デフォルトのネットワーク分析ポリシーの設定 2749
ネットワーク分析ルール 2750
ネットワーク分析ポリシールール条件 2750
ネットワーク分析ルールの設定 2752
ネットワーク分析ルールの管理 2753

第 77 章 ネットワーク分析ポリシーの開始 2755
ネットワーク分析ポリシーの基本 2755
ネットワーク分析ポリシーのライセンス要件 2756

ネットワーク分析ポリシーの要件と前提条件 2756
ネットワーク分析ポリシーの管理 2756
ネットワーク分析ポリシーの作成 2757
ネットワーク分析ポリシーの変更 2758
Snort 2 の場合のカスタムネットワーク分析ポリシーの作成 2758
カスタム ネットワーク分析ポリシーの作成 2759
Snort 2 のネットワーク分析ポリシー管理 2760
ネットワーク分析ポリシーの設定とキャッシュされた変更 2761
ネットワーク分析ポリシーの編集 2761
Snort 2 のネットワーク分析ポリシーでのプリプロセッサの構成 2762
インライン導入でのプリプロセッサによるトラフィックの変更 2764
ネットワーク分析ポリシーの注記におけるプリプロセッサの設定 2764

第 78 章 アプリケーション層プリプロセッサ 2767
アプリケーション層のプリプロセッサの概要 2767
アプリケーション層プリプロセッサのライセンス要件 2768
アプリケーション層プリプロセッサの要件と前提条件 2768
DCE/RPC プリプロセッサ 2768
コネクションレス型およびコネクション型 DCE/RPC トラフィック 2769
DCE/RPC ターゲット ベース ポリシー 2770
RPC over HTTP トランスポート 2771
DCE/RPC グローバル オプション 2772
DCE/RPC ターゲットベース ポリシー オプション 2774
トラフィックに関連する DCE/RPC ルール 2780
DCE/RPC プリプロセッサの設定 2780
DNS プリプロセッサ 2782
DNS プリプロセッサ オプション 2784
DNS プリプロセッサの設定 2785
FTP/Telnet デコーダ 2787
グローバル FTP および Telnet オプション 2787
Telnet オプション 2787

サーバーレベルの FTP オプション 2788
FTP コマンドの検証ステートメント 2791
クライアントレベルの FTP オプション 2792
FTP/Telnet デコーダの設定 2794
HTTP Inspect プリプロセッサ 2796
グローバル HTTP 正規化オプション 2797
サーバーレベルの HTTP 正規化オプション 2798
サーバーレベルの HTTP 正規化エンコード オプション 2808
HTTP インスペクト プリプロセッサの設定 2812
その他の HTTP 検査プリプロセッサ ルール 2814
Sun RPC プリプロセッサ 2815
Sun RPC プリプロセッサのオプション 2816
Sun RPC プリプロセッサの設定 2816
SIP プリプロセッサ 2818
SIP プリプロセッサのオプション 2819
SIP プリプロセッサの設定 2821
その他の SIP プリプロセッサ ルール 2822
GTP プリプロセッサ 2824
GTP プリプロセッサ ルール 2824
GTP プリプロセッサの設定 2824
IMAP プリプロセッサ 2826
IMAP プリプロセッサ オプション 2826
IMAP プリプロセッサの設定 2828
その他の IMAP プリプロセッサ ルール 2829
POP プリプロセッサ 2829
POP プリプロセッサ オプション 2830
POP プリプロセッサの設定 2831
その他の POP プリプロセッサ ルール 2832
SMTP プリプロセッサ 2833
SMTP プリプロセッサのオプション 2833
SMTP デコードの設定 2838

SSH プリプロセッサ 2840
SSH プリプロセッサのオプション 2841
SSH プリプロセッサの設定 2844
SSL プリプロセッサ 2845
SSL 前処理の仕組み 2845
SSL プリプロセッサのオプション 2847
SSL プリプロセッサの設定 2848
SSL プリプロセッサ ルール 2849

第 79 章 SCADA プリプロセッサ 2851
SCADA プリプロセッサの概要 2851
SCADA プリプロセッサのライセンス要件 2852
SCADA プリプロセッサの要件と前提条件 2852
Modbus プリプロセッサ 2852
Modbus プリプロセッサ ポート オプション 2853
Modbus プリプロセッサの設定 2853
Modbus プリプロセッサ ルール 2854
DNP3 プリプロセッサ 2855
DNP3 プリプロセッサ オプション 2855
DNP3 プリプロセッサの設定 2855
DNP3 プリプロセッサ ルール 2857
CIP プリプロセッサ 2857
CIP プリプロセッサのオプション 2858
CIP イベント 2858
CIP プリプロセッサ ルール 2859
CIP プリプロセッサの設定のガイドライン 2859
CIP プリプロセッサの設定 2861
S7Commplus プリプロセッサ 2862
S7Commplus プリプロセッサの設定 2862

第 80 章 トランスポート層およびネットワーク層のプリプロセッサ 2865

トランスポート層およびネットワーク層のプリプロセッサの概要 2865
トランスポート層およびネットワーク層のプリプロセッサのライセンス要件 2866
トランスポート層およびネットワーク層のプリプロセッサの要件と前提条件 2866
トランスポート/ネットワーク プリプロセッサの詳細設定 2866
無視される VLAN ヘッダー 2866
侵入廃棄ルールでのアクティブ応答 2867
トランスポート/ネットワーク プリプロセッサの詳細オプション 2868
トランスポート/ネットワーク プリプロセッサの詳細設定の構成 2869
チェックサム検証 2870
チェックサム検証オプション 2870
チェックサムの確認 2871
インライン正規化プリプロセッサ 2872
インライン正規化オプション 2873
インライン正規化の設定 2879
IP 最適化プリプロセッサ 2881
IP フラグメンテーション エクスプロイト 2881
ターゲット ベースの最適化ポリシー 2882
IP 最適化オプション 2882
IP 最適化の設定 2885
パケット デコーダ 2887
パケット デコーダ オプション 2887
パケット復号化の設定 2891
TCP ストリームの前処理 2892
状態に関連する TCP エクスプロイト 2893
ターゲット ベースの TCP ポリシー 2893
TCP ストリームの再構成 2894
TCP ストリームのプリプロセス オプション 2895
TCP ストリームの前処理の設定 2904
UDP ストリームの前処理 2906
UDP ストリームのプリプロセス オプション 2906
UDP ストリームの前処理の設定 2907

第 81 章 特定の脅威の検出 2909

特定の脅威の検出の概要 2909

特定の脅威の検出のライセンス要件 2910

特定の脅威の検出の要件と前提条件 2910

Back Orifice の検出 2910

Back Orifice 検出プリプロセッサ 2910

Back Orifice の検出 2911

ポートスキャン検出 2912

ポートスキャン タイプ、プロトコル、フィルタリング感度レベル 2913

ポートスキャン イベント生成 2916

ポートスキャン イベント パケット ビュー 2917

ポートスキャン検出の設定 2919

レート ベースの攻撃防御 2921

レート ベースの攻撃防御の例 2922

detection_filter キーワードの例 2923

ダイナミック ルール状態のしきい値構成または抑制の例 2924

ポリシー全体のレート ベース検出としきい値構成または抑制の例 2925

複数のフィルタリング方法によるレート ベース検出の例 2926

レート ベースの攻撃防御オプションと設定 2927

レートベースの攻撃防御、検出フィルタリング、しきい値処理または抑制 2929

レートベース攻撃防止の設定 2929

第 82 章 アダプティブ プロファイル 2933

アダプティブ プロファイルについて 2933

アダプティブプロファイルのライセンス要件 2934

アダプティブプロファイルの要件と前提条件 2934

アダプティブプロファイルの更新 2934

アダプティブプロファイルの更新とシスコの推奨ルール 2935

適応型プロファイルのオプション 2936

適応型プロファイルの設定 2937

第 XV 部： Threat Intelligence Director 2939

第 83 章 Secure Firewall Threat Intelligence Director 2941

Secure Firewall Threat Intelligence Director の概要 2941

Threat Intelligence Director およびセキュリティ インテリジェンス 2943

Threat Intelligence Director のパフォーマンスへの影響 2944

Threat Intelligence Director の要件と前提条件 2944

プラットフォーム、要素、およびライセンスに関する要件 2945

ソース要件 2946

ソース コンテンツの制限事項 2947

Threat Intelligence Director のセットアップ方法 2947

Threat Intelligence Director をサポートするためのポリシーの設定 2948

データ ソースを取り込むためのオプション 2950

ソースとして使用する TAXII フィードの取得 2950

URL からのソースの取得 2952

ソースとして使用するローカル ファイルのアップロード 2954

重複インジケータの処理 2955

Threat Intelligence Director ソースの TLS/SSL 設定の構成 2955

Threat Intelligence Director アクセス権を持つユーザー ロール 2957

Threat Intelligence Director データのバックアップおよび復元について 2957

Threat Intelligence Director インシデントおよびオブザベーション データの分析 2958

監視とインシデント生成 2958

インシデントの表示と管理 2960

インシデント サマリー情報 2961

インシデントの詳細 2963

Threat Intelligence Director オブザベーションのイベントの表示 2967

Secure Firewall Management Center イベントでの Threat Intelligence Director オブザベーション 2968

アクションに影響を与える要因 2968

Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け 2969

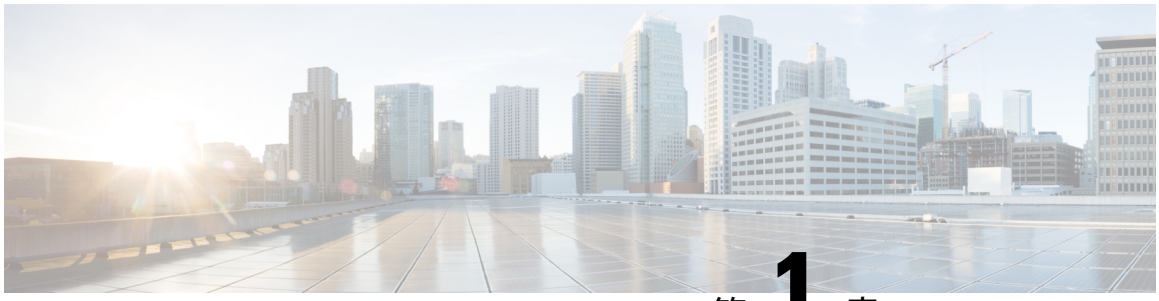
Threat Intelligence Director 設定の表示および変更 2975

要素（管理対象デバイス）の Threat Intelligence Director ステータスの表示 2975
ソースの表示と管理 2976
ソース サマリー情報 2977
ソース ステータスの詳細 2978
インジケータの表示と管理 2980
インジケータ サマリー情報 2981
インジケータの詳細 2982
オブザーバブルの表示と管理 2983
オブザーバブル サマリー情報 2984
テーブル ビューでの Threat Intelligence Director データのフィルタ処理 2985
Threat Intelligence Director 設定における継承 2986
複数の親からの TID 設定の継承 2986
継承された TID 設定の上書きについて 2987
ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 2988
公開の一時停止について 2989
Threat Intelligence Director の一時停止と要素からの Threat Intelligence Director データの消去 2990
ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 2990
オブザーバブルのパブリケーション頻度の変更 2991
Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について 2992
Threat Intelligence Director オブザーバブルのブロックしないリストへの追加 2993
STIX ソース ファイルの表示 2993
Threat Intelligence Director のトラブルシューティング 2994
Threat Intelligence Director の履歴 2996

第 部

デバイス設定のスタートアップガイド

- デバイス管理 （1 ページ）
- デバイス設定 （55 ページ）
- ユーザー （131 ページ）
- 設定の展開 （155 ページ）



第 1 章

デバイス管理

このガイドは、プライマリマネージャまたは分析専用マネージャとしてのオンプレミスの Secure Firewall Management Center に適用されます。Cisco Defense Orchestrator（CDO）クラウド提供型 Firewall Management Center をプライマリマネージャとして使用する場合、オンプレミスの Firewall Management Center は分析のみに使用できます。クラウド提供型 Firewall Management Center の管理にはこのガイドを使用しないでください。「Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理」を参照してください。

Secure Firewall Management Center でデバイスを追加および管理できます。

- デバイス管理について （1 ページ）
- デバイス管理の要件と前提条件 （11 ページ）
- デバイスのコマンド ライン インターフェイス（CLI）へのログイン （12 ページ）
- Firewall Threat Defense 初期設定の完了 （14 ページ）
- デバイスの管理 （32 ページ）
- マネージャの切り替え （42 ページ）
- Cisco Secure Firewall 3100 での SSD のホットスワップ （49 ページ）
- デバイス管理の履歴 （52 ページ）

デバイス管理について

Firewall Management Center を使用してデバイスを管理します。

Firewall Management Center およびデバイス管理について

Firewall Management Center がデバイスを管理するときは、デバイスとの間に、双方向の SSL 暗号化通信チャネルをセットアップします。Firewall Management Center はこのチャネルを使用して、そのデバイスへのネットワーク トラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを Firewall Management Center に送信します。

Firewall Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを一箇所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Firewall Management Center からデバイスのヘルス ステータスをモニターできます。

（注） CDO 管理対象デバイスがあり、オンプレミス Firewall Management Center を分析のみに使用している場合、オンプレミス Firewall Management Center はポリシーの設定またはアップグレードをサポートしません。デバイス設定およびその他のサポートされていない機能に関連するこのガイドの章と手順は、プライマリマネージャが CDO のデバイスには適用されません。

Firewall Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンスデータを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Firewall Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。

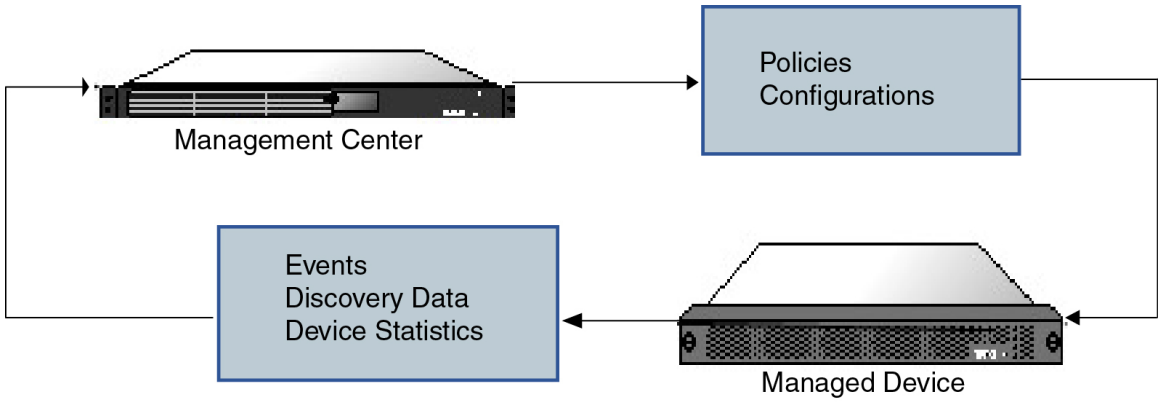
（注） Firewall Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で入手可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは、最新バージョンの Firewall Threat Defense ソフトウェアが必要な新しい機能は利用できません。一部の Firewall Management Center 機能は、以前のバージョンで使用できる場合があります。

Secure Firewall Management Center で管理できるデバイス

Firewall Threat Defense デバイスを管理するための集中管理ポイントとして Secure Firewall Management Center を使用できます。

デバイスを管理する際の情報は、SSL で暗号化されたセキュアな TLS-1.3 暗号化通信チャネルを介して、Firewall Management Center とデバイスの間で送信されます。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

次の図に、Firewall Management Center と管理対象デバイスの間で送信される情報を示します。アプライアンス間で送信されるイベントとポリシーのタイプは、デバイスタイプに基づくことに注意してください。



管理接続について

Firewall Management Center 情報を使用してデバイスを設定し、デバイスを Firewall Management Center に追加した後に、デバイスまたは Firewall Management Center のいずれかで管理接続を確立できます。初期設定に応じて、以下のようになります。

- デバイスまたは Firewall Management Center のいずれかから開始できる。
- デバイスのみが開始できる。
- Firewall Management Center のみが開始できる。

初期化は常に Firewall Management Center の eth0 またはデバイスの最も番号が小さい管理インターフェイスから始まります。接続が確立されていない場合は、追加の管理インターフェースが試行されます。Firewall Management Center の複数の管理インターフェイスにより、個別のネットワークに接続したり、管理トラフィックとイベントトラフィックを分離したりできます。ただし、イニシエータは、ルーティングテーブルに基づいて最適なインターフェイスを選択しません。

管理接続が安定しており、過度なパケット損失がなく、少なくとも 5 Mbps のスループットがあることを確認します。デフォルトでは、管理接続は TCP ポート 8305 を使用します（このポートは設定可能です）。デバイスと Firewall Management Center の間に別の Firewall Threat Defense を配置する場合は、管理の中断を防ぐために、プレフィルタポリシーを適用して管理トラフィックをディープインスペクションから除外してください。

（注） 管理接続は、それ自身とデバイスの間の安全な TLS-1.3 暗号化通信チャネルです。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

ポリシーとイベント以外の機能

Firewall Management Center では、ポリシーをデバイスに展開したり、デバイスからイベントを受信するだけでなく、以下のデバイス関連のタスクも実行できます。

デバイスのバックアップ

FTD CLIから物理的な管理対象デバイスをバックアップすることはできません。設定データと統合ファイル（任意）をバックアップするには、デバイスを管理している Firewall Management Center を使用してデバイスのバックアップを実行します。

イベントデータをバックアップするには、デバイスを管理している Firewall Management Center のバックアップを実行します。

デバイスの更新

シスコは適宜、Firepower システムの更新プログラムをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新（新しいルールや更新された侵入ルールが含まれる場合があります）
- 脆弱性データベース（VDB）の更新
- 地理位置情報の更新
- ソフトウェア パッチおよびアップデート

Firewall Management Center を使用して、管理対象デバイスに更新プログラムをインストールできます。

デバイス管理インターフェイスについて

各デバイスには Firewall Management Center と通信するための専用の管理インターフェイスが 1 つ含まれています。必要に応じて、専用の管理インターフェイスではなく、管理用のデータインターフェイスを使用するようにデバイスを設定できます。

管理インターフェイスまたはコンソールポートで初期設定を実行できます。

管理インターフェイスは、スマート ライセンス サーバーとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

Firewall Threat Defense の管理インターフェイスとイベントインターフェイス

デバイスをセットアップするときに、接続先とする Firewall Management Center の IP アドレスまたはホスト名を指定します（既知の場合）。この場合、デバイスが接続を開始すると、初期登録時には、管理トラフィックとイベントトラフィックの両方がこのアドレスに送信されます。Firewall Management Center が不明な場合、Firewall Management Center が最初の接続を確立します。この場合、Firewall Threat Defense で指定されたものとは異なる Firewall Management Center管理インターフェイスから接続が開始される可能性があります。以降の接続では、指定

された IP アドレスの Firewall Management Center 管理インターフェイスを使用する必要があります。

Firewall Management Center に別のイベント専用インターフェイスがある場合、ネットワークが許可する場合、管理対象デバイスは後続のイベントトラフィックを Firewall Management Center イベント専用インターフェイスに送信します。さらに、一部の管理対象デバイスモデルには、イベント専用トラフィック用に構成できる追加の管理インターフェイスが含まれています。管理用のデータインターフェイスを設定する場合は、個別管理およびイベントインターフェイスを使用できません。イベントネットワークがダウンすると、イベントトラフィックは、Firewall Management Center および/または管理対象デバイスの通常の管理インターフェイスに戻ります。

管理のための Firewall Threat Defense データインターフェイスの使用について

Firewall Management Center との通信には、専用の管理インターフェイスか、または通常のデータインターフェイスを使用できます。データインターフェイスでのマネージャアクセスは、外部インターフェイスからリモートで Firewall Threat Defense を管理する場合、または別の管理ネットワークがない場合に便利です。さらに、データインターフェイスを使用する場合、プライマリインターフェイスがダウンした場合に管理機能を引き継ぐよう、冗長セカンダリインターフェイスを構成することになります。

マネージャのアクセス要件

データインターフェイスからのマネージャのアクセス要件は、次のとおりです。

- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスまたは EtherChannel を使用することはできません。マネージャアクセスインターフェイスでサブインターフェイスを作成することもできません。冗長性を目的として、Firewall Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Firewall Threat Defense と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Firewall Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。Amazon Web Services の Firewall Threat Defense Virtual の場合、コンソールポートは使用できないため、管理インターフェイスへの SSH アクセスを維持する必要があります。設定を続行する前に、管理用の静的ルートを追加します。または、マネージャアクセス用のデータインターフェイスを設定する前に、すべての CLI 構成（**configure manager add** コマンドを含む）を終了してから接続を切断します。

- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。
- ハイアベイラビリティはサポートされません。この場合、管理インターフェイスを使用する必要があります。

デバイスモデルごとの管理インターフェイスのサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストレーションガイドを参照してください。

（注） Firepower 4100/9300 の場合、MGMT インターフェイスは Firewall Threat Defense の論理デバイスを管理するためではなく、シャーシを管理するために使用します。mgmt タイプ（または firepower-eventing タイプあるいはその両方）の別個のインターフェイスを設定してから、そのインターフェイスを Firewall Threat Defense 論理デバイスに割り当てる必要があります。

（注） シャーシ上の Firewall Threat Defense の場合、物理管理インターフェイスは、診断論理インターフェイス（SNMP または syslog に利用できて、Firewall Management Center でデータインターフェイスと併せて設定されます）と、Firewall Management Center 通信用の管理論理インターフェイスの間で共有されます。詳細については、管理/診断インターフェイス （629ページ）を参照してください。

管理対象デバイスの各モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 *1*: 管理対象デバイスでサポートされる管理インターフェイス

モデル	管理インターフェイス	オプションのイベント インターフェイス
Firepower 1000	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 2100	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし

モデル	管理インターフェイス	オプションのイベント インターフェイス
Cisco Secure Firewall 3100	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 4100 および 9300	management0 （注） management0 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。	management1 （注） management1 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。
ISA 3000	br1 （注） br1 は、管理 1/1 インターフェイスの内部名です。	サポートなし
Secure Firewall Threat Defense Virtual	eth0	サポートなし

管理インターフェイス上のネットワークルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモート ネットワークに到達するためのスタティック ルートのみをサポートしています。管理対象デバイスをセットアップすると、セットアップ プロセスにより、指定したゲートウェイ IP アドレスへのデフォルトルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

（注） 管理インターフェイスのルーティングは、データインターフェイスに対して設定するルーティングとは完全に別のものです。専用の管理インターフェイスを使用する代わりに管理用のデータインターフェイスを設定すると、トラフィックはバックプレーンを介してルーティングされ、データルーティングテーブルが使用されます。ここで説明する内容は適用されません。

一部のプラットフォームでは、複数の管理インターフェイス（管理インターフェイスとイベント専用インターフェイス）を設定できます。デフォルトルートには出力インターフェイスが含まれていないため、選択されるインターフェイスは、指定したゲートウェイアドレスと、ゲートウェイが属するインターフェイスのネットワークによって異なります。デフォルト ネットワーク上に複数のインターフェイスがある場合、デバイスは出力インターフェイスとして番号の小さいインターフェイスを使用します。

リモートネットワークにアクセスするには、管理インターフェイスごとに1つ以上のスタティックルートを使用することをお勧めします。他のデバイスから Firewall Threat Defense へのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。

（注） 管理接続に使用されるインターフェイスは、ルーティングテーブルによって決定されません。常に最も番号の小さいインターフェイスを最初に使用して接続が試行されます。

NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベートネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Firewall Management Center 通信に支障はありませんが、ポート アドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PATルータの背後にあるデバイスへの接続は開始できません。

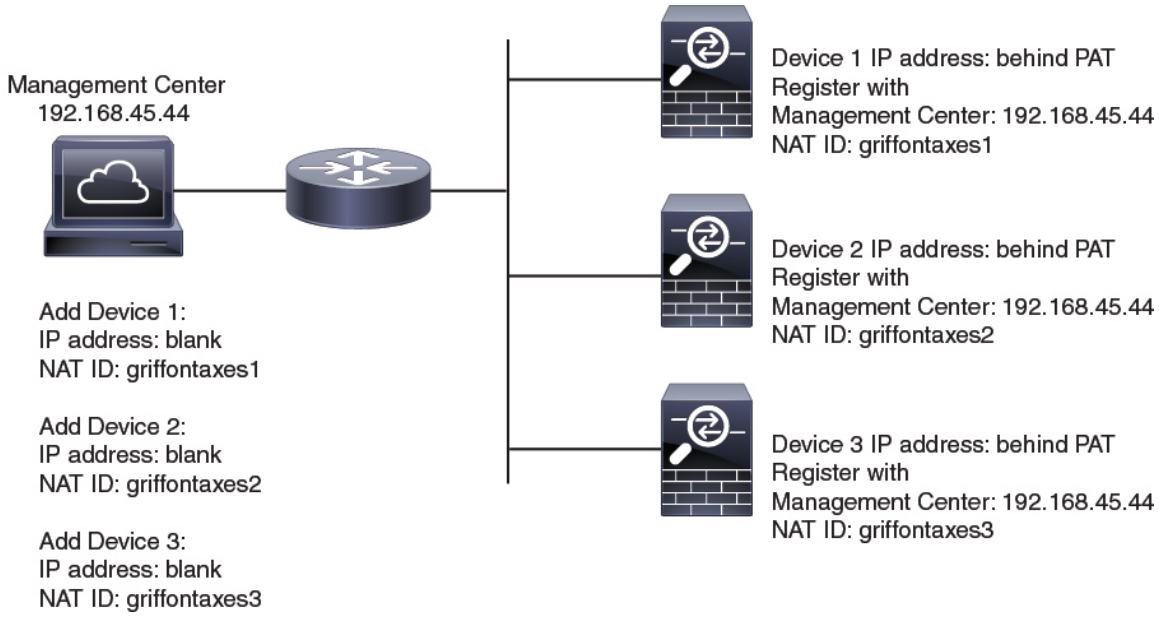
通常は、ルーティングと認証の両方の目的で両方のIPアドレス（登録キー付き）が必要です。デバイスを追加するときに、Firewall Management Center がデバイスの IP アドレスを指定し、デバイスが Firewall Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Firewall Management Centerおよびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

たとえば、デバイスを Firewall Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを Firewall Management Center に指定します。IP アドレスは空白のままにします。デバイス上で、Firewall Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが Firewall Management Center の IP アドレスに登録されます。この時点で、Firewall Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Firewall Management Center に追加することができます。Firewall Management Center で、追加するデバイスごとに IP アドレスは空白のままにして一意の NAT ID を指定し、次に各デバイスで、Firewall Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。

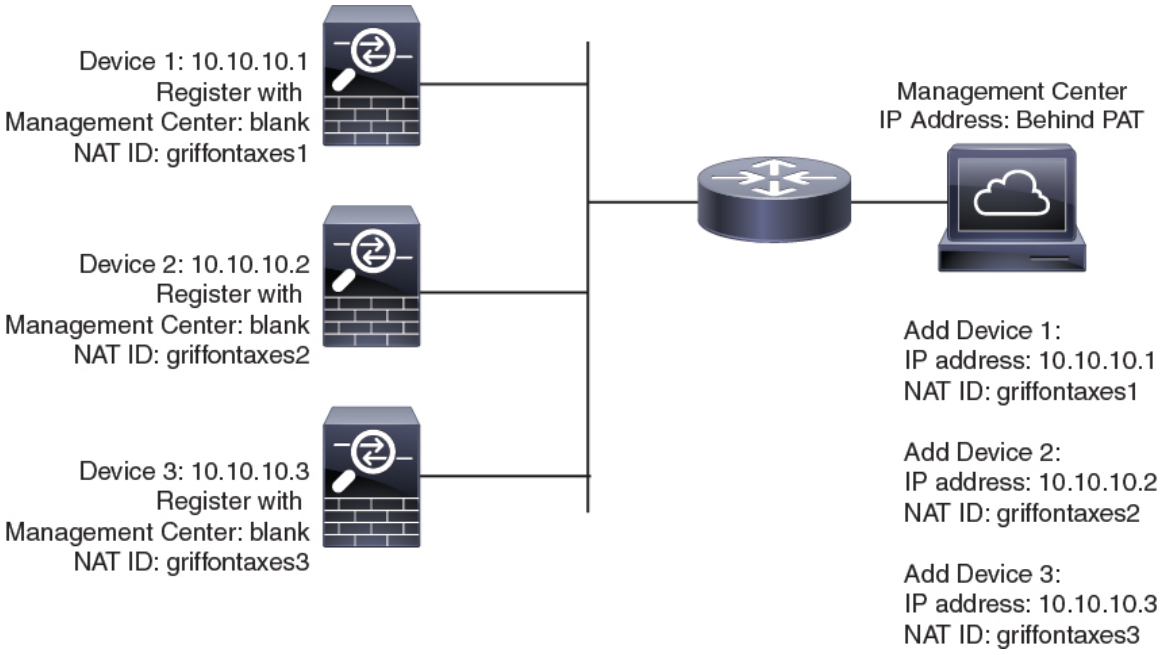
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、Firewall Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の Firewall Management Center の IP アドレスを指定します。

図 *1 : PAT* の背後にある管理対象デバイスの *NAT ID*



次の例に、PAT IP アドレスの背後にある Firewall Management Center を示します。この場合、Firewall Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、Firewall Management Center 上のデバイスの IP アドレスを指定します。

図 *2 : PAT* の背後にある *FMC* の *NAT ID*

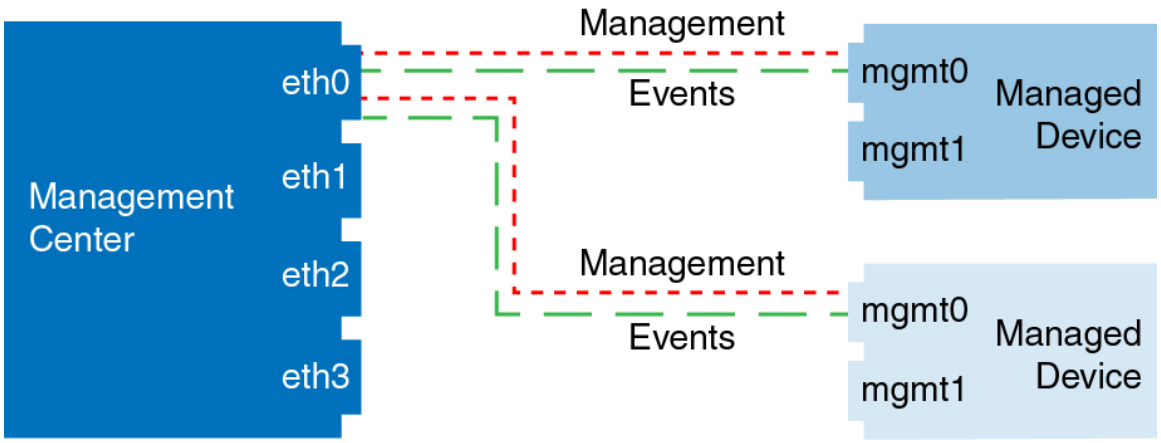


管理およびイベント トラフィック チャネルの例

（注） 管理用のデータインターフェイスを Firewall Threat Defense で使用する場合は、そのデバイスに個別の管理インターフェイスとイベントインターフェイスを使用することはできません。

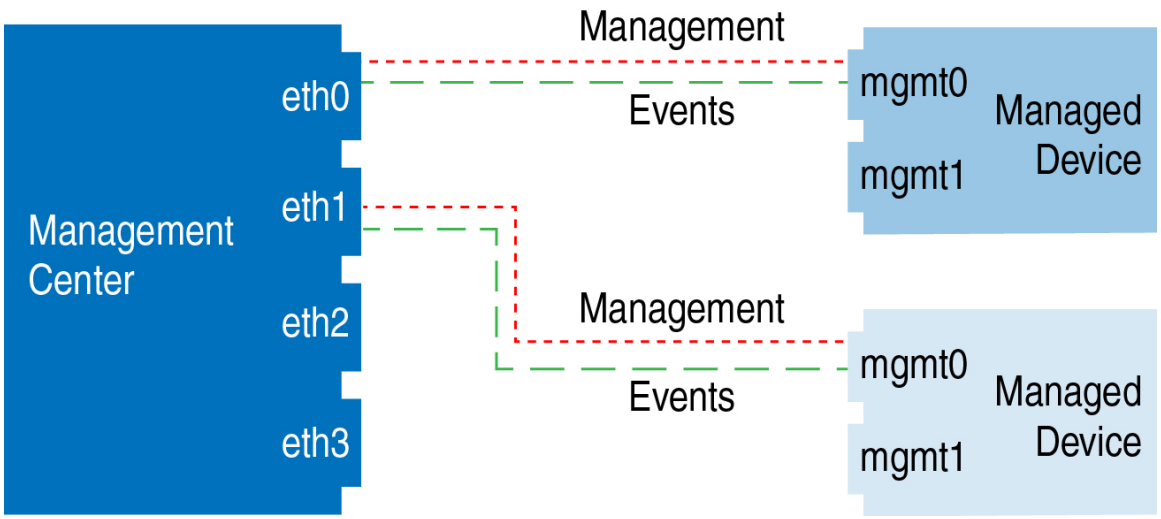
以下に、Firewall Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 *3 : Secure Firewall Management Center* 上で単一の管理インターフェイスを使用する場合



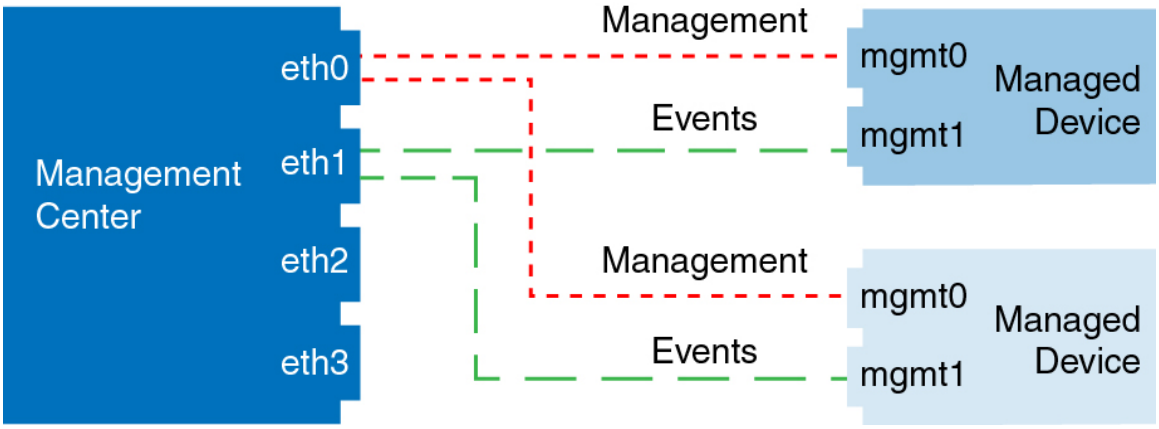
以下に、Firewall Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 *4 : Secure Firewall Management Center* の複数の管理インターフェイス



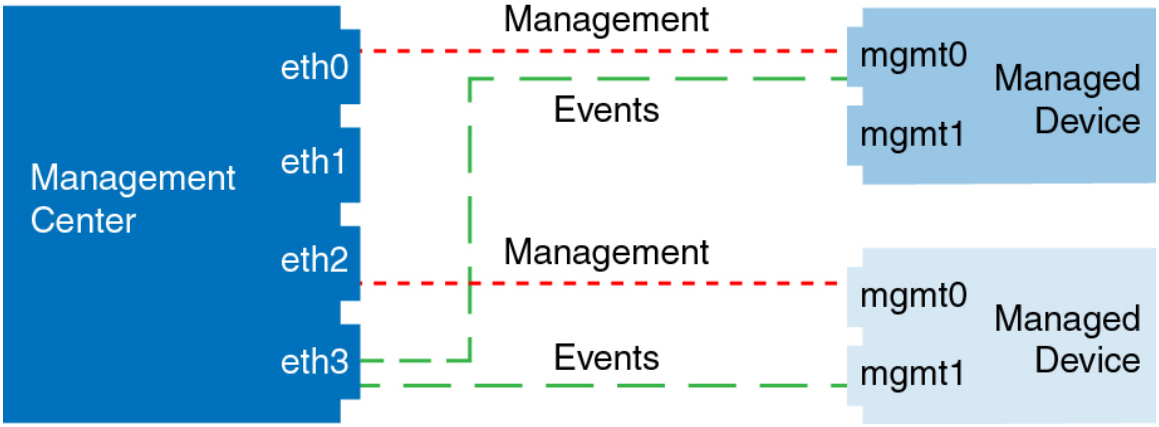
以下に、個別のイベント インターフェイスを使用する Firewall Management Center と管理対象デバイスの例を示します。

図 *5 : Secure Firewall Management Center*上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Firewall Management Center 上で複数の管理インターフェイスと個別のイベント インターフェイスが混在し、個別のイベントインターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 *6 :* 管理インターフェイスとイベント インターフェイスを混在させて使用する場合



デバイス管理の要件と前提条件

サポートされるドメイン

デバイスが存在するドメイン。

ユーザの役割

- 管理者
- ネットワーク管理者

管理接続

管理接続が安定しており、過度なパケット損失がなく、少なくとも 5 Mbps のスループットがあることを確認します。

ゼロ タッチ プロビジョニング の要件

クラスタリングまたはマルチインスタンスモードではゼロ タッチ プロビジョニング はサポートされません。

ゼロタッチプロビジョニング は DHCP を使用しますが、データインターフェイスと高可用性ではDHCPがサポートされていないため、高可用性は管理インターフェイスを使用する場合にのみサポートされます。

ゼロ タッチ プロビジョニング は、7.4 以降を使用する次のモデルでサポートされます。

- Firepower 1010
- Firepower 1100
- Firepower 2100（サポートされているバージョンに搭載）
- Cisco Secure Firewall 3100

デバイスのコマンド ライン インターフェイス（CLI）へのログイン

Firewall Threat Defense デバイスのコマンドライン インターフェイスに直接ログインできます。初めてログインする場合は、デフォルトの **admin** ユーザーを使用して初期設定プロセスを完了します。CLI を使用した Firewall Threat Defense 初期設定の実行の完了 （21 ページ）を参照してください。

（注） SSH を介した CLI へのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

- **configure user add** コマンドを使用して、CLI にログインできる追加のユーザー アカウントを作成します。
- コンソールポートに接続したときに、読み取れない文字が表示される場合は、ポートの設定を確認してください。設定が正しい場合は、同じ設定を使用して別のデバイスでそのケーブルを試します。ケーブルに問題がない場合は、コンソールポートのハードウェアを交換する必要がある可能性があります。別のワークステーションでの接続を試みることも検討してください。

手順

ステップ 1 コンソール ポートまたは SSH を使用して、Firewall Threat Defense CLI に接続します。

Firewall Threat Defense デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。特定のデータ インターフェイスへの SSH 接続を許可する方法については、Shellの確保 （843 ページ）を参照してください。

物理デバイスの場合、デバイスのコンソールポートに直接接続できます。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

コンソールポートの CLI は FXOS です（通常の Firewall Threat Defense CLI である ISA 3000 を除く）。基本設定、モニタリング、および通常のシステムのトラブルシューティングには Firewall Threat Defense CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

ステップ 2 **admin** のユーザー名とパスワードでログインします。

例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ 3 コンソールポートを使用した場合は、 Firewall Threat Defense CLI にアクセスします。

connect ftd

（注）
この手順は、ISA 3000 には適用されません。

例：

```
firepower# connect ftd
>
```

ステップ 4 CLI プロンプト（>）で、コマンドライン アクセス レベルで許可されている任意のコマンドを使用します。

コンソールポートの FXOS に戻るには、**exit**と入力します。

ステップ 5 （任意） SSH を使用した場合は、FXOS に接続できます。

connect fxos

Firewall Threat Defense CLI に戻るには、**exit** と入力します。

ステップ 6 （オプション）診断 CLI にアクセスします。

system support diagnostic-cli

この CLI を使用して、高度なトラブルシューティングを行います。この CLI には追加の **show** およびその他のコマンドがあります。

この CLI にはサブモードとして、ユーザー実行モード、特権 EXEC モードがあります。特権 EXEC モードでは、ユーザー実行モードよりも多くのコマンドを利用できます。特権 EXEC モードを開始するには、**enable** コマンドを入力し、プロンプトに対してパスワードを入力せずに Enter を押します。

例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

通常の CLI に戻るには、**Ctrl+a**、**d** を入力します。

Firewall Threat Defense 初期設定の完了

Firepower 4100/9300 を除くすべてのモデルについて、CLI または Firewall Device Managerを使用して Firewall Threat Defense の初期設定を実行できます。Firepower 4100/9300 の場合、論理デバイスを展開する際に初期設定を実行します。Firepower 4100/9300 の論理デバイス （213 ページ）を参照してください。

Firewall Device Manager を使用した Firewall Threat Defense の初期設定の完了

初期セットアップに Firewall Device Manager を使用すると、管理インターフェイスとマネージャアクセスの設定に加えて、次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- Ethernet 1/2（Firepower 1010 の場合は VLAN1 インターフェイス）：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得

他の設定（内部の DHCP サーバー、アクセス コントロール ポリシー、セキュリティゾーンなど）は設定されないことに注意してください。

Firewall Management Center に登録する前に Firewall Device Manager 内で追加のインターフェイス固有の設定を実行すると、その設定は保持されます。

CLI を使用すると、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。

- この手順は、オンプレミスの Firewall Management Center を分析のみに使用する CDO 管理対象デバイスには適用されません。Firewall Device Manager の構成は、プライマリマネージャを構成するためのものです。分析用にデバイスを構成する方法の詳細については、CLI を使用した Firewall Threat Defense 初期設定の実行の完了 （21 ページ） を参照してください。
- この手順は、Firepower 4100/9300 と ISA 3000 を除く他のすべてのデバイスに適用されます。Firewall Device Manager を使用してこれらのデバイスを Firewall Management Center にオンボーディングできますが、他のプラットフォームとはデフォルト設定が異なるため、この手順の詳細はこれらのプラットフォームには適用されない場合があります。

手順

ステップ 1 Firewall Device Manager にログインします。

a) ブラウザに次の URL を入力します。

- 内部：**https://192.168.95.1**。
- 管理：**https://***management_ip*。管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバーによって異なります。この手順の一環として、管理 IP アドレスを静的アドレスに設定する必要があるため、接続が切断されないように内部インターフェイスを使用することをお勧めします。

b) ユーザー名 **admin**、デフォルト パスワード **Admin123** を使用してログインします。

c) エンド ユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

ステップ 2 初期設定を完了するには、最初に Firewall Device Manager にログインしたときにセットアップウィザードを使用します。必要に応じて、ページの下部にある [デバイスの設定をスキップ（Skip device setup）] をクリックしてセットアップウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイスのデフォルト設定に加えて、Firewall Management Center の管理に切り替えるときに維持される外部（Ethernet1/1）インターフェイスも設定できます。

a) 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

1. [外部インターフェイスアドレス（Outside Interface Address）]— このインターフェイスは通常インターネット ゲートウェイであり、マネージャ アクセス インターフェイスとして使用される場合があります。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

   マネージャアクセスに外部（または内部）とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

   [IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、手動で静的 IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

   [IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、手動で静的 IP アドレス、プレフィックスマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

2. **[管理インターフェイス（Management Interface）]**

   CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。

   データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

   [DNS サーバ（DNS Servers）]：システムの管理アドレスの DNS サーバ。名前解決に使用する DNS サーバのアドレスを 1 つ以上入力します。デフォルトは、OpenDNS パブリック DNS サーバーです。フィールドを編集した後、デフォルトに戻す場合は、[OpenDNS を使用（Use OpenDNS）] をクリックすると該当する IP アドレスがフィールドにリロードされます。

   [ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

b) [時刻設定（NTP）（Time Setting (NTP)）] を設定し、[次へ（Next）] をクリックします。

   1. [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。
   2. [NTP タイム サーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、手動で NTP サーバのアドレスを入力するかを選択します。バックアップ用に複数のサーバを追加できます。

c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。

Firewall Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは Firewall Management Center で実行されます。

d) [終了（Finish）] をクリックします。

e) [クラウド管理（Cloud Management）]または[スタンドアロン（Standalone）] を選択するよう求められます。Firewall Management Center の管理については、[スタンドアロン（Standalone）] を選択してから、[Got It（了解）] を選択します。

ステップ 3 （必要に応じて）管理インターフェイスを設定します。

マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Firewall Device Manager 接続に管理インターフェイスを使用していた場合は、Firewall Device Manager に再接続する必要があります。

- マネージャアクセス用のデータインターフェイス：管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCPからゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。
- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

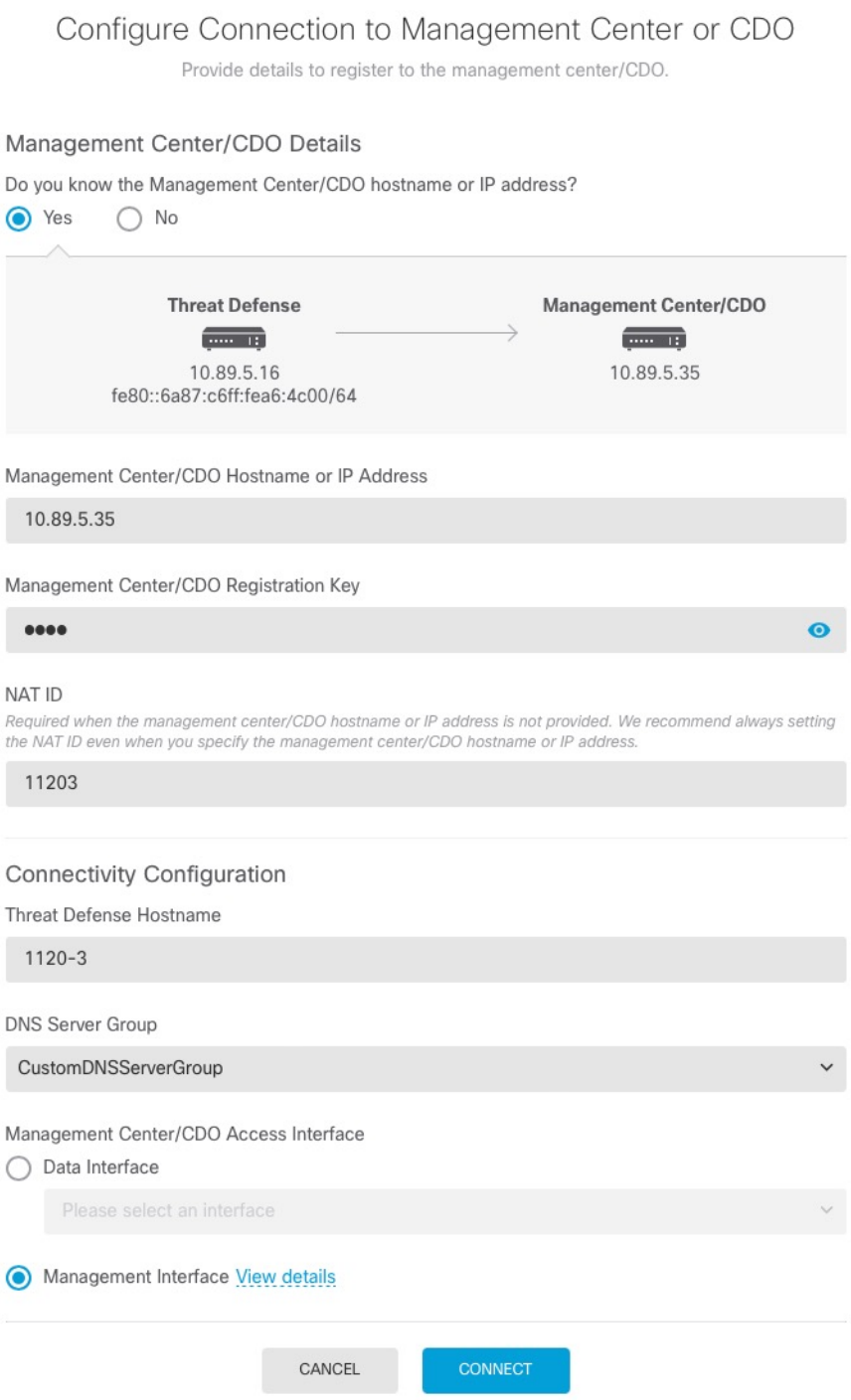
ステップ 4 マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーのリンクをクリックします。

Firewall Management Center にデバイスを登録すると、Firewall Device Manager の他の構成は保持されません。

ステップ 5 **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[集中管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Firewall Management Center の管理を設定します。

ステップ 6 [Management Center/SCCCDOの詳細（Management Center/**CDO** Details）] を設定します。

図 *7 : Management Center/CDO* の詳細



a) [Management Center/SCCCDOのホスト名またはIPアドレスを知っていますか（Do you know the Management Center/**CDO** hostname or IP address?）] で、IP アドレスまたはホスト名を使用して Firewall Management Center に到達できる場合は [はい（Yes）] をクリックし、Firewall

Management CenterCDO が NAT の背後にあるか、パブリック IP アドレスまたはホスト名がない場合は [いいえ（No）] をクリックします。

双方向の TLS-1.3 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Firewall Management Center または Firewall Threat Defense デバイス）に到達可能な IP アドレスが必要です。

b) [はい（Yes）] を選択した場合は、[Management Center/SCCCDOのホスト名/IPアドレス（Management Center/**CDO** Hostname or IP Address）] を入力します。

c) [Management Center/SCCCDO登録キー（Management Center/**CDO** Registration Key）] を指定します。

このキーは、Firewall Threat Defense デバイスを登録するときに Firewall Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する複数のデバイスに使用できます。

a) [NAT ID] を指定します。

この ID は、Firewall Management Center でも指定する任意の 1 回限りの文字列です。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する他のデバイスには使用できません。NAT IDは、接続元が正しいデバイスあることを確認するためにIPアドレスと組み合わせて使用されます。IPアドレス/NAT IDの認証後にのみ、登録キーが確認されます。任意である場合でも常にNAT IDを使用することを推奨しますが、次の場合は必須です。

- Firewall Management Center IP アドレスを **DONTRESOLVE** に設定する。
- Firewall Management Center でデバイスを追加するときに、到達可能なデバイスの IP アドレスまたはホスト名を指定していない。
- 両側でIPアドレスを指定する場合でも、管理にデータインターフェイスを使用する。
- Firewall Management Center が複数の管理インターフェイスを使用する。

ステップ 7 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のアクセスにデータインターフェイスを使用する場合、FQDN がこのインターフェイスに使用されます。

b) [DNSサーバグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは CiscoUmbrellaDNSServerGroup と呼ばれ、OpenDNS サーバが含まれます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバ

は、管理トラフィックに使用されます。データDNSサーバは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由でDNSサーバーに到達するため、管理に使用したものと同じ DNS サーバーグループを選択する可能性があります。

Firewall Management Center では、この Firewall Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイスDNSサーバーが設定されます。Firewall Management Center に Firewall Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS設定を含むFirewall Threat Defenseデバイスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Firewall Management Center とFirewall Threat Defenseデバイスを同期させるには、この設定に一致するようにDNSプラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカルDNSサーバーは、DNSサーバーが初期登録で検出された場合にのみFirewall Management Center で保持されます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）]**[FMCアクセスインターフェイス（FMC Access Interface）]** の管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを設定します。

c) [Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] については、任意の設定済みインターフェイスを選択します。

管理インターフェイスは、Firewall Threat Defense デバイスを Firewall Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

ステップ 8 （任意）外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Firewall Management Centerに接続する前にデフォルトルートを手動で設定する必要があります。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意のゲートウェイとして設定する必要があります。

ステップ 9 （任意） データインターフェイスを選択した場合は、[ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、 IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）でFirewall Threat Defenseデバイスに到達できるようにします。[デバイス（Device）] > [システム設定（System Settings）] > [DDNSサービス（DDNS Service）] を参照して DDNS を設定します。

Firewall Management Center に Firewall Threat Defense デバイスを追加する前に DDNS を設定すると、Firewall Threat Defense デバイスは、Cisco Trusted Root CA バンドルからすべての主要 CA

の証明書を自動的に追加し、Firewall Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。 Firewall Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

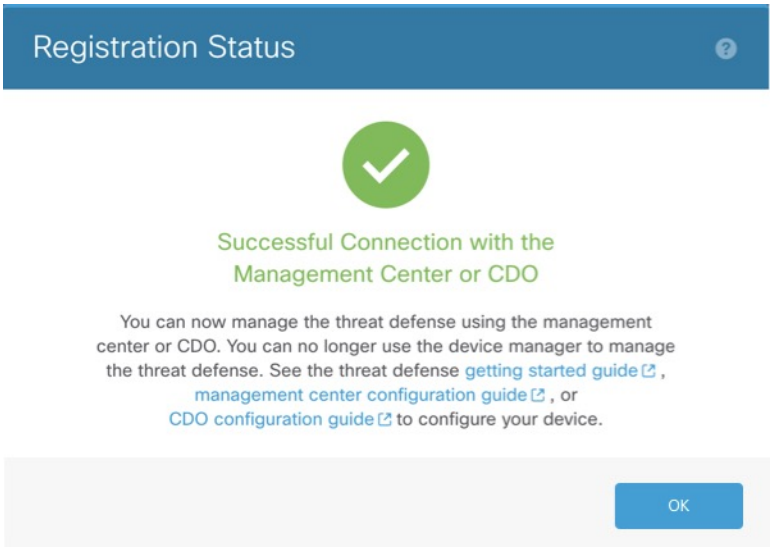
マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

ステップ 10 [接続（Connect）] をクリックします。**[登録ステータス（Registration Status）]** ダイアログボックスには、Firewall Management Center への切り替えに関する現在のステータスが表示されます。[Management Center/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップの後、Firewall Management Center に移動してファイアウォールを追加します。

Firewall Management Center への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。キャンセルしない場合は、[Management Center/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップが完了するまで Firewall Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Firewall Device Manager に再接続した場合のみ再開されます。

[Management Center/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップの後に Firewall Device Manager に接続したままにする場合、その後 [Management CenterまたはSCCCDOとの正常接続（Successful Connection with Management Center/**CDO**）] ダイアログボックスが表示され、Firewall Device Manager から切断されます。

図 *8* : 正常接続



CLI を使用した Firewall Threat Defense 初期設定の実行の完了

Firewall Threat Defense CLI に接続して初期設定を実行します。これには、セットアップウィザードを使用した管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の

指定などが含まれます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。マネージャアクセスに管理インターフェイスを使用しない場合は、代わりに CLI を使用してデータインターフェイスを設定できます。また、Firewall Management Center 通信の設定を行います。Firewall Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定に加えて、管理のために Firewall Management Center に切り替えたときに、Firewall Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーなどの他のデフォルト設定は保持されないことに注意してください。

この手順は、Firepower 4100/9300 を除くすべてのモデルに適用されます。Firepower 4100/9300 で論理デバイスを展開し、初期構成を完了するには、「Firepower 4100/9300 の論理デバイス, on page 213」を参照してください。

Procedure

ステップ 1 コンソールポートから、または管理インターフェイスへの SSH を使用して、Firewall Threat Defense CLI に接続します。デフォルトで DHCP サーバーから IP アドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

（Firepower および Cisco Secure Firewall ハードウェアモデル）コンソールポートは FXOS CLI に接続します。SSH セッションは Firewall Threat Defense CLI に直接接続します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

（Firepower および Cisco Secure Firewall ハードウェアモデル）コンソールポートで FXOS CLI に接続します。初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の Firewall Threat Defense ログインにも使用されます。

Note
パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。

Firepower および Cisco Secure Firewall ハードウェアの場合は、Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 と Threat Defense の Cisco FXOS トラブルシューティング ガイド [英語] の「Reimage Procedures」を参照してください。

ISA 3000 の場合は、『Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide』を参照してください。

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
```

```
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 3 （Firepower および Cisco Secure Firewall ハードウェアモデル）コンソールポートで FXOS に接続した場合は、Firewall Threat Defense CLI に接続します。

connect ftd

Example:

```
firepower# connect ftd
>
```

ステップ 4 Firewall Threat Defense に初めてログインすると、エンドユーザーライセンス契約書（EULA）に同意し、SSH 接続を使用している場合は、管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

Note
設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップウィザードを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。threat defense のコマンドリファレンスを参照してください。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

Note
データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

次のガイドラインを参照してください。

- [IPv4を設定しますか?（Do you want to configure IPv4?）]、[IPv6を設定しますか?（Do you want to configure IPv6?）]：これらのタイプのアドレスの少なくとも 1 つに **y** を入力します。
- [管理インターフェイスのIPv4デフォルトゲートウェイを入力（Enter the IPv4 default gateway for the management interface）]、[管理インターフェイスのIPv6ゲートウェイを入力（Enter the IPv6 gateway for the management interface）]：管理インターフェイスではなくデータインターフェイスをマネージャアクセスに使用する場合は、[手動（manual）] を選択します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。ルーティングの問題を防ぐために、このインターフェイスがマネージャ アクセス インターフェイスとは異なるサブネット上にあることを確認してください。管理インターフェイスが DHCP に設定されている場合、管理用のデータインターフェイスを設定することはできません。これは、**data-interfaces** である必要が

あるデフォルトルートがDHCPサーバーから受信したルートで上書きされる可能性があるためです。

- [管理インターフェイスのIPv4デフォルトゲートウェイを入力（Enter the IPv4 default gateway for the management interface）]、[DHCP、ルータ経由、または手動でIPv6を設定しますか?（Configure IPv6 via DHCP, router, or manually?）]：管理インターフェイスではなくデータインターフェイスをマネージャアクセスに使用する場合は、ゲートウェイを[data-interfaces]に設定します。この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。マネージャアクセスに管理インターフェイスを使用する場合は、管理 1/1 ネットワークでゲートウェイ IP アドレスを設定する必要があります。
- **ネットワーク情報が変更された場合は再接続が必要**：SSHで接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか（Manage the device locally?）]：Firewall Management Center を使用するには「**no**」を入力します。**yes** と入力すると、代わりに Secure Firewall Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか（Configure firewall mode?）]：初期設定でファイアウォールモードを設定することをお勧めします。初期設定後にファイアウォールモードを変更すると、実行コンフィギュレーションが消去されます。データ インターフェイス マネージャ アクセスは、ルーテッド ファイアウォール モードでのみサポートされることに注意してください。

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:


System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.89.5.1
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 10.89.5.1 on management0
```

```
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

ステップ 5 この Firewall Threat Defense を管理する Firewall Management Center を特定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*] [*display_name*]

Note
管理に CDO を使用している場合は、このステップで CDO が生成した **configure manager add** コマンドを使用します。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Firewall Management Center.Firewall Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。また、*nat_id* も指定します。双方向の TLS-1.3 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Firewall Management Center または Firewall Threat Defense）に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、到達可能な IP アドレスまたはホスト名が Firewall Threat Defense に必要です。
- reg_key：Firewall Threat Defense を登録するときに Firewall Management Center でも指定する任意のワンタイム登録キーを指定します。登録キーは 2 ～ 36 文字である必要がありま

す。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。

- nat_id：Firewall Threat Defense を登録するときに Firewall Management Center でも指定する、任意で一意の 1 回限りの文字列を指定します。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。 IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。任意である場合でも常にNAT IDを使用することを推奨しますが、次の場合は必須です。
  - Firewall Management Center IP アドレスを **DONTRESOLVE** に設定する。
  - Firewall Management Center でデバイスを追加するときに、到達可能なデバイスの IP アドレスまたはホスト名を指定していない。
  - 両側でIPアドレスを指定する場合でも、管理にデータインターフェイスを使用する。
  - Firewall Management Center が複数の管理インターフェイスを使用する。
- *display_name*：**show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Firewall Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。
  - *hostname* | *IP_address*（**DONTRESOLVE** キーワードを使用しない場合）
  - **manager-***timestamp*

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Example:

Firewall Management Center が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに登録キーを入力し、ホスト名の代わりに DONTRESOLVE を指定します。

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Example:

Firewall Threat Defense が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに Firewall Management Center IP アドレスまたはホスト名を入力します。

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

ステップ 6 プライマリマネージャとして CDO を使用していて、オンプレミス Firewall Management Center を分析のみに使用する場合は、オンプレミス Firewall Management Center を特定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*] [*display_name*]

Example:

次の例では、CDO で生成した表示名で CDO 用に生成したコマンドを使用して、分析専用のオンプレミス Firewall Management Center を表示名「analytics-FMC」を使用して指定しています。

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

ステップ 7 (Optional) マネージャアクセス用のデータインターフェイスを設定します。

configure network management-data-interface

その後、データインターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

Note
このコマンドを使用する場合は、コンソールポートを使用する必要があります。管理インターフェイスに SSH を使用すると、接続が切断され、コンソールポートに再接続する必要が生じる場合があります。SSH の詳細な使用方法については、次を参照してください。

このコマンドの使用については、次の詳細を参照してください。管理のための Firewall Threat Defense データインターフェイスの使用について, on page 5も参照してください。

- データインターフェイスを管理に使用する場合、元の管理インターフェイスは DHCP を使用できません。初期セットアップ時に IP アドレスを手動で設定しなかった場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用して設定できるようになりました。ルーティングの問題を防ぐために、このインターフェイスがマネージャ アクセス インターフェイスとは異なるサブネット上にあることを確認してください。管理インターフェイス ゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- Firewall Threat Defense を Firewall Management Center に追加すると、Firewall Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Firewall Management Center では、後でマネージャ アクセス インターフェイス構成を変更できますが、Firewall Threat Defense または Firewall Management Center が管理接続の再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、Firewall Threat Defense には以前の展開を復元する **configure policy rollback** コマンドが含まれます。
- DDNS は、IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）で Firewall Threat Defense に到達できるようにします。DDNS サーバー更新の URL を設定すると、Firewall Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Firewall Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Firewall Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

  Firewall Management Center では、この Firewall Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Firewall Management Center に Firewall Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Firewall Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Firewall Management Center と Firewall Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

  また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Firewall Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、FTD 設定と一致するように、DNS サーバーを含むこれらの設定すべてを Firewall Management Center で手動で設定する必要があります。

- 管理インターフェイスは、Firewall Threat Defense を Firewall Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network,
if you wish to change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network,
if you wish to change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 8 (Optional) 特定のネットワーク上のマネージャへのデータ インターフェイス アクセスを制限します。

configure network management-data-interface client *ip_address netmask*

デフォルトでは、すべてのネットワークが許可されます。

What to do next

デバイスを Firewall Management Center に登録します。

イベントインターフェイスの設定

管理トラフィック用の管理インターフェイスが常に必要です。デバイスに 2 番目の管理インターフェイス（Firepower 4100/9300 など）がある場合は、イベント専用トラフィックに対してそのインターフェイスを有効にすることができます。

始める前に

別のイベントインターフェイスを使用するには、Firewall Management Center でイベントインターフェイスを有効にする必要もあります。Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

手順

ステップ 1 2 番目の管理インターフェイスをイベント専用インターフェイスとして有効にします。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

必要に応じて、**configure network management-interface disable-events-channel** コマンドを使用してメイン管理インターフェイスのイベントを無効にできます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

インターフェイス上でイベントチャネルと管理チャンネルの両方を無効にすることはできません。

例：

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

ステップ 2 イベントインターフェイスの IP アドレスを設定します。

イベントインターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。

a) IPv4 アドレスを設定します。

configure network ipv4 manual *ip_address netmask gateway_ip* **management1**

このコマンド内の *gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。つまり、management0 インターフェイスにすでに設定した値を入力する必要があります。イベントインターフェイス用の個別のスタティックルートは作成されません。管理インターフェイスとは異なるネットワークでイベント専用インターフェイスを使用している場合は、イベント専用インターフェイス用に別のスタティックルートを作成することを推奨します。

例：

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

b) IPv6 アドレスを設定します。

- ステートレス自動設定

  configure network ipv6 router management1

  例：

  ```
  > configure network ipv6 router management1
  Setting IPv6 network configuration.
  Network settings changed.
  ```

```
>
```

- 手動設定

  configure network ipv6 manual *ip6_address ip6_prefix_length* **management1**

  例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

ステップ 3 Firewall Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。

configure network static-routes {**ipv4** | **ipv6**}**add management1** *destination_ip netmask_or_prefix gateway_ip*

デフォルトルートの場合は、このコマンドを使用しないでください。デフォルト ルート ゲートウェイの IP アドレスの変更は、**configure network ipv4** コマンドまたは **ipv6** コマンドを使用した場合のみ可能です（「ステップ 2 （30 ページ）」を参照）。

例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

スタティック ルートを表示するには、**show network-static-routes** を入力します（デフォルトルートは表示されません）。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
[…]
```

デバイスの管理

[デバイス（Device）]>**[デバイス管理（Device Management）]**ページには、さまざまな情報とオプションがあります。

- **[表示単位（View By）]**：グループ、ライセンス、モデル、バージョン、またはアクセスコントロール ポリシーに基づいてデバイスが表示されます。
- **[デバイス状態（Device State）]**：デバイスを状態（**エラー**、**警告**など）に基づいて表示します。状態アイコンをクリックして、その状態に属するデバイスを表示できます。状態に属するデバイスの数は、括弧内に示されます。
- **[デバイスの検索（Search Device）]**：デバイス名、ホスト名またはIPアドレスを使用して、デバイスを検索します。
- **[追加（Add）]**：デバイスおよびその他の管理可能なコンポーネントを追加します。
- 列の見出しをクリックすると列ごとにソートできます。
  - **[名前（Name）]**
  - **モデル**
  - **バージョン**
  - **[シャーシ（Chassis）]**：サポートされているモデルの場合、**[管理（Manage）]**をクリックすると統合シャーシ マネージャが表示されます。Firepower 4100/9300の場合、リンクは Firewall Chassis Manager を相互起動します。
  - **ライセンス**
  - **[アクセス コントロール ポリシー（Access Control Policy）]**：デバイスに展開されているポリシーを表示するには、[アクセス コントロール ポリシー（Access Control Policy）] 列のリンクをクリックします。
  - **[自動ロールバック（Auto-Rollback）]**：展開によって管理接続がダウンした場合に、構成の自動ロールバックが有効（）か無効（）かを示します。「展開設定の編集（118 ページ）」を参照してください。
- **[編集（Edit）]**：デバイスごとに、[編集（Edit）]（）アイコンを使用してデバイス設定を編集します。

  単にデバイス名または IP アドレスをクリックすることもできます。
- **[詳細（More）]**：デバイスごとに、[その他（More）]（）アイコン をクリックして、他のアクションを実行します。
  - [登録解除（Unregister）] [削除（Unregister）]：デバイスの登録を解除します。

- **[パケット トレーサ（Packet Tracer）]**：モデルパケットをシステムに挿入することにより、デバイスのポリシー設定を調べるためのパケットトレーサページに移動します。
- **[パケット キャプチャ（Packet Capture）]**：パケット キャプチャ ページに移動します。このページでは、パケットの処理中にシステムが実行する判定とアクションを表示できます。
- **[アップグレードを元に戻す（Revert Upgrade）]**：最後のアップグレード後に行われたアップグレードと構成の変更を元に戻します。この操作により、デバイスがアップグレード前のバージョンに復元されます。
- **[ヘルスモニター（Health Monitor）]**：デバイスのヘルス モニタリング ページに移動します。
- **[トラブルシューティング ファイル（Troubleshooting Files）]**：レポートに含めるデータのタイプを選択できるトラブルシューティング ファイルを生成します。

デバイス グループの追加

Firewall Management Center でデバイスをグループ化すると、複数のデバイスへのポリシーの展開やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。

高可用性ペア内のプライマリデバイスをグループに追加すると、両方のデバイスがグループに追加されます。高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[グループの追加（Add Group）] を選択します。

既存のグループを編集するには、編集するグループの[編集（Edit）]（✎）をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。

ステップ 5 [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

ステップ 6 必要に応じて、デバイスグループからデバイスを削除するには、削除するデバイスの横にある[削除（Delete）]（🗑）をクリックします。

ステップ 7 [OK] をクリックして、デバイス グループを追加します。

Management Center への登録

Firewall Management Center では、デバイスを登録するための複数の方法が提供されています。

デバイスの追加

Firewall Management Center に 1 つのデバイスを追加するには、次の手順を実行します。ハイアベイラビリティのためにデバイスをリンクする場合でも、この手順を使用する必要があります。ハイ アベイラビリティ ペアの追加 （305 ページ） を参照してください。クラスタリングについては、お使いのモデルのクラスタリングに関する章を参照してください。

この手順を使用して、クラウド提供型 Firewall Management Center によって管理されるデバイスを追加することもできます。オンプレミスの Firewall Management Center はイベントのロギングと分析の目的のみに使用します。

Firewall Management Center ハイアベイラビリティを使用する場合は、アクティブ Firewall Management Center にのみデバイスを追加します。アクティブな Firewall Management Center に登録されているデバイスはスタンバイに自動的に登録されます。

始める前に

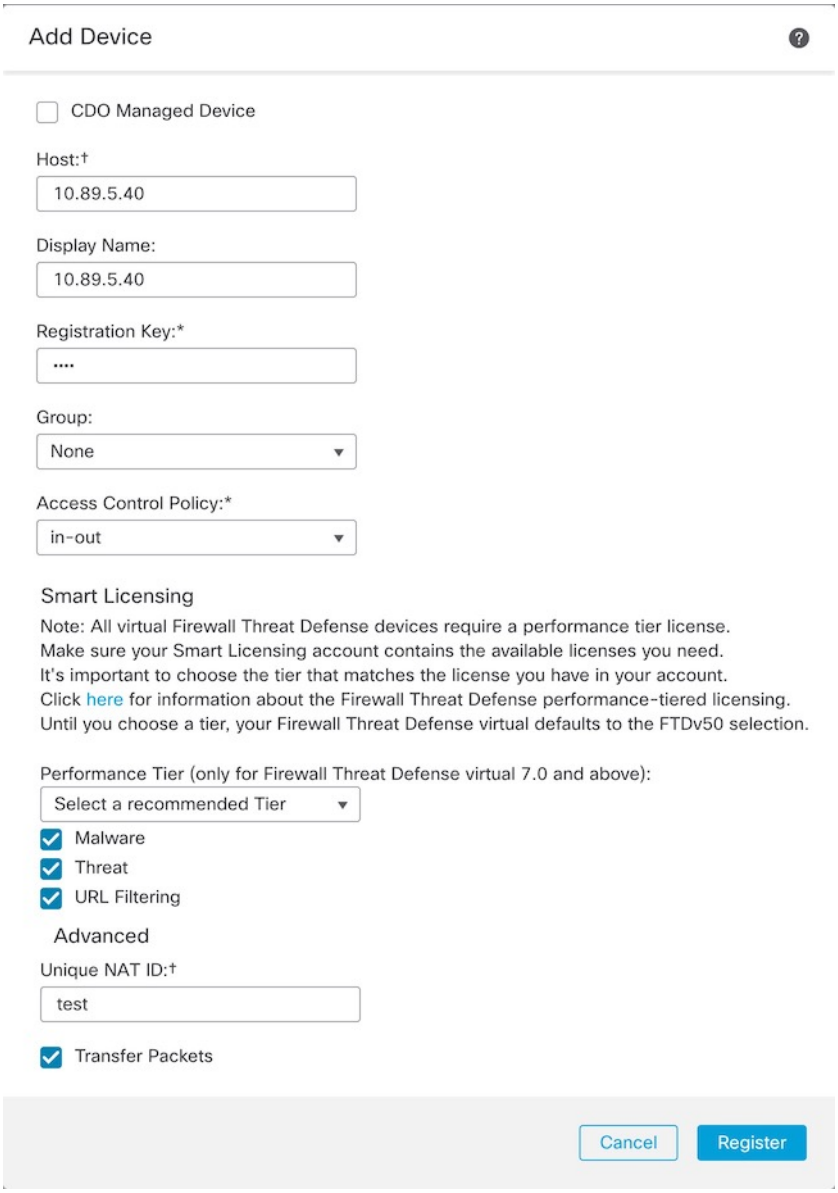
- デバイスを Firewall Management Center の管理対象として設定します。参照：
  - Firewall Threat Defense 初期設定の完了 （14 ページ）
  - 使用モデルのスタートアップガイド
- Firewall Management Center が Smart Software Manager に登録されている必要があります。有効な評価ライセンスで十分ですが、有効期限が切れると、正常に登録するまで新しいデバイスを追加できなくなります。
- IPv4 を使用して登録したデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 [追加（Add）] ドロップダウンメニューから、[デバイス（Device）] を選択します。

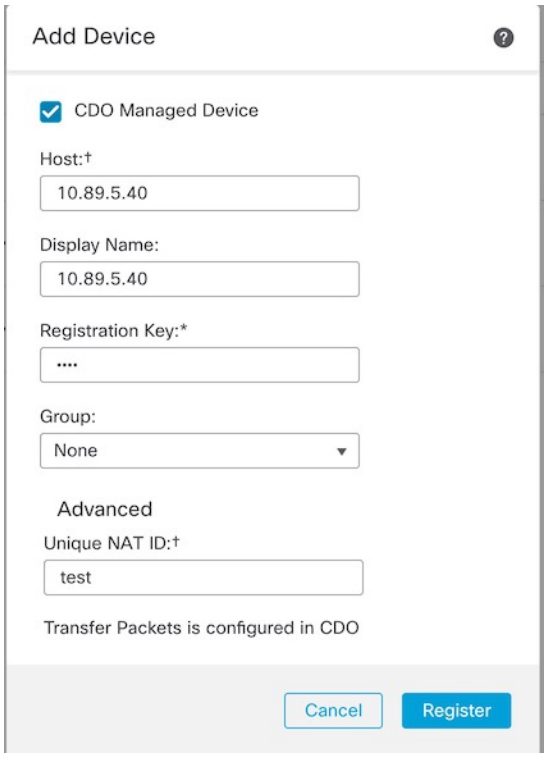
図 *9*：デバイスの追加



ステップ 3 分析専用にクラウド管理対象デバイスをオンプレミスの Firewall Management Center に追加する場合は、**[CDO管理対象デバイス（CDO Managed Device）]** をオンにします。

ライセンスとパケット転送の設定は CDO（旧 CDO）によって管理されるため、システムでは表示されません。これらのステップはスキップできます。

図 *10 : CDO* 用のデバイスの追加



ステップ 4 [ホスト（Host）] には、追加デバイスの IP アドレスまたはホスト名を入力します。デバイスの IP アドレスが不明な場合（NAT の背後にある場合など）は、このフィールドを空白のままにします。

このフィールドを空白のままにする場合は、デバイスの初期設定で、到達可能な Firewall Management Center の IPアドレスまたはホスト名と NAT ID が指定されている必要があります。詳細については、NAT 環境 （8 ページ）を参照してください。

ステップ 5 [表示名（Display name）] フィールドに、Firewall Management Center でのデバイスの表示名を入力します。この名前は変更できません。

ステップ 6 [登録キー（Registration key）] には、初期設定で指定したものと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。キーは英数字（A～Z、a～z、0～9）、およびハイフン（-）を使用して、37 文字以内で指定します。登録キーはデバイスごとに一意である必要はありません。

ステップ 7 （任意） デバイスをデバイス**グループ**に追加します。

ステップ 8 登録後すぐに、デバイスに展開する最初の [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。

デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。この障害の原因を解決した後、デバイスに手作業で設定を行います。

ステップ 9 デバイスに適用するライセンスを選択します。

デバイスを追加した後、**[システム（System）]** > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** ページからライセンスを適用することもできます。

Firewall Threat Defense Virtual の場合は、[パフォーマンス階層（Performance Tier）] も選択する必要があります。使用アカウントにあるライセンスと一致する階層を選択することが重要です。階層を選択するまで、デバイスではデフォルトでFTDv50が選択されます。Firewall Threat Defense Virtualで使用可能なパフォーマンス階層ソフトウェア利用資格の詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*FTDv Licenses*」を参照してください。

（注）
Firewall Threat Defense Virtual をバージョン 7.0 以上にアップグレードする場合は、[FTDv -変数（FTDv - Variable）] を選択して現在のライセンスコンプライアンスを維持できます。

ステップ 10 初期設定時に NAT ID を指定した場合は、[詳細（Advanced）] セクションの [一意のNAT ID（Unique NAT ID）] に同じ NAT ID を入力します。

[一意のNAT ID（Unique NAT ID）] には、任意の一意のワンタイム文字列を指定します。この文字列は、初期設定時にデバイスでも指定します。このワンタイム文字列は、一方の側で到達可能な IPアドレスやホスト名が指定されていない場合に必要になります。たとえば、[ホスト（Host ）] フィールドを空白のままにした場合などです、技術的にはオプションですが、特定の状況で必要になるため、両側の IP アドレスがわかっている場合でも、常に NAT ID を指定することを推奨します。ID は英数字（A～Z、a～z、0～9）、およびハイフン（-）を使用して、37 文字以内で指定します。この ID は、Firewall Management Center に登録する他のデバイスには使用できません。

ステップ 11 [パケットの転送（Transfer Packets）] チェックボックスをオンにして、侵入イベントが発生するたびに、デバイスが検査のためにパケットを Firewall Management Center に転送するようにします。

このオプションは、デフォルトで有効です。侵入イベントごとに、デバイスは、イベント情報とイベントをトリガーしたパケットを検査のために Firewall Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Firewall Management Center に送信され、パケットは送信されません。

ステップ 12 [登録（Register）] をクリックします。

Firewall Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。デバイスの登録に失敗した場合は、次の項目を確認してください。

- ping：デバイスの CLI にアクセスし、次のコマンドを使用して Firewall Management Center の IP アドレスへの ping を実行します。

  ping system *ip_address*

ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。デバイスの IP アドレスを変更する必要がある場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用します。

- 登録キー、NAT ID、および Firewall Management Center IP アドレス：両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、デバイスで登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、https://cisco.com/go/fmc-reg-error を参照してください。

新しい Management Center への登録

この手順では、新しい Firewall Management Center に登録する方法を示します。新しい Firewall Management Center が古い Firewall Management Center の IP アドレスを使用している場合でも、次の手順を実行する必要があります。

手順

ステップ 1 古い Firewall Management Center に管理対象デバイスが存在する場合はこれを削除します。Firewall Management Center からのデバイスの削除（登録解除） （39 ページ）を参照してください。

Firewall Management Center とのアクティブな接続がある場合は、Firewall Management Center IP アドレスを変更できません。

ステップ 2 SSH などを使用して、デバイスの CLI に接続します。

ステップ 3 新しい Firewall Management Center を設定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*] [*display_name*]

- {*hostname* | *IPv4_address* | *IPv6_address*}：Firewall Management Center のホスト名、IPv4 アドレス、または IPv6 アドレスを設定します。
- **DONTRESOLVE**：Firewall Management Center を直接アドレス指定できない場合は、ホスト名または IP アドレスの代わりに **DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、*nat_id* が必要です。このデバイスを Firewall Management Center に追加する場合は、デバイスの IP アドレスと *nat_id* の両方を必ず指定してください。接続の片側で IP アドレスを指定し、両側で同じ一意の NAT ID を指定する必要があります。
- *regkey*：登録時に Firewall Management Center とデバイス間で共有する登録キーを作成します。このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。Firewall Threat Defense を追加するときに、Firewall Management Center に同じキーを入力します。

- *nat_id*：一方が IP アドレスを指定しない場合に、Firewall Management Center とデバイス間の登録プロセス中のみに使用する 1 ～ 37 文字の英数字文字列を作成します。この NAT ID は、登録時にのみ使用されるワンタイムパスワードです。NAT ID が一意であり、登録を待機している他のデバイスによって使用されていないことを確認します。Firewall Threat Defense を追加するときに、Firewall Management Center で同じ NAT ID を指定します。
- *display_name*：**show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Firewall Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。
  - *hostname* | *IP_address*（**DONTRESOLVE** キーワードを使用しない場合）
  - **manager-***timestamp*

例：

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

ステップ 4 デバイスを Firewall Management Center に追加します。

Firewall Management Center からのデバイスの削除（登録解除）

デバイスを管理する必要がなくなった場合、Firewall Management Center からデバイスの登録を解除できます。

クラスタ、クラスタノード、または高可用性ペアの登録を解除するには、それらの展開の章を参照してください。

デバイスの登録解除：

- Firewall Management Center とそのデバイスとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからデバイスが削除されます。
- デバイスのプラットフォーム設定ポリシーで、NTP を使用して Firewall Management Center から時間を受信するように設定されている場合は、デバイスがローカル時間管理に戻されます。
- 設定はそのままになるため、デバイスはトラフィックの処理を続行します。

  NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Firewall Management Center にデバイスを再登録すると、設定が削除されるため、デバイスはその時点でトラフィックの処理を停止します。

デバイスを削除する前に、再登録時にデバイスレベルの設定（インターフェイス、ルーティングなど）を再適用できるように、設定のエクスポート、を行ってください。保存された設定がない場合は、デバイス設定を再構成する必要があります。

デバイスを再度追加し、保存した設定をインポートするか、または設定を再構成した後、トラフィックの受け渡しを再開する前に、設定を展開する必要があります。

始める前に

Firewall Management Center に再度追加した場合に、デバイスレベルの設定を再適用するには

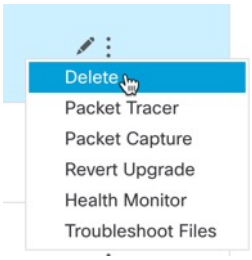
- デバイス設定をエクスポートします。 デバイス設定のエクスポートとインポート （59 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 登録を解除するデバイスの横にある[その他（More）] (⋮) をクリックし、**[削除（Delete）]**をクリックします。

図 *11* : 消去



ステップ 3 デバイスの登録を解除することを確認します。

ステップ 4 マネージャを変更できるようになりました。

- この Firewall Management Center にデバイスを再登録する：登録キーと NAT ID が分かっている場合は、デバイスの追加 （34 ページ） を実行できます。それらをリセットする必要がある場合は、マネージャを新しいものであるかのように再設定できます。新しい Management Center への登録 （38 ページ） を参照してください。
- 新しい Firewall Management Center に登録する：新しい Management Center への登録 （38 ページ）。
- Firewall Device Manager に変更を加える：Firewall Management Center から Firewall Device Manager への切り替え （48 ページ）。

- 新しいマネージャを指定せずにマネージャを削除する：新しいマネージャを識別せずに（マネージャなしのモード）、Firewall Threat Defense で管理接続を切断するには、Firewall Threat Defense の CLI から **configure manager delete** コマンドを使用します。

デバイスのシャットダウンまたは再起動

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されていて、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールをグレースフルシャットダウンできないことを覚えておいてください。

システムを適切にシャットダウンまたは再起動するには、以下のタスクを参照してください。

（注） デバイスを再起動すると、管理接続を再確立できなかったというエラーが表示される場合があります。場合により、デバイスの管理インターフェイスの準備が整う前に接続が試行されます。接続は自動的に再試行され、15 分以内に確立されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 再起動するデバイスの横にある [編集（Edit）]（ ） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 デバイスを再起動するには、次の手順を実行します。

a) [デバイスの再起動（Restart Device）]（ ） をクリックします。
b) プロンプトが表示されたら、デバイスを再起動することを確認します。

ステップ 5 デバイスをシャットダウンするには、次の手順を実行します。

a) [システム（System）] セクションで [デバイスのシャットダウン（Shut Down Device）]（ ） をクリックします。
b) プロンプトが表示されたら、デバイスのシャットダウンを確認します。
c) コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

コンソールから接続していない場合は、約 3 分間待ってシステムがシャットダウンしたことを確認します。

ISA 3000 の場合、シャットダウンが完了すると、システム LED が消灯します。電源を切る前に、少なくとも 10 秒待ってください。

マネージャの切り替え

必要に応じてマネージャを切り替えることができます。

Firewall Device Manager から Firewall Management Center への切り替え

Firewall Device Manager から Firewall Management Center へ切り替えると、管理インターフェイスとマネージャアクセス設定に加えて、すべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他の設定は保持されないことに注意してください。

Firewall Management Center に切り替えると、Firewall Device Manager を使用して Firewall Threat Defense デバイスを管理できなくなります。

始める前に

ファイアウォールが高可用性用に設定されている場合は、まず、Firewall Device Manager（可能な場合）または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから高可用性を中断することをお勧めします

手順

ステップ 1 Firewall Device Manager で、Cisco Smart Software Manager からデバイスを登録解除します。

ステップ 2 （必要に応じて）管理インターフェイスを設定します。

マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Firewall Device Manager 接続に管理インターフェイスを使用していた場合は、Firewall Device Manager に再接続する必要があります。

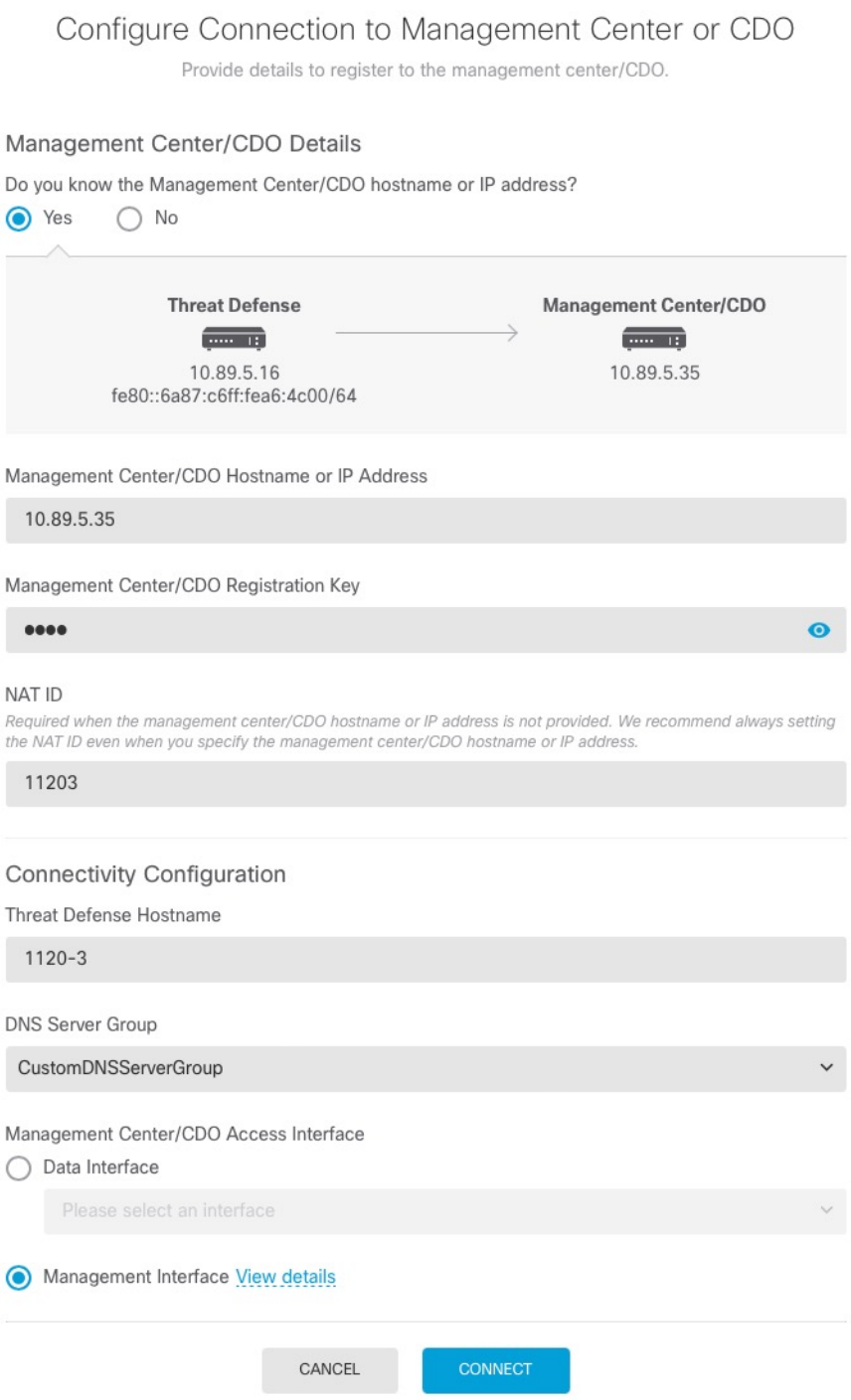
- マネージャアクセス用のデータインターフェイス：管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。
- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定して

ください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

ステップ 3 **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[集中管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Firewall Management Center の管理を設定します。

ステップ 4 [Management Center/SCCCDOの詳細（Management Center/**CDO** Details）] を設定します。

図 *12 : Management Center/CDO* の詳細



a) [Management Center/SCCCDOのホスト名またはIPアドレスを知っていますか（Do you know the Management Center/**CDO** hostname or IP address?）] で、IP アドレスまたはホスト名を使用して Firewall Management Center に到達できる場合は [はい（Yes）] をクリックし、Firewall

Management CenterCDO が NAT の背後にあるか、パブリック IP アドレスまたはホスト名がない場合は [いいえ（No）] をクリックします。

双方向の TLS-1.3 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Firewall Management Center または Firewall Threat Defense デバイス）に到達可能な IP アドレスが必要です。

b) [はい（Yes）] を選択した場合は、[Management Center/SCCCDOのホスト名/IPアドレス（Management Center/**CDO** Hostname or IP Address）] を入力します。

c) [Management Center/SCCCDO登録キー（Management Center/**CDO** Registration Key）] を指定します。

このキーは、Firewall Threat Defense デバイスを登録するときに Firewall Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する複数のデバイスに使用できます。

a) [NAT ID] を指定します。

この ID は、Firewall Management Center でも指定する任意の 1 回限りの文字列です。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する他のデバイスには使用できません。NAT IDは、接続元が正しいデバイスあることを確認するためにIPアドレスと組み合わせて使用されます。IPアドレス/NAT IDの認証後にのみ、登録キーが確認されます。任意である場合でも常にNAT IDを使用することを推奨しますが、次の場合は必須です。

- Firewall Management Center IP アドレスを **DONTRESOLVE** に設定する。
- Firewall Management Center でデバイスを追加するときに、到達可能なデバイスの IP アドレスまたはホスト名を指定していない。
- 両側でIPアドレスを指定する場合でも、管理にデータインターフェイスを使用する。
- Firewall Management Center が複数の管理インターフェイスを使用する。

ステップ 5 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のアクセスにデータインターフェイスを使用する場合、FQDN がこのインターフェイスに使用されます。

b) [DNSサーバグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは CiscoUmbrellaDNSServerGroup と呼ばれ、OpenDNS サーバが含まれます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] のデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバ

は、管理トラフィックに使用されます。データDNSサーバは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由でDNSサーバーに到達するため、管理に使用したものと同じ DNS サーバーグループを選択する可能性があります。

Firewall Management Center では、この Firewall Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイスDNSサーバーが設定されます。Firewall Management Center に Firewall Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS設定を含むFirewall Threat Defenseデバイスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Firewall Management Center とFirewall Threat Defenseデバイスを同期させるには、この設定に一致するようにDNSプラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカルDNSサーバーは、DNSサーバーが初期登録で検出された場合にのみFirewall Management Center で保持されます。

[Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）]**[FMCアクセスインターフェイス（FMC Access Interface）]** の管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを設定します。

c) [Management Center/SCCCDOアクセスインターフェイス（Management Center/**CDO** Access Interface）] については、任意の設定済みインターフェイスを選択します。

管理インターフェイスは、Firewall Threat Defense デバイスを Firewall Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

ステップ 6 （任意）外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Firewall Management Centerに接続する前にデフォルトルートを手動で設定する必要があります。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意のゲートウェイとして設定する必要があります。

ステップ 7 （任意） データインターフェイスを選択した場合は、[ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、 IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）でFirewall Threat Defenseデバイスに到達できるようにします。[デバイス（Device）] > [システム設定（System Settings）] > [DDNSサービス（DDNS Service）] を参照して DDNS を設定します。

Firewall Management Center に Firewall Threat Defense デバイスを追加する前に DDNS を設定すると、Firewall Threat Defense デバイスは、Cisco Trusted Root CA バンドルからすべての主要 CA

の証明書を自動的に追加し、Firewall Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。 Firewall Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

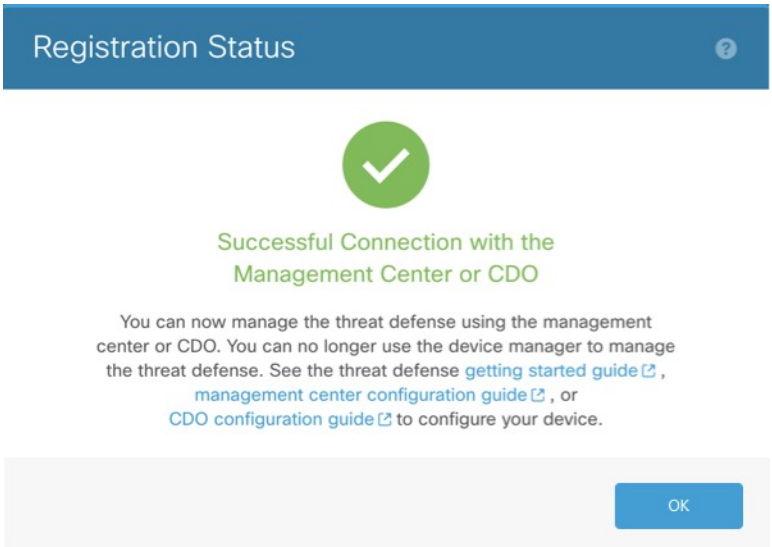
マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

ステップ 8 [接続（Connect）] をクリックします。**[登録ステータス（Registration Status）]** ダイアログボックスには、Firewall Management Center への切り替えに関する現在のステータスが表示されます。[Management Center/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップの後、Firewall Management Center に移動してファイアウォールを追加します。

Firewall Management Center への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。キャンセルしない場合は、[Management Center/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップが完了するまで Firewall Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Firewall Device Manager に再接続した場合のみ再開されます。

[Management Center/SCCCDO登録設定の保存（Saving Management Center/**CDO** Registration Settings）] のステップの後に Firewall Device Manager に接続したままにする場合、その後 [Management CenterまたはSCCCDOとの正常接続（Successful Connection with Management Center/**CDO**）] ダイアログボックスが表示され、Firewall Device Manager から切断されます。

図 *13* : 正常接続



Firewall Management Center から Firewall Device Manager への切り替え

代わりにFirewall Device Managerを使用するように、オンプレミスまたはクラウド提供型のFirewall Management Centerによって現在管理されている Firewall Threat Defense デバイスを設定できます。

ソフトウェアを再インストールすることなく、Firewall Management CenterからFirewall Device Managerに切り替えることができます。Firewall Management CenterからFirewall Device Managerに切り替える前に、Firewall Device Managerがすべての設定要件を満たしていることを確認します。Firewall Device Manager から Firewall Management Center に切り替える場合は、Firewall Device Manager から Firewall Management Center への切り替え （42 ページ） を参照してください。

注意 Firewall Device Manager に切り替えると、デバイスの設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は維持されます。

手順

ステップ 1 Firewall Management Center で、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** ページからファイアウォールを削除します。

ステップ 2 SSH またはコンソールポートを使用して、Firewall Threat Defense CLI に接続します。SSH の場合、管理 IP アドレスへの接続を開き、admin ユーザー名（または管理者権限を持つ他のユーザー）で Firewall Threat Defense CLI にログインします。

（Firepower モデル）コンソールポートはデフォルトで FXOS CLI になります。**connect ftd** コマンドを使用して、Firewall Threat Defense CLI に接続します。SSH セッションは Firewall Threat Defense CLI に直接接続します。

管理 IP アドレスに接続できない場合は、次のいずれかを実行します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理IPアドレスとゲートウェイが設定されていることを確認します。**configure network ipv4/ipv6 manual**コマンドを使用します。

ステップ 3 現在、リモート管理モードになっていることを確認します。

show managers

例：

```
> show managers
Type                    : Manager
Host                    : 10.89.5.35
Display name            : 10.89.5.35
Identifier              : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration            : Completed
```

ステップ 4 リモート マネージャを削除すると、マネージャなしのモードになります。

configure manager delete *uuid*

リモート管理からローカル管理に直接移行することはできません。複数のマネージャが定義されている場合は、識別子（UUID とも呼ばれます。**show managers** コマンドを参照）を指定する必要があります。各マネージャ エントリを個別に削除します。

例：

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ 5 ローカル マネージャを設定します。

configure manager local

これで、Web ブラウザで **https://***management-IP-address* にアクセスしてローカル マネージャを開くことができるようになりました。

例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Cisco Secure Firewall 3100 での SSD のホットスワップ

SSD が 2 つある場合、起動時に RAID が形成されます。ファイアウォールの電源が入っている状態で Firewall Threat Defense CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

手順

ステップ 1 SSD の 1 つを取り外します。

a) SSD を RAID から取り外します。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure キーワードは SSD を RAID から削除し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。SSD を RAID から削除するだけでデータをそのまま維持する場合は、**remove** キーワードを使用できます。

例：

```
> configure raid remove-secure local-disk 2
```

b) SSD がインベントリに表示されなくなるまで、RAID ステータスを監視します。

show raid

SSD が RAID から削除されると、**操作性**と**ドライブの状態**が**劣化**として表示されます。2 つ目のドライブは、メンバーディスクとして表示されなくなります。

例：

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
```

```
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  degraded
Presence:                     equipped
Lifecycle:                    available
Drive State:                  degraded
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     1
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) SSD をシャーシから物理的に取り外します。

ステップ 2 SSD を追加します。

a) SSD を空のスロットに物理的に追加します。

b) SSD を RAID に追加します。

configure raid add local-disk {**1** | **2**}

新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。ステータスを表示するには、**show raid** コマンドを使用します。

以前に別のシステムで使用されており、まだロックされている SSD を取り付ける場合は、次のコマンドを入力します。

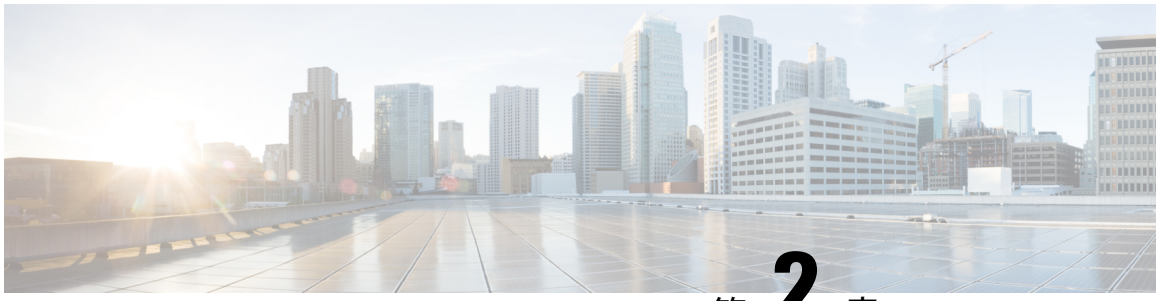
configure raid add local-disk {**1** | **2**} *psid*

psid は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。

デバイス管理の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ISA 3000 システム LED によるシャットダウンのサポート。	7.0.5/7.3.0	7.0.5/7.3.0	ISA 3000 をシャットダウンすると、システム LED が消灯します。電源を切る前に、少なくとも 10 秒待ってください。
ISA 3000 によるシャットダウンのサポート。	7.0.2/7.2.0	7.0.2/7.2.0	ISA 3000 をシャットダウンできるようになりました。以前は、デバイスを再起動することしかできませんでした。
マルチマネージャのサポート。	7.2.0	7.2.0	クラウド提供型の管理センターを導入しました。このクラウド提供型の管理センターは、Cisco Defense Orchestrator（CDO）プラットフォームを使用して、複数のシスコのセキュリティ ソリューションの管理を統合します。マネージャの更新についてはシスコが行います。 バージョン 7.2 以降を実行しているハードウェアまたは仮想管理センターでは、クラウド管理型のデバイスを「共同管理」できますが、用途はイベントのロギングと分析に限られます。このハードウェアまたは仮想管理センターからは、デバイスにポリシーを展開できません。 新規/変更されたコマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers** 新規/変更された画面： • クラウド管理型デバイスをハードウェアまたは仮想管理センターに追加する場合は、新しい [CDO管理対象デバイス（CDO Managed Device）] チェックボックスをオンにして、それが分析専用であることを指定します。 • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択すると、分析専用のデバイスが表示されます。 詳細については、CDOのドキュメントを参照してください。
Cisco Secure Firewall 3100 での SSD の RAID サポート。	7.1.0	7.1.0	SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 新規/変更されたコマンド： **configure raid, show raid, show ssd**
管理接続での TLS 1.3 のサポート。	7.1.0	7.1.0	FMC デバイス管理接続で TLS 1.3 が使用されるようになりました。以前は、TLS 1.2 がサポートされていました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
FDM を使用して、FMC による管理用に FTD を設定します。	7.1.0	7.1.0	FDMを使用して初期設定を実行すると、管理およびマネージャアクセス設定に加えて、管理のためにFMCに切り替えたときに、FDMで完了したすべてのインターフェイス設定が保持されます。アクセスコントロールポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。FMC CLIを使用すると、管理設定とマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 新規/変更された FDM 画面：**[システム設定（System Settings）]** > **[管理センター（Management Center）]**
アップグレードステータスでデバイスをフィルタする。	6.7.0	6.7.0	[デバイス管理（Device Management）]ページに、デバイスがアップグレードされているかどうか（およびそのアップグレードパス）や、最後のアップグレードが成功したか失敗したかなどの、管理対象デバイスに関するアップグレード情報が表示されるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**
Firepower Chassis Manager へのワンクリックアクセス。	6.4.0	6.4.0	Firepower 4100/9300 シリーズデバイスの場合は、[デバイス管理（Device Management）]ページに、Firepower Chassis Manager Web インターフェイスへのリンクが表示されます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**
正常性と展開のステータスでデバイスをフィルタする。バージョン情報を表示する。	6.2.3	6.2.3	[デバイス管理（Device Management）] ページに管理対象デバイスのバージョン情報が表示されるようになり、正常性および展開のステータスでデバイスをフィルタする機能が追加されました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**



第 2 章

デバイス設定

デバイスを追加したら、[デバイス（Device）] ページでデバイス関連の設定を編集できます。

1. **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。
2. 変更するデバイスの横にある [編集（Edit）]（ ） をクリックします。
3. [Device] をクリックします。

- 全般設定の編集 （55 ページ）
- ライセンス設定の編集 （63 ページ）
- システム情報の表示 （64 ページ）
- 検査エンジンの表示 （65 ページ）
- 正常性設定の編集 （66 ページ）
- 管理設定の編集 （66 ページ）
- インベントリ詳細の表示 （111 ページ）
- 適用されたポリシーの編集 （111 ページ）
- 詳細設定の編集 （113 ページ）
- 展開設定の編集 （118 ページ）
- クラスタのヘルスモニター設定の編集 （121 ページ）
- デバイス設定の履歴 （127 ページ）

全般設定の編集

[デバイス（Device）] タブの [全般（General）] セクションには、以下の表に記載された設定が表示されます。

図 *14 :* 一般

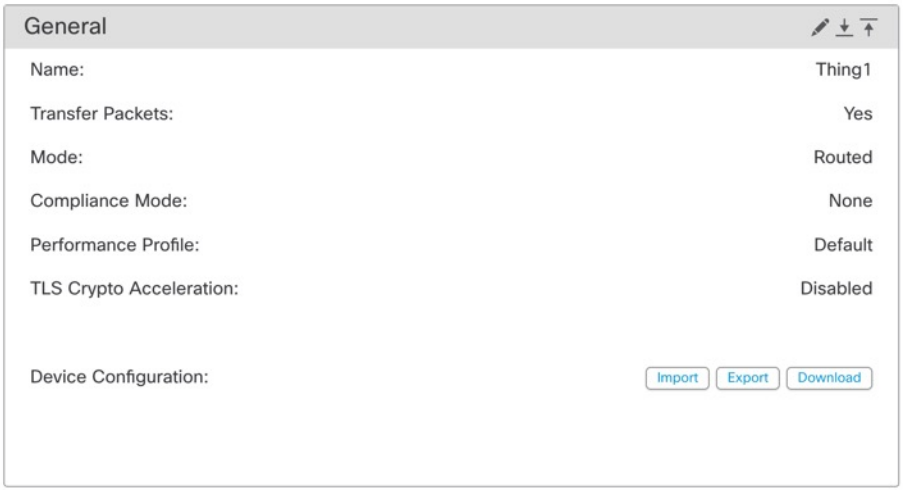


表 *2 : [*全般（***General***）*]* セクション テーブルのフィールド

フィールド	説明
名前	Firewall Management Center でのデバイスの表示名。
パケット転送（Transfer Packets）	管理対象デバイスがイベントを含むパケット データを Firewall Management Center に送信するかどうかを表示します。
モード（Mode）	デバイスの管理インターフェイスのモード（[ルーテッド（routed）] または [トランスペアレント（transparent）]）を表示します。
コンプライアンスモード（Compliance Mode）	デバイスのセキュリティ認定準拠が表示されます。有効な値は、CC、UCAPL および None です。
パフォーマンスプロファイル（Performance Profile）	プラットフォーム設定ポリシーで設定された、デバイスのコア割り当てパフォーマンスプロファイルが表示されます。
TLS暗号化アクセラレーション：（TLS Crypto Acceleration:）	TLS 暗号化アクセラレーションが有効か無効かを示します。
デバイス設定（Device Configuration）	構成をコピー、エクスポート、またはインポートできます。別のデバイスへの構成のコピー （57 ページ）およびデバイス設定のエクスポートとインポート （59 ページ）を参照してください。

これらの設定の一部は、このセクションから編集できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

ステップ 2 変更するデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [Device] をクリックします。

ステップ 4 [General] セクションで、[編集（Edit）]（✎） をクリックします。

a) [Name] に、管理対象デバイスの名前を入力します。

b) パケットデータをイベントと一緒に Firewall Management Center に保存できるようにするには、[パケットの転送（Transfer Packets）] チェックボックスをオンにします。

c) [Force Deploy] をクリックし、デバイスに現在のポリシーとデバイス設定の展開を強制します。

（注）
強制展開は、Firewall Threat Defense に展開されるポリシールールの完全な生成をともなうため、通常の展開よりも時間がかかります。

ステップ 5 [デバイス構成（Device Configuration）] アクションについては、別のデバイスへの構成のコピー（57 ページ）およびデバイス設定のエクスポートとインポート （59 ページ）を参照してください。

ステップ 6 [Deploy] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

別のデバイスへの構成のコピー

新しいデバイスをネットワークに展開する場合、新しいデバイスを手動で再設定する代わりに、事前設定されているデバイスの設定とポリシーを簡単にコピーすることができます。

始める前に

次の項目を確認します。

- コピー元とコピー先のデバイスが同じモデルであり、同じバージョンのソフトウェアを実行している。
- コピー元がスタンドアロン デバイスまたは高可用性ペアである。
- コピー先のデバイスがスタンドアロン デバイスである。
- コピー元とコピー先のデバイスに同じ数の物理インターフェイスがある。

- コピー元とコピー先のデバイスが同じファイアウォールモード（ルーテッドまたはトランスペアレント）になっている。
- コピー元とコピー先のデバイスが同じセキュリティ認定コンプライアンスモードになっている。
- コピー元とコピー先のデバイスが同じドメインにある。
- コピー元またはコピー先デバイスのいずれでも設定の展開が進行中ではない。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 2 変更するデバイスの横にある [編集（Edit）]（ ） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [全般（General）] セクションで、次のいずれかの操作を実行します。

- [デバイス設定の取得（Get Device Configuration）]（ ） をクリックして、別のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定の取得（Get Device Configuration）] ページの [デバイスの選択（Select Device）] ドロップダウンリストで、送信元デバイスを選択します。
- [デバイス設定のプッシュ（Push Device Configuration）]（ ） をクリックして、現在のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定のプッシュ（Push Device Configuration）] ページの [ターゲットデバイス（Target Device）] ドロップダウンリストで、設定をコピーする宛先を選択します。

ステップ 5 （オプション）[共有ポリシーの設定を含める（Include shared policies configuration）] チェックボックスをオンにして、ポリシーをコピーします。

AC ポリシー、NAT、プラットフォーム設定、および FlexConfig ポリシーなどの共有ポリシーは、複数のデバイス間で共有できます。

ステップ 6 [OK] をクリックします。

デバイス設定のコピータスクのステータスは、メッセージセンターの [タスク（Tasks）] でモニターできます。

デバイス設定のコピー タスクが開始されると、ターゲット デバイスの設定が削除され、送信元デバイスの設定が宛先のデバイスにコピーされます。

警告 デバイス設定のコピー タスクの完了後に、ターゲット デバイスを元の設定に戻すことはできません。

デバイス設定のエクスポートとインポート

[デバイス（Device）]ページで設定可能な、次のようなデバイス固有の設定をすべてエクスポートできます。

- インターフェイス
- インラインセット
- ルーティング
- DHCP
- VTEP
- 関連オブジェクト

次の使用例で、同じデバイスに保存された設定をインポートできます。

- 別の Firewall Management Center へのデバイスの移動：最初に元の Firewall Management Center からデバイスを削除 してから、新しい Firewall Management Center にデバイスを追加します。これで保存された設定をインポートできます。
- ドメイン間でのデバイスの移動：ドメイン間でデバイスを移動する場合、サポートするオブジェクト（セキュリティゾーンのインターフェイスグループなど）が新しいドメインに存在しないため、一部のデバイス固有の設定が保持されません。ドメインの移動後に設定をインポートすると、そのドメインに必要なオブジェクトが作成され、デバイス設定が復元されます。
- 古い設定の復元：デバイスの動作に悪影響を与える変更を展開した場合は、既知の動作設定のバックアップコピーをインポートして、以前の動作状態を復元できます。
- デバイスの再登録：デバイスを Firewall Management Center から削除した後で追加し直す場合は、保存した設定をインポートできます。

次のガイドラインを参照してください。

- 設定は同じデバイスにのみインポートできます（UUID が一致する必要があります）。同じモデルであっても、設定を別のデバイスにインポートすることはできません。
- エクスポートとインポートの間に、デバイスで実行されているバージョンを変更しないでください。バージョンは一致する必要があります。
- スタンドアロン設定をエクスポートする場合、高可用性ペアにインポートすることはできません。その逆も同様です。
- 異なる Firewall Management Center にデバイスを移動する場合、ターゲットの Firewall Management Center バージョンは、ソースバージョンと同じである必要があります。
- オブジェクトが存在しない場合は作成されます。オブジェクトが存在するが値が異なる場合は、以下を参照してください。

表 *3*:オブジェクトのインポートアクション

シナリオ	インポートアクション
同じ名前と値のオブジェクトが存在する。	既存のオブジェクトを再利用します。
同じ名前で値が異なるオブジェクトが存在する。	ネットワークおよびポートオブジェクト：このデバイスのオブジェクトオーバーライドを作成します。「オブジェクトのオーバーライド（1310 ページ）」を参照してください。 インターフェイス オブジェクト：新しいオブジェクトを作成します。たとえば、タイプ（セキュリティゾーンまたはインターフェイスグループ）とインターフェイスタイプ（ルーテッドまたはスイッチドなど）の両方が一致しない場合、新しいオブジェクトが作成されます。 他のすべてのオブジェクト：値が異なっていても、既存のオブジェクトを再利用します。
オブジェクトが存在しない。	新しいオブジェクトを作成します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 編集するデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

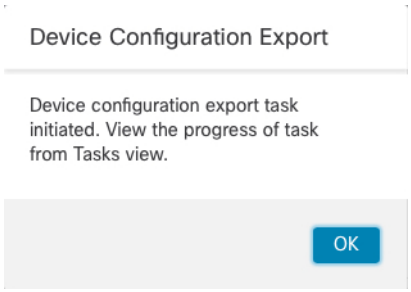
ステップ 4 設定をエクスポートします（設定のエクスポート）。

a) [General（全般）] エリアで [エクスポート（Export）] をクリックします。

図 *15*:デバイス設定のエクスポート

エクスポートを確認するよう求められます。[OK] をクリックします。

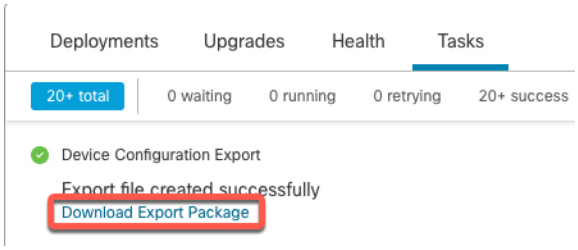
図 *16* : エクスポートの確認



[タスク（Tasks）] ページでエクスポートの進行状況を表示できます。

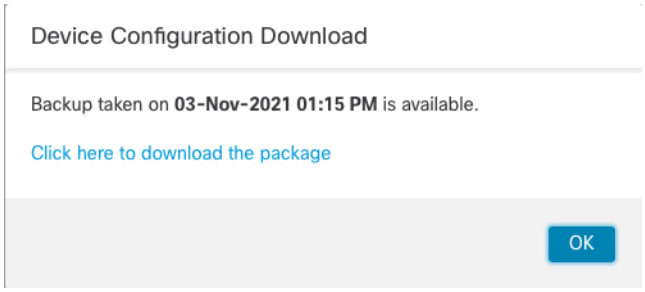
b) **[通知（Notifications）]**>**[タスク（Tasks）]**ページで、エクスポートが完了したことを確認します。[エクスポートパッケージのダウンロード（Download Export Package）] をクリックします。または、[全般（General）] エリアの [ダウンロード（Download）] ボタンをクリックすることもできます。

図 *17* : タスクのエクスポート



パッケージをダウンロードするように求められます。[ここをクリックしてパッケージをダウンロード（Click here to download the package）] をクリックしてローカルでファイルを保存し、[OK] をクリックしてダイアログボックスを終了します。

図 *18* : パッケージのダウンロード



ステップ 5 設定をインポートします。

a) [General（全般）] エリアで [インポート（Import）] をクリックします。

図 *19* : デバイス設定のインポート

現在の設定が置き換えられることを確認するよう求められます。[はい（Yes）] をクリックし、設定パッケージに移動します（接尾辞 .sfo が付いています。このファイルはバックアップファイルや復元ファイルとは異なることに注意してください）。

図 *20* : パッケージのインポート

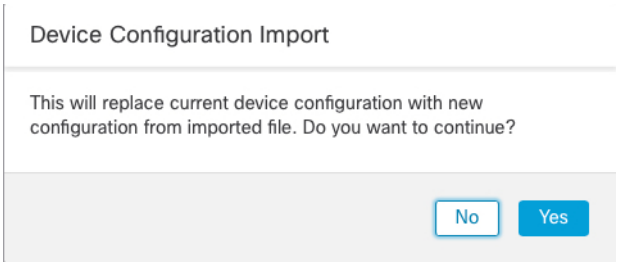
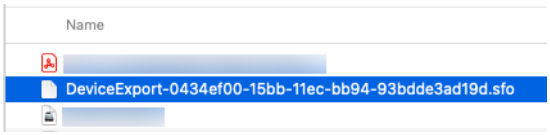
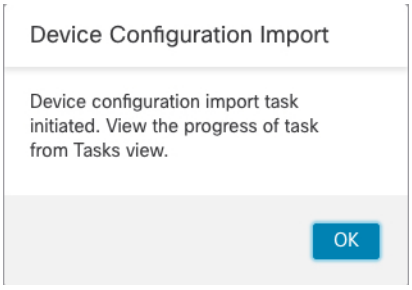


図 *21* : パッケージに移動



インポートを確認するよう求められます。[OK] をクリックします。

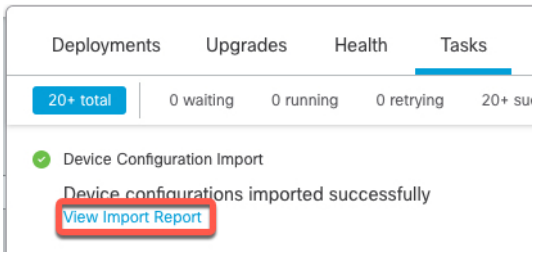
図 *22* : インポートの確認



[タスク（Tasks）] ページでインポートの進行状況を表示できます。

b) インポートレポートを表示して、何がインポートされたかを確認します。インポートタスクの**[通知（Notifications）]** > **[タスク（Tasks）]**ページで、[インポートレポートの表示（View Import Report）] をクリックします。

図 *23 :* インポートレポートの表示



[デバイス設定のインポートレポート（Device Configuration Import Reports）] ページには、利用可能なレポートへのリンクが表示されます。

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

ライセンス設定の編集

[デバイス（Device）]ページの [ライセンス（License）] セクションでは、そのデバイスに対して有効になっているライセンスが表示されます。

Firewall Management Center で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 ライセンスを有効または無効にするデバイスの横にある[編集（Edit）]（✎）をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [ライセンス（License）] セクションで、[編集（Edit）]（✎）をクリックします。

ステップ 5 管理対象デバイスに対して有効または無効にするライセンスの横にあるチェックボックスをオンまたはオフにします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

システム情報の表示

[デバイス（Device）] ページの [システム（System）] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

デバイスをシャットダウンまたは再起動することもできます。

図 *24 :* システム

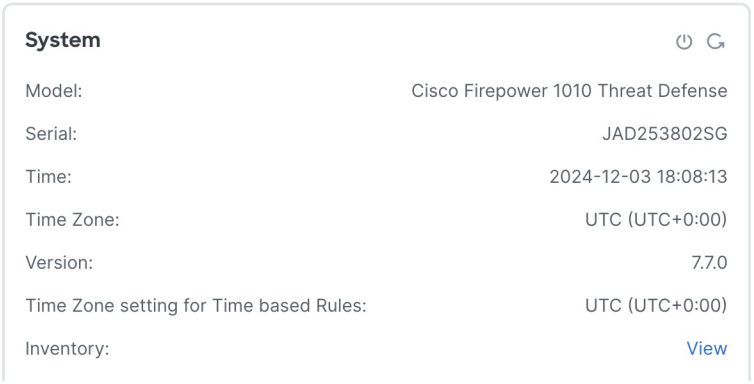


表 *4 : [*システム（*System***）*]* セクション テーブルのフィールド**

フィールド	説明
[デバイスのシャットダウン（Shut Down Device）] （）	デバイスをシャットダウンします。「デバイスのシャットダウンまたは再起動 （41 ページ）」を参照してください。
[デバイスの再起動（Restart Device）] （）	デバイスを再起動します。「デバイスのシャットダウンまたは再起動 （41 ページ）」を参照してください。
モデル	管理対象デバイスのモデル名と番号。
シリアル（Serial）	管理対象デバイスのシャーシのシリアル番号。
Time	デバイスの現在のシステム時刻。
タイム ゾーン	タイムゾーンを表示します。

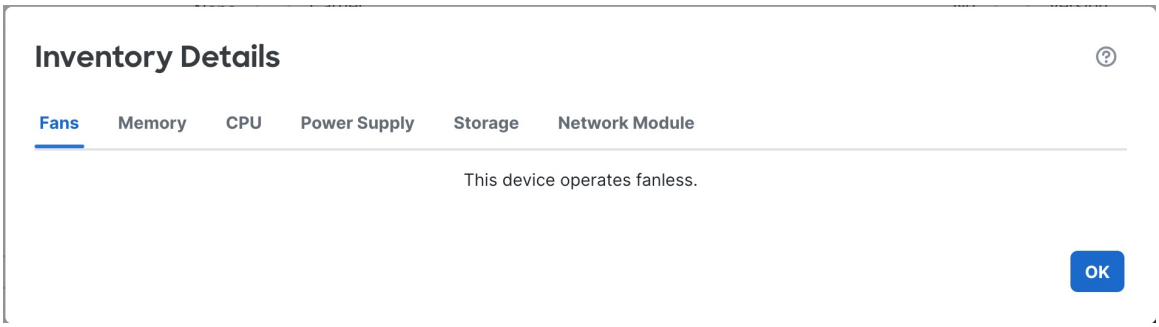
フィールド	説明
Version	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
時刻ベースルールのタイムゾーン設定（Time Zone setting for time-based rules）	デバイスのプラットフォーム設定で指定されたタイムゾーンでの、デバイスの現在のシステム時刻。
インベントリ	インベントリの詳細を表示します。デバイスインベントリの表示を参照してください。

デバイス インベントリの表示

[システム（System）] セクションの **[インベントリ（Inventory）]** の横にある **[表示（View）]** をクリックして、デバイスインベントリのテーブル（[ファン（Fans）]、[メモリ（Memory）]、[CPU]、[電源（Storage）]、[ネットワークモジュール（Network Modules）]）を表示します。

インベントリの詳細テーブルには、製品識別子（PID）が割り当てられている Threat Defense デバイスにインストールされているすべてのシスコ製品に関する情報が表示されます。PID は、製品を注文できる製品名です。

図 *25 :* インベントリの詳細（*Inventory Details*）



検査エンジンの表示

[デバイス（Device）] ページの [検査エンジン（Inspection Engine）] セクションには、デバイスが Snort 2 と Snort 3のデバイスで使用できる唯一のエンジンです。検索エンジンを切り替えるには、Cisco Secure Firewall Management Center Snort 3 Configuration Guide個々のデバイス上での *Snort 3* の有効化を参照してください。

正常性設定の編集

[デバイス（Device）] ページの [正常性（Health）] セクションには、以下の表に記載された情報が表示されます。

表 *5: [*ヘルス（*Health*）*]* セクション テーブルのフィールド

フィールド	説明
ステータス	デバイスの現在のヘルス ステータスを表すアイコン。アイコンをクリックすると、アプライアンスのヘルス モニタが表示されます。
ポリシー	現在デバイスで展開されている、読み取り専用バージョンの正常性ポリシーへのリンク。
除外	**[正常性除外（Health Exclude）]** ページへのリンク。このページでは、正常性除外モジュールを有効化および無効化できます。

管理設定の編集

これらの設定は、Firewall Management Center とデバイスとの管理接続の確立方法を制御します。

冗長マネージャアクセス用データインターフェイスの設定

マネージャアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンしたときに管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。セカンダリインターフェイスは1つだけ構成できます。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含む ECMP ゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。

始める前に

- セカンダリインターフェイスは、プライマリインターフェイスとは別のセキュリティゾーンにある必要があります。
- プライマリインターフェイスに適用されるのと同じすべての要件がセカンダリインターフェイスに適用されます。管理のための Firewall Threat Defense データインターフェイスの使用について （5 ページ） を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Manageme）]**ページで、デバイスの [編集（Edit）]（✎） をクリックします。

ステップ 2 セカンダリインターフェイスのマネージャアクセスを有効にします。

この設定は、インターフェイスの有効化、名前の設定、セキュリティゾーンの設定、スタティック IPv4 アドレスの設定など、標準のインターフェイス設定に加えて行うものです。

a) **[インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）] > [マネージャアクセス（Manager Access）]**を選択します。

b) [このインターフェイス上の管理をマネージャに対して有効にする（Enable management on this interface for the Manager）] をオンにします。

c) [OK] をクリックします。

どちらのインターフェイスも、インターフェイスリストに[（マネージャアクセス）（(Manager Access)）] と表示されます。

図 *26 :* インターフェイスリスト

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

ステップ 3 [管理（Management）] 設定にセカンダリアドレスを追加します。

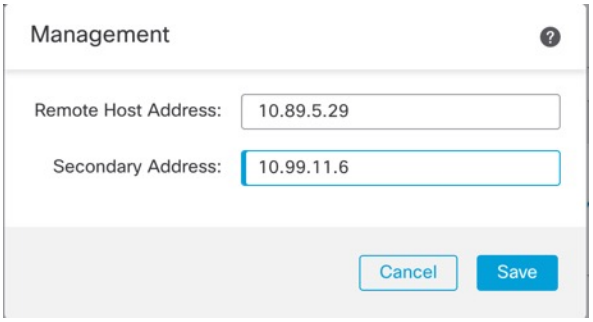
a) [Device] をクリックし、[Management] 領域を表示します。

b) [.] をクリックします。[編集（Edit）]（✎）

図 *27* : 管理アドレスの編集

c) [管理（Management）] ダイアログボックスで、[セカンダリアドレス（Secondary Address）] フィールドの名前または IP アドレスを変更します。

図 *28* : 管理 *IP* アドレス

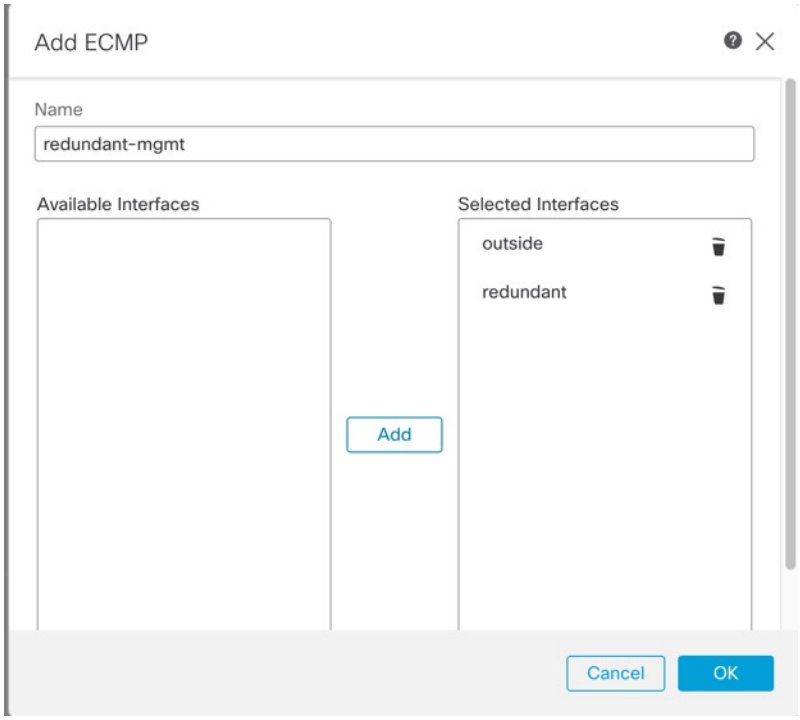


d) [保存（Save）] をクリックします。

ステップ 4 両方のインターフェイスで ECMP ゾーンを作成します。

a) [ルーティング（Routing）] をクリックします。
b) 仮想ルータドロップダウンから、プライマリインターフェイスとセカンダリインターフェイスが存在する仮想ルータを選択します。
c) [ECMP] をクリックし、[追加（Add）] をクリックします。
d) [名前（Name）] に ECMP ゾーンの名前を入力します。
e) [使用可能なインターフェイス（Available Interfaces）] ボックスでプライマリおよびセカンダリインターフェイスを選択し、[追加（Add）] をクリックします。

図 *29 : ECMP* ゾーンの追加

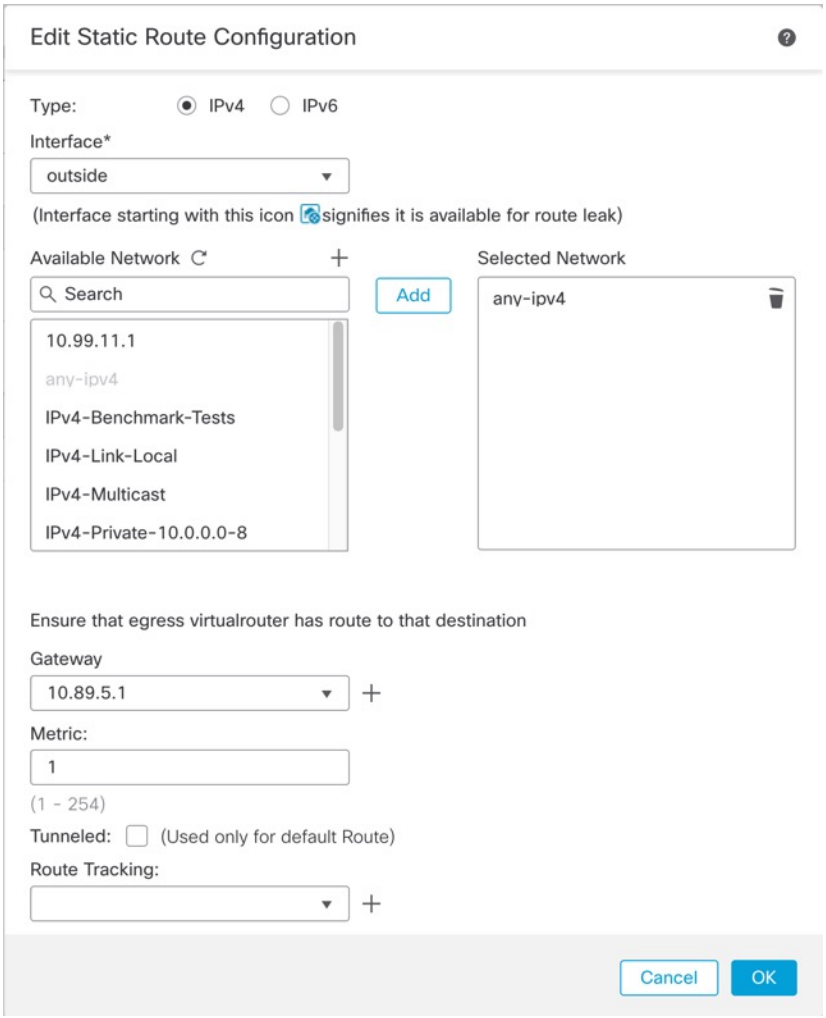


f) [OK] をクリックし、[保存（Save）] をクリックします。

ステップ 5 両方のインターフェイスに等コストのデフォルト スタティック ルートを追加し、両方で SLA トラッキングを有効にします。

ルートは、ゲートウェイを除いて同一であり、両方のメトリックが 1 である必要があります。プライマリインターフェイスには、編集可能なデフォルトルートがすでに存在している必要があります。

図 *30 : Add/Edit Static Route*



a) [Static Route] をクリックします。

b) [ルートを追加（Add Route）] をクリックして新しいルートを追加するか、既存のルートの場合は [編集（Edit）]（）をクリックします。

c) [インターフェイス（Interface）] ドロップダウンリストから、インターフェイスを選択します。

d) 宛先ネットワークとして、[使用可能なネットワーク（Available Networks）] ボックスから [any-ipv4] を選択し、[追加（Add）] をクリックします。

e) デフォルトの [ゲートウェイ（Gateway）] を入力します。

f) [ルートトラッキング（Route Tracking）] の場合、[追加（Add）] ()をクリックして新しい SLA モニターオブジェクトを追加します。

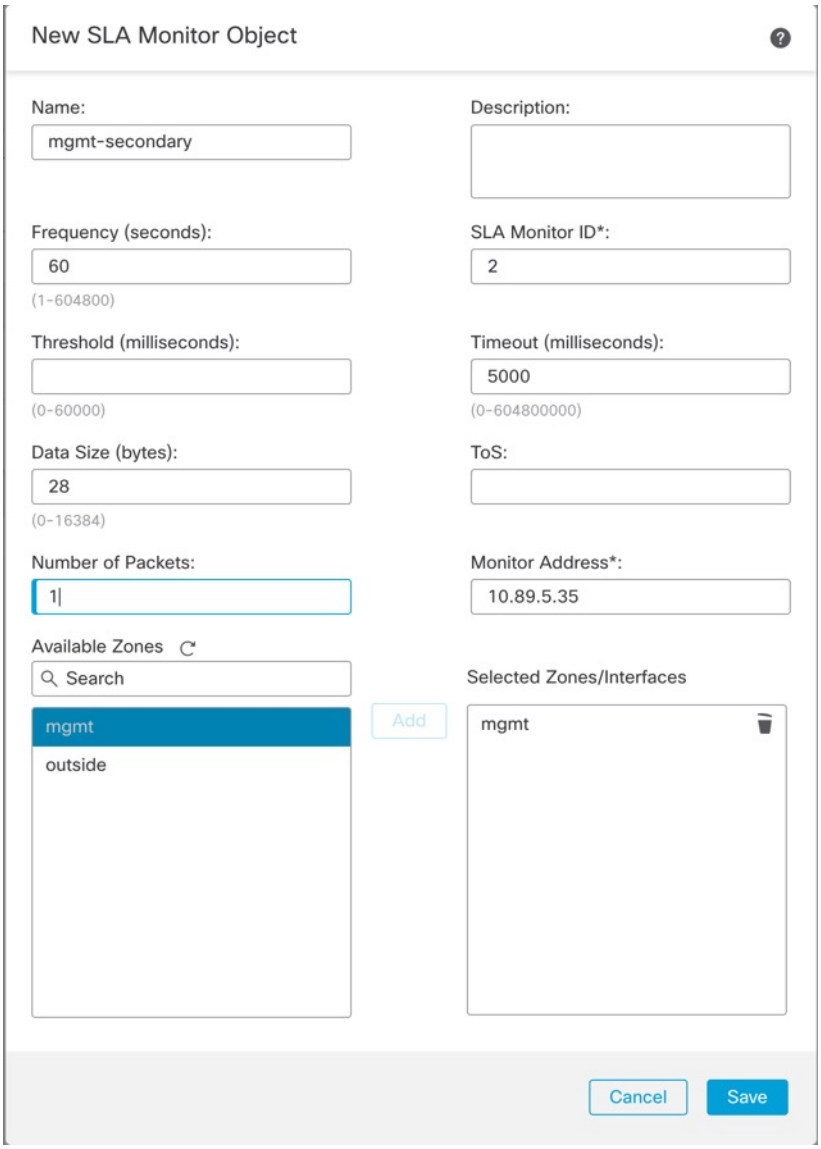
g) 次を含む必要なパラメータを入力します。

- Firewall Management Center IP アドレスとしての [モニターアドレス（Monitor Address）]。

- [使用可能なゾーン（Available Zones）] のプライマリまたはセカンダリ管理インターフェイスのゾーン。たとえば、プライマリ インターフェイス オブジェクトには外部ゾーンを選択し、セカンダリ インターフェイス オブジェクトには管理ゾーンを選択します。

詳細については、SLA モニタ （1399 ページ）を参照してください。

図 *31 : SLA* モニターの追加



h) [保存（Save）] をクリックし、[ルートトラッキング（Route Tracking）] ドロップダウンリストで、作成した SLA オブジェクトを選択します。

i) [OK] をクリックし、[保存（Save）] をクリックします。

j) もう一方の管理インターフェイスのデフォルトルートについてこの手順を繰り返します。

ステップ 6 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

この機能の展開において、Firewall Management Center は管理トラフィック用のセカンダリインターフェイスを有効にします。これには、管理トラフィックが適切なデータインターフェイスに到達するための自動生成されたポリシーベースのルーティング構成が含まれます。Firewall Management Center は、**configure network management-data-interface** コマンドの 2 番目のインスタンスも展開します。CLI でセカンダリインターフェイスを編集する場合、ゲートウェイを設定したり、デフォルトルートを変更したりすることはできません。このインターフェイスのスタティックルートは Firewall Management Center でしか編集できません。

マネージャ アクセス インターフェイス設定の変更

デバイスまたは Firewall Management Center のマネージャ インターフェイス設定を変更すると、管理接続が中断される可能性があります。インターフェイス設定を変更して管理接続を再確立するには、次のシナリオを参照してください。

デバイス IP アドレスを変更する

デバイス IP アドレスを変更し、Firewall Management Center のアドレスを更新します。

デバイス IP アドレスの設定

次のいずれかの方法を使用して、マネージャ アクセス インターフェイスの IP アドレスを設定します。

Firewall Threat Defense 管理インターフェイスの *CLI* での変更

CLI を使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設定を変更でき、さらに設定を追加できます（例：モデルでサポートされる場合にイベントインターフェイスを有効化する、スタティック ルートを追加する）。

（注） このトピックは、専用管理インターフェイスに適用されます。代わりに、管理用のデータインターフェイスを設定することもできます。このインターフェイスのネットワーク設定を変更する場合は、CLI ではなく Firewall Management Center 内で行う必要があります。切断された管理接続をトラブルシューティングする必要があり、Firewall Threat Defense で直接変更する必要がある場合は、管理に使用される Firewall Threat Defense データインターフェイスの CLI での変更 （79 ページ） を参照してください。

Firewall Threat Defense CLI の詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンス を参照してください。

（注） SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスが必要になります。

（注） デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド（新しい Management Center への登録 （38 ページ） を参照）を使用してデバイスの初期設定時に Firewall Management Center を特定した方法に応じて、Firewall Management Center 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし。**到達可能な IP アドレスを使用して Firewall Management Center を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、Firewall Management Center に表示されるデバイス IP アドレスも変更することを推奨します。Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ） を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。**注**：到達不能な Firewall Management Center IP アドレスを指定した場合は、以下の NAT ID の手順を参照してください。
- **NAT IDのみ：接続を手動で再確立。**NAT ID のみを使用して Firewall Management Center を識別した場合、接続は自動的に再確立されません。この場合、Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ） に従って Firewall Management Center のデバイス管理 IP アドレスを変更します。

（注） ハイアベイラビリティ Firewall Management Center 構成では、管理 IP アドレスをデバイスの CLI または Firewall Management Center から変更した場合、HA 同期後も、セカンダリ Firewall Management Center には変更が反映されません。セカンダリ Firewall Management Center も更新されるようにするには、2 つの Firewall Management Center の間でロールを切り替えて、セカンダリ Firewall Management Center をアクティブユニットにします。現在アクティブな Firewall Management Center のデバイス管理のページで、登録されているデバイスの管理 IP アドレスを変更します。

始める前に

- **configure user add** コマンドを使用して CLI にログイン可能なユーザー アカウントを作成できます。次を参照してください：CLI での内部ユーザーの追加 （134 ページ）外部認証 （832 ページ）に従って AAA ユーザーを設定することもできます。

手順

ステップ 1 コンソール ポートから、または SSH を使用して、デバイス CLI に接続します。

「デバイスのコマンド ライン インターフェイス（CLI）へのログイン （12 ページ）」を参照してください。

ステップ 2 管理者のユーザー名とパスワードでログインします。

ステップ 3 （Firepower 4100/9300のみ）2 番目の管理インターフェイスをイベント専用インターフェイスとして有効にします。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

管理トラフィック用の管理インターフェイスが常に必要です。デバイスに 2 番目の管理インターフェイスがある場合は、イベント専用トラフィックに対してそのインターフェイスを有効にすることができます。

必要に応じて、**configure network management-interface disable-events-channel** コマンドを使用してメイン管理インターフェイスのイベントを無効にできます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

インターフェイス上でイベントチャネルと管理チャンネルの両方を無効にすることはできません。

別のイベントインターフェイスを使用するには、Firewall Management Center でイベントインターフェイスを有効にする必要もあります。Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

例：

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

ステップ 4 管理インターフェイスまたはイベントインターフェイスの IP アドレスを設定します。

management_interface 引数を指定しない場合は、デフォルトの管理インターフェイスのネットワーク設定を変更します。イベントインターフェイスを設定する際は、必ず*management_interface* 引数を指定してください。イベントインターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  このコマンド内の *gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、

コマンドの一部として *gateway_ip* を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別のネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスと共に使用するように *gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別にスタティックルートを作成することを推奨します。

例：

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv4 dhcp

b) IPv6 アドレスを設定します。

- ステートレス自動設定

  configure network ipv6 router [*management_interface*]

  例：

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手動設定

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  このコマンド内の *ipv6_gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として *ipv6_gateway_ip* を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別のネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスと共に使用するように *ipv6_gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別にスタティックルートを作成することを推奨します。

  例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
```

```
Network settings changed.

>
```

- DHCPv6（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv6 dhcp

ステップ 5 IPv6 の場合、ICMPv6 エコー応答と宛先到達不能メッセージを有効または無効にします。デフォルトでは、これらのメッセージは有効になっています。

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。

例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

ステップ 6 デフォルト管理インターフェイスの DHCP サーバーが、接続されているホストに IP アドレスを提供することを可能にします。

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

管理インターフェイスの IP アドレスを手動で設定するときにのみ、DHCP サーバーを設定できます。このコマンドは、Firewall Management Center Virtual ではサポートされません。DHCP サーバーのステータスを表示するには、**show network-dhcp-server** を入力します。

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

ステップ 7 Firewall Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

デフォルトルートの場合は、このコマンドを使用しないでください。デフォルト ルート ゲートウェイの IP アドレスの変更は、**configure network ipv4** コマンドまたは **ipv6** コマンドを使用した場合のみ可能です（「ステップ 4 （74 ページ）」を参照）。

例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

スタティック ルートを表示するには、**show network-static-routes** を入力します（デフォルトルートは表示されません）。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

ステップ 8 ホスト名の設定

configure network hostname *name*

例：

```
> configure network hostname farscape1.cisco.com
```

Syslog メッセージは、再起動するまで新しいホスト名を反映しません。

ステップ 9 検索ドメインを設定します。

configure network dns searchdomains *domain_list*

例：

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

ステップ 10 カンマで区切った 3 つの DNS サーバーを設定します。

configure network dns servers *dns_ip_list*

例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

ステップ 11 Firewall Management Center で通信のリモート管理ポートを設定します。

configure network management-interface tcpport *number*

例：

```
> configure network management-interface tcpport 8555
```

Firewall Management Center および管理対象デバイスは、双方向の TLS-1.3 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

（注）
シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 12 （Firewall Threat Defense のみ）管理インターフェイスまたはイベントインターフェイスの MTU を設定します。デフォルトの MTU は 1500 バイトです。

configure network mtu [*bytes*] [*interface_id*]

- *bytes*：MTU をバイト単位で設定します。管理インターフェイスでは、IPv4 を有効にした場合は 64ー1500、IPv6 を有効にした場合は 1280ー1500 の値を指定できます。イベントインターフェイスでは、IPv4 を有効にした場合は 64ー9000、IPv6 を有効にした場合は 1280ー9000 です。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。
- *interface_id*：MTU を設定するインターフェイス ID を指定します。プラットフォームに応じて使用可能なインターフェイス ID（management0、management1、br1、eth0など）を表示するには、**show network** コマンドを使用します。インターフェイスを指定しない場合は、管理インターフェイスが使用されます。

例：

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

ステップ 13 HTTP プロキシを設定します。デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシサーバーを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザーは尋ねられます。認証が必要な場合はプロキシ

のユーザー名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

（注）
Firewall Threat Defense のプロキシパスワードには、A～Z、a～z と 0～9 の文字のみを使用できます。

configure network http-proxy

例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

ステップ 14 デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド（新しい Management Center への登録 （38 ページ） を参照）を使用してデバイスの初期設定時に Firewall Management Center を特定した方法に応じて、Firewall Management Center 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし。**到達可能な IP アドレスを使用して Firewall Management Center を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、Firewall Management Center に表示されるデバイス IP アドレスも変更することを推奨します。Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ） を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。**注**：到達不能な Firewall Management Center IP アドレスを指定した場合は、Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ） を使用して手動で接続を再確立する必要があります。
- **NAT IDのみ：接続を手動で再確立。**NAT ID のみを使用して Firewall Management Center を識別した場合、接続は自動的に再確立されません。この場合、Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ） に従って Firewall Management Center のデバイス管理 IP アドレスを変更します。

管理に使用される *Firewall Threat Defense* データインターフェイスの *CLI* での変更

Firewall Threat Defense と Firewall Management Center の間の管理接続が中断され、古いインターフェイスを置き換える新しいデータインターフェイスを指定する場合は、Firewall Threat Defense CLI を使用して新しいインターフェイスを設定します。

管理接続がアクティブな場合は、Firewall Management Center を使用して既存のデータインターフェイスに変更を行う必要があります（GUI で [管理（Management）] に使用する Firewall Threat Defense データインターフェイスを修正する （82 ページ） を参照）。データ管理インターフェイスの初期設定については、「CLI を使用した Firewall Threat Defense 初期設定の実行の完了

（21 ページ）」の **configure network management-data-interface** コマンドを参照してください。

（注） このトピックは、専用の管理インターフェイスではなく、管理用に設定したデータインターフェイスに適用されます。管理インターフェイスのネットワーク設定を変更する場合は、Firewall Threat Defense 管理インターフェイスの CLI での変更 （72 ページ）を参照してください。

Firewall Threat Defense CLI の詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンス を参照してください。

手順

ステップ 1 データ管理インターフェイスを新しいインターフェイスに変更する場合は、現在のインターフェイスケーブルを新しいインターフェイスに移動します。

ステップ 2 デバイスの CLI に接続します。

これらのコマンドを使用する場合は、コンソールポートを使用する必要があります。初期設定の実行中に、管理インターフェイスから切断される可能性があります。管理接続が中断されたために設定を編集しており、専用管理インターフェイスに SSH アクセスできる場合は、その SSH 接続を使用できます。

「デバイスのコマンド ライン インターフェイス（CLI）へのログイン （12 ページ）」を参照してください。

ステップ 3 **admin** のユーザー名とパスワードでログインします。

ステップ 4 インターフェイスを無効にして、設定を再構成できるようにします。

configure network management-data-interface disable

（注）
同じインターフェイスで新しい IPv4 アドレスを設定するだけで、その他の変更は行わない場合は、この手順をスキップできます。その他の変更では、最初にインターフェイスを無効にする必要があります。

例：

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a
gateway on management interface using the command 'configure network'
```

ステップ 5 マネージャアクセス用の新しいデータインターフェイスを設定します。

configure network management-data-interface

その後、データインターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

データ管理インターフェイスを同じネットワーク上の新しいインターフェイスに変更する場合は、インターフェイス ID を除き、前のインターフェイスと同じ設定を使用します。さらに、**Do you wish to clear all the device configuration before applying ? (y/n) [n]:** オプションに **y** を選択します。この選択により、古いデータ管理インターフェイスの設定がクリアされるため、IP アドレスとインターフェイス名を新しいインターフェイスで正常に再利用できます。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
 change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 6 （任意）特定のネットワーク上の Firewall Management Center へのデータ インターフェイス アクセスを制限します。

configure network management-data-interface client *ip_address netmask*

デフォルトでは、すべてのネットワークが許可されます。

ステップ 7 Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ）。

接続は自動的に再確立されますが、Firewall Management Center で接続を無効にしてから再度有効にすると、接続の再確立を速く実行できます。または、リンクされた手順を実行して、Firewall Management Center でデバイス IP アドレスを更新する必要があります。

ステップ 8 管理接続が再確立されたことを確認します。

sftunnel-status-brief

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
```

```
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

ステップ 9 Firewall Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**、[編集（Edit）]（✎） の順に選択します。**[デバイス（Device）]** > **[管理（Management）]** エリアで、**[マネージャアクセス - 構成詳細（Manager Access - Configuration Details）]** の横にある **[更新（Refresh）]** をクリックします。

Firewall Management Center は、インターフェイスとデフォルトルートの構成変更を検出し、デプロイへのデプロイメントをブロックします。デバイスのデータインターフェイス設定をローカルで変更する場合は、Firewall Management Center でそれらの変更を手動で調整する必要があります。 **と [構成（Configuration）]** タブのデバイス間の不一致を確認できます。

ステップ 10 **[インターフェイス（Interfaces）]** を選択して、次の変更を行います。

a) IP アドレスと名前を古いデータ管理インターフェイスから削除し、このインターフェイスでマネージャアクセスを無効にします。

b) 新しい設定（CLI で使用したインターフェイス）が適用された新しいデータ管理インターフェイスを構成し、それに対して、マネージャアクセスを有効にします。

ステップ 11 **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** の順に選択し、古いデータ管理インターフェイスのデフォルトのルートを新しいものに変更します。

ステップ 12 [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに戻り、[確認（Acknowledge）] をクリックして展開ブロックを削除します。

Firewall Management Center 設定は、次回展開時に Firewall Threat Defense の残りの競合する設定を上書きします。再展開の前に Firewall Management Center の設定を手動で修正する必要があります。

「Config was cleared」および「Manager Access changed and acknowledged」という想定されるメッセージが表示されます。

GUI で [管理（Management）] に使用する Firewall Threat Defense データインターフェイスを修正する

管理接続が稼働しているが、マネージャアクセスに使用するデータインターフェイスの IP アドレスを変更する場合は、次の手順を実行します。たとえば、ゼロタッチプロビジョニングを使用してデバイスを登録した場合、高可用性を有効にする前に、IP アドレスを静的アドレスに変更する必要があります。

または CLI でインターフェイス設定を変更することもできますが、これは、管理接続が停止している場合にのみ使用することをお勧めします。CLI で行った変更は、いずれの場合においても GUI で複製される必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 2 **[インターフェイス（Interface）]** を選択します。

ステップ 3 マネージャアクセスに使用するインターフェイスを変更する場合は、次の手順を実行します。

a) IPアドレスと名前を古いデータ管理インターフェイスから削除し、このインターフェイスでマネージャアクセスを無効にします。

b) 新しい設定が適用された新しいデータ管理インターフェイスを構成し、それに対して、マネージャアクセスを有効にします。

c) 静的IPアドレスを使用する場合は、デフォルトルートを使用するようにリマインダが表示されます。[Yes] をクリックします。

d) **[OK]** をクリックして、インターフェイスを終了します。

e) [インターフェイス（Interfaces）] ページで [保存（Save）] をクリックします。

ステップ 4 IP アドレスのみを変更する場合は、次の手順を実行します。

a) IPアドレスを変更してください。

b) 静的IPアドレスを使用する場合は、デフォルトルートを使用するようにリマインダが表示されます。[Yes] をクリックします。

c) **[OK]** をクリックして、インターフェイスを終了します。

d) [インターフェイス（Interfaces）] ページで [保存（Save）] をクリックします。

ステップ 5 **[ルーティング（Routing）]**>**[スタティックルート（Static Route）]** の順に選択し、マネージャアクセスインターフェイスのデフォルトまたはスタティックルートを追加または変更します。

ステップ 6 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

Firewall Management Center が現在の接続経由で構成の変更をデプロイします。デプロイメント後、データインターフェイスには、新しい IP アドレスが割り当てられるため、管理接続を再度確立する必要があります。

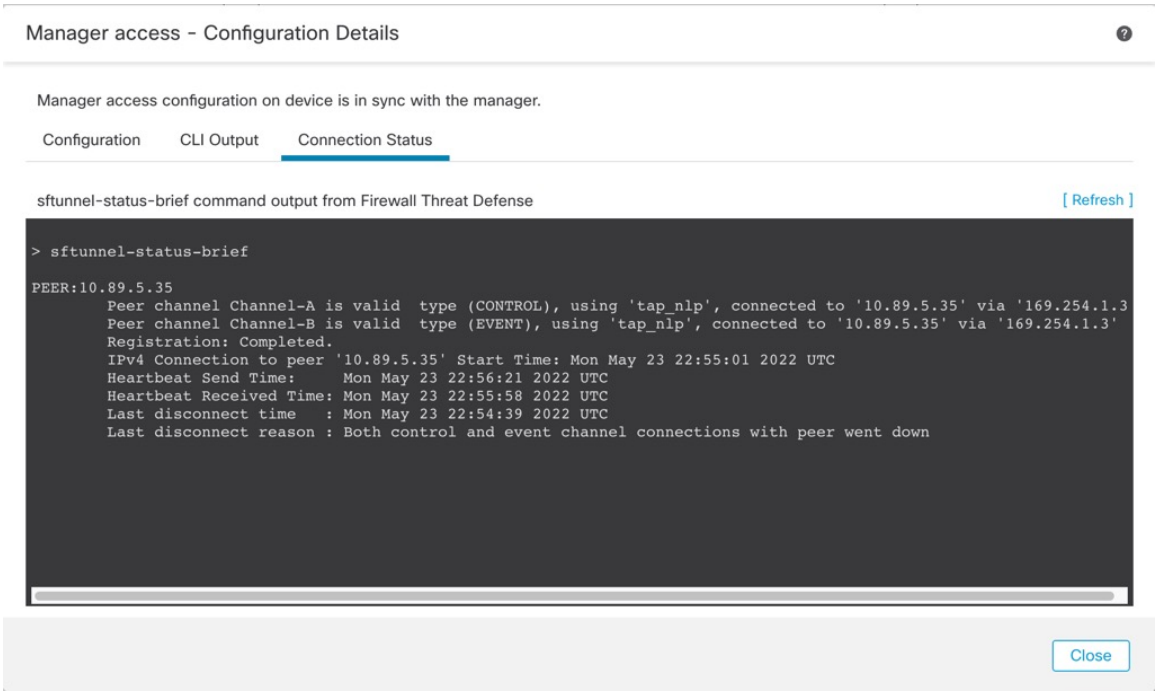
ステップ 7 Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ）。

ステップ 8 管理接続が再確立されたことを確認します。

[デバイス（Device）] > **[管理（Management）]** エリアで、**[マネージャアクセス詳細：構成（Manager Access Details: Configuration）]** をクリックし、**[接続ステータス（Connection Status）]**をクリックします。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *32* : 接続ステータス



接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。「データインターフェイスでの管理接続のトラブルシューティング （106 ページ）」を参照してください。

Firewall Management Center でのホスト名または IP アドレスの更新

（デバイスの CLI を使用するなどして）デバイスを Firewall Management Center に追加した後にそのデバイスのホスト名または IP アドレスを編集する場合は、次の手順を使用して管理側の Firewall Management Center のホスト名または IP アドレスを手動で更新する必要があります。

デバイスのデバイス管理 IP アドレスを変更するには、Firewall Threat Defense 管理インターフェイスの CLI での変更 （72 ページ）を参照してください。

デバイスの登録時に NAT ID のみを使用した場合、IP はこのページに [NO-IP] として表示され、IP アドレス/ホスト名を更新する必要はありません。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

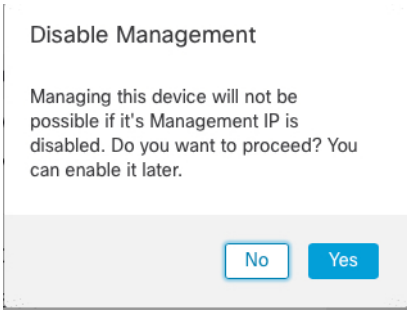
ステップ 2 管理オプションを変更するデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [Device] をクリックし、[Management] 領域を表示します。

ステップ 4 スライダをクリックして管理を一時的に無効にすることで、[無効なスライダ（Slider disabled）]（ ）を無効化します。

図 *33* : 管理を無効にする

管理の無効化を続行するように求められます。 [Yes] をクリックします。



管理を無効化すると、Firewall Management Center とデバイス間の接続がブロックされますが、Firewall Management Center からデバイスは削除**されません**。

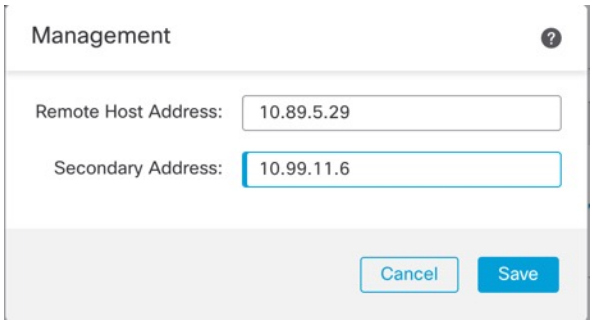
ステップ 5 **[リモートホストアドレス（Remote Host Address）]** の IP アドレスおよびオプションの [セカンダリアドレス（Secondary Address）]（冗長データインターフェイスを使用する場合）または [編集（Edit）]（✎）をクリックしてホスト名を編集します。

図 *34* : 管理アドレスの編集

ステップ 6 [管理（Management）] ダイアログボックスの **[リモートホストアドレス（Remote Host Address）]** フィールドおよびオプションの [セカンダリアドレス（Secondary Address）] フィールドで名前または IP アドレスを変更し、[保存（Save）] をクリックします。

セカンダリ マネージャ アクセス データ インターフェイスの使用については、冗長マネージャアクセス用データインターフェイスの設定 （66 ページ）を参照してください。

図 *35 :* 管理 *IP* アドレス



ステップ 7 スライダをクリックして管理を再度有効[有効なスライダ（Slider enabled）]（ ）にします。

図 *36 :* 管理接続の有効化

Firewall Management Center IP アドレスの変更

Firewall Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Firewall Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Firewall Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Firewall Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

手順

ステップ 1 Firewall Management Center の IP アドレスを変更してください。

注意
Firewall Management Center インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Firewall Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

a) [システム（System）]（⚙）>**[設定（Configuration）]**>**[管理インターフェイス（Management Interfaces）]**を選択します。
b) [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。
c) IP アドレスを変更し、[保存（Save）] をクリックします。

ステップ 2 Firewall Threat Defense CLI で、Firewall Management Center 識別子を表示します。

show managers

例：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

ステップ 3 Firewall Threat Defense CLI で、Firewall Management Center IP アドレスまたはホスト名を編集します。

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

Firewall Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

管理接続がダウンした後、再確立されます。**sftunnel-status** コマンドを使用して、接続の状態をモニターできます。

例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

Firewall Management Center と Threat Defense の両方の IP アドレスの変更

Firewall Management Center と Firewall Threat Defense の IP アドレスを新しいネットワークに移動する場合は、両方を変更することをお勧めします。

手順

ステップ 1 管理接続を無効にします。

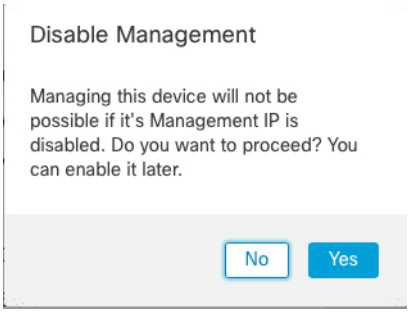
高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) **[デバイス（Devices）]**>**[デバイス管理（Device Management）]**を選択します。

b) デバイスの横にある [編集（Edit）]（✎） をクリックします。
c) [Device] をクリックし、[Management] 領域を表示します。
d) スライダをクリックして管理を一時的に無効にすることで、（ ） を無効化します。

図 *37* : 管理を無効にする

管理の無効化を続行するように求められます。 [Yes] をクリックします。



ステップ 2 Firewall Management Center 内のデバイスの IP アドレスを新しいデバイスの IP アドレスに変更します。

デバイスの IP アドレスは後で変更します。

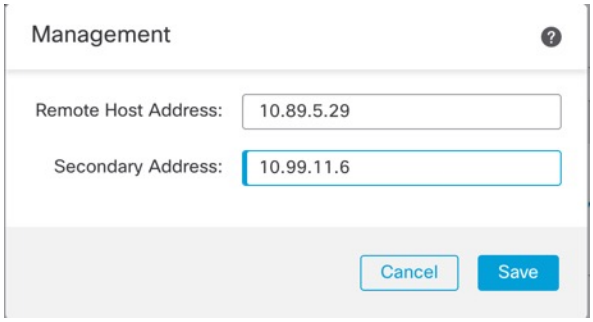
高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) **[リモートホストアドレス（Remote Host Address）]** の IP アドレスおよびオプションの [セカンダリアドレス（Secondary Address）]（冗長データインターフェイスを使用する場合）または [編集（Edit）]（✎）をクリックしてホスト名を編集します。

図 *38* : 管理アドレスの編集

b) [管理（Management）] ダイアログボックスの **[リモートホストアドレス（Remote Host Address）]** フィールドおよびオプションの [セカンダリアドレス（Secondary Address）] フィールドで名前または IP アドレスを変更し、[保存（Save）] をクリックします。

図 *39 :* 管理 *IP* アドレス



ステップ 3 Firewall Management Center の IP アドレスを変更してください。

注意
Firewall Management Center インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Firewall Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

a) [システム（System）]（⚙）>**[設定（Configuration）]**>**[管理インターフェイス（Management Interfaces）]**を選択します。
b) [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。
c) IP アドレスを変更し、[保存（Save）] をクリックします。

ステップ 4 デバイスのマネージャ IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) Firewall Threat Defense CLI で、Firewall Management Center 識別子を表示します。

show managers

例：

```
> show managers
Type                    : Manager
Host                    : 10.10.1.4
Display name            : 10.10.1.4
Identifier              : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration            : Completed
Management type         : Configuration
```

b) Firewall Management Center IP アドレスまたはホスト名を編集します。

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

Firewall Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

ステップ 5 コンソールポートでマネージャ アクセス インターフェイスの IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

専用管理インターフェイスを使用している場合：

configure network ipv4

configure network ipv6

専用管理インターフェイスを使用している場合：

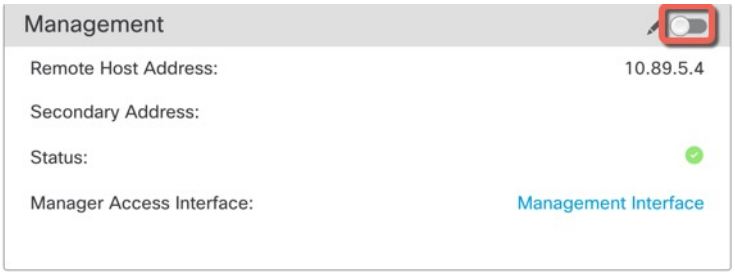
configure network management-data-interface disable

configure network management-data-interface

ステップ 6 スライダをクリックして管理を再度有効（ ）にします。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

図 *40* : 管理接続の有効化



ステップ 7 （マネージャアクセスにデータインターフェイスを使用している場合）Firewall Management Center でデータインターフェイス設定を更新します。

高可用性ペアの場合は、両方のユニットでこの手順を実行します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）]** を選択し、[更新（Refresh）] をクリックします。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** を選択し、新しいアドレスと一致するように IP アドレスを設定します。

c) [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに戻り、[確認（Acknowledge）] をクリックして展開ブロックを削除します。

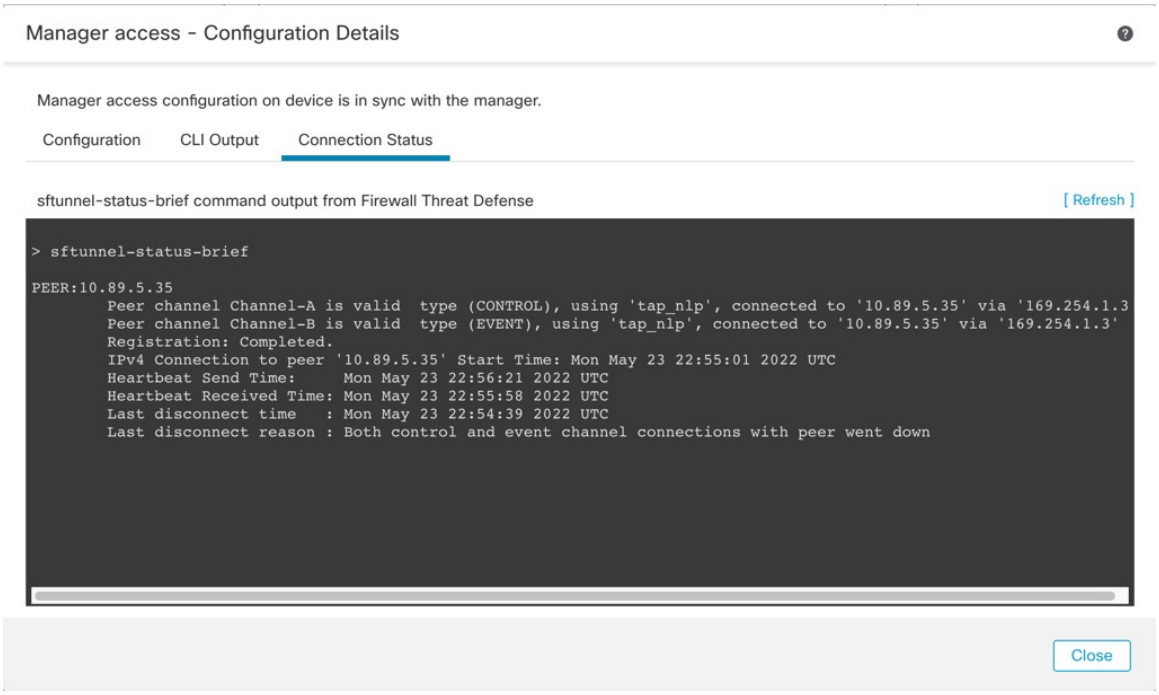
ステップ 8 管理接続が再確立されたことを確認します。

Firewall Management Center で、**[Devices]** > **[Device Management]** > **[Device]** > **[Management]** > **[Manager Access - Configuration Details]** > **[Connection Status]** ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *41* : 接続ステータス



ステップ 9 （高可用性 Firewall Management Center ペアの場合）セカンダリ Firewall Management Center で設定変更を繰り返します。

a) セカンダリ Firewall Management Center IP アドレスを変更します。
b) 両方のユニットで新しいピアアドレスを指定します。
c) セカンダリユニットをアクティブユニットにします。
d) デバイスの管理接続を無効にします。
e) Firewall Management Center でデバイスの IP アドレスを変更します。
f) 管理接続を再度有効にします。

マネージャ アクセス インターフェイスの変更

デバイスを登録したら、マネージャ アクセス インターフェイスを、管理インターフェイスまたは別のデータ インターフェイスに変更できます。

管理アクセスインターフェイスの管理からデータへの変更

専用の管理インターフェイスまたはデータインターフェイスから Firewall Threat Defense を管理できます。デバイスを Firewall Management Center に追加した後にマネージャ アクセス インターフェイスを変更する場合は、次の手順に従って管理インターフェイスからデータインターフェイスに移行します。逆の方向に移行するには、マネージャ アクセス インターフェイスをデータから管理に変更する （96 ページ）を参照してください。

管理からデータへのマネージャアクセスの移行を開始すると、Firewall Management Center は Firewall Threat Defense への展開時にブロックを適用します。ブロックを削除するには、データインターフェイスでマネージャアクセスを有効にします。

次の手順を参照して、データインターフェイスでマネージャアクセスを有効にし、その他の必要な設定も構成します。

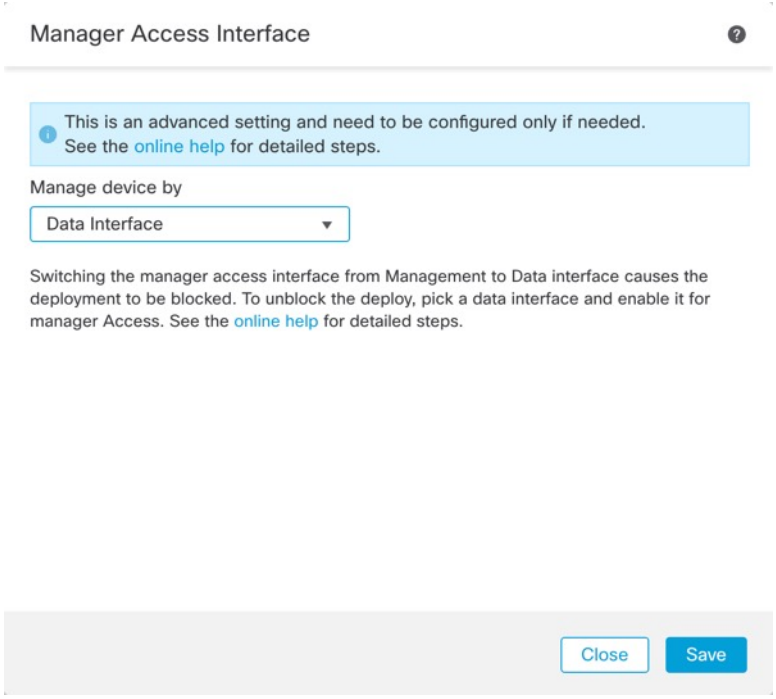
手順

ステップ 1 インターフェイスの移行を開始します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** ページで、デバイスの [編集（Edit）]（ ） をクリックします。**[デバイス（Device）]** をクリックし、**[管理（Management）]** エリアで、**[マネージャアクセスインターフェイス（Manager Access Interface）]** のリンクをクリックします。

[マネージャ アクセス インターフェイス（Manager Access Interface）] [FMCアクセスインターフェイス（FMC Access Interface）] フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理（Manage device by）] ドロップダウンリストで新しいインターフェイスタイプである [データインターフェイス（Data Interface）] を選択します。

図 *42* : マネージャ アクセス インターフェイス



b) [OK] をクリックし、[閉じる（Close）] をクリックします。

データインターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理（Management）] 領域には、[マネージャ アクセス インターフェイス：データインターフェイス（Manager Access Interface: Management Interface）] [FMCアクセスインターフェイス：データインターフェイス（FMC Access Interface: Management Interface）] と、[マネージャアクセスの詳細：構成（Manager Access Details: Configuration）] [FMCアクセスの詳細：構成（FMC Access Details: Configuration）] が表示されます。

図 *43* : マネージャアクセス

[構成（Configuration）] をクリックすると、[マネージャアクセス - 構成の詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成の詳細（FMC Access - Configuration Details）] ダイアログボックスが開きます。[マネージャアクセスモード（Manager Access Mode）] [FMCアクセスモード（FMC Access Mode）] は、展開保留状態を示しています。

ステップ 2 データインターフェイスでマネージャアクセスを有効化します。**[インターフェイス（Interface）]**、インターフェイスの [編集（Edit）]（✎）、**[マネージャアクセス（Manager Access）]**、 の順に選択します。

[管理アクセスの有効化（Enable management access）] をオンにして、[OK] をクリックします。デフォルトでは、すべてのネットワークが許可されますが、Firewall Management Center アドレスが許可されている限り、アクセスを制限できます。

マネージャ アクセス インターフェイスが静的 IP アドレスを使用している場合は、そのためのルーティングを設定するように求められます。

[インターフェイス（Interfaces）] ページで [保存（Save）] をクリックします。インターフェイス設定の詳細については、ルーテッドモードのインターフェイスの設定 （717ページ）を参照してください。マネージャアクセスは 1 つのルーテッド データ インターフェイスとオプションのセカンダリインターフェイスで有効にできます。これらのインターフェイスが名前と IP アドレスで完全に構成され、有効になっていることを確認してください。

冗長性のためにセカンダリインターフェイスを使用する場合は、必要な追加構成について冗長マネージャアクセス用データインターフェイスの設定 （66 ページ）を参照してください。

ステップ 3 （任意） インターフェイスに DHCP を使用する場合は、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [DHCP] > [DDNS]**ページで Web タイプ DDNS 方式を有効にします。

ダイナミック DNS の設定 （794 ページ）を参照してください。DDNS は、FTD の IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）で Firewall Threat Defense に到達できるようにします。

ステップ 4 Firewall Threat Defense がデータインターフェイスを介して Firewall Management Center にルーティングできることを確認します。必要に応じて、[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [スタティックルート（Static Route）] でスタティックルートを追加します。 > > >

スタティック ルートの追加 （1075 ページ）を参照してください。

ステップ 5 （任意） プラットフォーム設定ポリシーで DNS を構成し、**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [DNS]**でこのデバイスに適用します。

DNS （828 ページ）を参照してください。DDNS を使用する場合は DNS が必要です。セキュリティポリシーで FQDN に DNS を使用することもできます。

ステップ 6 （任意） プラットフォーム設定ポリシーでデータインターフェイスの SSH を有効にし、**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [セキュアシェル（Secure Shell）]**でこのデバイスに適用します。

Shellの確保 （843 ページ）を参照してください。SSH はデータインターフェイスでデフォルトで有効になっていないため、SSH を使用して Firewall Threat Defense を管理する場合は、明示的に許可する必要があります。

ステップ 7 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

マネージャ アクセス インターフェイスを変更することを確認するための検証エラーが表示されます。[警告を無視（Ignore warnings）] をオンにして、再度展開します。

Firewall Management Center は、現在の管理インターフェイスを介して設定の変更を展開します。展開後、データインターフェイスを使用できるようになりましたが、管理への元の管理接続はアクティブなままです。

ステップ 8 Firewall Threat Defense CLI（できればコンソールポートから）で、静的 IP アドレスを使用するように管理インターフェイスを設定し、データインターフェイスを使用するようにゲートウェイを設定します。

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask*：管理インターフェイスを使用する予定はありませんが、ゲートウェイを [データインターフェイス（data-interfaces）] に設定できるように、プライベートアドレスなどの静的 IP アドレスを設定する必要があります（次の箇条書きを参照）。[data-interfaces] である必要があるデフォルトルートは、DHCP サーバーから受信したルートで上書きされる可能性があるため、DHCP は使用できません。
- **data-interfaces** — この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。

管理インターフェイスのネットワーク設定を変更すると、SSH セッションが切断されるため、SSH 接続の代わりにコンソールポートを使用することをお勧めします。

ステップ 9 必要に応じて、データインターフェイスの Firewall Management Center に到達できるように Firewall Threat Defense のケーブルを再接続します。

ステップ 10 Firewall Management Center で、管理接続を無効にし、**[デバイス（Devices）]** > **[管理（Management）]** エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** ページで、Firewall Threat Defense の **[リモートホストアドレス（Remote Host Address）]**[IPアドレス（IP address）] およびオプションの **[セカンダリアドレス（Secondary Address）]** を更新し、接続を再度有効にします。

Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ）を参照してください。Firewall Threat Defense を Firewall Management Center に追加したときに Firewall Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

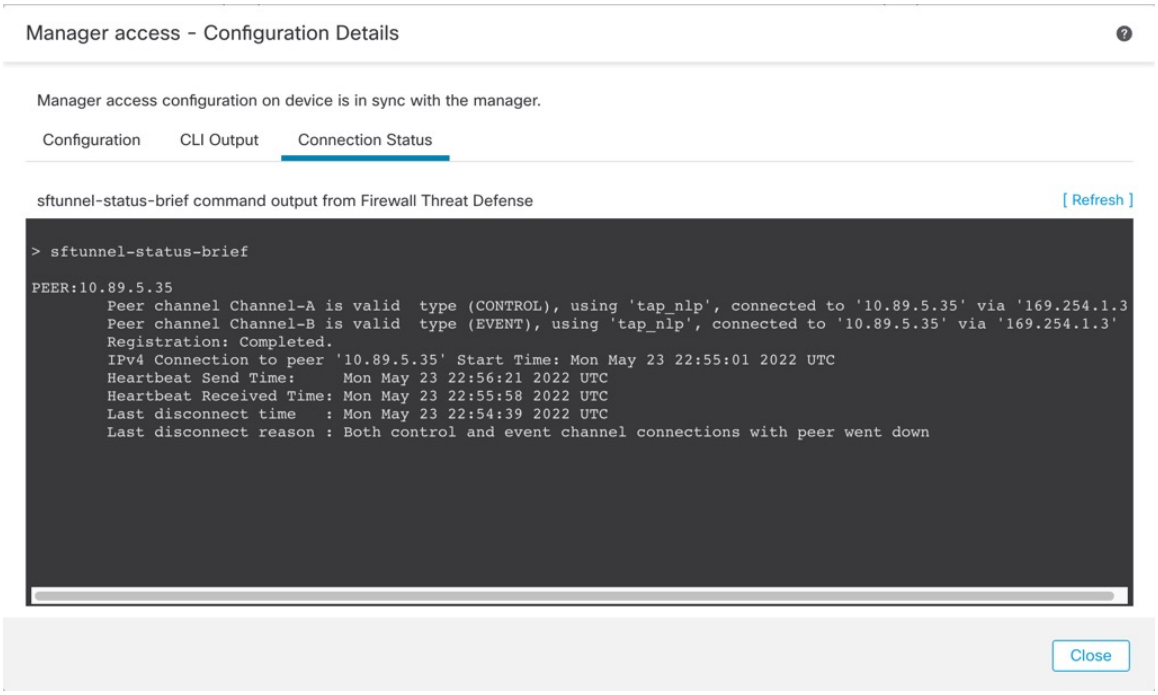
ステップ 11 管理接続が再確立されたことを確認します。

[デバイス（Device）] > **[管理（Management）]** エリアで、**[マネージャアクセス詳細：構成（Manager Access Details: Configuration）]** をクリックし、**[接続ステータス（Connection Status）]**をクリックします。

または、Firewall Threat Defense CLI で確認できます。管理接続のステータスを表示するには、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *44* : 接続ステータス



接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。「データインターフェイスでの管理接続のトラブルシューティング （106ページ）」を参照してください。

マネージャ アクセス インターフェイスをデータから管理に変更する

専用の管理インターフェイスまたはデータインターフェイスから Firewall Threat Defense を管理できます。デバイスを Firewall Management Center に追加した後にマネージャ アクセス インターフェイスを変更する場合は、次の手順に従ってデータインターフェイスから管理インターフェイスに移行します。逆の方向に移行するには、管理アクセスインターフェイスの管理からデータへの変更 （92 ページ）を参照してください。

データから管理へのマネージャアクセスの移行を開始すると、Firewall Management Center は Firewall Threat Defense への展開時にブロックを適用します。ブロックを削除するには、データインターフェイスでマネージャアクセスを無効にする必要があります。

次の手順を参照して、データインターフェイスでマネージャアクセスを無効にし、その他の必要な設定も構成します。

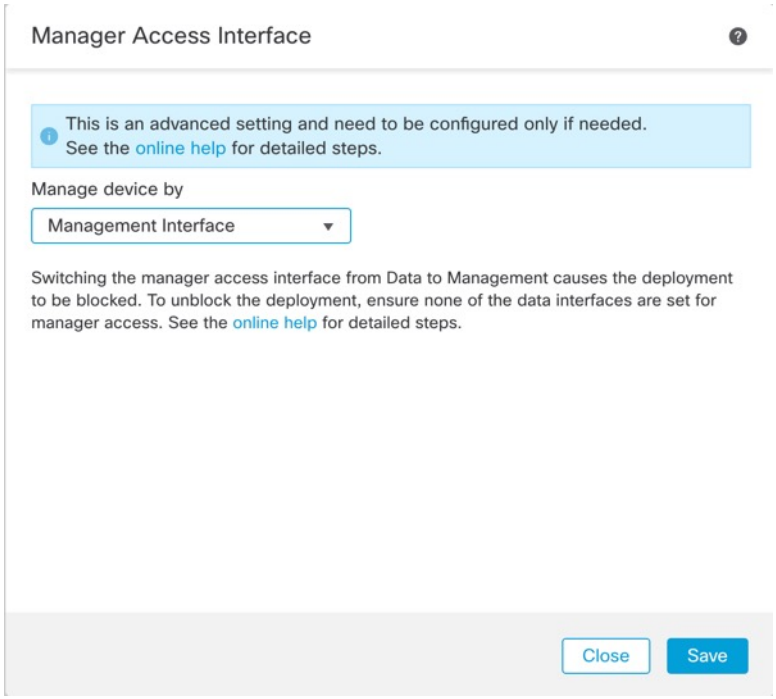
手順

ステップ 1 インターフェイスの移行を開始します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** ページで、デバイスの [編集（Edit）]（✎） をクリックします。**[デバイス（Device）]** をクリックし、**[管理（Management）]** エリアで、**[マネージャアクセスインターフェイス（Manager Access Interface）]** のリンクをクリックします。

[マネージャ アクセス インターフェイス（Manager Access Interface）] [FMCアクセスインターフェイス（FMC Access Interface）] フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理（Manage device by）] ドロップダウンリストで新しいインターフェイスタイプである [管理インターフェイス（Management Interface）] を選択します。

図 *45*：マネージャ アクセス インターフェイス



b) [保存（Save）] をクリックします。

[OK] をクリックし、[閉じる（Close）] をクリックします。

管理インターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理（Management）] 領域には、**[マネージャ アクセス インターフェイス：管理インターフェイス（Manager Access Interface: Management Interface）]**が表示されます。

図 *46 :* マネージャアクセス

ステップ 2 データインターフェイスでマネージャアクセスを無効にします。**[インターフェイス（Interface）]**、インターフェイスの [編集（Edit）]（✎）、**[マネージャアクセス（Manager Access）]**、 の順に選択します。

[管理アクセスの有効化（Enable management access）] をオフにして、[OK] をクリックします。[インターフェイス（Interfaces）] ページで [保存（Save）] をクリックします。この手順により、展開時のブロックが削除されます。

ステップ 3 まだ行っていない場合は、プラットフォーム設定ポリシーでデータインターフェイスの DNS 設定を構成し、**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [DNS]** でこのデバイスに適用します。

DNS （828 ページ）を参照してください。データインターフェイスでマネージャアクセスを無効にする Firewall Management Center 展開では、ローカル DNS 設定が削除されます。その DNS サーバーがアクセスルールの FQDN などのセキュリティポリシーで使用されている場合は、Firewall Management Center を使用して DNS 設定を再適用する必要があります。

ステップ 4 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

Firewall Management Center は、現在のデータインターフェイスを介して設定の変更を展開します。

ステップ 5 必要に応じて、管理インターフェイスの Firewall Management Center に到達できるように Firewall Threat Defense のケーブルを再接続します。

ステップ 6 Firewall Threat Defense CLI で、静的 IP アドレスまたは DHCP を使用して、管理インターフェイスの IP アドレスとゲートウェイを設定します。

最初にマネージャアクセス用のデータインターフェイスを設定したとき、管理ゲートウェイはデータインターフェイスに設定されていました。これにより、バックプレーン経由で管理トラフィックが転送され、マネージャ アクセス データ インターフェイスを介してルーティングできるようになりました。ここで、管理ネットワーク上のゲートウェイの IP アドレスを設定する必要があります。

スタティック IP アドレス：

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP：

configure network{**ipv4** | **ipv6**} **dhcp**

ステップ 7 Firewall Management Center で、管理接続を無効にし、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[管理（Management）]** セクションで Firewall Threat Defense の **[リモートホストアドレス（Remote Host Address）]** IP アドレスとオプションの [セカンダリアドレス（Secondary Address）] を更新して、接続を再度有効にします。

Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ）を参照してください。Firewall Threat Defense を Firewall Management Center に追加したときに Firewall Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

ステップ 8 管理接続が再確立されたことを確認します。

Firewall Management Center で、[デバイス（Devices）] [デバイス管理（Device Management）] [デバイス（Device）] [管理（Management）] [ステータス（Status）] フィールドで管理接続ステータスを確認するか、Firewall Management Center で通知を表示します。 > > > >

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。「データインターフェイスでの管理接続のトラブルシューティング （106 ページ）」を参照してください。

データインターフェイス管理用のマネージャアクセスの詳細を表示する

専用の管理インターフェイスを使用する代わりに、Firewall Management Center 管理にデータインターフェイスを使用する場合は、Firewall Management Centerでデバイスのインターフェイスとネットワークの設定を変更するときに接続を中断しないように注意します。デバイスのデータインターフェイス設定をローカルで変更することもできます。その場合は、Firewall Management Center でそれらの変更を手動で調整する必要があります。[デバイス（Devices）]>[デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details）] ダイアログボックスは、Firewall Management Center と Firewall Threat Defense のローカル設定の間の矛盾を解決するために役立ちます。 > > > >

通常、Firewall Threat Defense を Firewall Management Center に追加する前に、Firewall Threat Defense の初期設定の一環としてマネージャアクセスデータインターフェイスを構成します。Firewall Threat Defense を Firewall Management Center に追加すると、Firewall Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバーの場合、登録中に検出された場合、構成はローカルに保持されます。ただし、Firewall Management Center のプラットフォーム設定ポリシーには追加されません。

Firewall Threat Defense を Firewall Management Center に追加した後、**configure network management-data-interface** コマンドを使用してローカルで Firewall Threat Defense のデータインターフェイス構成を変更すると、Firewall Management Center が構成変更を検出し、Firewall Threat Defense への展開をブロックします。Firewall Management Center は、以下のいずれかの方法を使用して構成の変更を検出します。

- Firewall Threat Defense への展開。Firewall Management Center の展開の前に、構成の差異を検出してデプロイを停止します。
- [インターフェイス（Interfaces）] ページの [同期（Sync）] ボタン。
- [マネージャアクセス - 構成の詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成の詳細（FMC Access - Configuration Details）] ダイアログボックスの [更新（Refresh）] ボタン

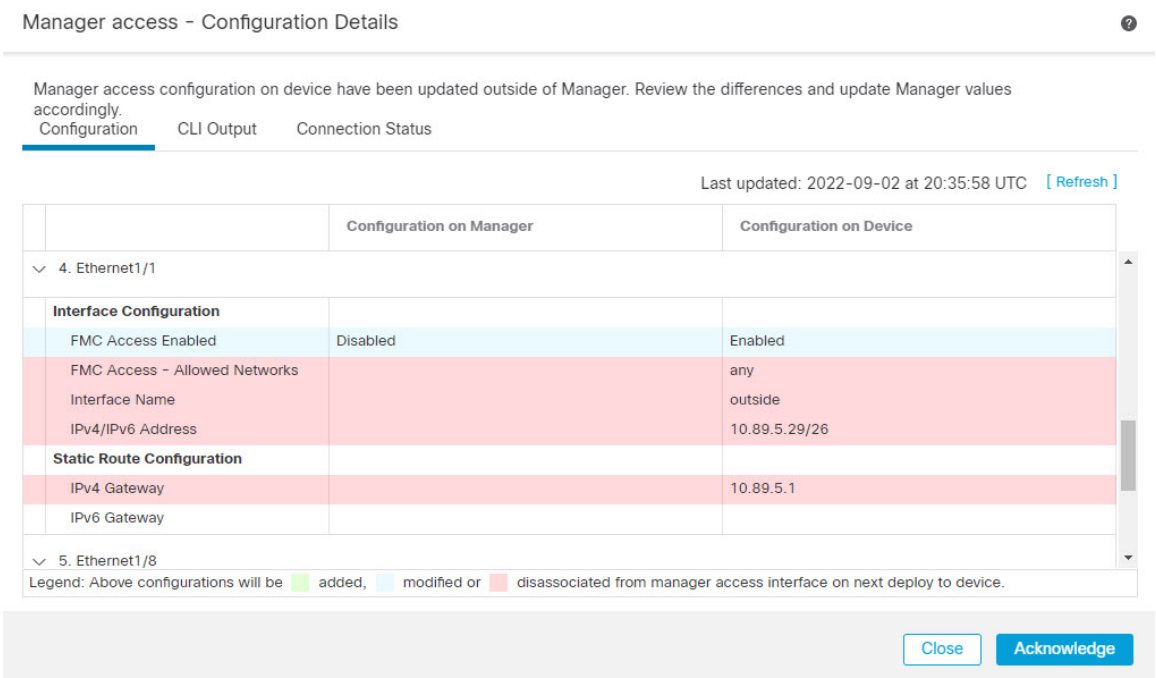
ブロックを削除するには、[マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに移動し、[確認（Acknowledge）] をクリックする必要があります。Firewall Management Center 設定は、次回展開時に Firewall Threat Defense の残りの競合する設定を上書きします。再展開の前に Firewall Management Center の設定を手動で修正する必要があります。

このダイアログボックスに関する以下のページを参照してください。

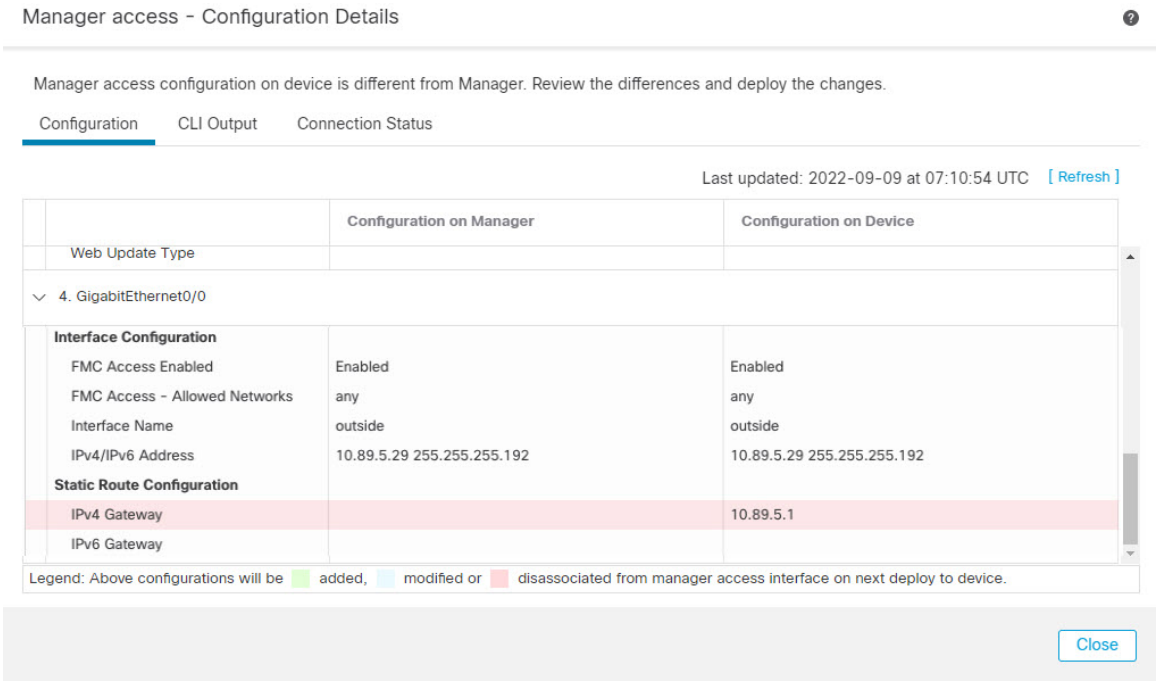
設定

Firewall Management Center および Firewall Threat Defense のマネージャ アクセス データ インターフェイスの構成比較を表示します。

次の例は、**configure network management-data-interface** コマンドが Firewall Threat Defense に入力された Firewall Threat Defense の構成詳細を示しています。ピンクのハイライトは、相違点を**確認**したものの、Firewall Management Center の構成と一致しない場合、Firewall Threat Defense の構成が削除されることを示しています。青色のハイライトは、Firewall Threat Defense で変更される構成を示しています。緑のハイライトは、Firewall Threat Defense に追加される構成を示しています。



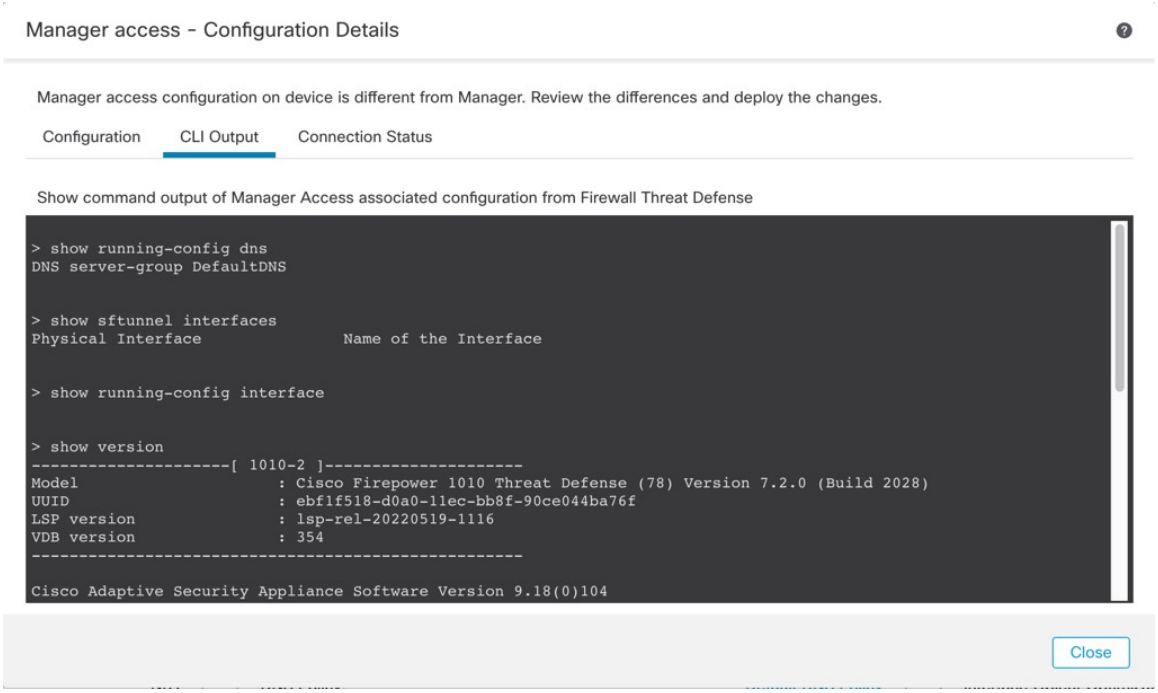
Firewall Management Center でインターフェイスを設定した後のこのページの例を以下に示します。インターフェイス設定が一致し、ピンクのハイライトが消えています。

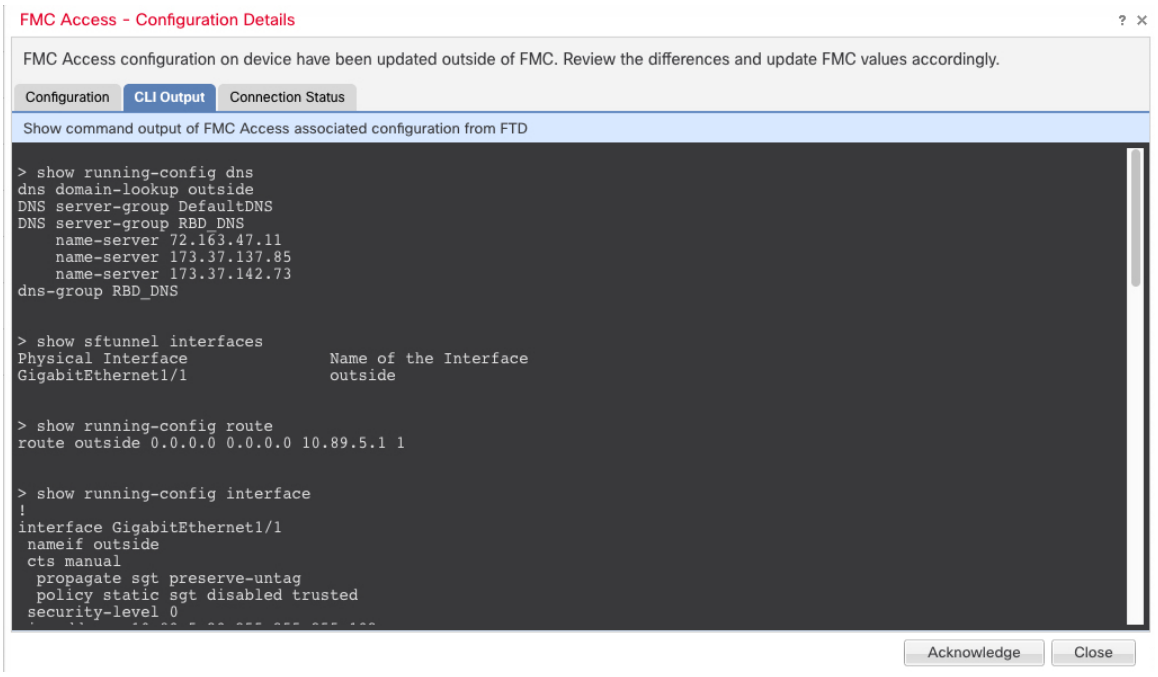


CLI 出力

マネージャ アクセス データ インターフェイスの CLI 構成を表示します。これは、基盤となる CLI に精通している場合に役立ちます。

図 *47 : CLI* 出力

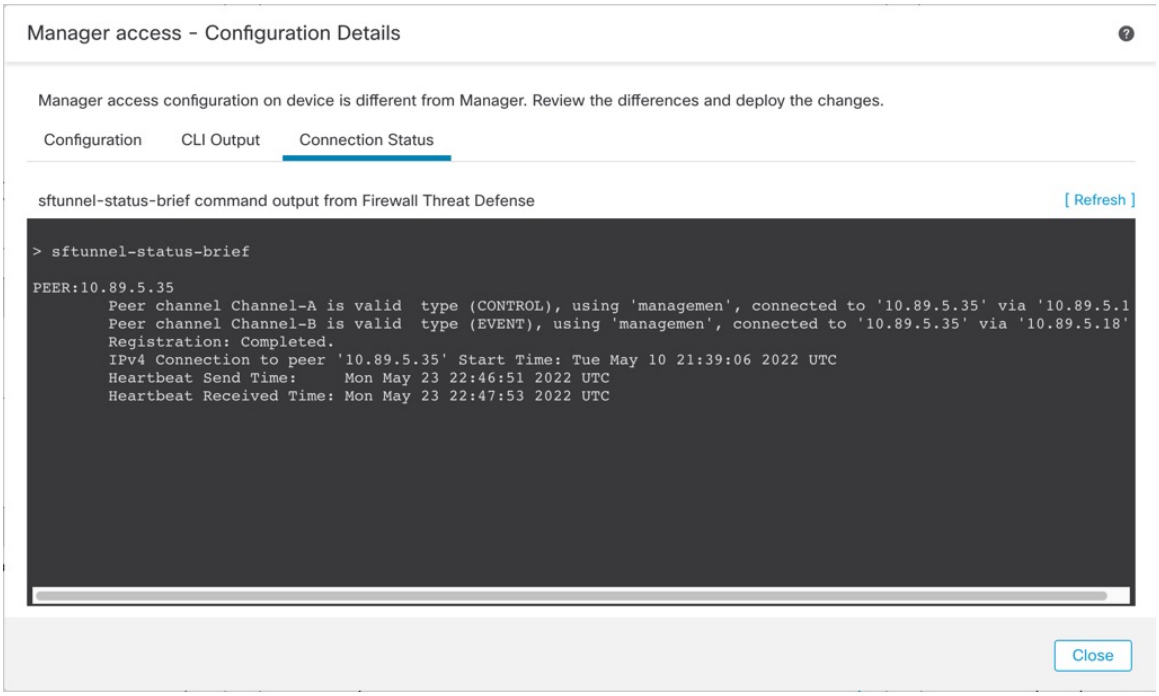




接続ステータス

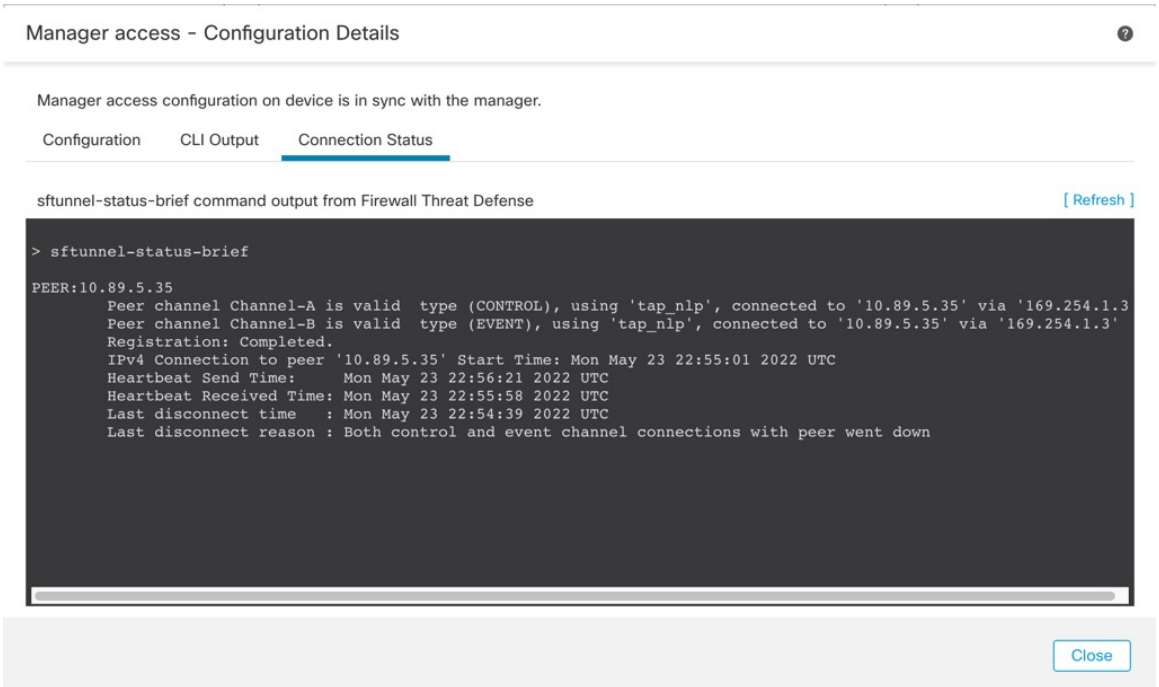
管理接続ステータスの表示次の例は、管理接続で引き続き管理「management0」インターフェースが使用されていることを示しています。

図 *48* : 接続ステータス



次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *49* : 接続ステータス



ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

管理接続のトラブルシューティング

•

Firewall Management Center の接続が失われた場合の構成の手動ロールバック

Firewall Threat Defense でマネージャアクセス用にデータインターフェイスを使用し、ネットワーク接続に影響する Firewall Management Center からの構成変更を展開する場合、Firewall Threat Defense の構成を最後に展開した構成にロールバックして、管理接続を復元できます。その後、ネットワーク接続が維持されるように Firewall Management Center で構成設定を調整し、再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

または、展開後に接続が失われた場合は、構成の自動ロールバックを有効にすることもできます。展開設定の編集 （118 ページ） を参照してください。

次のガイドラインを参照してください。

- 前回の展開のみ Firewall Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性ではサポートされていますが、クラスタリングの展開ではサポートされていません。
- ロールバックは、Firewall Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Firewall Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network**

management-data-interface コマンドを使用した最後の Firewall Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Firewall Management Center 設定にロールバックされます。

- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

ステップ 1 Firewall Threat Defense CLI で、以前の構成へロールバックします。

configure policy rollback

ロールバック後、Firewall Threat Defense はロールバックが正常に完了したことを Firewall Management Center に通知します。Firewall Management Center では、構成がロールバックされたことを示すバナーが展開画面に表示されます。

（注）
ロールバックが失敗し、Firewall Management Center 管理が復元された場合、一般的な展開の問題についてhttps://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.htmlを参照してください。場合によっては、Firewall Management Center 管理アクセスの復元後にロールバックが失敗することがあります。この場合、Firewall Management Center 構成の問題を解決して、Firewall Management Center から再展開できます。

例：

マネージャアクセスにデータインターフェイスを使用する Firewall Threat Defense の場合：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

ステップ 2 管理接続が再確立されたことを確認します。

Firewall Management Center で、**[Devices]** > **[Device Management]** > **[Device]** > **[Management]** > **[Manager Access - Configuration Details]** > **[Connection Status]** ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。「データインターフェイスでの管理接続のトラブルシューティング（106ページ）」を参照してください。

データインターフェイスでの管理接続のトラブルシューティング

専用の管理インターフェイスを使用する代わりに、マネージャアクセスにデータインターフェイスを使用する場合は、Firewall Management Center で Firewall Threat Defense のインターフェイスとネットワークの設定を変更する際、接続を中断しないように注意します。Firewall Threat Defense を Firewall Management Center に追加した後に管理インターフェイスタイプを変更する場合（データから管理へ、または管理からデータへ）、インターフェイスとネットワークの設定が正しく構成されていないと、管理接続が失われる可能性があります。

このトピックは、管理接続が失われた場合のトラブルシューティングに役立ちます。

管理接続ステータスの表示

Firewall Management Center で、**[Devices]** > **[Device Management]** > **[Device]** > **[Management]** > **[Manager Access - Configuration Details]** > **[Connection Status]** ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went
down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
```

```
'10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Firewall Threat Defense ネットワーク情報の表示

Firewall Threat Defense CLI で、管理および マネージャ アクセス データ インターフェイスのネットワーク設定を表示します。

show network

```
> show network
===============[ System Information ]===============
Hostname                  : FTD-4
Domains                   : cisco.com
DNS Servers               : 72.163.47.11
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces

==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : 1gbps
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.4
Netmask                   : 255.255.255.192
Gateway                   : 169.254.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               : 72.163.47.11
Interfaces                : Ethernet1/1

==================[ Ethernet1/1 ]===================
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:A4
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.6
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
```

```
Configuration            : Disabled
```

Firewall Management Center への Firewall Threat Defense の登録の確認

Firewall Threat Defense CLI で、Firewall Management Center 登録が完了したことを確認します。このコマンドは、管理接続の現在のステータスを表示するものではないことに注意してください。

show managers

```
> show managers
Type                     : Manager
Host                     : 10.10.1.4
Display name             : 10.10.1.4
Identifier               : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration             : Completed
Management type          : Configuration
```

Firewall Management Center に ping する

Firewall Threat Defense CLI で、次のコマンドを使用して、データインターフェイスから Firewall Management Center に ping します。

ping *fmc_ip*

Firewall Threat Defense CLI で、次のコマンドを使用して、管理インターフェイスから Firewall Management Center に ping します。これは、バックプレーンを介してデータインターフェイスにルーティングされます。

ping system *fmc_ip*

Firewall Threat Defense 内部インターフェイスでのパケットのキャプチャ

Firewall Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

内部インターフェイスのステータス、統計、およびパケット数の確認

Firewall Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）に関する情報を参照してください。

show interface detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

ルーティングと NAT の確認

Firewall Threat Defense CLI で、デフォルトルート（S*）が追加されていること、および管理インターフェイス（nlp_int_tap）に内部 NAT ルールが存在することを確認します。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface
service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
 tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
```

```
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
 ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、Firewall Management Center の **[Devices]** > **[Device Management]** > **[Device]** > **[Management]** > **[Manager Access - Configuration Details]** > **[CLI Output]** ページでも確認できます。

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
       preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

DDNS の更新が成功したかどうかを確認する

Firewall Threat Defense CLI で、DDNS の更新が成功したかどうかを確認します。

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

更新に失敗した場合は、**debug http** コマンドと **debug ssl** コマンドを使用します。証明書の検証が失敗した場合は、ルート証明書がデバイスにインストールされていることを確認します。

show crypto ca certificates *trustpoint_name*

DDNS の動作を確認するには：

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Firewall Management Center ログファイルの確認

https://cisco.com/go/fmc-reg-error を参照してください。

インベントリ詳細の表示

[デバイス（Device）] ページの [インベントリの詳細（Inventory Details）] セクションには、シャーシの詳細情報（CPU やメモリなど）が表示されます。

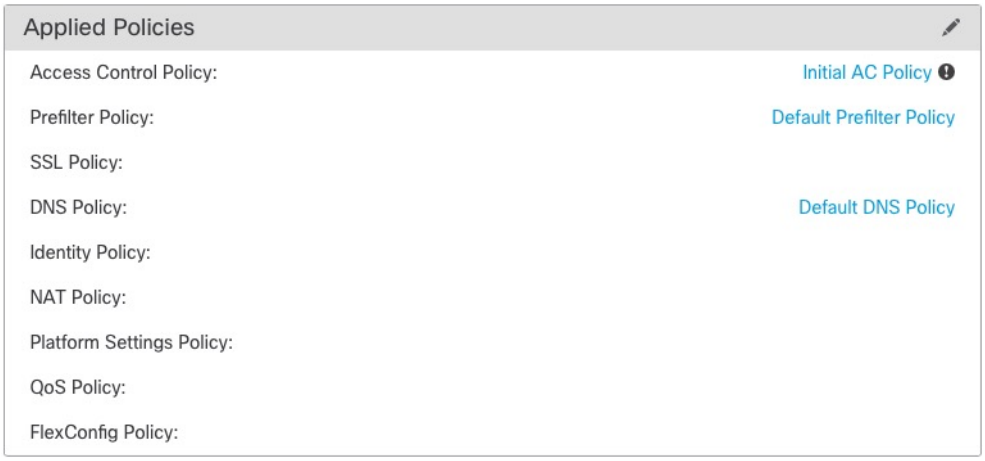
図 *50* : インベントリの詳細（*Inventory Details*）

情報を更新するには、[更新（Refresh）]（）をクリックします。

適用されたポリシーの編集

[デバイス（Device）] ページの [適用されたポリシー（Applied Policies）] セクションには、ファイアウォールに適用されている次のポリシーが表示されます。

図 *51 : [*適用されたポリシー（***Applied Policies***）*]*



リンクのあるポリシーの場合、リンクをクリックしてポリシーを表示できます。

アクセス コントロール ポリシーについては、[感嘆符（Exclamation）]（） アイコンをクリックして [トラブルシューティングのためのアクセスポリシー情報（Access Policy Information for Troubleshooting）] ダイアログボックスを表示します。このダイアログボックスには、アクセス ルールがアクセス コントロール エントリ（ACE）に展開される方法が表示されます。

図 *52 : [*トラブルシューティングのためのアクセスポリシー情報（***Access Policy Information for Troubleshooting***）*]*

[デバイス管理（Device Management）] ページから、個々のデバイスにポリシーを割り当てることができます。

手順

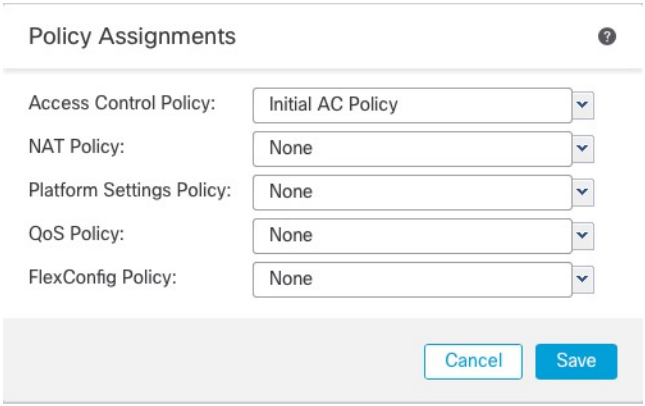
ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

ステップ 2 ポリシーを割り当てるデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [適用されたポリシー（Applied Policies）] セクションで、[編集（Edit）]（✎） をクリックします。

図 *53* : ポリシー割り当て



ステップ 5 ポリシータイプごとに、ドロップダウンメニューからポリシーを選択します。既存のポリシーのみが一覧表示されます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

詳細設定の編集

[デバイス（Device）] ページの [詳細設定（Advanced Settings）] セクションには、以下で説明する詳細設定のテーブルが表示されます。これらの設定はいずれも編集できます。

表 *6* : *[詳細設定（Advanced）]* セクションのテーブルのフィールド

フィールド	説明
アプリケーションバイパス（Application Bypass）	デバイスでの自動アプリケーション バイパスの状態。

フィールド	説明
バイパスしきい値（Bypass Threshold）	自動アプリケーション バイパスのしきい値（ミリ秒）。
オブジェクトグループの検索	デバイスでのオブジェクトグループ検索の状態。動作中、FTD デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイス オブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイス オブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されるか、または Firepower Management Center にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。 （注） デフォルトでは、Management Center で初めて Threat Defense を追加すると、[オブジェクトグループ検索（Object Group Search）] が有効になります。
インターフェイス オブジェクトの最適化	デバイスでのインターフェイス オブジェクトの最適化の状態。展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに 1 つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。このオプションを選択する場合は、[オブジェクトグループ検索（Object Group Search）] オプションも選択して、デバイスのメモリ使用量を減らします。

次のトピックでは、デバイスの詳細設定を編集する方法について説明します。

（注） [パケットの転送（Transfer Packets）] 設定については、全般設定の編集 （55 ページ）を参照してください。

自動アプリケーションバイパスの設定

自動アプリケーションバイパス（AAB）を使用すると、Snort がダウンしている場合や、従来型デバイスで、パケットの処理に時間がかかりすぎる場合に、パケットが検出をバイパスできます。AAB により、Snort は障害から 10 分以内に再起動します。また、Snort 障害の原因を調査するために分析できるトラブルシューティング データが生成されます。

⚠

注意 AAB のアクティブ化は、いくつかのパケットのインスペクションを一時的に中断する Snort プロセスを部分的に再起動します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。

次の動作を確認してください。

Firewall Threat Defense の動作：Snort がダウンしている場合、指定されたタイマー期間の後に AAB がトリガーされます。Snort が稼働している場合、パケット処理が設定されたタイマーを超えても、AAB はトリガーされません。

従来型デバイスの動作：AAB は、インターフェイスを介してパケットを処理するために許可される時間を制限します。パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。

この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

一般に、遅延しきい値を超えた後は、高速パス パケットに対して侵入ポリシーの [ルール遅延しきい値（Rule Latency Thresholding）] を使用します。[ルール遅延しきい値（Rule Latency Thresholding）]により、エンジンがシャットダウンされたり、トラブルシューティング データが生成されることはありません。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。

AAB はデフォルトで無効になっています。AAB を有効にするには、次の手順を実行します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 詳細設定を編集するデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [デバイス（Devices）] をクリックし、[詳細設定（Advanced Settings）] セクションの [編集（Edit）]（✎） をクリックします。

ステップ 4 [自動アプリケーション バイパス（Automatic Application Bypass）] をオンにします。

ステップ 5 [バイパスしきい値（Bypass Threshold）] に 250 ～ 60,000 ミリ秒を入力します。デフォルト設定は 3000 ミリ秒（ms）です。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

オブジェクトグループ検索の構成

動作中、Firewall Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイスオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイスオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されているかや、Firewall Management Center にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。

オブジェクトグループ検索を有効にすると、ネットワークオブジェクトまたはインターフェイスオブジェクトを含むアクセスコントロールポリシーのメモリ要件が軽減されます。ただし、オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU使用率が増大する可能性があることに注意してください。CPU に対する影響と、特定のアクセスコントロールポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。

デフォルトでは、Firewall Management Center で初めて追加された Threat Defense デバイスではオブジェクトグループ検索が有効になっています。アップグレードされたデバイスの場合、デバイスでオブジェクトグループ検索が無効に設定されている場合は、手動で有効にする必要があります。一度に1つのデバイスで有効にできます。グローバルに有効にすることはできません。ネットワークオブジェクトまたはインターフェイスオブジェクトを使用するアクセスルールを展開するすべてのデバイスで有効にすることを推奨します。

（注） オブジェクトグループの検索を有効にしてから、デバイスを設定し、しばらくの間操作した場合、後からこの機能を無効にすると、望ましくない結果になる可能性があることに注意してください。オブジェクトグループの検索を無効にすると、既存のアクセス制御ルールがデバイスの実行コンフィギュレーションで拡張されます。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。デバイスが正常に動作している場合は、一度有効にしたオブジェクトグループ検索を無効にしないでください。

始める前に

- モデルのサポート：Threat Defense
- 各デバイスでトランザクションコミットも有効にすることを推奨します。デバイスCLIから **asp rule-engine transactional-commit access-group** コマンドを入力します。
- この設定を変更すると、デバイスがACLを再コンパイルしている間、システムの動作が中断される可能性があります。この設定はメンテナンス期間中にのみ変更することを推奨します。
- FlexConfigを使用して **object-group-search threshold** コマンドを設定し、しきい値を有効にしてパフォーマンスの低下を防止することができます。しきい値を使用した動作では、接続ごとに送信元と宛先の両方のIPアドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の1万倍を超えると接続が切断されます。一致件数が膨大になることを防ぐためにルールを設定します。

手順

ステップ1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ2 ルールを設定するFirewall Threat Defenseデバイスの横にある[編集（Edit）]（✎）をクリックします。

ステップ3 [デバイス（Devices）]タブをクリックし、[詳細設定（Advanced Settings）]セクションの[編集（Edit）]（✎）をクリックします。

ステップ4 [オブジェクトグループの検索（Object Group Search）]をオンにします。

ステップ5 ネットワークオブジェクトに加えてインターフェイス オブジェクトでオブジェクトグループの検索を機能させるには、[インターフェイスオブジェクトの最適化（Interface Object Optimization）]をオンにします。

[インターフェイスオブジェクトの最適化（Interface Object Optimization）]を選択しない場合は、システムで、ルールで使用されているセキュリティゾーンとインターフェイスグループが使用されずに、送信元/インターフェイスのペアごとに個別のルールが展開されます。これは、インターフェイスグループがオブジェクトグループの検索処理に使用できないことを意味します。

ステップ6 [保存（Save）]をクリックします。

インターフェイス オブジェクトの最適化の設定

展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィ

ルタルールごとに1つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。このオプションを選択する場合は、[オブジェクトグループ検索（Object Group Search）]オプションも選択して、デバイスのメモリ使用量を減らします。

インターフェイス オブジェクトの最適化はデフォルトで無効になっています。一度に1つのデバイスで有効にできます。グローバルに有効にすることはできません。

（注） インターフェイス オブジェクトの最適化を無効にすると、既存のアクセス制御ルールはインターフェイス オブジェクトを使用せずに展開されるため、展開に時間がかかる場合があります。また、オブジェクトグループ検索が有効になっている場合、その利点はインターフェイスオブジェクトには適用されず、デバイスの実行中の設定のアクセス制御ルールが拡張されることがあります。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。

始める前に

モデルのサポート：Threat Defense

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 2 ルールを設定する FTD デバイスの横にある[編集（Edit）]（✎）をクリックします。

ステップ 3 [デバイス（Devices）]タブをクリックし、[詳細設定（Advanced Settings）]セクションの[編集（Edit）]（✎）をクリックします。

ステップ 4 [インターフェイスオブジェクトの最適化（Interface Object Optimization）]をオンにします。

ステップ 5 [保存（Save）]をクリックします。

展開設定の編集

[Device] ページの [Deployment Settings] セクションには、以下の表に記載された情報が表示されます。

図 *54 :* 展開設定

表 7: 展開設定

フィールド	説明
Auto Rollback Deployment if Connectivity Fails	[Enabled] と [Disabled] があります。 展開の結果として管理接続が失敗した場合は、自動ロールバックを有効にすることができます。特に、管理センターへのアクセスにデータを使用し、データインターフェイスを誤って構成した場合に当てはまります。
Connectivity Monitor Interval (in Minutes)	構成をロールバックする前に待機する時間を示します。

[デバイス管理（Device Management）]ページから展開設定を設定できます。展開設定には、展開の結果として管理接続が失敗した場合の展開の自動ロールバックの有効化が含まれます。特に、管理センターへのアクセスにデータを使用し、データインターフェイスを誤って構成した場合です。代替として、**configure policy rollback** コマンドを使用して、構成を手動でロールバックすることもできます（Firewall Management Center の接続が失われた場合の構成の手動ロールバック （104 ページ）を参照）。

次のガイドラインを参照してください。

- 前回の展開のみ Firewall Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性ではサポートされていますが、クラスタリングの展開ではサポートされていません。
- ロールバックは、Firewall Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Firewall Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Firewall Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Firewall Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

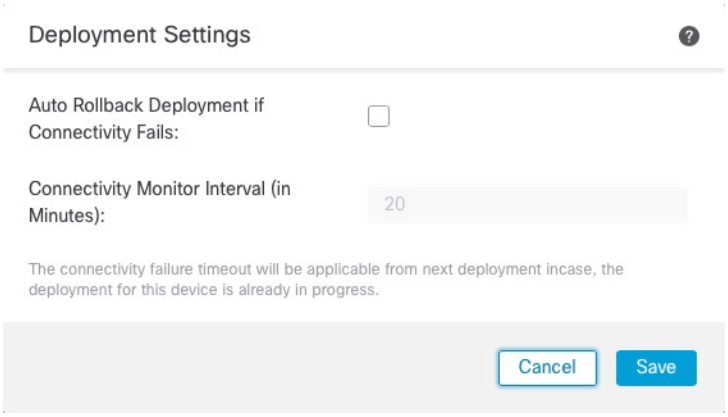
ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 2 ポリシーを割り当てるデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [展開設定（Deployment Settings）] セクションで、[編集（Edit）]（✎） をクリックします。

図 *55 :* 展開設定



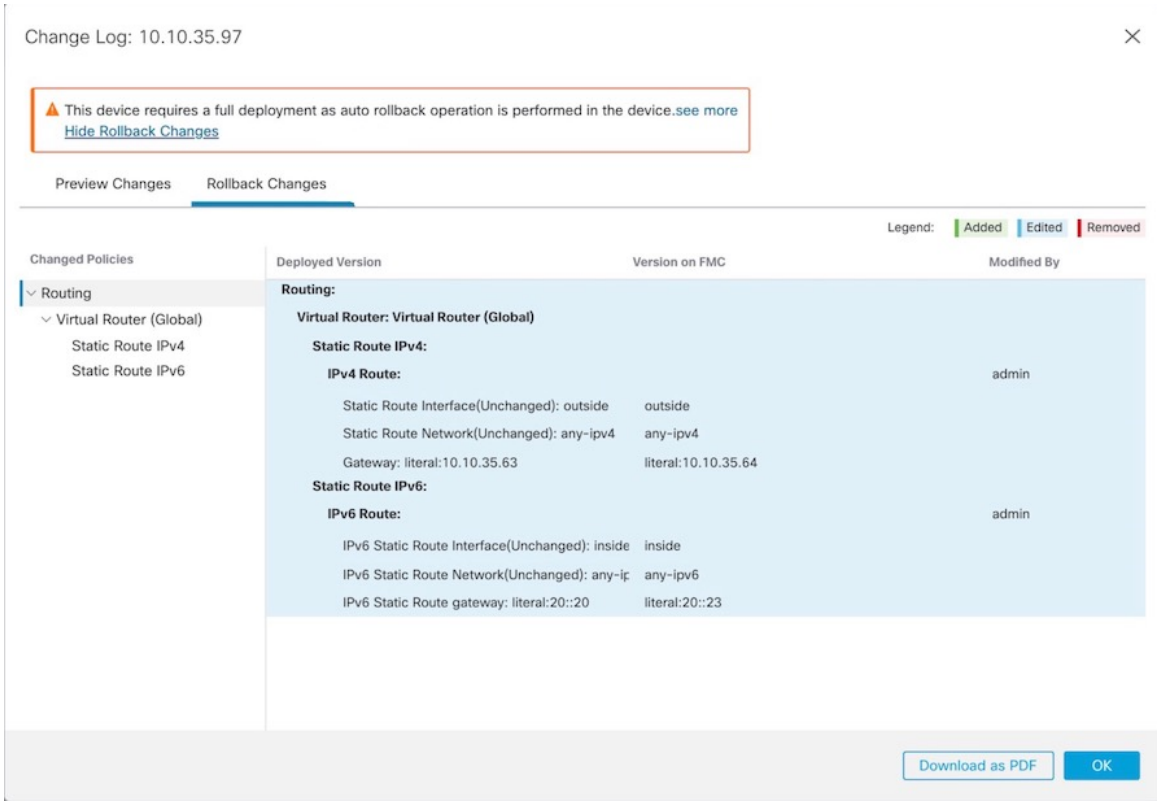
ステップ 5 自動ロールバックを有効にするには、[接続が失敗した場合の自動ロールバック展開（Auto Rollback Deployment if Connectivity Fails）] をオンにします。

ステップ 6 [接続モニタ間隔（分）（Connectivity Monitor Interval (in Minutes)）] を設定して、構成をロールバックする前に待機する時間を設定します。デフォルトは 20 分です。

ステップ 7 ロールバックが発生した場合は、次の手順について以下を参照してください。

- 自動ロールバックが成功した場合は、フル展開を行うように指示する成功メッセージが表示されます。
- **[展開（Deploy）]** > **[高度な展開（Advanced Deploy）]** 画面に移動し、[プレビュー（Preview）]（🔍） アイコンをクリックして、ロールバックされた設定の一部を表示することもできます（設定変更の展開 （172 ページ）を参照）。[ロールバックの変更を表示（Show Rollback Changes）] をクリックして変更を表示し、[ロールバックの変更を非表示（Hide Rollback Changes）] をクリックして変更を非表示にします。

図 *56* : ロールバックの変更



- [展開履歴のプレビュー（Deployment History Preview）] で、ロールバックの変更を表示できます。「展開履歴の表示 （180 ページ）」を参照してください。

ステップ 8 管理接続が再確立されたことを確認します。

Firewall Management Center で、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[デバイス（Device）]**>**[管理（Management）]**>**[FMCアクセスの詳細（FMC Access Details）]**>**[接続ステータス（Connection Status）]**ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。「データインターフェイスでの管理接続のトラブルシューティング （106 ページ）」を参照してください。

クラスタのヘルスモニター設定の編集

[クラスタ（Cluster）]ページの[クラスタヘルスモニターの設定（Cluster Health Monitor Settings）]セクションには、次の表で説明されている設定が表示されます。

図 *57 :* クラスタのヘルスモニターの設定

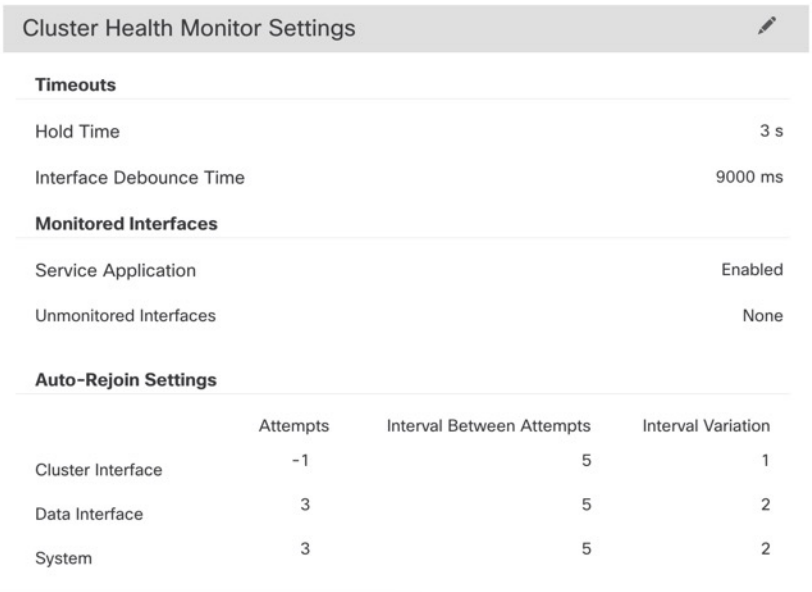


表 *8 : [*クラスタヘルスモニターの設定（***Cluster Health Monitor Settings***）*]* セクションテーブルのフィールド

フィールド	説明
タイムアウト（Timeouts）	
保留時間（Hold Time）	指定できる範囲は 0.3 ～ 45 秒です。デフォルトは 3 秒です。ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間（Interface Debounce Time）	指定できる範囲は 300 ～ 9000 ミリ秒です。デフォルトは 500 ms です。インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると見なされ、クラスタからノードが削除されるまでの時間です。
Monitored Interfaces（モニタリング対象インターフェイス）	インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。

フィールド	説明
サービスアプリケーション（Service Application）	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。
モニタリング対象外のインターフェイス（Unmonitored Interfaces）	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定（Auto-Rejoin Settings）	
クラスタインターフェイス（Cluster Interface）	クラスタ制御リンクに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは -1（無制限）です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 1 倍です。試行ごとに間隔を長くするかどうかを定義します。
データインターフェイス（Data Interfaces）	データインターフェイスに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。
システム（System）	内部エラーが発生した後に自動再結合の設定を表示します。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。

（注） システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

これらの設定は、このセクションから変更できます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI やBVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

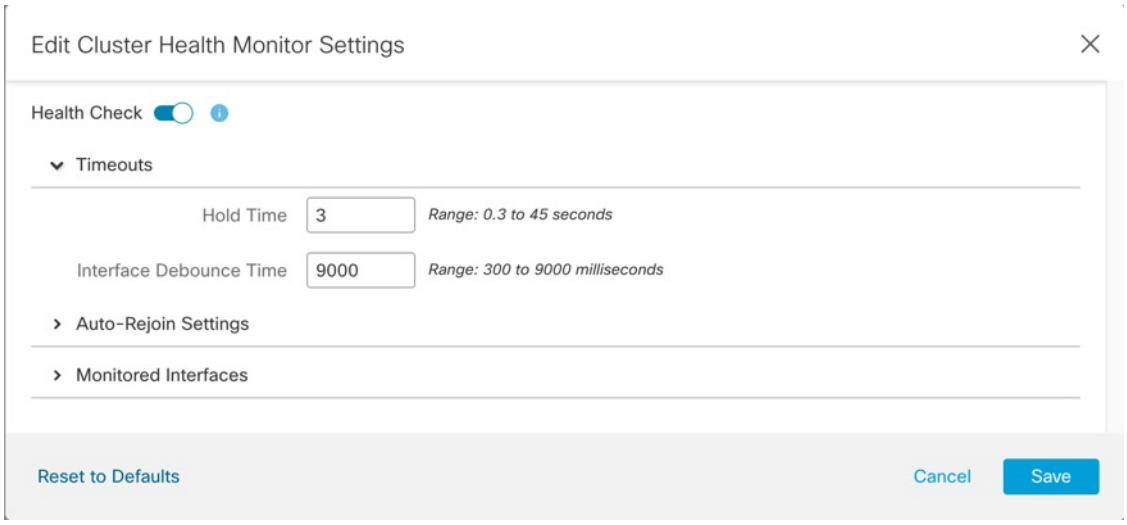
ステップ 2 変更するクラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [クラスタ（Cluster）] をクリックします。

ステップ 4 [クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）] セクションで、[編集（Edit）]（✎） をクリックします。

ステップ 5 [ヘルスチェック（Health Check）] スライダをクリックして、システムのヘルスチェックを無効にします。

図 *58 :* システムヘルスチェックの無効化



何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノー

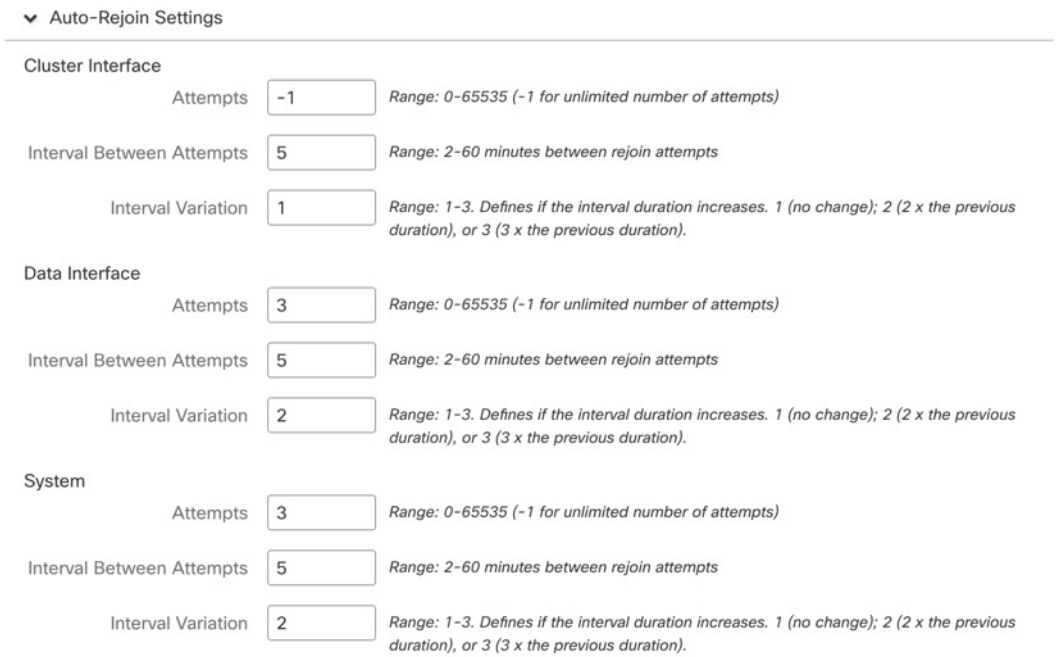
ドに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間（Hold Time）]：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ～ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間（Interface Debounce Time）]：デバウンス時間は 300 ～ 9000 ms の範囲で値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 *59*：自動再結合の設定

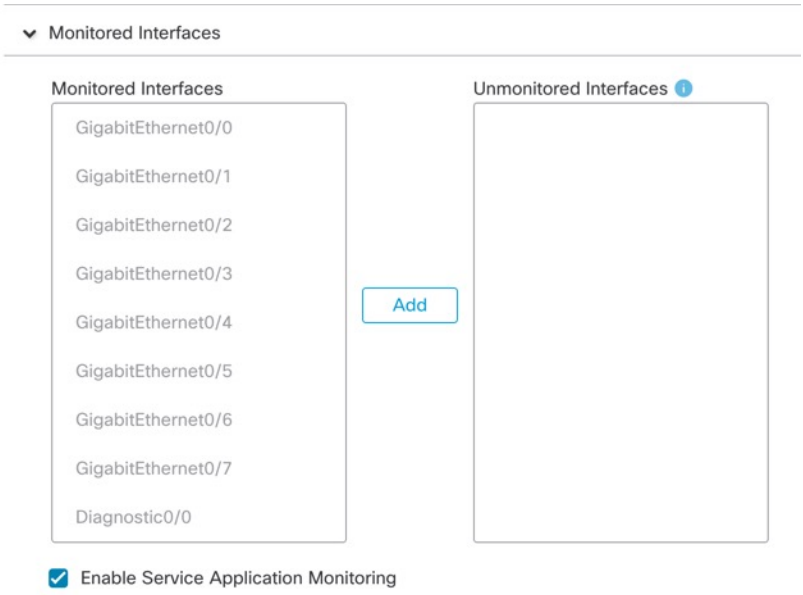


[クラスタインターフェイス（Cluster Interface）]、[データインターフェイス（Data Interface）]、および[システム（System）]に次の値を設定します（内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります）。

- [試行数（Attempts）]：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。[クラスタインターフェイス（Cluster Interface）] のデフォルト値は -1（無制限）です。[データインターフェイス（Data Interface）] と [システム（System）] のデフォルト値は 3 です。
- [試行の間隔（Interval Between Attempts）]：再結合試行の間隔を 2 ～ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [間隔のバリエーション（Interval Variation）]：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、[クラスタインターフェイス（Cluster Interface）] の場合は **1**、[データインターフェイス（Data Interface）] および [システム（System）] の場合は **2** です。

ステップ 8 [モニタリング対象のインターフェイス（Monitored Interfaces）] または [モニタリング対象外のインターフェイス（Unmonitored Interfaces）] ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリングを有効にする（Enable Service Application Monitoring）] をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 *60*：モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異

なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングを無効にできます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存（Save）] をクリックします。

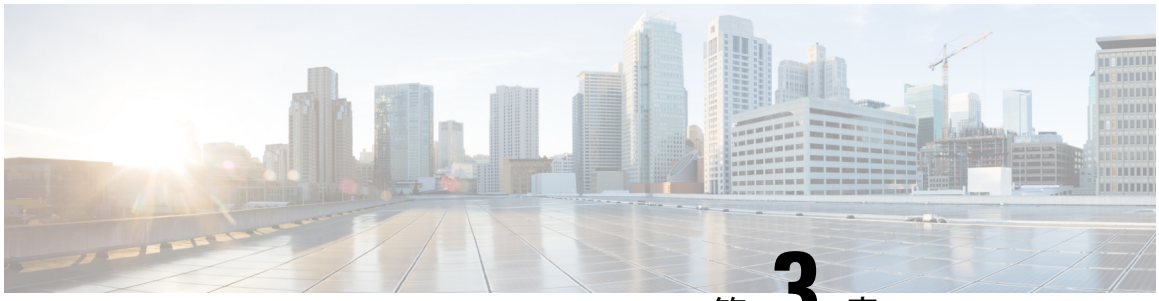
ステップ 10 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

デバイス設定の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタのヘルスモニターの設定。	7.3.0	いずれか	クラスタのヘルスモニター設定を編集できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）]** （注） 以前に FlexConfig を使用してこれらの設定を行った場合は、展開前に必ず FlexConfig の設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
冗長マネージャアクセス データ インターフェイス。	7.3.0	7.3.0	マネージャアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンしたときに管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含むECMPゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）] > [インターフェイス（Interfaces）] > [マネージャアクセス（Manager Access）]**
ポリシーのロールバックは高可用性デバイスでサポートされています。	7.2.0	7.2.0	**configure policy rollback** コマンドは高可用性デバイスでサポートされています。
展開で管理接続が失われた場合の自動ロールバック。	7.2.0	7.2.0	展開によって Management Center と Threat Defense 間の管理接続がダウンした場合に備えて、設定の自動ロールバックを有効にできるようになりました。以前は、**configure policy rollback** コマンドを使用して手動で設定をロールバックすることしかできませんでした。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [展開設定（Deployment Settings）]** • **[展開（Deploy）] > [高度な展開（Advanced Deploy）] > [プレビュー（Preview）]** • **[展開（Deploy）] > [展開履歴（Deployment History）] > [プレビュー（Preview）]**
アクセスコントロールルールではオブジェクトグループ検索がデフォルトで有効です。	7.2.0	7.2.0	バージョン 7.2.0 以降の管理対象デバイスでは、**オブジェクトグループ検索**の設定がデフォルトで有効です。このオプションは、[デバイス管理（Device Management）] ページでデバイス設定を編集するときの [詳細設定（Advanced Settings）] セクションにあります。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
デバイス設定のインポート/エクスポート。	7.1.0	7.1.0	次の使用例で、デバイス固有の設定をエクスポートし、同じデバイスに保存された設定をインポートできます。 • デバイスを別の FMC に移動する。 • 古い設定を復元する。 • デバイスを再登録する。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）] > [デバイス（Device）] > [全般（General）]
FTD での FMC IP アドレスの更新。	6.7.0	6.7.0	FMC IP アドレスを変更する場合に、FTD CLI を使用してデバイスを更新できるようになりました。 新規/変更されたコマンド： **configure manager edit**



第 3 章

ユーザー

管理対象デバイスには、CLI アクセス用のデフォルトの**管理者**アカウントが含まれています。この章では、カスタムユーザーアカウントを作成する方法について説明します。

- ユーザについて （131 ページ）
- デバイスのユーザーアカウントの要件と前提条件 （133 ページ）
- デバイスのユーザーアカウントの注意事項と制約事項 （133 ページ）
- CLI での内部ユーザーの追加 （134 ページ）
- FTD の外部認証の設定 （136 ページ）
- LDAP 認証接続のトラブルシューティング （150 ページ）
- ユーザーの履歴 （152 ページ）

ユーザについて

内部ユーザーとして、または LDAP または RADIUS サーバーの外部ユーザーとして、管理対象デバイスにカスタムユーザーアカウントを追加できます。各管理対象デバイスは、個別のユーザーアカウントを保持します。たとえば、Firewall Management Center にユーザーを追加した場合は、そのユーザーは Firewall Management Center にのみアクセスできます。そのユーザー名を使用して管理対象デバイスに直接ログインすることはできません。管理対象デバイスにユーザーを別途追加する必要があります。

内部および外部ユーザ

管理対象デバイスは次の 2 つのタイプのユーザーをサポートしています。

- 内部ユーザー：デバイスは、ローカル データベースでユーザー認証を確認します。
- 外部ユーザー：ユーザーがローカル データベースに存在しない場合は、システムは外部 LDAP または RADIUS の認証サーバーに問い合わせます。

CLI アクセス

Firepower デバイスには、Linux の上部で実行する Firepower CLI が含まれます。デバイスでは CLI を使用して内部ユーザーを作成できます。Firewall Management Center を使用して Firewall Threat Defense デバイスで外部ユーザーを確立できます。

⚠

注意 CLI の Config レベルのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスでき、Linux シェルの `sudoers` 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システムセキュリティ上の理由から、次の点を強くお勧めします。

- TAC の監督のもとで、または Firepower ユーザーマニュアルに明示的な手順がある場合に限り、Linux シェルを使用します。
- CLI アクセス権を持つユーザーのリストを適切に制限していることを確認します。
- CLI アクセス権限を付与する場合は、構成レベルのアクセス権を付与されたユーザーのリストを制限します。
- Linux シェルでユーザを直接追加しないでください。この章の手順のみを使用してください。
- Cisco TAC による指示または Firepower ユーザーマニュアルの明示的な手順による指示がない限り、CLI エキスパートモードを使用して Firepower デバイスにアクセスしないでください。

CLI ユーザー ロール

管理対象デバイスでは、CLI のコマンドへのユーザーのアクセス権は割り当てるロールによって異なります。

None

ユーザは、コマンド ラインでデバイスにログインすることはできません。

Config

ユーザは、設定コマンドを含むすべてのコマンドにアクセスできます。このアクセス レベルをユーザーに割り当てるときには注意してください。

Basic

ユーザーは、非設定コマンドにのみアクセスできます。内部ユーザーと Firewall Threat Defense 外部 RADIUS ユーザーのみが基本ロールをサポートします。

デバイスのユーザーアカウントの要件と前提条件

モデルのサポート

- Threat Defense ：内部および外部ユーザー

サポートされるドメイン

任意

ユーザの役割

外部ユーザーの設定：管理者 FMC ユーザー

内部ユーザーの設定：管理 CLI ユーザー

デバイスのユーザーアカウントの注意事項と制約事項

ユーザ名

- 内部ユーザーと外部ユーザーの両方に同じユーザー名を追加することはできません。外部サーバーが重複するユーザー名を使用している場合、デバイスへの展開は失敗します。
- ユーザー名は、次のように Linux に対して有効である必要があります。
  - 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
  - すべて小文字
  - 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

デフォルト

すべてのデバイスに、**admin**ユーザがローカルユーザアカウントとして含まれています。**admin** ユーザを削除することはできません。デフォルトの初期パスワードは**Admin123** です。初期化プロセス中に、この初期パスワードの変更が強制されます。エージェントは、変更されたログイン情報を Windows レジストリに保存し、 Firewall Management Centerと同じ暗号化、つまり暗号ブロック連鎖（CBC）を使用します。システム初期化の詳細については、ご使用のモデルのスタートアップガイドを参照してください。

ユーザーアカウント数

Cisco Firepower 1000 および 2100 シリーズ デバイスでは、最大 43 のユーザーアカウントを作成できます。

CLI での内部ユーザーの追加

CLI を使用して、Firewall Threat Defense で内部ユーザーを作成します。

手順

ステップ 1 設定権限を持つアカウントを使用してデバイス CLI にログインします。

admin ユーザ アカウントには必要な権限がありますが、設定権限を持つ任意のアカウントで作業できます。SSH セッションまたはコンソール ポートを使用できます。

特定の Firewall Threat Defense モデルの場合、コンソール ポートで FXOS CLI に入ります。**connect ftd** を使用して Firewall Threat Defense の CLI にアクセスします。

ステップ 2 ユーザ アカウントを作成します。

configure user add *username* {**basic** | **config**}

- *username*：ユーザー名を設定します。ユーザー名は、次のように Linux に対して有効である必要があります。
  - 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
  - すべて小文字
  - 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可
- **basic**：ユーザーに基本的なアクセス権を付与します。このロールはユーザーに設定コマンドの入力を許可しません。
- **config**：ユーザーに設定アクセス権を付与します。このロールはユーザーにすべてのコマンドへの完全な管理者権限を与えます。

例：

次の例では、johncrichton という名前の設定アクセス権を持つユーザー アカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

（注）
自分のパスワードを **configure password** コマンドを使用して変更できることをユーザーに伝えます。

ステップ 3 （任意） セキュリティ要件を満たすアカウントの特性を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging** *username max_days warn_days*

  ユーザパスワードの有効期限を設定します。パスワードが有効である最大日数に続いて、有効期限前にユーザに今後の期限切れを警告する日数を指定します。値は共に 1 から 9999 ですが、警告日数は最大日数よりも小さくなければなりません。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** *username*

  次回ログイン時にユーザにパスワードを強制的に変更するよう要求します。

- **configure user maxfailedlogins** *username number*

  アカウントがロックされる前の連続したログイン失敗の最大回数を 1 ~ 9999 までで設定します。Use the **configure user unlock** command to unlock accounts. 新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

- **configure user minpasswdlen** *username number*

  パスワードの最小の長さを 1 から 127 に設定します。

- **configure user strengthcheck** ユーザ名 {**enable** | **disable**}

  パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

ステップ 4 必要に応じてユーザ アカウントを管理します。

ユーザのアカウントをロックアウトできます。そうしないとアカウントの削除やその他の問題の修正が必要な場合があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

- **configure user access** ユーザ名 {**basic** | **config**}

  ユーザ アカウントの権限を変更します。

- **configure user delete** *username*

  指定したアカウントを削除します。

- **configure user disable** *username*

  指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。

- **configure user enable** *username*

  指定したアカウントを有効にします。

- **configure user password** *username*

指定したユーザのパスワードを変更します。ユーザーは通常 **configure password** コマンドを使用して自分のパスワードを変更する必要があります。

注意
管理者ユーザーのパスワードを変更する場合、エキスパートモードで Linux の **passwd** コマンドを使用しないでください。このコマンドは、ファイルシステムの破損を引き起こす可能性があります。通常の Firewall Threat Defense CLI の **configure user password admin** コマンド（管理者でない場合）、または **configure password** コマンド（管理者である場合）のみを使用します。パスワードがわからなくなり、全くログインできない場合は、パスワードの回復手順を参照してください。

- **configure user unlock** *username*

  連続して失敗したログイン試行が最大数を超えたためにロックされたユーザアカウントのロックを解除します。

FTD の外部認証の設定

FTD デバイスの外部認証を有効にするには、1 つ以上の外部認証オブジェクトを追加する必要があります。

Firewall Threat Defense の外部認証について

Firewall Threat Defense ユーザーの外部認証を有効にすると、Firewall Threat Defense により外部認証オブジェクトで指定された LDAP または RADIUS サーバーを使用してユーザークレデンシャルが検証されます。

外部認証オブジェクトは、Firewall Management Center および Firewall Threat Defense デバイスで使用できます。さまざまなアプライアンス/デバイスタイプで同じオブジェクトを共有することも、別々のオブジェクトを作成することもできます。Firewall Threat Defense では、デバイスに展開するプラットフォーム設定で 1 つの外部認証オブジェクトのみをアクティブ化できます。

（注） タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（LDAP の場合は 1 ー 30 秒、RADIUS の場合は 1 ー 300 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense 外部認証設定が機能しません。

Firewall Threat Defense SSH アクセスでは、外部認証オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを他のデバイス タイプにも使用する場合は、それらのフィールドが使用されます。

LDAP ユーザーには常に Config 権限があります。RADIUS ユーザーは、Config ユーザーまたは Basic ユーザーとして定義できます。

RADIUS サーバーのユーザーを定義する（Service-Type 属性を使用）か、外部認証オブジェクト内にユーザーリストを事前に定義することができます。LDAP では、LDAP サーバーの CLI ユーザーと一致するようにフィルタを指定できます。

（注） CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。次のことを実行してください。

- Linux シェルアクセスが付与されるユーザーのリストを制限します。
- Linux シェルユーザーを作成しないでください。

LDAP について

Lightweight Directory Access Protocol（LDAP）により、ユーザ クレデンシャルなどのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。こうすると、複数のアプリケーションがこれらのクレデンシャルと、クレデンシャルの記述に使用される情報にアクセスできます。ユーザーのクレデンシャルを変更する必要がある場合も、常に 1 箇所でクレデンシャルを変更できます。

Microsoft 社は、2020 年に Active Directory サーバーで LDAP バインディングと LDAP 署名の適用を開始すると発表しました。Microsoft 社がこれらを要件にするのは、デフォルト設定で Microsoft Windows を使用する場合に権限昇格の脆弱性が存在するために、中間者攻撃者が認証要求を Windows LDAP サーバーに正常に転送できる可能性があるからです。詳細については、Microsoft 社のサポートサイトで「2020 LDAP channel binding and LDAP signing requirement for Windows」を参照してください。

まだ行っていない場合は、Active Directory サーバーによる認証で TLS/SSL 暗号化の使用を開始することをお勧めします。

RADIUS について

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバーで、認証オブジェクトを作成できます。

Cisco Secure Firewall デバイスは、SecurID トークンの使用をサポートします。SecurID を使用したサーバーによる認証を設定した場合、そのサーバーに対して認証されるユーザーは、自身の SecurID PIN の末尾に SecurID トークンを追加したものをログイン時にパスワードとして使用します。SecurID をサポートするために、Cisco Secure Firewall デバイスで追加の設定を行う必要はありません。

Firewall Threat Defense 用の LDAP 外部認証オブジェクトの追加

Firewall Threat DefenseF 管理用に外部ユーザーをサポートするために、LDAP サーバーを追加します。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

外部認証オブジェクトの共有

外部 LDAP オブジェクトは、Firewall Management Center および Firewall Threat Defense デバイスで使用できます。同じオブジェクトを Firewall Management Center とデバイス間で共有することも、別々のオブジェクトを作成することもできます。オブジェクトを共有していない場合でも、Firewall Threat Defense と Firewall Management Center の両方が LDAP サーバーに到達できることを確認します。Firewall Management Center は、ユーザーリストを取得してデバイスにダウンロードするために必要です。

（注） LDAP の場合、タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の短いタイムアウト範囲（1 ー 30 秒）を超えないようにしてください。タイムアウトをこれより高い値に設定すると、Firewall Threat Defense への展開が失敗します。

Firewall Threat Defense サポート対象フィールド

Firewall Threat Defense SSH アクセスでは、LDAP オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを Firewall Management Centerにも使用する場合は、それらのフィールドが使用されます。この手順は、Firewall Threat Defense でサポートされているフィールドのみを対象とします。その他のフィールドについては、Firewall Management Center 用の LDAP 外部認証オブジェクトの追加を参照してください。

ユーザー名

ユーザー名は Linux で有効な名前で、かつ、小文字のみである必要があり、英数文字とピリオド（.）およびハイフン（-）を使用できます。アットマーク（@）やスラッシュ（/）など、その他の特殊文字はサポートされていません。外部認証に **admin** ユーザーを追加することはできません。外部ユーザーは、Firewall Management Center で（外部認証オブジェクトの一部として）追加することしかできません。CLI では追加できません。内部ユーザーは、Firewall Management Center ではなく、CLI でしか追加できないことに注意してください。

内部ユーザーとして同じユーザー名が **configure user add** コマンドを使用して設定されていた場合は、Firewall Threat Defense は最初にその内部ユーザーのパスワードをチェックし、それが失敗した場合は LDAP サーバーをチェックします。後から外部ユーザと同じ名前の内部ユーザを追加できないことに注意してください。既存の内部ユーザしかサポートされません。

Privilege Level

LDAP ユーザーには常に Config 権限があります。

始める前に

デバイス上にドメイン名ルックアップの DNS サーバーを指定する必要があります。この手順で LDAP サーバーのホスト名ではなく IP アドレスを指定した場合、ホスト名に含めることができる認証用の URI を LDAP サーバーが返す場合があります。ホスト名を解決するには DNS ルックアップが必要です。DNS サーバーを追加するには「Firewall Threat Defense 管理インターフェイスの CLI での変更 （72 ページ）」を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 （＋）**[外部認証オブジェクトの追加（Add External Authentication Object）]** をクリックします。

ステップ 4 [認証方式（Authentication Method）] を [LDAP] に設定します。

ステップ 5 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 6 ドロップダウン リストから [サーバタイプ（Server Type）] を選択します。

ステップ 7 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

ステップ 8 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 9 （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 10 [LDAP固有のパラメータ（LDAP-Specific Parameters）] を入力します。

a) ユーザーがアクセスする LDAP ディレクトリの [ベースDN（Base DN）] を入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。または、[DNの取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。

b) （任意） [基本フィルタ（Base Filter）] を入力します。たとえば、ディレクトリ ツリー内のユーザー オブジェクトに `physicalDeliveryOfficeName` 属性が設定されており、New York 支店のユーザーに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザーだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

c) LDAP サーバを参照するために十分なクレデンシャルを持つユーザの [ユーザ名（User Name）] を入力します。たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

d) [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドにユーザ パスワードを入力します。

e) （任意）[詳細オプションを表示（Show Advanced Options）] をクリックして、次の詳細オプションを設定します。

- **[暗号化（Encryption）]**：**[なし（None）]**、**[TLS]**、または **[SSL]** をクリックします。

  ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされます。[なし（None）] または [TLS] の場合、ポートはデフォルト値の 389 にリセットされます。[SSL] 暗号化を選択した場合、ポートは 636 にリセットされます。

- [SSL証明書アップロードパス（SSL Certificate Upload Path）]：SSL または TLS 暗号化の場合は、[ファイルの選択（Choose File）] をクリックして証明書を選択する必要があります。

  以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、設定をデバイスに再展開して、新しい証明書を上書きコピーします。

  （注）
  TLS 暗号化には、すべてのプラットフォームで証明書が必要です。SSL の場合、Firewall Threat Defense も証明書を必要とします。他のプラットフォームの場合、SSL は証明書を必要としません。ただし、中間者攻撃を防ぐため、SSL 証明書を常にアップロードしておくことをお勧めします。

- （未使用）[ユーザー名テンプレート（User Name Template）]：Firewall Threat Defense では使用されていません。

- [タイムアウト（秒）（Timeout (Seconds)）]：バックアップ接続にロールオーバーするまでの秒数（1 ー 30 秒）を入力します。デフォルトは 30 です。

  （注）
  タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（1 ー 30 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense LDAP 設定が機能しません。

ステップ 11 [属性マッピング（Attribute Mapping）] を設定して、属性に基づいてユーザーを取得します。

- [UI アクセス属性（UI Access Attribute）] を入力します。**注**：このフィールドは、デバイスの CLI アクセスには使用されません。ただし、これは必須フィールドであるため、値を入力する必要があります。[CLIアクセス属性（CLI Access Attribute）] に入力する値と同じ値を入力できます。

- ユーザー識別タイプ以外の CLI アクセス属性を使用する場合は、[CLIアクセス属性（CLI Access Attribute）] を設定します。たとえば、Microsoft Active Directory Server で、`sAMAccountName` シェル CLI アクセス属性を使用して CLI アクセスユーザーを取得するには、`sAMAccountName` と入力します。

  （注）
  CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ

上のリスクが生じる可能性があります。CLI または Linux シェルアクセスが付与されるユーザーのリストを制限してください。

（注）
CLI アクセス権を持つ多数のユーザーを許可する外部認証オブジェクトを展開すると、ユーザーの作成を待機している間に展開がタイムアウトし、失敗する可能性があります。

ステップ 12 [CLIアクセスフィルタ（CLI Access Filter）] を設定します。

次のいずれかの方法を選択します。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] チェックボックスをオンにします。
- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

ユーザ名は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

（注）
内部ユーザーに同じユーザー名を以前に設定している場合、Firewall Threat Defense は内部ユーザーに対して最初にパスワードを確認し、失敗した場合は LDAP サーバーを確認します。後から外部ユーザと同じ名前の内部ユーザを追加できないことに注意してください。既存の内部ユーザしかサポートされません。

ステップ 13 [保存（Save）] をクリックします。

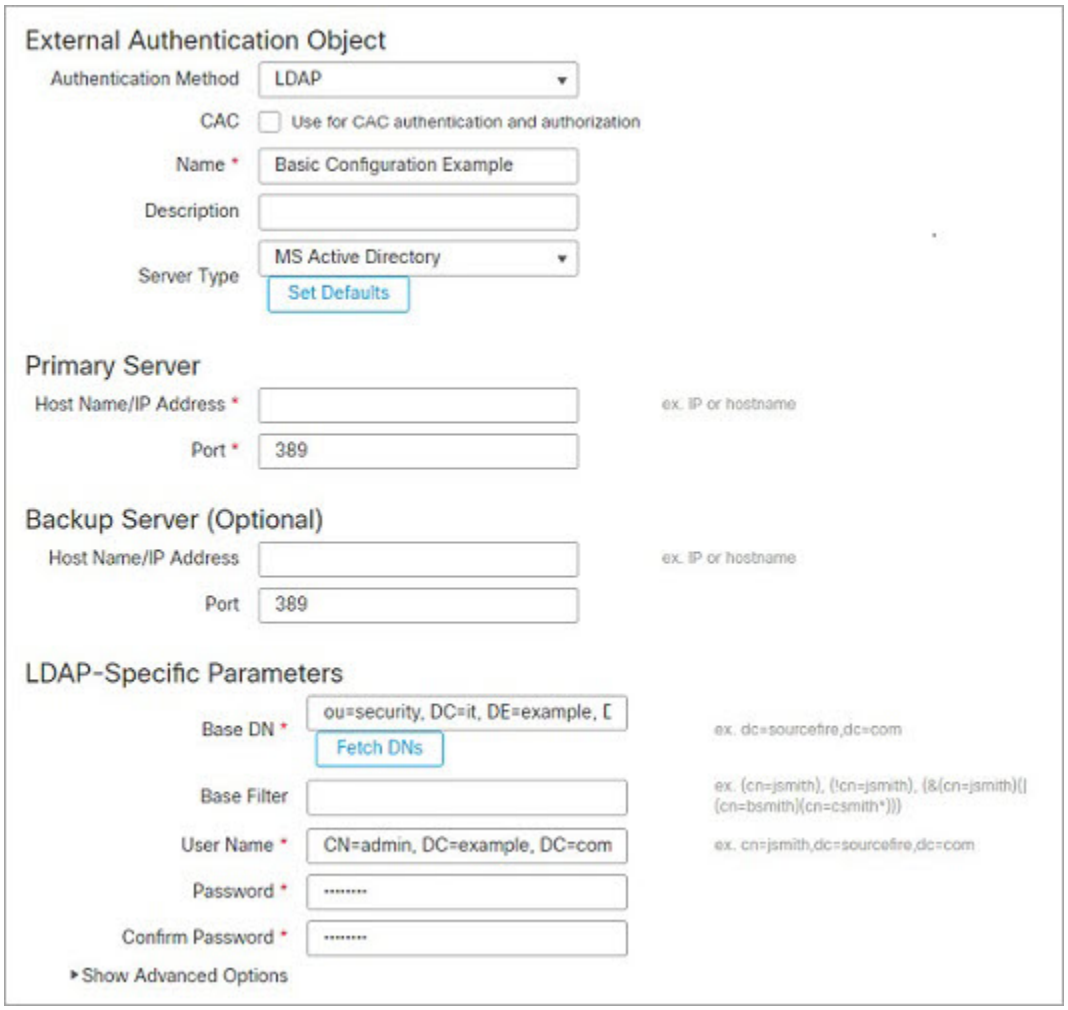
ステップ 14 このサーバーの使用を有効にします。外部認証 （832 ページ）を参照してください。

ステップ 15 LDAP サーバーで後からユーザーを追加または削除する場合は、、管理対象デバイスのプラットフォーム設定を再展開する必要があります。Firewall Management Center はユーザーリストを再ダウンロードし、デバイスに展開します。「設定変更の展開 （172 ページ）」を参照してください。

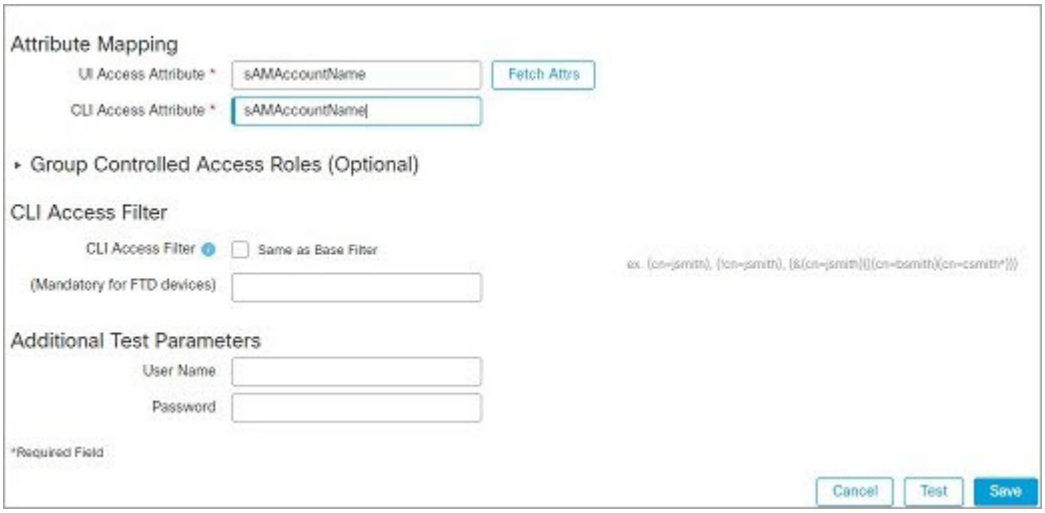
例

基本的な例

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバーの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。

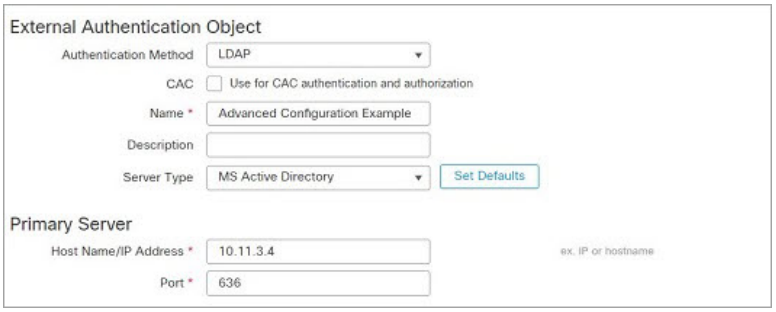


[CLIアクセス属性（CLI Access Attribute）] が `sAMAccountName` の場合、ユーザーが Firewall Threat Defense にログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

基本フィルタはこのサーバに適用されないため、Firewall Threat Defenseはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバーへの接続は、デフォルトの期間（または LDAP サーバーで設定されたタイムアウト期間）の経過後にタイムアウトします。

高度な例

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバーの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。ただし、このサーバーに基本フィルタ `(cn=*smith)` が設定されていることに注意してください。このフィルタは、サーバーから取得するユーザーを、一般名が `smith` で終わるユーザーに限定します。

サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（秒）（Timeout (Seconds)）] の設定により、60 秒経過後にサーバーへの接続がタイムアウトします。

このサーバーが Microsoft Active Directory Server であるため、ユーザー名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。

[CLIアクセス属性（CLI Access Attribute）] が `sAMAccountName` の場合、ユーザーが Firewall Threat Defense にログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

次の例では、CLI アクセスフィルタが基本フィルタと同じように設定されています。

Firewall Threat Defense 用の RADIUS 外部認証オブジェクトの追加

Firewall Threat Defense 用に外部ユーザーをサポートするために、RADIUS サーバーを追加します。

外部認証オブジェクトの共有

同じオブジェクトを Firewall Management Center とデバイス間で共有することも、別々のオブジェクトを作成することもできます。Firewall Threat Defense は RADIUS サーバーでのユーザーの定義をサポートしますが、Firewall Management Center では外部認証オブジェクトのユーザーリストを事前定義する必要があることに注意してください。Firewall Threat Defense には事前に定義されているリスト方式を使用できますが、RADIUS サーバーでユーザーを定義する場合は Firewall Threat Defense と Firewall Management Center に個別のオブジェクトを作成する必要があります。

（注） タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の短いタイムアウト範囲（1 ー 300 秒）を超えないようにしてください。タイムアウトをもっと長い値に設定すると、Firewall Threat Defense RADIUS 設定が機能しません。

Firewall Threat Defense サポート対象フィールド

Firewall Threat Defense SSH アクセスでは、RADIUS オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを Firewall Management Centerにも使用する場合は、それらのフィールドが使用されます。この手順は、Firewall Threat Defense でサポートされているフィールドのみを対象とします。他のフィールドについては、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Add a RADIUS External Authentication Object for Firewall Management Center」を参照してください。

ユーザー名

外部認証に **admin** ユーザーを追加することはできません。外部ユーザーは、Firewall Management Center で（外部認証オブジェクトの一部として）追加することしかできません。CLI では追加できません。内部ユーザーは、Firewall Management Center ではなく、CLI でしか追加できないことに注意してください。

内部ユーザーとして同じユーザー名が **configure user add** コマンドを使用して設定されていた場合は、Firewall Threat Defense は最初にその内部ユーザーのパスワードをチェックし、それが失敗した場合は RADIUS サーバーをチェックします。後から外部ユーザーと同じ名前の内部ユーザーを追加できないことに注意してください。既存の内部ユーザーしかサポートされません。RADIUS サーバーで定義されているユーザーの場合は、内部ユーザーの権限レベルと同じに設定してください。そうしないと、外部ユーザーパスワードを使用してログインできません。

手順

ステップ 1 Service-Type 属性を使用して RADIUS サーバー上のユーザーを定義します。

次に、Service-Type 属性でサポートされている値を示します。

- Administrator (6)：CLI への config アクセス認証を提供します。これらのユーザーは、CLI ですべてのコマンドを使用できます。
- NAS Prompt (7) または 6 以外のレベル：CLI への基本的なアクセス認証を提供します。これらのユーザーは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字

- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、記号（@）やスラッシュ（/）は使用不可

または、外部認証オブジェクトにユーザーを事前定義できます（ステップ 12（146 ページ）を参照）。Firewall Threat Defense に対して Service-Type 属性メソッドを使用しているときに Firewall Threat Defense および Firewall Management Center に同じ RADIUS サーバーを使用するには、同じ RADIUS サーバーを識別する外部認証オブジェクトを 2 つ作成します。一方のオブジェクトには事前に定義した [CLIアクセスフィルタ（CLI Access Filter）] ユーザーを含め（Firewall Management Center で使用）、もう一方のオブジェクトの [CLIアクセスフィルタ（CLI Access Filter）] は空のままにします（Firewall Threat Defense で使用）。

ステップ 2 Firewall Management Centerで、[システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

ステップ 3 [外部認証（External Authentication）] をクリックします。

ステップ 4 [外部認証オブジェクトの追加（Add External Authentication Object）]（＋）をクリックします。

ステップ 5 [認証方式（Authentication Method）] を [RADIUS] に設定します。

ステップ 6 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 7 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

IPv4 だけがサポートされます。

（注）
証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要があります。

ステップ 8 （任意）[ポート（Port）] をデフォルトから変更します。

ステップ 9 [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

ステップ 10 （任意）[バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 11 （任意）[RADIUS固有のパラメータ（RADIUS-Specific Parameters）] を入力します。

a) プライマリサーバーを再試行するまでの [タイムアウト（秒）（Timeout (Seconds)）] を 1 ～ 300 の秒単位で入力します。デフォルトは 30 です。

（注）
タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の短いタイムアウト範囲（1 ー 300 秒）を超えないようにしてください。タイムアウトをもっと長い値に設定すると、Firewall Threat Defense RADIUS 設定が機能しません。

b) バックアップサーバーにロールオーバーするまでの [再試行（Retries）] を入力します。デフォルトは 3 です。

ステップ 12 （任意）RADIUS 定義ユーザー（ステップ 1（145 ページ）を参照）を使用する代わりに、[CLIアクセスフィルタ（CLI Access Filter）] 領域の [管理者CLIアクセスユーザーリスト（Administrator

CLI Access User List）] フィールドに、CLI アクセスが必要なユーザー名をカンマで区切って入力します。たとえば、**jchrichton, aerynsun, rygel** と入力します。

Firewall Threat Defense で [CLIアクセスフィルタ（CLI Access Filter）] メソッドを使用すると、Firewall Threat Defense およびその他のプラットフォームタイプで同一の外部認証オブジェクトを使用できます。

（注）
RADIUS 定義ユーザーを使用する場合は、[CLIアクセスフィルタ（CLI Access Filter）] を空のままにする必要があります。

これらのユーザー名が RADIUS サーバーのユーザー名と一致していることを確認します。名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

（注）
CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。CLI または Linux シェルアクセスが付与されるユーザーのリストを制限してください。

（注）
CLI アクセス権を持つ多数のユーザーを許可する外部認証オブジェクトを展開すると、ユーザーの作成を待機している間に展開がタイムアウトし、失敗する可能性があります。

ステップ 13 （任意） RADIUS サーバーへの Firewall Management Center 接続をテストするには、[テスト（Test）] をクリックします。

この機能は、RADIUS サーバーへの Firewall Management Center 接続のみをテストできます。管理対象デバイスの RADIUS サーバーへの接続をテストする機能はありません。

ステップ 14 （任意） [追加のテストパラメータ（Additional Test Parameters）] を入力して、認証できるようにするユーザのユーザ クレデンシャルをテストすることもできます。[ユーザ名（User Name）] と [パスワード（Password）] を入力してから、[テスト（Test）] をクリックします。

ヒント
テストユーザーの名前とパスワードを誤って入力すると、サーバー設定が正しい場合でもテストが失敗します。サーバー設定が正しいことを確認するには、最初に [Additional Test Parameters] フィールドにユーザー情報を入力せずに [Test] をクリックします。正常に完了した場合は、テストする特定ユーザーのユーザー名とパスワードを指定します。

例：

Example 社の JSmith ユーザ クレデンシャルを取得できるかどうかをテストするには、JSmith と正しいパスワードを入力します。

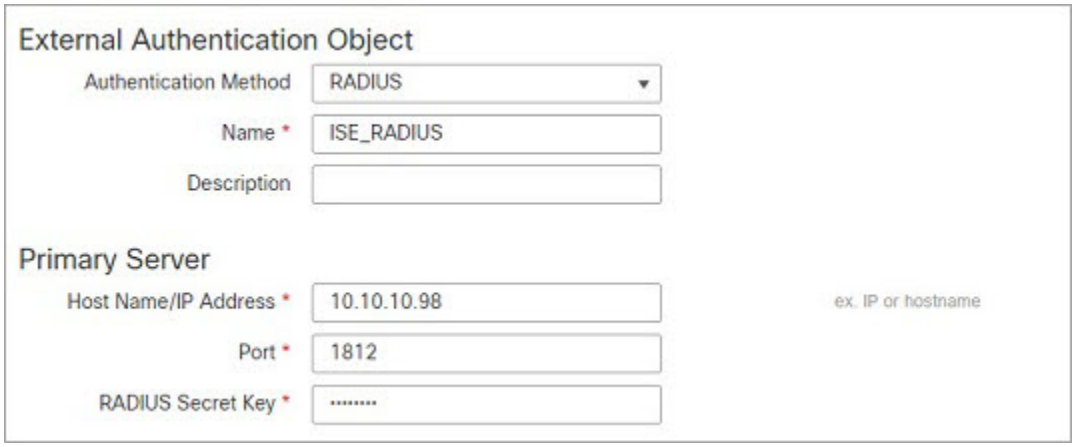
ステップ 15 [保存（Save）] をクリックします。

ステップ 16 このサーバーの使用を有効にします。外部認証 （832 ページ）を参照してください

例

単純なユーザー ロールの割り当て

次の図は、IP アドレスが 10.10.10.98 のポート 1812 で Cisco Identity Services Engine（ISE）が稼働しているサーバーのサンプル RADIUS ログイン認証オブジェクトを示します。バックアップサーバーは定義されていません。



次の例は、システムがバックアップサーバー（存在する場合）への接続を試みるまでのタイムアウト（30 秒）と失敗した再試行の数を含む、RADIUS 固有のパラメータを示しています。

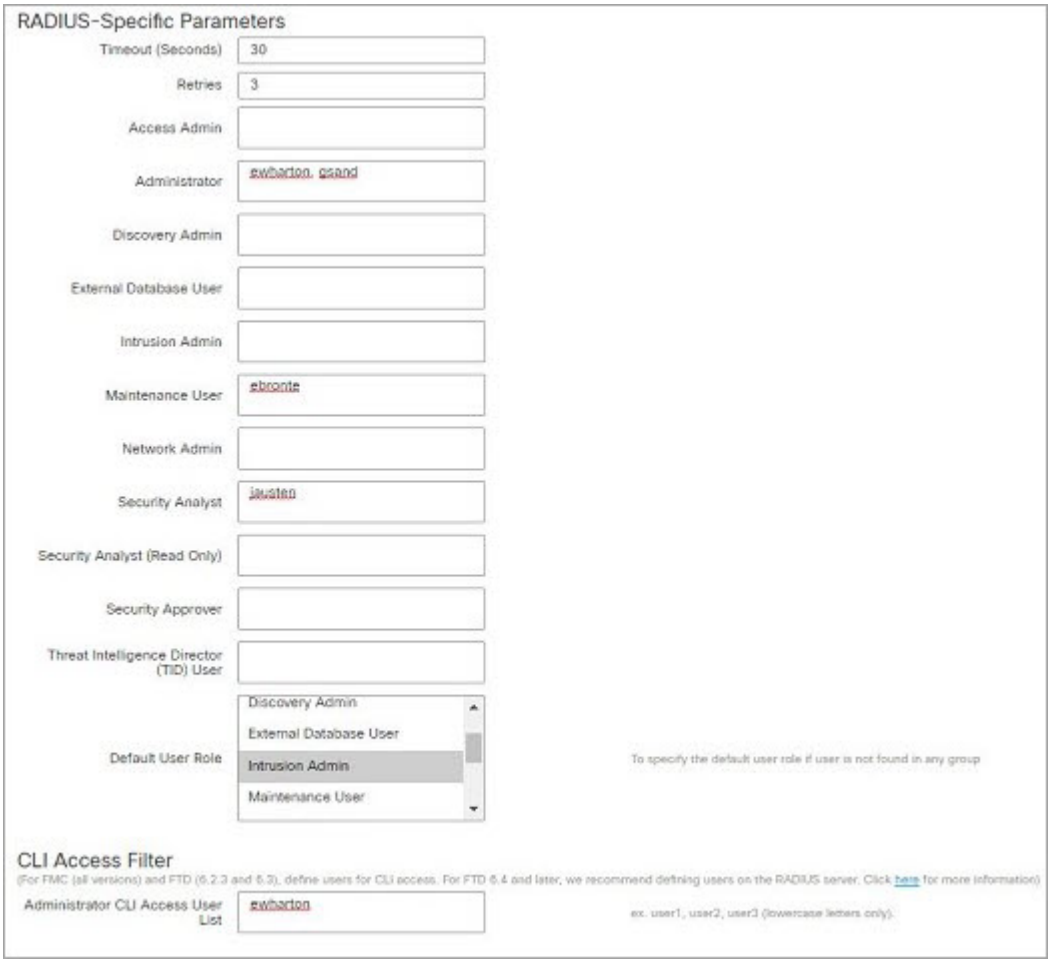
次の例は、RADIUS ユーザー ロール設定の重要な特徴を示します。

ユーザ ewharton および gsand には、Web インターフェイスの管理アクセスが付与されます。

ユーザ cbronte には、Web インターフェイスのメンテナンス ユーザ アクセスが付与されます。

ユーザー jausten には、Web インターフェイスのセキュリティ アナリスト アクセスが付与されます。

ユーザー ewharton は、CLI アカウントを使用してデバイスにログインできます。



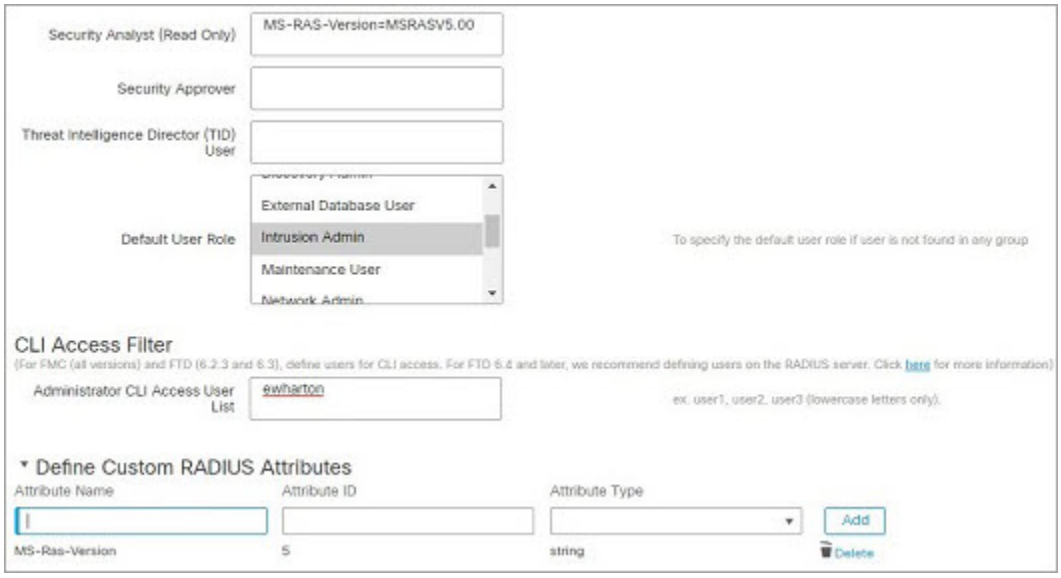
次の図に、この例のロール設定を示します。

属性と値のペアに一致するユーザーのロール

属性と値のペアを使用して、特定のユーザー ロールが付与される必要があるユーザーを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ ISE サーバーのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバーが使用されているため、1 つ以上のユーザーの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモートアクセス サーバー経由で RADIUS にログインするすべてのユーザーに対し、[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。



FTD デバイスのユーザーに対する外部認証の有効化

Firepower Threat Defense プラットフォーム設定で外部認証を有効にして、管理対象デバイスに設定を展開します。詳細については、外部認証 （832 ページ）を参照してください。

LDAP 認証接続のトラブルシューティング

LDAP 認証オブジェクトを作成したが、選択したサーバーへの接続が失敗したか、または必要なユーザーのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- Web インターフェイス画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザー名とパスワードが有効であることを確認します。
  - サードパーティの LDAP ブラウザを使用して LDAP サーバーに接続し、ベース識別名に示されているディレクトリを参照する権限があることを確認します。
  - ユーザー名が、LDAP サーバーのディレクトリ情報ツリーで一意であることを確認します。
  - テスト出力に LDAP バインド エラー 49 が示される場合は、ユーザーのユーザー バインディングが失敗しています。サードパーティ アプリケーションを使用してサーバー認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。

- サーバーを正しく指定していることを確認します。
  - サーバーの IP アドレスまたはホスト名が正しいことを確認します。
  - ローカル アプライアンスから、接続する認証サーバーに TCP/IP でアクセスできることを確認します。
  - サーバーへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
  - 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバーに使用されているホスト名と一致している必要があります。
  - CLI アクセスを認証する場合は、サーバー接続に IPv6 アドレスを使用していないことを確認します。
  - サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[デフォルトを設定（Set Default）] をもう一度クリックしてデフォルト値をリセットします。
- ベース識別名を入力した場合は、[DNを取得（Fetch DNs）] をクリックし、サーバーで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたは CLI アクセスフィルタを使用している場合は、フィルタがカッコで囲まれていて、有効な比較演算子を使用していることを確認します（囲み用のカッコを含めて最大 450 文字）。
- より制限された基本フィルタをテストするには、特定のユーザーだけを取得するため、フィルタにそのユーザーのベース識別名を設定します。
- 暗号化接続を使用する場合：
  - 証明書の LDAP サーバーの名前が、接続に使用するホスト名と一致していることを確認します。
  - 暗号化されたサーバー接続で IPv6 アドレスを使用していないことを確認します。
- テストユーザーを使用する場合、ユーザー名とパスワードが正しく入力されていることを確認します。
- テストユーザーを使用する場合、ユーザー資格情報を削除してオブジェクトをテストします。
- LDAP サーバーに接続し、次の構文を使用して、使用しているクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'
```

```
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

たとえば、`domainadmin@myrtle.example.com` ユーザーと基本フィルタ (`cn=*`) を使用して `myrtle.example.com` のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、プラットフォーム設定ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、デバイスに適用されるプラットフォーム設定ポリシーで有効になっていることを確認します。

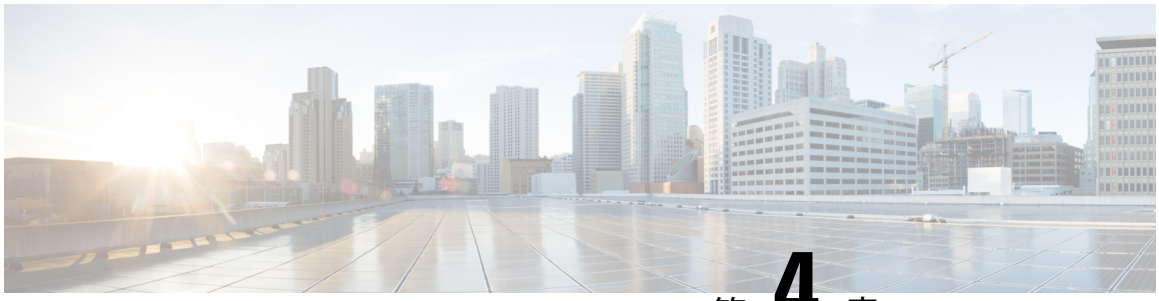
正常に接続したが、接続で取得されたユーザーリストを調整する必要がある場合は、基本フィルタまたはCLIアクセスフィルタを追加または変更するか、ベースDNをさらに制限するか制限を緩めて使用することができます。

Active Directory（AD）サーバーへの接続を認証しているときに、ADサーバーへの接続が成功しても、接続イベントログにブロックされたLDAPトラフィックが示されることはほとんどありません。この不正な接続ログは、ADサーバーが重複したリセットパケットを送信したときに発生します。Firewall Threat Defenseデバイスは、2番目のリセットパケットを新しい接続要求の一部として識別し、ブロックアクションを使用して接続をログに記録します。

ユーザーの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
RADIUSサーバーに定義されている Firewall Threat Defense ユーザーの Service-Type 属性のサポート	6.4.0	いずれか	Firewall Threat Defense CLI ユーザーの RADIUS の認証では、以前は RADIUS 外部認証オブジェクトにユーザー名を定義してから、RADIUS サーバーに認証されているユーザー名とリストが一致していることを手動で確認する必要がありました。Service-Type 属性を使用して RADIUS サーバーで CLI ユーザーを定義できるようになりました。また、Basic と Config の両方のユーザー ロールも定義できます。このメソッドを使用するには、外部認証オブジェクトのシェルアクセスフィルタを空白のままにしてください。 新規/変更された画面：**[システム（System）]** > **[ユーザー（Users）]** > **[外部認証（External Authentication）]** > **[外部認証オブジェクトの追加（Add External Authentication Object）]** > **[シェルアクセスフィルタ（Shell Access Filter）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firewall Threat Defense SSH アクセスの外部認証	6.2.3	いずれか	LDAP または RADIUS認証を使用して Firewall Threat Defense への SSH の外部認証を設定できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [外部認証（External Authentication）]**



第 4 章

設定の展開

この章では、1 つ以上の管理対象デバイスに設定の変更をダウンロードする方法について説明します。

- 設定の展開について （155 ページ）
- ポリシー管理の要件と前提条件 （170 ページ）
- 設定変更を展開するためのベストプラクティス （170 ページ）
- 設定の展開 （172 ページ）
- 展開の管理 （180 ページ）
- 設定の展開の履歴 （193 ページ）

設定の展開について

すべてのデバイス設定はFirewall Management Centerによって管理され、管理対象デバイスに展開されます。

展開が必要な設定変更

システムは、失効したポリシーに赤色のステータステキストでマークを付けます。このテキストには、ポリシーの更新を必要とするターゲットデバイスの数が示されます。失効ステータスをクリアするには、ポリシーをデバイスに再展開する必要があります。

展開が必要

展開が必要な設定変更には、次のものがあります。

- アクセス コントロール ポリシー自体の変更：アクセス コントロール ルール、デフォルト アクション、ポリシー ターゲット、セキュリティ インテリジェンス フィルタリング、前処理などの詳細オプションの変更。
- アクセス コントロール ポリシーが呼び出すポリシーの変更：SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、アイデンティティ ポリシー、または DNS ポリシー。

- 呼び出されるアクセス コントロール ポリシーで使用される再利用可能オブジェクトまたは設定の変更：
  - ネットワーク、ポート、VLAN タグ、URL、地理位置情報オブジェクト
  - セキュリティ インテリジェンス リストおよびフィード
  - アプリケーション フィルタまたはディテクタ
  - 侵入ポリシーの変数セット
  - ファイル リスト
  - 復号関連のオブジェクトとセキュリティ ゾーン
- システム ソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

Webインターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクトマネージャ（**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**）を使用してセキュリティゾーンを変更できますが、デバイスの設定（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**）でインターフェイスのタイプを変更すると、ゾーンも変更され、展開が必要になります。

展開が不要

次の更新では、展開は**必要ありません**。

- セキュリティ インテリジェンス フィードへの自動更新およびコンテキストメニューを使用したセキュリティインテリジェンスのグローバルのブロックリストまたはブロックしないリストへの追加
- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

展開のプレビュー

[プレビュー（Preview）]には、デバイス上に展開するポリシーとオブジェクトのすべての変更のスナップショットが表示されます。ポリシーの変更には、新しいポリシー、既存のポリシーの変更、および削除されたポリシーが含まれます。オブジェクトの変更には、ポリシーで使用される追加および変更されたオブジェクトが含まれます。未使用のオブジェクトの変更は、デバイスに展開されていないため表示されません。

プレビューには、インターフェイスまたはプラットフォーム設定ポリシーが初めて追加されたときに、変更されていない場合でも、他の設定済みの設定とともに、すべてのデフォルト値が表示されます。同様に、高可用性関連のポリシーと設定のデフォルト値は、高可用性ペアが設定または中断した後の最初のプレビューで、変更されていない場合でも表示されます。

自動ロールバックによる変更を表示するには、展開設定の編集（118ページ）を参照してください。

サポートされない機能

- オブジェクトがデバイスまたはインターフェイスに関連付けられている場合にのみ、オブジェクトの追加と属性の変更がプレビューに表示されます。オブジェクトの削除は表示されません。
- プレビューは、次のポリシーではサポートされていません。
  - ハイアベイラビリティ
  - ネットワーク検出
  - ネットワーク分析
  - デバイス設定
- ルールレベルのユーザー情報は、侵入ポリシーでは利用できません。
- プレビューには、ポリシー間のルールの順序変更は表示されません。

  DNSポリシーの場合、順序が変更されたルールは、ルールの追加および削除のようにプレビューリストに表示されます。たとえば、ルールの順序でルールを位置1から位置3に移動すると、そのルールが位置1から削除されて新しいルールとして位置3に追加されたように表示されます。同様に、ルールを削除すると、その下のルールは位置が変更されるため、編集済みのルールとして表示されます。変更は、ポリシーに示される最終順序で表示されます。
- プレビューは、次の HA シナリオではサポートされていません。
  - デバイスがスタンドアロンモードになっていてチェーンが作成された場合、自動展開がトリガーされます。その特定のジョブでは、プレビューはサポートされません。[プレビュー（Preview）]（）にカーソルを合わせると、HAブートストラップ展開であり、プレビューはサポートされないことを示すメッセージが表示されます。
  - **設定グループ**：デバイスが最初はスタンドアロンであったフローについて検討します。その後、3 つの展開が行われました。4 つ目の展開では、デバイスは HA ブートストラップ展開でした。その後、ユーザーはデバイス5、6、および7を展開します。展開 7 は HA 解除展開であり、ユーザーはデバイス 8、9、および 10 を展開します。

    このフローでは、4 が HA 展開だったため、3 と 5 の間のプレビューはサポートされません。同様に、8 と 3 の間のプレビューもサポートされません。プレビューは、3 から 1 と、7、6、5、4 と、10、9、8 でのみサポートされます。
  - デバイスが切断されている（HA が解除されている）場合、新しいデバイスは新規デバイスと見なされます。

選択的ポリシーの展開

Firewall Management Center では、展開が予定されているデバイス上の変更すべてのリスト内で特定のポリシーを選択し、選択したポリシーのみを展開することができます。選択的な展開は、次のポリシーに対してのみ使用できます。

- アクセス コントロール ポリシー
- 侵入ポリシー
- マルウェアおよびファイル ポリシー
- DNS ポリシー
- アイデンティティ ポリシー
- SSL ポリシー
- Quality of Service（QoS）ポリシー
- プレフィルタ ポリシー
- ネットワーク検出
- NAT ポリシー
- ルーティングポリシー
- VPN ポリシー

ポリシーを選択的に展開するには、特定の制限があります。次の表の内容に従って、選択的ポリシー導入を使用できる場合について理解します。

表 *9 :* 選択的展開の制限事項

タイプ	説明	シナリオ
フル展開	特定の展開シナリオではフル展開が必要であり、Firewall Management Center はこのようなシナリオでの選択的展開をサポートしていません。このようなシナリオでエラーが発生した場合、デバイス上の展開へのすべての変更を選択して続行することもできます。	フル展開が必要なシナリオは次のとおりです。 • Firewall Threat Defense または Firewall Management Center をアップグレードした後の最初の展開。 • Firewall Threat Defense を復元した後の最初の展開。 • Firewall Threat Defense インターフェイスの設定を変更した後の最初の展開。 • 仮想ルータの設定を変更した後の最初の展開。 • Firewall Threat Defense デバイスが新しいドメインに移動された場合（グローバルからサブドメインへ、またはサブドメインからグローバルへ）。
関連付けられたポリシーの展開	Firewall Management Center は、相互に関連する相互依存ポリシーを特定します。相互に関連するポリシーのいずれかを選択すると、残りの相互に関連するポリシーが自動的に選択されます。	関連付けられたポリシーが自動的に選択されるシナリオは次のとおりです。 • 新しいオブジェクトが既存のポリシーに関連付けられている場合。 • 既存のポリシーのオブジェクトが変更された場合。 複数のポリシーが自動的に選択されるシナリオは次のとおりです。 • 新しいオブジェクトが既存のポリシーに関連付けられていて、同じオブジェクトがすでに他のポリシーに関連付けられている場合、関連付けられているすべてのポリシーが自動的に選択されます。 • 共有オブジェクトが変更されると、関連付けられているすべてのポリシーが自動的に選択されます。

タイプ	説明	シナリオ
相互依存ポリシーの変更（色分けされたタグを使用して表示）	Firewall Management Center は、ポリシー間および共有オブジェクトとポリシー間の依存関係を動的に検出します。オブジェクトまたはポリシーの相互依存性は、色分けされたタグを使用して表示されます。	色分けされた相互依存ポリシーまたはオブジェクトが自動的に選択されるシナリオは次のとおりです。 • すべての期限切れのポリシーに相互に依存する変更がある場合。 たとえば、アクセス コントロール ポリシー、侵入ポリシー、および NAT ポリシーが失効している場合などです。アクセス コントロール ポリシーと NAT ポリシーはオブジェクトを共有するため、すべてのポリシーが展開用に一緒に選択されます。 • すべての期限切れのポリシーがオブジェクトを共有し、そのオブジェクトが変更された場合。

タイプ	説明	シナリオ
アクセスポリシーグループの仕様	[表示（View）]（ ）をクリックすると、アクセスポリシーグループのポリシーが、[アクセスポリシーグループ（Access Policy Group）] の下のプレビューウィンドウにまとめて表示されます。	アクセスポリシーグループのポリシーのシナリオと想定される動作は次のとおりです。 • アクセス コントロール ポリシーが失効している場合、そのアクセス コントロール ポリシーが展開用に選択されると、ファイルポリシーと侵入ポリシーを除き、このグループにあるすべての期限切れポリシーが展開されます。 ただし、アクセス コントロール ポリシーが失効している場合でも、依存関係に変更がない限り、アクセス コントロール ポリシーが選択されているかどうかに関係なく、侵入ポリシーとファイルポリシーを個別に選択または選択解除できます。たとえば、新しい侵入ポリシーがアクセスコントロールルールに割り当てられると、依存関係に変化が生じることになります。その結果、アクセス コントロール ポリシーと侵入ポリシーのいずれかが選択されると、その両方が自動的に選択されます。 • アクセス コントロール ポリシーが失効していない場合は、このグループ内の他の古いポリシーを個別に選択して展開することができます。

システムユーザー名

Firewall Management Center では、次の動作に関してユーザー名が「**system**」と表示されます。

- ロールバック（Rollback）
- アップグレード
- Firewall Threat Defense バックアップおよび復元
- SRU の更新
- LSP の更新
- VDB の更新

アプリケーションディテクタの自動有効化

アプリケーション制御の実行時に必要なディテクタが無効になっている場合、システムは、ポリシーの展開時にシステムによって提供される適切なディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

ネットワーク検出ポリシーの変更によるアセットの再検出

ネットワーク検出ポリシーに変更を展開する場合、システムは、監視対象ネットワーク内のホストのネットワーク マップから MAC アドレス、TTL、およびホップ情報を削除してから、再検出を行います。また、影響を受ける管理対象デバイスは、まだ Firewall Management Center に送信されていない検出データを破棄します。

Snort 再起動のシナリオ

管理対象デバイス上の Snort プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。 また、Snort プロセスが再起動するかどうかに関係なく、展開時にリソース需要が高まった結果、いくつかのパケットがインスペクションを実行せずにドロップされることがあります。

次の表に示すいずれかのシナリオでは、Snort プロセスが再起動されます。

表 *10 : Snort* 再起動のシナリオ

再起動のシナリオ	詳細情報
Snort プロセスの再起動が必要な特定の設定を展開した場合。	展開またはアクティブ化された際に Snort プロセスを再起動する設定 （167 ページ）
Snort プロセスを直ちに再起動するように設定を変更した場合。	変更により Snort プロセスがただちに再起動する場合 （169 ページ）
現在展開されている自動アプリケーション バイパス（AAB）設定のトラフィックをアクティブにした場合。	自動アプリケーションバイパスの設定 （115 ページ）
「RAM ディスクへの接続イベントのロギング」機能の有効化または無効化。	『Troubleshoot Drain of FMC Unprocessed Events』の「**Log to Ramdisk**」を参照してください。

関連トピック

アクセス コントロール ポリシーの詳細設定 （1759 ページ）

展開またはアクティブ化された際に Snort プロセスを再起動する設定 （167 ページ）

デバイスの再起動の警告

展開時、展開ページの [検査の中断（Inspect Interruption）] 列に、構成を展開したときに Firewall Threat Defense デバイスで Snort プロセスが再起動するかどうかが表示されます。*Snort* プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。トラフィックが中断されるか中断中にインスペクションなしで受け渡されるかどうかは、デバイスがトラフィックを処理する方法によって変わります。展開の続行、展開のキャンセル、および設定の変更を実行できます。または、展開によるネットワークへの影響が最小となる時間まで展開を遅らせることができます。

[インスペクションの中断（Inspect Interruption）] 列に [あり（Yes）] と表示されているときにデバイス設定リストを展開すると、システムは Snort プロセスを再起動する特定の設定タイプを [インスペクションの中断（Inspect Interruption）]（） と一緒に表示します。このアイコンにマウスポインタを合わせると、設定を展開するときにトラフィックが中断される可能性があるというメッセージが表示されます。

次の表に、インスペクション中断の警告を[展開（Deploy）] ページに表示する方法を示します。

表 *11* : インスペクション中断のインジケータ

タイプ	インスペクションの中断	説明
Firewall Threat Defense	[インスペクションの中断（Inspect Interruption）]（）はい（Yes）	少なくとも1つの設定は、展開するとデバイスでインスペクションが中断します。また、デバイスがトラフィックを処理する方法によって、トラフィックが中断されることがあります。デバイス設定リストを展開して、詳細を確認できます。
	--	展開されている設定は、デバイスのトラフィックを中断しません。
	不明	システムは、展開されている設定がデバイスのトラフィックを中断するかどうか特定できません。 最初の展開の前の、ソフトウェア アップグレードの後に、または場合によってはサポートコール中に、不明ステータスが表示されます。
	エラー（）	内部エラーにより、システムはステータスを特定できません。 操作をキャンセルして再度 [展開（Deploy）] をクリックすると、システムは [インスペクションの中断（Inspect Interruption）] ステータスを特定しなおすことができます。問題が解決しない場合は、サポートにご連絡ください。
センサー	--	センサーとして識別されるデバイスは Firewall Threat Defense デバイスではありません。システムは、構成を展開するとこのデバイスのトラフィックが中断されるかどうかを特定しません。

すべてのデバイス タイプの Snort プロセスを再起動する全設定の詳細については、展開またはアクティブ化された際に Snort プロセスを再起動する設定（167 ページ）を参照してください。

ポリシー適用中のトラフィックの検査

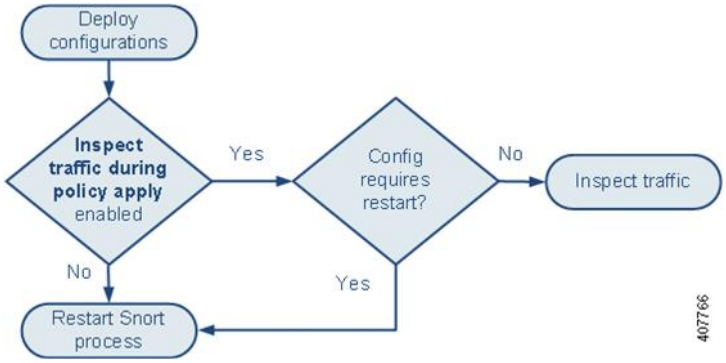
[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] は、管理対象デバイスが設定変更の展開時にトラフィックを検査できるようにするための詳細アクセス コントロール ポリシーの一般設定です。これは、展開する設定で Snort プロセスの再起動が不要な場合に限ります。このオプションは、次のように設定できます。

- [有効（Enabled）]：特定の設定で Snort 処理を再起動する必要な場合を除き、トラフィックは展開時に検査されます。

  展開する設定に Snort の再起動が必要でなければ、システムは現在展開されているアクセス コントロール ポリシーを使用してトラフィックを検査し、導入中に、展開しているアクセス コントロール ポリシーに切り替えます。

- [無効（Disabled）]：展開時にトラフィックは検査されません。Snort プロセスは展開時に必ず再起動されます。

次の図に、[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] を有効にした場合と無効にした場合の Snort の再起動の仕組みを示します。



注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作 （165 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（167 ページ）を参照してください。

Snort の再起動によるトラフィックの動作

次の表に、Snort プロセスが再起動した場合のさまざまなデバイスのトラフィックの処理方法を示します。

表 *12 : Firewall Threat Defense* および *Firewall Threat Defense Virtual* の再起動によるトラフィックの動作

インターフェイス コンフィギュレーション	再起動によるトラフィックの動作
inline: **Snort Fail Open: Down**: disabled	dropped

インターフェイス コンフィギュレーション	再起動によるトラフィックの動作
inline：**Snort Fail Open**：**Down**：enabled	検査なしで受け渡される Snort がダウンしていることをシステムが認識するまでに、一部のパケットがバッファ内で数秒間遅延することがあります。この遅延は、負荷分散によって異なります。ただし、バッファされたパケットは最終的に渡されます。
ルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む）：**preserve-connection** は enabled（**configure snort preserve-connection enable**、デフォルト） 詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。	既存の TCP/UDP フロー：Snort がダウンしている間、1 つでもパケットが着信すると、検査なしで渡されます。 新規 TCP/UDP フローとすべての非 TCP/UDP フロー：ドロップされる **preserve-connection** が有効になっている場合でも、次のトラフィックはドロップされることに注意してください。 • プレーンテキスト、パススルー プレフィルタ トンネル トラフィック（**Analyze** ルール アクションまたは**Analyze all tunnel traffic** デフォルト ポリシー アクションと一致） • アクセスコントロールルールと一致せず、デフォルトアクションによって代わりに処理される接続。 • 復号された TLS/SSL トラフィック • セーフ サーチ フロー • キャプティブ ポータル フロー
ルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む）：**preserve-connection** は disabled（**configure snort preserve-connection disable**）	dropped
inline: tap mode	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし

（注） Snort が再起動中に Snort プロセスがダウンした場合のトラフィックの処理に加え、Snort プロセスがビジーの場合、[Snortフェールオープン（Snort Fail Open）] の [ビジー（Busy）] オプション（インラインセットを設定します。（773 ページ）を参照）の設定によってトラフィックがインスペクションなしで転送されたり、ドロップされたりすることがあります。デバイスでは、[フェールセーフ（Failsafe）] オプションまたは [Snort フェール オープン（Snort Fail Open）] オプションのいずれかをサポートしていますが、同時に両方はサポートされません。

（注） 設定の導入時に Snort プロセスがビジーになったが、ダウンしなかった場合、CPU の合計負荷が 60 % を超えると一部のパケットがルーテッド、スイッチド、またはトランスペアレント インターフェイスでドロップする場合があります。

警告 Snort ルールの更新中は、システムを再起動しないでください。

Snort が十分な速度でパケットを処理できない場合、Snort ビジードロップが発生します。処理の遅延が原因でSnortがビジー状態にあるかどうか、またはコールブロッキングが原因でスタックしているかどうかは、Lina で認識されません。伝送キューがいっぱいになると、Snort ビジードロップが発生します。送信キューの使用率に基づいて、Linaはキューがスムーズに処理されている場合にアクセスを試みます。

展開またはアクティブ化された際に Snort プロセスを再起動する設定

AAB以外の構成を展開すると、Snortプロセスが再起動されます。AABの展開自体には再起動が伴いませんが、パケットの遅延が大きすぎると、現在展開されている AAB 設定がアクティブになり、Snort プロセスが部分的に再起動されます。

アクセス コントロール ポリシーの詳細設定

- [ポリシー適用時にトラフィックのインスペクションを実行する（Inspect traffic during policy apply）] が無効な場合に展開します。
- SSL ポリシーを追加または削除します。

ファイルポリシー（File Policy）

次のいずれかの構成の最初または最後を展開します。これらのファイルポリシー構成を展開しても再起動は発生しませんが、非ファイルポリシー構成を展開すると再起動が発生する可能性があることに注意してください。

- 次のいずれかの操作を行います。

- 展開されたアクセス コントロール ポリシーに 1 つ以上のファイル ポリシーが含まれている場合は、[アーカイブを検査する（Inspect Archives）] を有効または無効にします。
- [アーカイブを検査する（Inspect Archives）] が有効になっている場合は、最初のファイル ポリシー ルールを追加するか、または最後のファイル ポリシー ルールを削除します（[アーカイブを検査する（Inspect Archives）] が有意味であるためには 1 つ以上のルールが必要であることに注意してください）。

- [ファイルを検出（Detect Files）] または [ファイルをブロック（Block Files）] ルールで、[ストア ファイル（Store files）] を有効または無効にします。
- [マルウェアクラウドのルックアップ（Malware Cloud Lookup）] または [マルウェアをブロック（Block Malware）] ルールアクションと、分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[ダイナミック分析（Dynamic Analysis）] または [ローカル マルウェア分析（Local Malware Analysis）]）またはストアファイルオプション（[マルウェア（Malware）]、[不明（Unknown）]、[クリーン（Clean）] または [カスタム（Custom）]）を組み合わせた最初のアクティブファイルルールを追加するか、または最後のアクティブ ファイル ルールを削除します。

これらのファイル ポリシー構成をセキュリティ ゾーンまたはトンネル ゾーンに展開するアクセス コントロール ルールによって再起動が発生するのは、構成が次の条件を満たす場合だけであることに注意してください。

- アクセス コントロール ルールに含まれる送信元または宛先セキュリティ ゾーンは、ターゲット デバイス上のインターフェイスに関連付けられたセキュリティ ゾーンと一致する必要があります。
- アクセス コントロール ルールに含まれる宛先ゾーンが [任意（any）] でないかぎり、ルールに含まれる送信元トンネル ゾーンは、プレフィルタ ポリシーに含まれるトンネル ルールに割り当てられているトンネル ゾーンと一致する必要があります。

ID ポリシー

- SSL 復号が無効になっている場合（つまり、アクセス コントロール ポリシーに SSL ポリシーが含まれていない場合）は、最初のアクティブ認証ルールを追加するか、または最後のルールを削除します。

  アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれます。

ネットワーク検出（Network Discovery）

- ネットワーク検出ポリシーを使用して、HTTP、FTP、または MDNS プロトコル経由で権限のないトラフィックベースのユーザ検出を有効または無効にします。

Device Management

- MTU：デバイス上のすべての非管理インターフェイスの中で最大の MTU 値を変更します。
- 自動アプリケーションバイパス（AAB）：現在展開されている AAB 構成は、Snort プロセスの誤動作またはデバイスの誤設定により、単一のパケットが過度の処理時間を使用した場合にアクティブになります。その結果、Snort プロセスが部分的に再起動され、非常に大きい遅延が緩和されるか、または完全なトラフィックの停止が防止されます。この部分的な再起動により、デバイスがトラフィックをどのように処理するかに応じて、いくつかのパケットがインスペクションなしで通過するか、またはドロップされます。

Updates

- システムアップデート：新しいバージョンの Snort バイナリまたはデータ収集ライブラリ（DAQ）を含むソフトウェアアップデートの後に初めて構成を展開します。
- Snort 3 を実行している管理対象デバイスでは、脆弱性データベース（VDB）更新のインストール後に初めて構成を展開すると、一時的にアプリケーションの検出が中断する可能性がありますが、トラフィックは中断しません。

関連トピック

設定変更の展開 （172 ページ）
Snort 再起動のシナリオ （162 ページ）

変更により Snort プロセスがただちに再起動する場合

以下の変更を行うと、展開プロセスを経ることなく Snort プロセスが直ちに再起動されます。再起動がトラフィックにどのような影響を与えるかは、ターゲットデバイスがトラフィックを処理する方法によって異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。

- アプリケーションまたはアプリケーションディテクタに関する次の操作のいずれかを実行します。
  - システムまたはカスタム アプリケーション ディテクタを有効または無効にします。
  - アクティブ化されたカスタム ディテクタを削除します。
  - アクティブ化されたカスタム ディテクタを**保存して再アクティブ化**します。
  - ユーザ定義のアプリケーションを作成します。

  この操作を続けると管理対象のすべてのデバイスで Snort プロセスが再起動するという警告メッセージが表示され、キャンセルが可能になります。再起動は、現在のドメインまたはその子ドメインのいずれかの管理対象デバイスで発生します。
- Firewall Threat Defense ハイアベイラビリティペアを作成または解除します。

ハイアベイラビリティペアの作成を続行すると、プライマリデバイスとセカンダリデバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

ポリシー管理の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- ネットワーク管理者
- セキュリティ承認者

設定変更を展開するためのベストプラクティス

次に、設定変更の展開に関するガイドラインを示します。

信頼性の高い管理接続

Firewall Management Center とデバイスの間の管理接続は、それ自身とデバイスの間の安全な TLS-1.3 暗号化通信チャネルです。

セキュリティ上の理由から、サイト間VPNなどの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPNがダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

⚠

注意 デバイスの管理接続は、デバイス自体で終端する VPN トンネルを経由させないことをお勧めします。VPNがダウンする原因となる設定変更を展開すると、管理接続が切断され、デバイスに直接接続しないと設定を回復できなくなります。

管理トラフィックが VPN 終端インターフェイスから出る場合は、必ず、VPN トンネルから管理トラフィックを除外してください。

同時展開の最大数

同じジョブで Firewall Management Center に許可される最大デバイス数の 25% を超えるデバイスに展開しないでください。たとえば、FMCv300 の場合、最大ジョブサイズは 75 デバイス（300 の 25%）です。これより多いデバイスに同時に展開すると、パフォーマンスの問題が発生する可能性があります。

共有ポリシーの展開

最大限のパフォーマンスを実現するには、同じポリシーを使用するデバイスに展開します。ポリシーを共有するデバイスのグループごとに個別の展開ジョブを作成してください。

展開までの時間とメモリの制限

展開までの所要時間は、次の複数の要因（これらに限定されません）によって変わります。

- デバイスに送信する設定。たとえば、ブロックするセキュリティ インテリジェンス エントリの数を大幅に増やすと、展開にかかる時間が長くなることがあります。
- デバイス モデルとメモリ。メモリが少ないデバイスの場合、展開時間が長くなります。

デバイスの機能を超えないように注意してください。ターゲットデバイスでサポートされるルールまたはポリシーの最大数を超えると、システムが警告を表示します。最大数はいくつかの要因によって変わります。デバイスのメモリ量やプロセッサの数だけではなく、ポリシーやルールの複雑さも影響します。ポリシーとルールの最適化については、アクセス制御ルールのベストプラクティス （1736 ページ）を参照してください。

メンテナンスウィンドウの使用によるトラフィック中断の影響の軽減

メンテナンスウィンドウまたは中断の影響が最小限になる時間に展開することを強くお勧めします。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作 （165 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（167 ページ）を参照してください。

Firewall Threat Defense デバイスの場合、[展開（Deploy）] ダイアログの [検査の中断（Inspect Interruption）] 列に、展開するとトラフィックフローまたは検査が中断する可能性があることについて警告が表示されます。展開を続行、キャンセル、または延期できます。詳細については、デバイスの再起動の警告 （163 ページ）を参照してください。

関連トピック

Snort 再起動のシナリオ （162 ページ）

設定の展開

導入を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を導入する必要があります。導入のステータスは、メッセージ センターで確認できます。

導入を行うと、以下のコンポーネントが更新されます。

- デバイスとインターフェイスの設定
- デバイス関連ポリシー：NAT、VPN、QoS、プラットフォーム設定
- アクセス コントロールおよび関連するポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、プレフィルタ、SSL
- ネットワーク検出ポリシー
- 侵入ルールの更新
- これらの要素のいずれかに関連付けられている設定とオブジェクト

システムにポリシーを自動的に導入させるには、導入タスクをスケジュールするか、あるいは侵入ルールの更新をインポートする際に導入するようにシステムを設定します。特に、侵入ポリシーの更新によって侵入およびネットワーク分析に関するシステム定義の基本ポリシーを変更できるようにしている場合は、ポリシーの導入を自動化すると役立ちます。侵入ルール更新によって、アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細設定オプションのデフォルト値が変更されることもあります。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。メンテナンスの時間帯か、またはトラフィックフローとインスペクションに対する中断の影響が最小限になる時間に展開することを強くお勧めします。

⚠

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作 （165 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（167 ページ）を参照してください。

始める前に

- すべての管理対象デバイスが同じバージョンのセキュリティ ゾーン オブジェクトを使用していることを確認してください。セキュリティ ゾーン オブジェクトを編集している場合：同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、デ

バイスに設定変更を展開しないでください。すべての管理対象デバイスに同時に展開する必要があります。

- 展開の変更をプレビューするには、REST API アクセスを有効にします。REST API アクセスを有効にするには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Enabling REST API Access*」 の手順に従います。

（注） 展開時にデバイス CLI でデバイス設定が読み取られている場合、その展開プロセスは失敗します。展開中に **show running-config** などのコマンドを実行しないでください。

手順

ステップ 1 Firewall Management Center メニュー バーで、[展開（Deploy）] をクリックします。

ステップ 2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開（Deploy）] をクリックするか、[すべて展開（Deploy All）] をクリックしてすべてのデバイスを展開します。それ以外の場合は、追加の展開オプションを設定するために、[高度な展開（Advanced Deploy）] をクリックします。

この手順の残りの部分は、[高度な展開（Advanced Deploy）] 画面に適用されます。

図 *61* : 迅速な展開

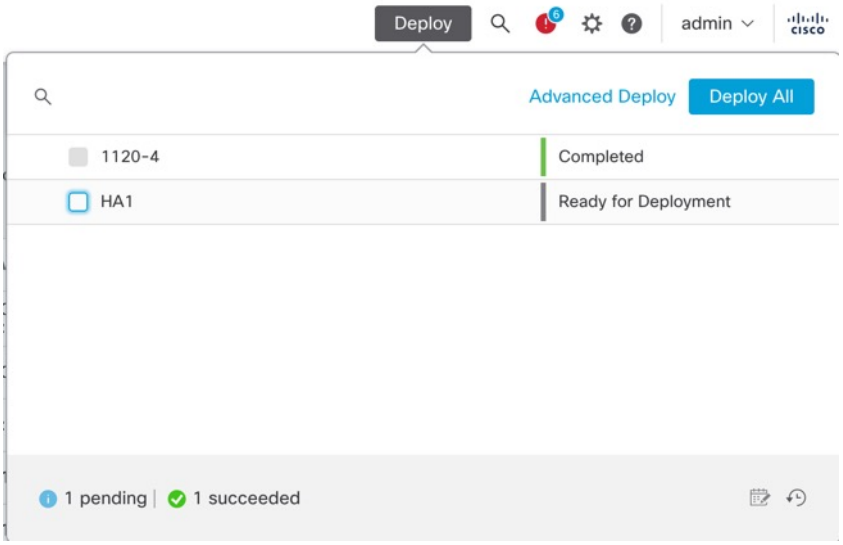
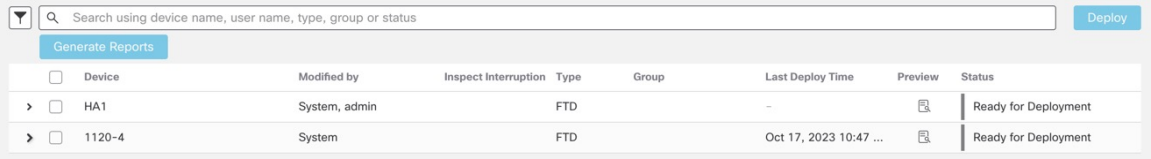
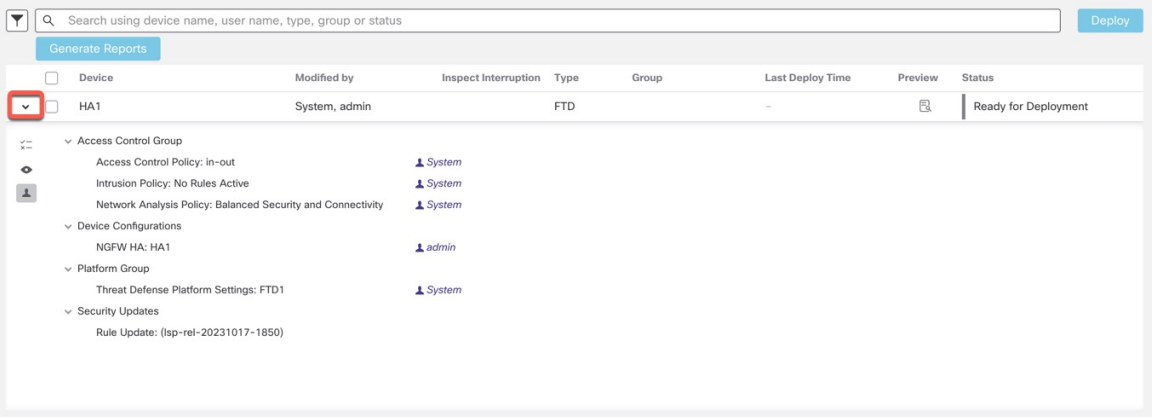


図 *62* : 高度な展開



ステップ 3 展開するデバイス固有の設定変更を表示するには、**展開矢印**（ › ） をクリックします。

図 *63* : 拡張



- [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザが表示されます。**システム**ユーザー（ログインユーザーではなく）が表示される場合の詳細については、システムユーザー名 （161 ページ）を参照してください。

  （注）
  削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断（Inspect Interruption）] 列には、展開時にデバイスでトラフィックインスペクションの中断が発生する可能性があるかどうかが示されます。

  ステータスに [あり（Yes）] と表示されている場合は、展開によって Firewall Threat Defense デバイスでインスペクションと、場合によってはトラフィックが中断され、展開されたリストには中断の原因となった特定の設定が [インスペクションの中断（Inspect Interruption）]（ ） で示されます。

  デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィックインスペクションが中断されないことを示します。

  Firewall Threat Defense デバイスへの展開時にトラフィックの検査を中断させたり、トラフィック自体を中断させる可能性のある構成の特定に役立つ例については、デバイスの再起動の警告 （163 ページ） を参照してください。

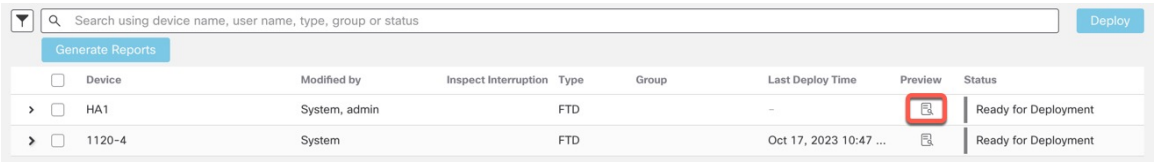
- [最終変更時刻（Last Modified Time）] 列は、最後に設定変更を行った時刻を指定します。

- [プレビュー（Preview）] 列では、次の展開の変更をプレビューできます。

- [ステータス（Status）] 列には、各展開のステータスが表示されます。詳細については、「展開ステータスの表示 （180 ページ）」を参照してください。

ステップ 4 [プレビュー（Preview）] 列で [プレビュー（Preview）]（） をクリックして、展開できる設定変更を表示します。

図 *64* : プレビュー

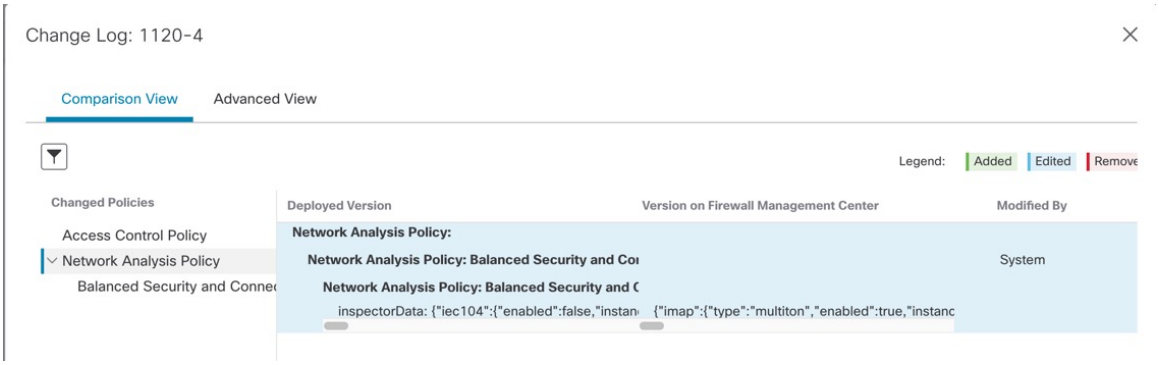


（注）
[システム（System）]（） > **[構成（Configuration）]** > **[情報（Information）]** で Firewall Management Center の名前を変更した場合、展開プレビューではこの変更が指定されませんが、展開が必要です。

プレビューでサポートされていない機能については、展開のプレビュー （156 ページ）を参照してください。

[比較ビュー（Comparison View）] タブには、すべてのポリシーおよびオブジェクトの変更が一覧表示されます。左ペインには、デバイス上で変更された異なるポリシータイプすべてがツリー構造でまとめて表示されます。

図 *65* : 比較ビュー



[フィルタ（Filter）]（） を使用すると、ユーザーレベルおよびポリシーレベルでポリシーをフィルタ処理できます。

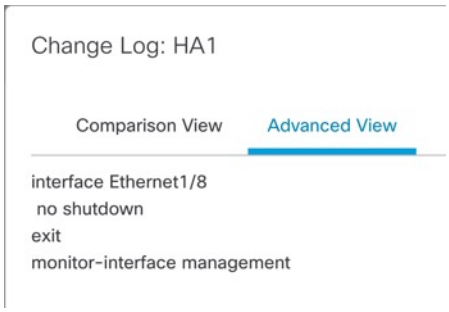
右側のペインには、ポリシー内のすべての追加、変更、または削除、あるいは左側のペインで選択したオブジェクトのリストが表示されます。右側のペインの 2 つの列には、最後に展開された設定（[展開済みのバージョン（Deployed Version）] 列）と、展開予定の変更（[Firewall Management Center でのバージョン（Version on Firewall Management Center）] 列）が示されます。最後に展開された設定は、デバイスからではなく、Firewall Management Center で最後に保存された展開のスナップショットから取得されます。設定の背景色は、ページの右上にある凡例に従って色分けされています。

[変更者（Modified By）]列には、設定を変更または追加したユーザーの一覧が表示されます。ポリシーレベルでは、Firewall Management Center はポリシーを変更したすべてのユーザーを表示し、ルールレベルでは、Firewall Management Center はルールを変更した最後のユーザーのみを表示します。

[レポートのダウンロード（Download Report）]ボタンをクリックすると、変更ログのコピーをダウンロードできます。

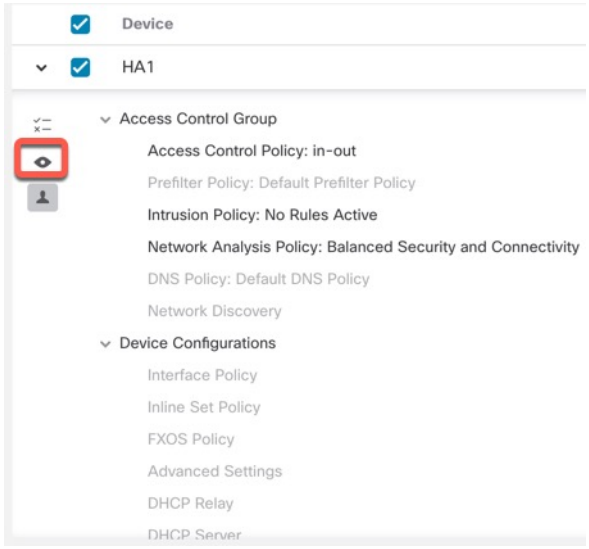
[詳細ビュー（Advanced View）] タブには、適用される CLI コマンドが表示されます。このビューは、Firewall Threat Defense のバックエンドで使用される ASA CLI に精通している場合に役立ちます。

図 *66* : 詳細ビュー



ステップ 5 [ポリシーの表示または非表示（Show or Hide Policy）]（） を使用して、関連付けられている未変更のポリシーを選択的に表示したり、非表示にしたりできます。

図 *67* : ポリシーの表示または非表示



ステップ 6 デバイス名の横にあるチェックボックスをオンにしてすべての設定変更を展開するか、[ポリシーの選択（Policy selection）]（） をクリックして、展開する個々のポリシーまたは設定を選択します（残りの変更は展開されずに保留されます）。

また、このオプションを使用して、特定のポリシーまたは設定に対する相互依存の変更を表示することもできます。Firewall Management Centerは、ポリシー間（たとえば、アクセスコントロールポリシーと侵入ポリシー間など）および共有オブジェクトとポリシーの間の依存関係を動的に検出します。相互依存の変更は、依存関係のある展開の変更を識別するために色分けされたタグを使用して示されます。展開変更のいずれかを選択した場合、相互依存の変更が自動的に選択されます。

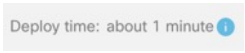
詳細については、選択的ポリシーの展開 （158 ページ）を参照してください。

（注）
- 共有オブジェクトの変更が展開されている場合は、影響を受けるポリシーも一緒に展開する必要があります。展開時に共有オブジェクトを選択すると、影響を受けるポリシーが自動的に選択されます。
- 選択的展開は、スケジュールされた展開と REST API を使用した展開はサポートされていません。これらの場合は、すべての変更を完全に展開することのみを選択できます。
- 警告とエラーの事前展開チェックは、選択したポリシーだけでなく、失効しているすべてのポリシーでも実行されます。したがって、警告またはエラーのリストには、選択していないポリシーも表示されます。
- 同様に、[展開（Deployment）] ページの[インスペクションの中断（Inspect Interruption）] 列の表示では、選択したポリシーだけでなく、失効しているすべてのポリシーも考慮されます。[インスペクションの中断（Inspect Interruption）] 列の情報については、デバイスの再起動の警告 （163 ページ） を参照してください。

ステップ 7 展開するデバイスまたはポリシーを選択したら、[概算見積（Estimate）] をクリックして展開期間の大まかな見積を取得します。

図 *68 :* 概算見積

図 *69 :* 展開時間



時間の長さは概算（70%の精度を含む）であり、導入にかかる実際の時間はいくつかのシナリオで異なる場合があります。20までのデバイスへの展開では、概算見積の信頼性が高いです。

選択したデバイスで最初に成功した展開が保留中であるため、概算見積が使用できない場合、データが使用できないことを示します。この状況は、Firewall Management Center の再イメージ化の後、バージョンアップグレードの後、または高可用性フェールオーバーの後に発生する可能性があります。

（注）
概算見積書がヒューリスティック手法に基づいているため、ポリシーの一括変更（一括ポリシーの移行の場合）および選択的な展開の場合、概算見積書は不正確で信頼性が高くありません。

ステップ 8 [展開（Deploy）] をクリックします。

ステップ 9 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ（Validation Messages）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

次の選択肢があります。

- [展開（Deploy）]：警告状態を解決せずに展開を続行します。警告を無視して変更を展開するには、[警告を無視する（Ignore warnings）] チェックボックスをオンにします。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次のタスク

- （オプション）展開ステータスをモニタします。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Viewing Deployment Messages*」を参照してください。
- 展開に失敗した場合は、設定変更を展開するためのベストプラクティス（170ページ）を参照してください。
- 展開中に、展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。たとえば、クラスタ環境で、サイト IP と同じサブネットにない IP アドレスの誤った設定がインターフェイスで設定されているとします。このエラーにより展開が失敗し、デバイスでロールバック操作の処理中に設定のクリアが試みられます。これらのイベントは、まとめて展開の失敗につながり、トラフィックが中断されます。

  展開が失敗したときにトラフィックの中断を引き起こす可能性がある設定変更については、次の表を参照してください。

設定の変更	存在するか	トラフィックへの影響
アクセス コントロール ポリシーでの **Threat Defense サービス**の変更	はい	はい
VRF	はい	はい
インターフェイス	はい	はい
QoS	はい	はい

（注） 展開中にトラフィックを中断する構成の変更は、Firewall Management Center と Firewall Threat Defense の両方がバージョン 6.2.3 以降である場合にのみ有効です。

関連トピック

Snort 再起動のシナリオ （162 ページ）

デバイスへの既存の設定の再展開

既存（変更なし）の設定を単一の管理対象デバイスに強制展開できます。メンテナンス ウィンドウで、またはトラフィック フローとインスペクションに対する中断の影響が最小限になる時間に、展開することを強くお勧めします。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作 （165 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（167 ページ）を参照してください。

始める前に

設定変更を展開するためのベストプラクティス （170ページ）で説明されているガイドラインを確認してください。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 強制導入するデバイスの横にある [編集（Edit）]（ ） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [全般（General）] セクション見出しの横にある [編集（Edit）]（ ） をクリックします。

ステップ 5 [展開を強制（Force Deploy）]（ ） をクリックします。

（注）
強制導入は、Firewall Threat Defense に導入されるポリシールールの完全な生成をともなうため、通常の導入よりも時間がかかります。

ステップ 6 [展開（Deploy）] をクリックします。

システムでは、展開中の設定で発生したエラーや警告が識別されます。[続行（Proceed）]をクリックすると、警告状態を解決せずに続行できます。ただし、システムがエラーを示している場合は、続行できません。

次のタスク

- （オプション）展開ステータスをモニタします。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Viewing Deployment Messages*」を参照してください。
- 展開が失敗した場合は、設定変更を展開するためのベストプラクティス（170ページ）を参照してください。

関連トピック

Snort 再起動のシナリオ （162 ページ）

展開の管理

展開ステータスの表示

[展開（Deployment）] ページの [ステータス（Status）] 列には、各デバイスの展開ステータスが表示されます。展開が進行中の場合は、展開の進行状況のライブステータスが表示されます。そうでない場合は、次のステータスのいずれかが表示されます。

- [保留中（Pending）]：展開するデバイスに変更があることを示します。
- [警告（Warnings）] または [エラー（Error）]：展開前のチェックで展開に関する警告またはエラーが検出されたことを示しており、展開には進んでいません。警告がある場合は展開を続行できますが、エラーがある場合は続行できません。

（注） [ステータス（Status）] 列には、[展開（Deployment）] ページの 1 つのユーザセッションに対してのみ、警告またはエラーのステータスが表示されます。ページから移動したり、ページを更新したりすると、ステータスは [保留中（Pending）] に変わります。

- [失敗（Failed）]：以前の展開の試行が失敗したことを示します。ステータスをクリックして詳細を表示します。
- [キュー内（In queue）]：展開が開始されたもののシステムが展開プロセスをまだ開始していないことを示します。
- [完了（Completed）]：展開が正常に完了したことを示します。

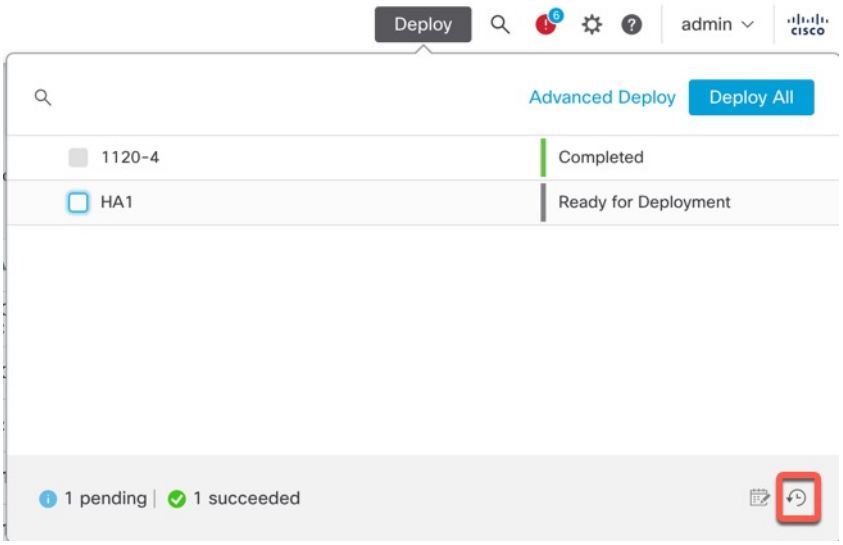
展開履歴の表示

展開履歴では、過去 10 回の成功した展開、最近 5 回の失敗した展開、および最近 5 回のロールバック展開がキャプチャされます。

手順

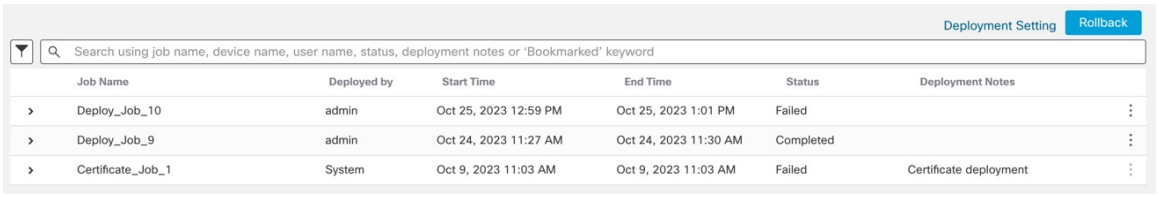
ステップ 1 Firewall Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開履歴（Deployment History）]（） をクリックします。

図 *70 : [*展開履歴（*Deployment History***）*]* アイコン**



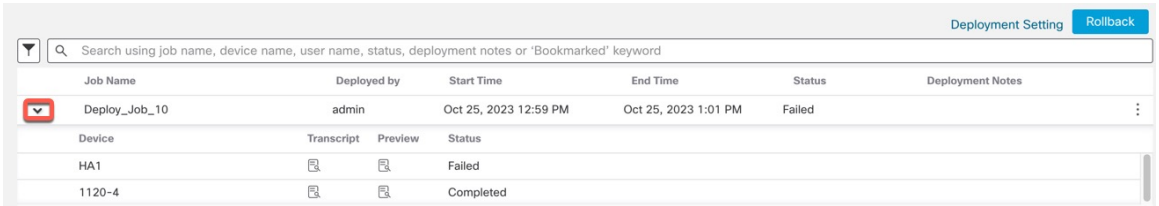
以前のすべての展開およびロールバックジョブのリストが、新しい順に表示されます。

図 *71 : [*展開履歴（*Deployment History***）*]* ページ**



ステップ 2 必要な展開ジョブの横にある **展開矢印**（ ） をクリックして、ジョブに含まれるデバイスとその展開ステータスを表示します。

図 *72 :* 拡張



- [展開に関する注（Deployment Notes）] 列で注意事項を確認します。

展開に関する注は、ユーザーが展開の一部として追加できるカスタムの注です。これらの注はオプションです。

ステップ 3 （オプション）[トランスクリプトの詳細（Transcript Details）]（）をクリックして、デバイスに送信されたコマンドと受信した応答を表示します。

図 *73* : [トランスクリプトの詳細（*Transcript Details*）] アイコン

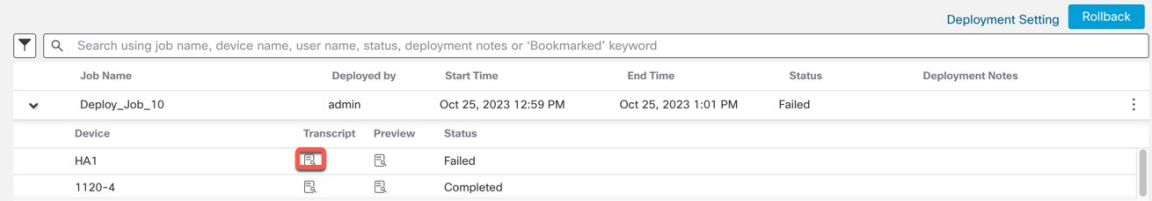
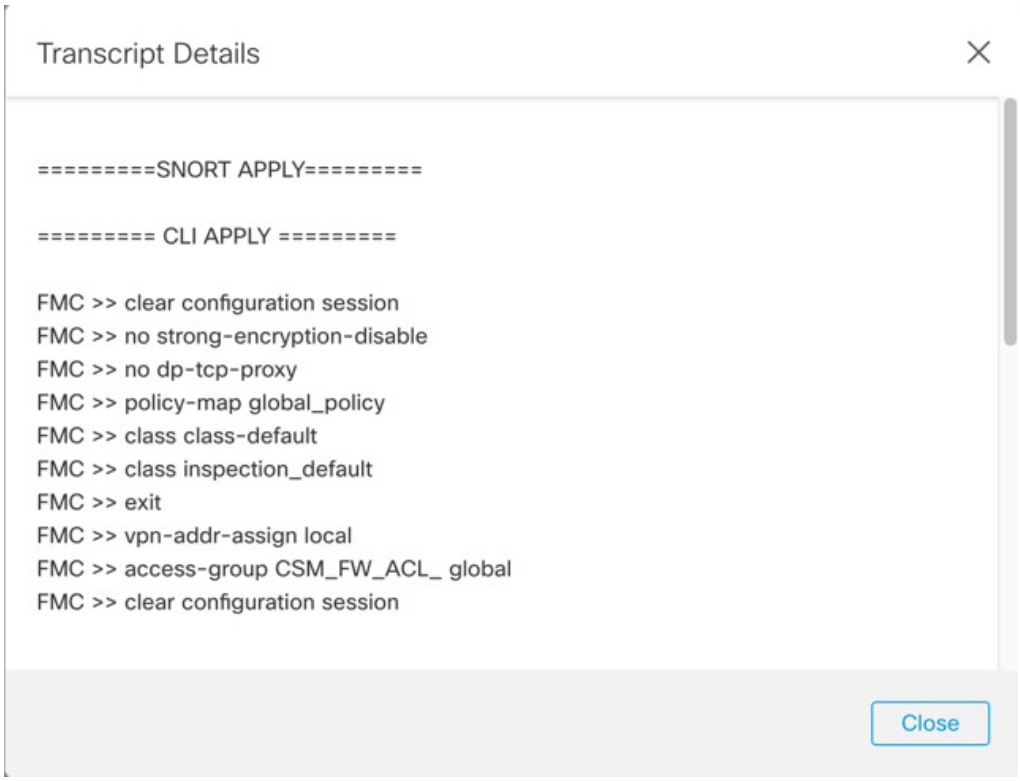


図 *74* : トランスクリプトの詳細



トランスクリプトには、次のセクションが含まれています。

- [Snortを適用（Snort Apply）]：Snort 関連ポリシーから障害または応答が発生すると、メッセージがこのセクションに表示されます。通常、このセクションは空です。
- [CLIを適用（CLI Apply）]：このセクションは、デバイスに送信されたコマンドを使用して設定される機能を対象にしています。

（注）

ロールバック操作のトランスクリプトでは、CLI コマンドの情報は提供されません。ロールバックコマンドを表示するには、展開ロールバックトランスクリプトの表示（190 ページ）を参照してください。

- [インフラストラクチャメッセージ（Infrastructure Messages）]：このセクションには、さまざまな導入モジュールのステータスが表示されます。

[CLIを適用（CLI Apply）]セクションでは、展開トランスクリプトには、デバイスに送信されたコマンド、およびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、コマンドを含むエラーを示すメッセージを探します。これらのエラーを調べることは、FlexConfig ポリシーを使用してカスタマイズされた機能を設定している場合に特に有用になる場合があります。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注）
管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

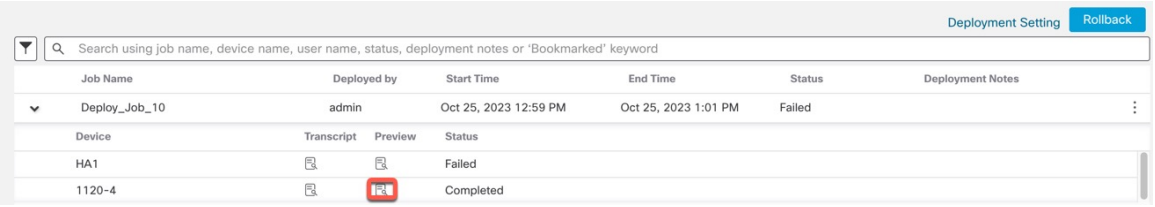
たとえば、次のシーケンスは、論理名が **outside** の GigabitEthernet0/0 を設定するコマンドを Firewall Management Center が送信したことを示しています。デバイスは、自動的にセキュリティレベルを 0 に設定したことを応答しました。Firewall Threat Defense がセキュリティレベルを使用することはありません。

```
========== CLI APPLY ==========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

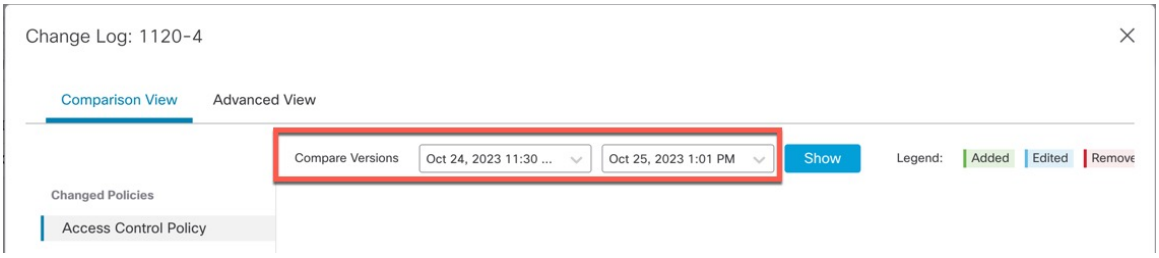
ステップ 4 （オプション）[プレビュー（Preview）]（） をクリックして、デバイスに展開されたポリシーとオブジェクトの変更を表示し、以前に展開されたバージョンと比較します。

図 *75 : [プレビュー（Preview）]アイコン*



1. 2 つのバージョンを比較して変更ログを表示するには、ドロップダウンボックスで必要なバージョンを選択し、[表示（Show）]ボタンをクリックします。ドロップダウンボックスには、展開ジョブの名前と展開の終了時間が表示されます。

図 *76 :* バージョンの比較



（注）
ドロップダウンボックスには、失敗した展開も表示されます。

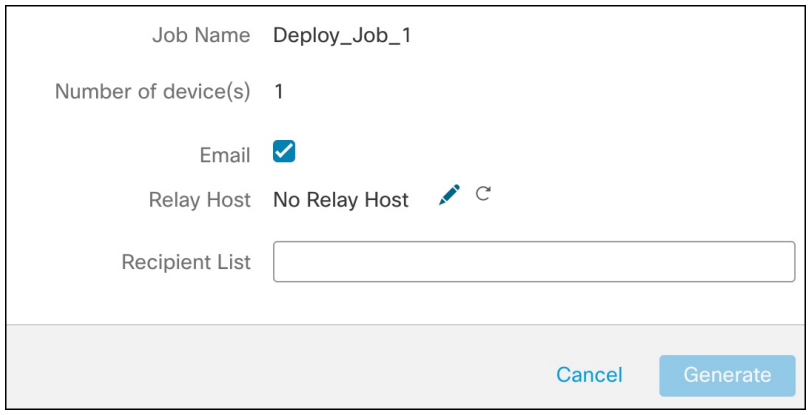
2. [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザーの一覧が表示されます。
   1. ポリシーレベルでは、Firewall Management Center はポリシーを変更したすべてのユーザーの名前を表示します。
   2. ルールレベルでは、Firewall Management Center はルールを変更した最後のユーザーを表示します。
3. [レポートのダウンロード（Download Report）] をクリックして、変更ログのコピーをダウンロードすることもできます。

（注）
- 展開履歴のプレビューは、証明書の登録、HA 操作、および失敗した展開ではサポートされていません。
- デバイスが登録されている場合でも、作成されたジョブ履歴レコードのプレビューはサポートされていません。

ステップ 5 （任意）各展開ジョブに対して、[その他（More）] アイコンをクリックして、他のアクションを実行します。

- [ブックマーク（Bookmark）] : 展開ジョブをブックマークします。
- [展開に関する注意の編集（Edit Deployment Notes）] : 展開ジョブに追加した、展開に関するカスタムの注意を編集します。
- [レポートの生成（Generate Report）] : 監査に使用できる展開レポートを生成します。このレポートには、プレビューとトランスクリプト情報を持つジョブプロパティが含まれており、レポートは PDF ファイルでダウンロードできます。
  1. [レポートの生成（Generate Report）] をクリックして、展開レポートを生成します。

図 77: レポートの作成



2. [レポートの生成（Generate Report）]ポップアップウィンドウで、[電子メール（Email）]チェックボックスをオンにします。
3. メールリレーホストが設定されている場合は、レポートを電子メールで送信することもできます。メールリレーホストが設定されていない場合は、[編集（Edit）]（）アイコンを使用してメールリレーホストを設定または変更します。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Configuring a Mail Relay Host and Notification Address」を参照してください。
4. [受信者リスト（Recipient List）] では、複数の電子メールアドレスをセミコロンで区切って入力することができます。
5. [生成（Generate）] をクリックしてレポートを生成します。このレポートは電子メールで受信者に送信されます。
6. [通知（Notifications）]タスクタブで、進捗状況を追跡できます。レポートの生成が完了したら、[通知（Notifications）]タスクタブのリンクをクリックして PDF レポートをダウンロードします。

展開のロールバック

デバイスを以前に展開した設定にロールバックできます。ポリシーの展開後に、デバイスを通過するトラフィックが意図しない方法で影響を受けた場合は、ロールバックにより、展開に失敗する前の状態にデバイスを戻すオプションが提供されます。

ロールバック中断を伴う操作です。既存のすべての接続とルートがドロップされ、トラフィックが中断されます。

中断を伴う設定の特定

展開がうまくいかず、意図しない方法でトラフィックの中断が発生した場合は、その状態の原因となっている展開の変更を特定し、展開が成功するように修正することを推奨します。

設定を比較するには、以下の方法を参照してください。

ロールバック前

1. **[展開（Deploy）]** > **[展開履歴（Deployment History）]** を選択し、最後に展開された（トラフィックの中断を引き起こした）ジョブを展開して、[プレビュー（Preview）]（ ）をクリックします。

   プレビューページには展開を比較するオプションがあり、以前の展開と比較した、展開の特定の変更を識別するために役立ちます。

2. 問題の原因となっている変更を特定したら、設定を修正し、デバイスに再展開します。

ロールバック後

1. ロールバック操作が成功したら、**[展開（Deploy）]** > **[展開（Deployment）]** を選択し、ロールバックされたデバイスの横にある [プレビュー（Preview）] アイコンをクリックします。
2. ロールバックされた設定と、展開が保留されている Firewall Management Center の最新の変更との間の変更点が表示されます。
3. 問題の原因となっている変更を特定したら、設定を修正し、デバイスに再展開します。

ロールバックのガイドラインと制約事項

- 現在展開されているバージョンより前の 10 個のバージョンのいずれかにロールバックできます。これより前のバージョンへのロールバックはサポートされていません。サポートされていないバージョンの場合、ロールバックアイコンはグレー表示になります。
- 再度ロールバックする前に、展開を実行する必要があります。
- ロールバックを実行すると、ロールバックされたデバイスは Firewall Management Center で期限切れとしてマークされます。設定に加えた変更は、次の展開のために保留されています。保留中の変更を表示するには、**[展開（Deploy）]** > **[展開（Deployment）]** を選択し、ロールバックされたデバイスの横にある [プレビュー（Preview）] アイコンをクリックします。
- [オブジェクトグループの検索（Object Group Search）] 設定が無効になっている場合、大きなアクセスリストを持つデバイスでは、ロールバック操作の完了に時間がかかることがあります。[オブジェクトグループの検索（Object Group Search）] 設定を確認するには、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスを選択して [詳細設定の編集（Edit Advanced Settings）] をクリックします。
- Firepower 4100/9300 の場合は、現在の Firewall Chassis Manager インターフェイス設定がどのロールバックバージョンでも同じであることを確認してください。そうでない場合、ロールバック インターフェイスの設定が実際のインターフェイスと一致しない可能性があります。

- マネージャ アクセス インターフェイス（マネージャまたはデータインターフェイス）がロールバックバージョンと現在のバージョンで異なる場合、ロールバックはサポートされません。
- 独立した証明書の登録も、[展開履歴（Deployment History）]ページに展開ジョブとして表示されます。ただし、これらのバージョンにロールバックすることはできません。証明書の登録後に作成された展開バージョンからのロールバックでは、証明書の関連付けも元に戻ります。ロールバック後の次の展開では、展開を続行する前に、証明書を手動で関連付けます。
- Firewall Management Center をアップグレードすると、デバイスをアップグレードしなかった場合でも、以前のソフトウェアリリースからのすべてのロールバックバージョンがデバイスで使用できなくなります。
- デバイスをアップグレードする場合は、現在のソフトウェアリリースのバージョンにのみロールバックできます。
- 展開頻度が [1回（Once）] に設定された FlexConfig オブジェクトがあるデバイスの展開がロールバックされた場合、プレビューページに古いと表示されていても、そのオブジェクトを再展開することはできなくなります。ロールバック後は、次の展開の前に、FlexConfig オブジェクトを手動で割り当て解除してから、デバイスに再割り当てする必要があります。
- ロールバックは以下の高可用性シナリオではサポートされていません。
  - ロールバックするバージョンに高可用性ブートストラップ設定が含まれている場合。つまり、スタンドアロンデバイスの高可用性を最初に形成したときの展開です。
  - 現在スタンドアロンモードのデバイスが、以前の展開バージョンで高可用性ペアの一部だった場合。
- クラスタリングについては、以下のガイドラインを参照してください。
  - 現在スタンドアロンモードのデバイスが、以前の展開バージョンでクラスタの一部だった場合、ロールバックはサポートされません。
  - （Secure Firewall 3100 およびプライベートクラウドの Firewall Threat Defense Virtual）クラスタリングブートストラップ設定を変更したり、ノードを追加または削除したりすると、それらの変更より前のバージョンにロールバックすることはできません。

ロールバック後に元に戻されない設定

ロールバックは、いくつかを除いて、デバイス上のすべての設定を元に戻します。詳細については、次の表を参照してください。

ロールバック中に元に戻される設定	ロールバック中に元に戻されない設定
• すべてのポリシー設定 • インターフェイス設定 • SRU 設定 • VDB 設定 • LSP 設定 • VPN 設定 • FXOS 設定	• Snort バイナリ • Geo DB

ロールバックの実行

デバイスを以前に展開した設定にロールバックできます。ポリシーの展開後に、デバイスを通過するトラフィックが意図しない方法で影響を受けた場合は、ロールバックにより、展開に失敗する前の状態にデバイスを戻すオプションが提供されます。

ロールバックは、選択したデバイス上の設定だけを元に戻します。

手順

ステップ 1 [展開（Deploy）] > [展開履歴（Deployment History）]（ ） を選択します。

以前のすべての展開ジョブのリストが、新しい順に表示されます。

ステップ 2 [ロールバック（Rollback）] をクリックします。

ステップ 3 [ジョブ（Job）] をクリックして [選択したジョブ（Selected Job）] ドロップダウンリストからジョブを選択するか、[デバイスリスト（Device List）] をクリックして、表示されるデバイスのリストをフィルタ処理します。

ステップ 4 （任意）[デバイスの検索（Search Device）] 検索ボックスにデバイス名を入力して、デバイスリストをフィルタ処理します。

ステップ 5 ロールバックするデバイスの横にあるボックスをオンにし、[ロールバックバージョン（Rollback Version）] ドロップダウンリストから各デバイスのバージョンを選択します。

図 *78* : 選択したジョブリスト

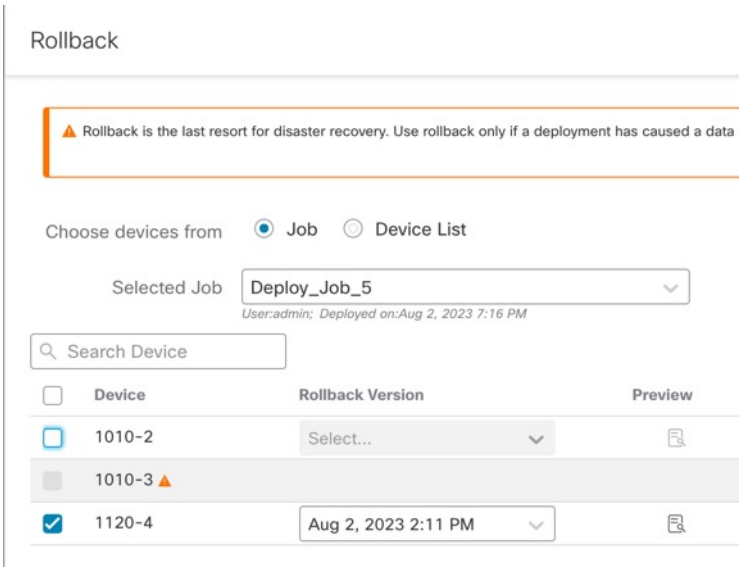
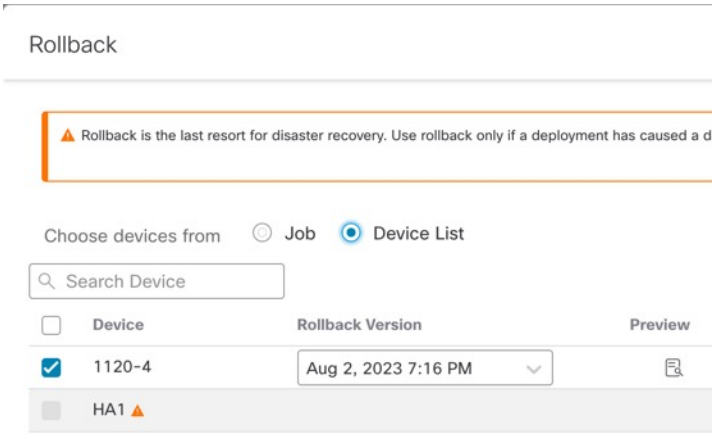


図 *79 : Device List*



特定のロールバックバージョンのジョブ名と関連する展開に関する注もリストされています。

ステップ 6 （任意）[プレビュー（Preview）]（） をクリックして、選択したバージョンで展開される変更を表示します。

ステップ 7 [ロールバック（Rollback）] をクリックします。

次のタスク

ロールバックのステータスを確認するには、**[展開（Deploy）]** > **[展開（Deployment）]** を選択します。デバイス名の横にあるロールバックステータスを確認できます。

展開ロールバック トランスクリプトの表示

ロールバック トランスクリプトは、デバイスから返される応答とともに、デバイスに送信されるコマンドの文章バージョンです。ロールバック操作が失敗した場合、[展開（Deploy）]>[展開履歴（Deployment History）] ページのトランスクリプトに失敗の理由が示されます。ただし、成功したロールバック操作で実行されたCLIコマンドを知るには、ロールバック操作の完了後に以下の手順に従ってください。この情報は、次回の展開までしか利用できないことに注意してください。

（注） CLI コマンド情報は、ロールバックの完了後に利用でき、次回の展開までのみ利用できます。ロールバック操作後の最初の展開では、ロールバック関連のすべての情報が消去されます。

（注） ロールバック展開では、[展開に関する注（Deployment Notes）] がロールバックジョブとして自動的に更新されます。[展開履歴（Deployment History）]ページで、ユーザーは[検索（Search）]オプションを使用してロールバックジョブを簡単にフィルタ処理できます。

手順

ステップ 1 Secure Firewall Management Center メニューバーで、**[システム（System）]**>**[正常性（Health）]**>**[モニター（Monitor）]** を選択します。

ステップ 2 左ペインからロールバックしたデバイスを選択します。

ステップ 3 [システムとトラブルシューティングの詳細を表示（View System & Troubleshooting Details）] リンクをクリックします。

ステップ 4 [詳細なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 5 [脅威防御 CLI（Threat Defense CLI）] をクリックします。

ステップ 6 [コマンド（Command）] ドロップダウンボックスから [show] を選択します。

ステップ 7 [パラメータ（Parameter）] フィールドに **`running`** と入力します。

ステップ 8 [実行（Execute）] をクリックします。

ポリシーの比較

変更後のポリシーが組織の標準に準拠することを確かめたり、システムパフォーマンスを最適化したりする目的で、2つのファイルポリシーの間の違いや、保存済みポリシーと実行中のポリシーの間の違いを調べることができます。

比較できるポリシーのタイプは次のとおりです。

- DNS

- ファイル
- ヘルス
- アイデンティティ
- ネットワーク分析
- SSL

比較ビューには、両方のポリシーが並べて表示されます。2 つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が2つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

始める前に

特定のポリシーに対するアクセス権と必要なライセンスがあり、ポリシーを設定するための正しいドメインにいる場合にのみ、ポリシーを比較できます。

手順

ステップ 1 比較するポリシーの管理ページにアクセスします。

- [DNS]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[DNS]**
- [ファイル（File）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[マルウェアとファイル（Malware & File）]**
- [状況（Health）]：[システム（System）]（⚙）> **[ヘルス（Health）]** > **[ポリシー（Policies）]**
- [ID（Identity）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アイデンティティ（Identity）]**
- ネットワーク分析：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]**に移動し、[ネットワーク分析ポリシー（**Network Analysis Policy**）] または **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**[をクリックし、**[ネットワーク分析ポリシー（Network Analysis Policies）]** をクリックします。

  （注）
  カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[復号（Decryption）]**

ステップ 2 [Compare Policies] をクリックします。

ステップ 3 [比較対象（Compare Against）] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[他のポリシー（Other Policy）] を選択します。
- 同じポリシーの2つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。
- 現在のアクティブポリシーを他のポリシーに対して比較するには、[実行中の設定（Running Configuration）] を選択します。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合、[ポリシーA（Policy A）] ドロップダウンリストと [ポリシーB（Policy B）] ドロップダウンリストから比較するポリシーを選択します。
- 実行中の設定を別のポリシーと比較する場合、[ポリシーB（Policy B）] ドロップダウンリストから 2 番目のポリシーを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 比較の結果を確認します。

- [比較ビューア（Comparison Viewer）]：比較ビューアを使用して、ポリシーの違いを個別に検索するには、タイトルバーの上にある [前へ（Previous）] または [次へ（Next）] をクリックします。
- [比較レポート（Comparison Report）]：2 つのポリシーの違いを示す PDF レポートを生成するには、[比較レポート（Comparison Report）] をクリックします。

現在のポリシーレポートの生成

ほとんどのポリシーには、2 種類のレポートを生成することができます。単一のポリシーに関するレポートには、現在保存されているポリシー設定の詳細が記載されます。一方、比較レポートには、2つのポリシー間の違いだけがリストされます。単一ポリシー レポートは、ヘルス ポリシーを除くすべてのポリシー タイプについて生成できます。

（注） 侵入ポリシー レポートには基本ポリシーの設定とポリシー階層の設定が結合され、どちらが基本ポリシーまたはポリシー レイヤのどちらに基づく設定であるかは区別されません。

始める前に

特定のポリシーに対するアクセス権と必要なライセンスがあり、ポリシーを設定するための正しいドメインにいる場合にのみ、ポリシーレポートを生成できます。

手順

ステップ 1 レポートを生成するポリシーの管理ページにアクセスします。

- アクセス制御—**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]**
- [DNS]：**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [DNS]**
- [ファイル（File）]：**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [マルウェアとファイル（Malware & File）]**
- [状況（Health）]：[システム（System）]（⚙）**>[ヘルス（Health）]>[ポリシー（Policies）]**
- [ID（Identity）]：**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（Identity）]**
- [侵入（Intrusion）]：**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**
- [NAT]：**[デバイス（Devices）] > [NAT]**
- [ネットワーク分析（Network Analysis）]：**[ポリシー（Policies）]>[アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]** をクリックします。

  （注）
  カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]**

ステップ 2 レポートの生成対象とするポリシーの横にある **[レポート（Report）]**（📄） をクリックします。

設定の展開の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
設定の変更を展開するときに、レポートを生成して電子メールで送信します。	7.2	任意（Any）	任意の展開のレポートを生成できるようになりました。 新規/変更された画面：**[展開（Deploy）] > [展開履歴アイコン（Deployment History icon）] > [詳細（More）] > [レポートの生成（Generate Report）]**

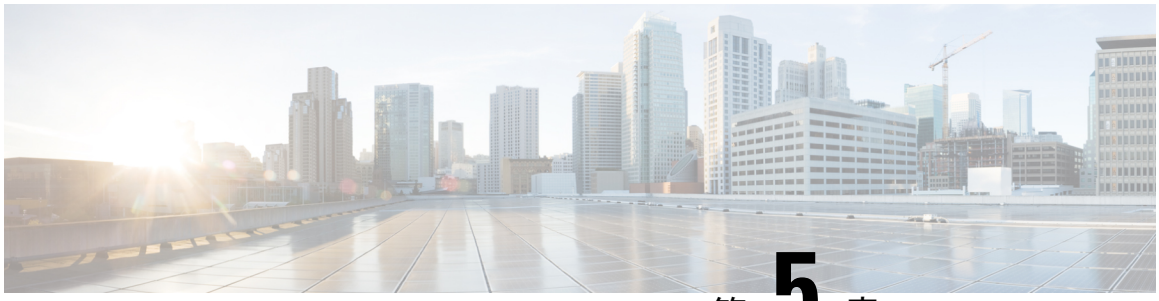
機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
展開プレビューとプレビュー時のユーザー情報。	7.0	任意（Any）	[展開（Deployment）] ページには、次の新たに追加された機能があります。 • [展開（Deployment）] ページの [変更者（Modified By）] 列には、各ポリシーリストに対してポリシーを変更したユーザーが一覧表示されます。 • 展開のフィルタサポート：[展開（Deployment）] ページに表示されるフィルタアイコンには、展開が保留されているデバイスのリストをフィルタ処理するオプションが用意されています。フィルタアイコンには、選択されたデバイスとユーザー名に基づいてリストをフィルタ処理するオプションがあります。 • 展開履歴のプレビュー：[プレビュー（Preview）] をクリックして、デバイスに展開されたポリシーとオブジェクトの変更を表示し、以前に展開されたバージョンと比較します。展開履歴では、最近 10 回の成功した展開、最近 5 回の失敗した展開、および最近 5 回のロールバック展開がキャプチャされます。 • 展開に関する注：[展開に関する注（Deployment Notes）] は、ユーザーが展開の一部として追加できるカスタムおよびオプションの注です。[展開履歴（Deployment History）] ページで [展開に関する注（Deployment Notes）] 列を表示できます。 • 展開のロールバックは、Snort 3 ポリシーでも利用できます。
Firewall Threat Defense デバイスでの展開のロールバック。	6.7	6.7	ロールバックは、Firewall Threat Defense デバイス上の既存の展開を削除し、以前に展開された構成でデバイスを再構成するために提供されている展開機能です。 新規/変更されたページ：**[展開（Deploy）]** > **[展開履歴（Deployment History）]** ページには、ロールバックアイコンのある新しい [ロールバック（Rollback）] 列が用意されています。ジョブを展開すると、同様のロールバックアイコンが表示されるため、デバイスレベルでロールバックを開始できます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しい展開 Web インターフェイス。	6.6	任意（Any）	Firewall Management Center メニューバーの [展開（Deploy）] ボタンが [展開（Deploy）] メニューに変更されました。その下に 2 つの新しいサブメニューオプションがあります。[展開（Deployment）] と [展開履歴（Deployment History）] です。[展開（Deployment）] ページは改善が施されたとともに新しい機能が追加され、新しい [展開履歴（Deployment History）] ページには、以前のすべての展開の凡例が表示されます。 [展開（Deployment）] ページには、次の新たに追加された機能があります。 • 展開のステータス：[展開（Deployment）] ページの [ステータス（Status）] 列には、各デバイスの展開ステータスが表示されます。 • 展開の概算見積：[展開（Deployment）] ページでは、デバイス、ポリシー、または設定を選択した後にのみ、[概算見積（Estimate）] リンクを使用できます。[概算見積（Estimate）] リンクをクリックすると、展開期間の概算見積を取得できます。 • 展開のプレビュー：プレビューには、デバイス上に展開するポリシーとオブジェクトのすべての変更のスナップショットが表示されます。ポリシーの変更には、新しいポリシー、既存のポリシーの変更、および削除されたポリシーが含まれます。オブジェクトの変更には、ポリシーで使用される追加および変更されたオブジェクトが含まれます。 • 選択的ポリシーの展開：Firewall Management Center では、展開が予定されているデバイス上の変更すべてのリスト内で特定のポリシーを選択し、選択したポリシーのみを展開することができます。

第 II 部

デバイスの操作

- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード （199 ページ）
- Firepower 4100/9300 の論理デバイス （213 ページ）
- 高可用性 （283 ページ）
- における Firewall Threat Defense のクラスタの展開Cisco Secure Firewall 3100 のクラスタリング （323 ページ）
- プライベートクラウドでの Threat Defense Virtual のクラスタリング （389 ページ）
- パブリッククラウドでの Threat Defense Virtual のクラスタリング （445 ページ）
- Firepower 4100/9300 のクラスタリング （543 ページ）



第 5 章

トランスペアレントファイアウォールモードまたはルーテッドファイアウォールモード

この章では、ファイアウォールモードをルーテッドまたはトランスペアレントに設定する方法と、各ファイアウォールモードでファイアウォールがどのように機能するかについて説明します。

（注） ファイアウォールモードは通常のファイアウォールインターフェイスにのみ影響を与えます。インライン セットやパッシブ インターフェイスなどの IPS 専用インターフェイスには影響を与えません。IPS 専用インターフェイスは両方のファイアウォールモードで使用可能です。IPS 専用インターフェイスの詳細については、インラインセットとパッシブインターフェイス（763 ページ）を参照してください。インライン セットは「トランスペアレント インライン セット」と呼ばれることもありますが、インライン インターフェイス タイプはこの章で説明するトランスペアレント ファイアウォール モードおよびファイアウォール タイプのインターフェイスとは無関係です。

注意

- FTD CLI コマンドを使用して「ファイアウォールモード」を設定します。

- ファイアウォール モードについて （200 ページ）
- デフォルト設定 （208 ページ）
- ファイアウォール モードのガイドライン （209 ページ）
- ファイアウォール モードの設定 （210 ページ）

ファイアウォール モードについて

Firewall Threat Defense は、通常のファイアウォール インターフェイスでルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの 2 つのファイアウォール モードをサポートします。

ルーテッド ファイアウォール モードについて

ルーテッド モードでは、Firewall Threat Defense デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。

統合ルーティングおよびブリッジングにより、ネットワーク上の複数のインターフェイスをまとめた「ブリッジグループ」を使用できます。そして、Firewall Threat Defense デバイス はブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。Firewall Threat Defense デバイス は BVI と通常のルーテッドインターフェイス間でルーティングを行います。クラスタリング、EtherChannel、またはメンバーインターフェイスが必要ない場合は、トランスペアレントモードではなくルーテッドモードの使用を検討してください。ルーテッド モードでは、トランスペアレント モードと同様に 1 つ以上の分離されたブリッジ グループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッド インターフェイスも含めることができます。

トランスペアレント ファイアウォール モードについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

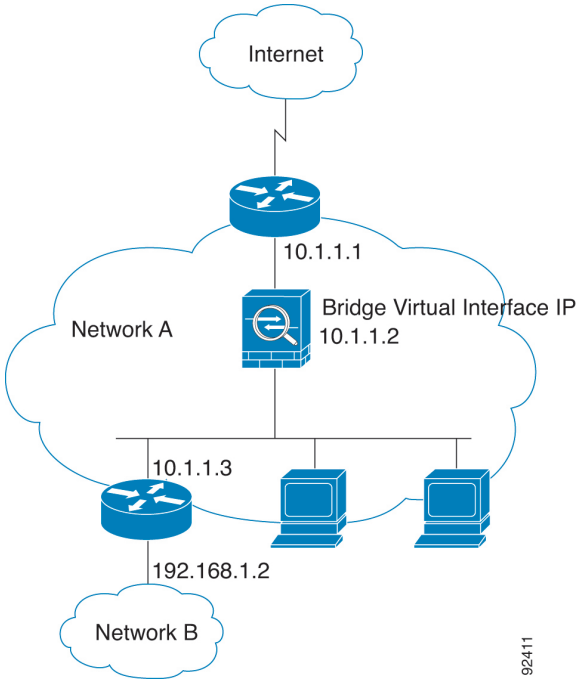
レイヤ2の接続は、ネットワーク上の内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して確立されます。また、Firewall Threat Defense デバイス はブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレント モードでは、これらのブリッジグループは相互通信できません。

ネットワークでのトランスペアレント ファイアウォールの使用

Firewall Threat Defense デバイス は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレント ファイアウォールはルーティングされたホップではないため、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータと各ホストは、外部ルータに直接接続されているように見えます。

図 *80*: トランスペアレント ファイアウォール ネットワーク



ルーテッド モード機能のためのトラフィックの通過

トランスペアレントファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセスルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、IP/TV で作成されるようなマルチキャスト トラフィックを許可したりできます。また、トランスペアレントファイアウォールを通過するルーティング プロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、または BGP トラフィックをアクセス ルールに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは Firewall Threat Defense デバイス を通過できます。

ブリッジグループについて

ブリッジ グループは、Firewall Threat Defense デバイス がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。他のファイアウォールインターフェイスのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のチェックがすべて実施されます。

ブリッジ仮想インターフェイス（BVI）

各ブリッジグループには、ブリッジ仮想インターフェイス（BVI）が含まれます。Firewall Threat Defenseデバイスは、ブリッジグループから発信されるパケットの送信元アドレスとしてこのBVI IPアドレスを使用します。BVI IPアドレスはブリッジグループ メンバー インターフェイスと同じサブネット上になければなりません。BVIでは、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IPアドレスと同じネットワーク上のトラフィックだけがサポートされています。

トランスペアレントモード：インターフェイスベースの各機能はブリッジグループのメンバーインターフェイスだけを指定でき、これらについてのみ使用できます。

ルーテッドモード：BVIはブリッジグループと他のルーテッドインターフェイス間のゲートウェイとして機能します。ブリッジグループ/ルーテッドインターフェイス間でルーティングするには、BVIを指定する必要があります。一部のインターフェイスベース機能に代わり、BVI自体が利用できます。

- DHCPv4サーバ：BVIのみがDHCPv4サーバの構成をサポートします。
- スタティックルート：BVIのスタティックルートを設定できます。メンバーインターフェイスのスタティック ルートは設定できません。
- Syslogサーバーと Firewall Threat Defense デバイス 由来の他のトラフィック：syslogサーバー（またはSNMPサーバー、Firewall Threat Defense デバイス からトラフィックが送信される他のサービス）を指定する際、BVIまたはメンバーインターフェイスのいずれかも指定できます。

ルーテッドモードでBVIを指定しない場合、Firewall Threat Defense デバイス はブリッジ グループのトラフィックをルーティングしません。この設定は、ブリッジグループのトランスペアレント ファイアウォール モードを複製します。クラスタリング、またはEtherChannelメンバーインターフェイスが不要であれば、ルーテッドモードの使用を検討すべきです。ルーテッド モードでは、トランスペアレント モードと同様に1つ以上の分離されたブリッジ グループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッド インターフェイスも含めることができます。

トランスペアレント ファイアウォール モードのブリッジグループ

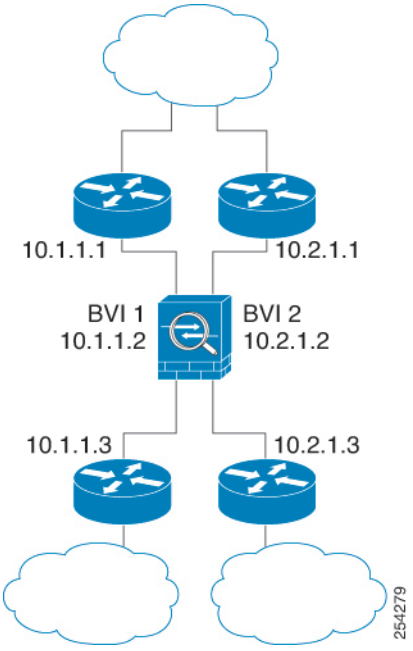
ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは Firewall Threat Defense デバイス 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから Firewall Threat Defense デバイス 内の他のブリッジ グループにルーティングされる前に、Firewall Threat Defense デバイス から出る必要があります。ブリッジング機能はブリッジグループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslogサーバまたはAAAサーバの設定は、すべてのブリッジ グループで共有されます。

1つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジグループとインターフェイスの正確な数については、ファイアウォールモードのガイドライン（209ページ）を参照してください。ブリッジグループごとに2つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセ

グメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが3つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2つのブリッジグループを持つ、Firewall Threat Defenseデバイスに接続されている2つのネットワークを示します。

図 *81 : 2* つのブリッジ グループを持つトランスペアレント ファイアウォール ネットワーク

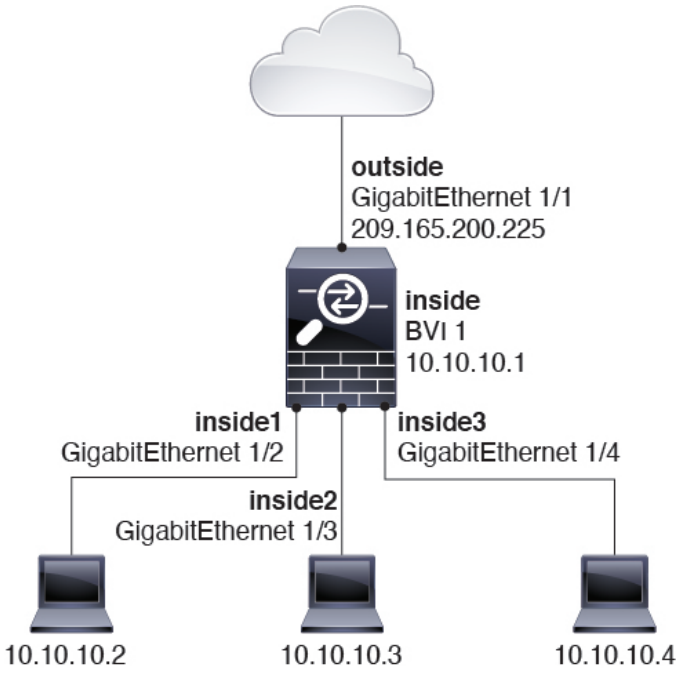


ルーテッド ファイアウォール モードのブリッジグループ

ブリッジグループ トラフィックは他のブリッジ グループまたはルーテッド インターフェイスにルーティングできます。ブリッジグループのBVIインターフェイスに名前を割り当てないことで、ブリッジグループのトラフィックを分離することもできます。BVIに名前を付けると、その BVI はその他の通常のインターフェイスと同様にルーティングに参加します。

ルーテッドモードでブリッジグループを使用する方法として、外部スイッチの代わりにFirewall Threat Defense 追加のインターフェイスを使用する方法があります。たとえば、デバイスの中には、通常のインターフェイスとして外部インターフェイスを持ち、その他すべてのインターフェイスが内部ブリッジグループに割り当てられているというデフォルト設定のものがあります。このブリッジグループは外部スイッチを置き換えることを目的としているので、すべてのブリッジグループ インターフェイスが自由に通信できるようにアクセス ポリシーを設定する必要があります。

図 *82*:内部ブリッジグループと外部ルーテッド インターフェイスからなるルーテッド ファイアウオール ネットワーク



レイヤ 3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックがブリッジグループを通過するにはアクセル ルールが必要です。
- ARP は、アクセス ルールなしで両方向にブリッジグループを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセス ルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャスト トラフィックは、アクセス ルールを使用して通過させることができます。

許可される MAC アドレス

アクセス ポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます（レイヤ 3 トラフィックの許可 （204 ページ）を参照）。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF の IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF の IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD に等しい BPDU マルチキャスト アドレス

BPDU 処理

スパニングツリープロトコルを使用するときのループを防止するために、デフォルトでBPDUが渡されます。

デフォルトでは、BPDUは高度なインスペクションにも転送されます。このインスペクションは、このタイプのパケットには必要なく、インスペクションの再起動によってブロックされた場合など、問題を引き起こす可能性があります。BPDUは高度なインスペクションから常に除外することをお勧めします。これを行うには、FlexConfigを使用してBPDUを信頼するEtherType ACLを設定し、各メンバー インターフェイス上の高度な検査からBPDUを除外します。FlexConfig ポリシー （2687 ページ）を参照してください。

FlexConfig オブジェクトは次のコマンドを展開する必要があります。ここで、<if-name> はインターフェイス名に置き換えます。必要な数の access-group コマンドを追加して、デバイス上の各ブリッジ グループのメンバー インターフェイスをカバーします。また、ACL に別の名前を選択することもできます。

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

MAC アドレスとルート ルックアップ

ブリッジ グループ内のトラフィックでは、パケットの発信インターフェイスは、ルート ルックアップではなく宛先 MAC アドレス ルックアップを実行することによって決定されます。

ただし、次の場合にはルート ルックアップが必要です。

- トラフィックの発信元が Firewall Threat Defense デバイス：syslog サーバーなどがあるリモート ネットワーク宛てのトラフィック用に、Firewall Threat Defense デバイス にデフォルト/スタティック ルートを追加します。
- Voice over IP（VoIP）および TFTP トラフィック、エンドポイントが 1 ホップ以上離れている：セカンダリ接続が成功するように、リモートエンドポイント宛てのトラフィック用に、Firewall Threat Defense デバイス にスタティック ルートを追加します。Firewall Threat Defenseデバイスは、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なるIPアドレスのセットが使用される可能性があるため、Firewall Threat Defenseデバイスは正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

  影響を受けるアプリケーションは次のとおりです。

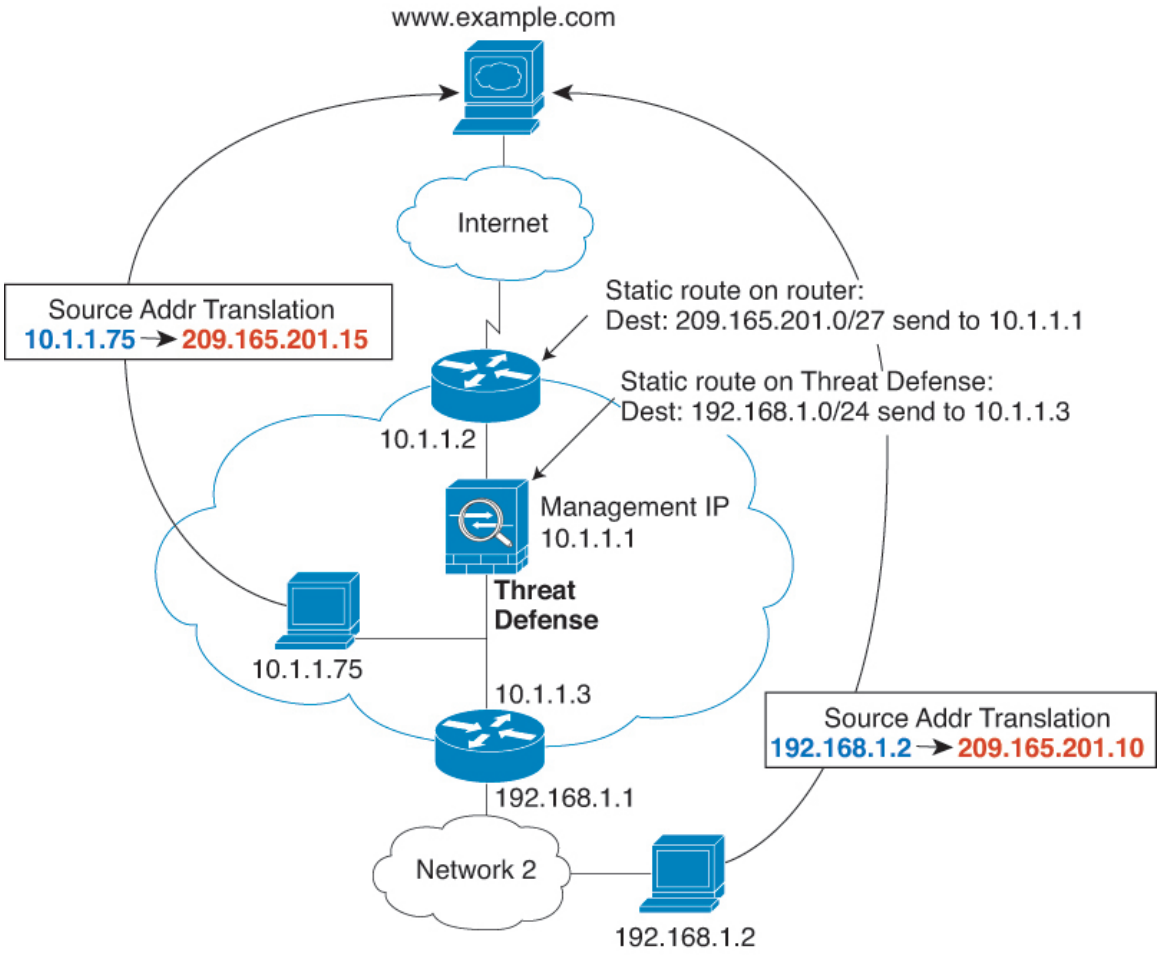
  - H.323
  - RTSP
  - SIP
  - Skinny（SCCP）
  - SQL*Net

- SunRPC
- TFTP

- Firewall Threat Defense デバイス が NAT を実行する 1 ホップ以上離れたトラフィック：リモート ネットワーク宛てのトラフィック用に、Firewall Threat Defense デバイス にスタティック ルートを設定します。また、Firewall Threat Defense デバイス に送信されるマッピング アドレス宛てのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

  このルーティング要件は、NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。Firewall Threat Defense デバイス は、変換を実行できるように正しい出力インターフェイスを識別する必要があります。

図 *83 : NAT* の例：ブリッジ グループ内の *NAT*



トランスペアレント モードのブリッジ グループのサポートされていない機能

次の表に、トランスペアレント モードのブリッジ グループでサポートされない機能を示します。

表 *13*：トランスペアレント モードでサポートされない機能

特長	説明
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	ブリッジグループ メンバー インターフェイスでは、DHCPv4 サーバのみがサポートされます。
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバーとして機能することができますが、DHCP リレーはサポートしません。2 つのアクセス ルール（1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバーからの応答を逆方向に許可します。）を使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループ メンバー インターフェイスの場合、Firewall Threat Defense デバイス で発信されたトラフィックにスタティック ルートを追加できます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが Firewall Threat Defense デバイス を通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが Firewall Threat Defense デバイス を通過できるようにすることができます。
QoS	-
通過トラフィック用の VPN 終端	トランスペアレント ファイアウォールは、ブリッジ グループ メンバー インターフェイスでのみ、管理接続用のサイト間 VPN トンネルをサポートします。これは、Firewall Threat Defense デバイスを通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックに ASA を通過させることはできますが、非管理接続は終端されません。

ルーテッド モードのブリッジ グループのサポートされていない機能

次の表に、ルーテッド モードのブリッジ グループでサポートされない機能を示します。

表 *14*：ルーテッド モードでサポートされない機能

特長	説明
EtherChannel メンバー インターフェイス	物理インターフェイス、冗長インターフェイス、およびサブインターフェイスのみがブリッジ グループ メンバー インターフェイスとしてサポートされます。 Diagnostic インターフェイスもサポートされていません。

特長	説明
クラスタリング	ブリッジ グループはクラスタリングでサポートされません。
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	DHCPv4 サーバーのみが BVI でサポートされます。
DHCP リレー	ルーテッドファイアウォールはDHCPv4 サーバーとして機能することができますが、DHCP リレーを BVI またはブリッジ グループ メンバー インターフェイスでサポートしません。
ダイナミック ルーティング プロトコル	ただし、BVI のスタティック ルートを追加することはできます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが Firewall Threat Defense デバイス を通過できるようにすることもできます。非ブリッジ グループ インターフェイスはダイナミック ルーティングをサポートします。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが Firewall Threat Defense デバイス を通過できるようにすることができます。非ブリッジ グループ インターフェイスはマルチキャスト ルーティングをサポートします。
QoS	非ブリッジ グループ インターフェイスは、QoS をサポートします。
通過トラフィック用の VPN 終端	VPN 接続を BVI で終端することはできません。非ブリッジ グループ インターフェイスは、VPN をサポートします。 ブリッジ グループ メンバー インターフェイスは、管理接続専用のサイト間 VPN トンネルをサポートします。これは、Firewall Threat Defense デバイスを通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックにブリッジ グループを通過させることはできますが、非管理接続は終端されません。

デフォルト設定

ブリッジ グループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジ グループ内で渡されます。

ファイアウォール モードのガイドライン

ブリッジグループのガイドライン（トランスペアレントおよびルーテッドモード）

- 64のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Firewall Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- デバイスとデバイス間の管理トラフィック、および Firewall Threat Defense デバイス を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- マルチインスタンスモードの場合、共有インターフェイスはブリッジ グループ メンバー インターフェイス（トランスペアレントモードまたはルーテッドモード）ではサポートされません。
- ブリッジされた ixgbevf インターフェイスを備えた VMware の Firewall Threat Defense Virtual の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードではサポートされていません。
- Firepower 2100 シリーズ では、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower 1010 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。
- Firepower 4100/9300 では、データ共有インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firewall Threat Defense の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ

適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は Diagnostic インターフェイスでサポートされません。
- 透過モードは、Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Oracle Cloud Infrastructure にデプロイされた脅威防御仮想インスタンスではサポートされていません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、Firewall Threat Defense 定義の EtherChannel インターフェイスがブリッジグループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、Firewall Threat Defense を介して許可されません。BFD を実行している Firewall Threat Defense の両側に 2 つのネイバーがある場合、Firewall Threat Defense は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

ファイアウォール モードの設定

ファイアウォール モードは、最初のシステム セットアップの実行時に CLI で設定できます。セットアップ時にファイアウォールモードを設定することをお勧めします。これは、ファイアウォールモードを変更すると、非適合の設定が発生しないように設定が消去されるためです。ファイアウォール モードの変更が後で必要になった場合は、CLI から変更する必要があります。

手順

ステップ 1 Firewall Management Center から Firewall Threat Defense デバイスを登録解除します。

モードの変更は、デバイスの登録を解除するまで実行できません。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。
b) 登録を解除するデバイスの横にある [その他（More）] (⋮) をクリックし、[削除（Delete）] をクリックします。

ステップ 2 Firewall Threat Defense デバイスの CLI にアクセスします。可能ならばコンソール ポートからアクセスします。

診断インターフェイスへの SSH を使用している場合、モードを変更すると、インターフェイスの設定が消去され、切断されます。代わりに、管理インターフェイスに接続する必要があります。

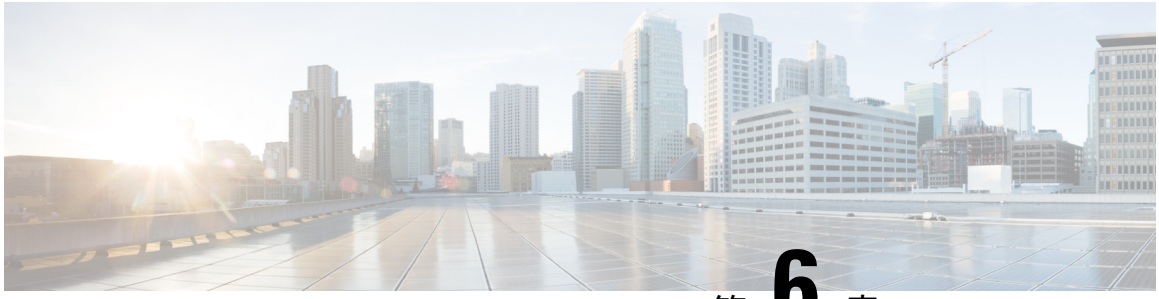
ステップ 3 ファイアウォール モードを変更します。

configure firewall [**routed** | **transparent**]

例：

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

ステップ 4 Firewall Management Center に再登録します。CLI を使用した Firewall Threat Defense 初期設定の実行の完了 （21 ページ）およびデバイスの追加 （34 ページ）を参照してください。



第 6 章

Firepower 4100/9300 の論理デバイス

Firepower 4100/9300 は柔軟なセキュリティ プラットフォームが 1 つまたは複数の論理デバイスをインストールすることができます。Firewall Threat Defense を Firewall Management Center に追加する前に、シャーシ インターフェイスを設定し、論理デバイスを追加し、Secure Firewall シャーシマネージャ または FXOS の CLI を使用して Firepower 4100/9300 シャーシ上のデバイスにインターフェイスを割り当てる必要があります。この章では、基本的なインターフェイスの設定、および Secure Firewall シャーシマネージャ を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、「Firepower 4100/9300 のクラスタリング （543 ページ）」を参照してください。FXOS CLI を使用するには、FXOS CLI コンフィギュレーション ガイドを参照してください。高度な FXOS の手順とトラブルシューティングについては、FXOS コンフィギュレーション ガイドを参照してください。

- インターフェイスについて （213 ページ）
- 論理デバイスについて （231 ページ）
- コンテナ インスタンスのライセンス （241 ページ）
- 論理デバイスの要件と前提条件 （242 ページ）
- 論理デバイスに関する注意事項と制約事項 （250 ページ）
- インターフェイスの設定 （254 ページ）
- 論理デバイスの設定 （260 ページ）
- 論理デバイスの履歴 （274 ページ）

インターフェイスについて

Firepower 4100/9300 シャーシ は、物理インターフェイス、コンテナインスタンス用の VLAN サブインターフェイス、および EtherChannel（ポートチャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバインターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firewall シャーシ マネージャ によって、FXOS シャーシの管理に使用されます。このインターフェイスはMGMTとして、[Interfaces] タブの上部に表示されます。[Interfaces] タブでは、このインターフェイスの有効化または無効化のみを実行できます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLIから設定にする必要があります。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたはSFPモジュールが取り外されている場合や、**mgmt-port shut** コマンドが実行されている場合や、論理デバイスがオフラインになっている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

インターフェイス タイプ

物理インターフェイス、コンテナインスタンスの VLAN サブインターフェイス、および EtherChannel（ポートチャネル）インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは 1 つまたは複数の論理デバイス/コンテナインスタンス（Firewall Threat DefenseFirewall Management Center 専用）で共有できます。 各コンテナインスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジ グループ メンバー インターフェイス（トランスペアレントモードまたはルーテッドモード）、インライン セット、パッシブインターフェイス、クラスタ、またはフェールオーバーリンクではサポートされません。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つ

だけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。個別のシャーシ管理インターフェイスについては、シャーシ管理インターフェイス（214 ページ）を参照してください。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： Firewall Management Center デバイスを使用した Firewall Threat Defense のセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、Firewall Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。詳細については、管理センター構成ガイドを参照してください。Eventing インターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。後で管理用のデータインターフェイスを設定する場合は、別のイベントインターフェイスを使用できません。

（注） 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。 マルチインスタンスクラスタリングの場合、デバイス間でクラスタタイプのインターフェイスを共有することはできません。各クラスタが別個のクラスタ制御リンクを使用でできるように、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。Firewall Device Manager および CDO はクラスタリングをサポートしていません。

（注） この章では、*FXOS* VLAN サブインターフェイスについてのみ説明します。Firewall Threat Defenseアプリケーション内でサブインターフェイスを個別に作成できます。詳細については、FXOS インターフェイスとアプリケーション インターフェイス（217 ページ）を参照してください。

スタンドアロン展開とクラスタ展開での Firewall Threat Defense および ASA アプリケーションのインターフェイスタイプのサポートについては、次の表を参照してください。

表 *15*：インターフェイスタイプのサポート

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	イベント（Eventing）	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
Firewall Threat Defense	スタンドアロン ネイティブ インスタンス	対応	—	—	—	○	○	—	—
	スタンドアロン コンテナ インスタンス	○	○	○	○	○	○	—	—
	クラスタ ネイティブ インスタンス	[はい（Yes）] に設定（シャーシ間クラスタリング専用の EtherChannel）	—	—	—	○	○	○	—
	クラスタ コンテナ インスタンス	[はい（Yes）] に設定（シャーシ間クラスタリング専用の EtherChannel）	—	—	—	○	○	○	○

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	イベント（Eventing）	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
ASA	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	—	対応	—
	クラスタ ネイティブ インスタンス	[はい（Yes）] に設定 （シャーシ間クラスタリング専用の EtherChannel）	—	—	—	対応	—	対応	—

FXOS インターフェイスとアプリケーション インターフェイス

Firepower 4100/9300 は、物理インターフェイス、コンテナインスタンスの LAN サブインターフェイス、および EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

続くセクションでは、インターフェイスの FXOS とアプリケーションの連携について説明します。

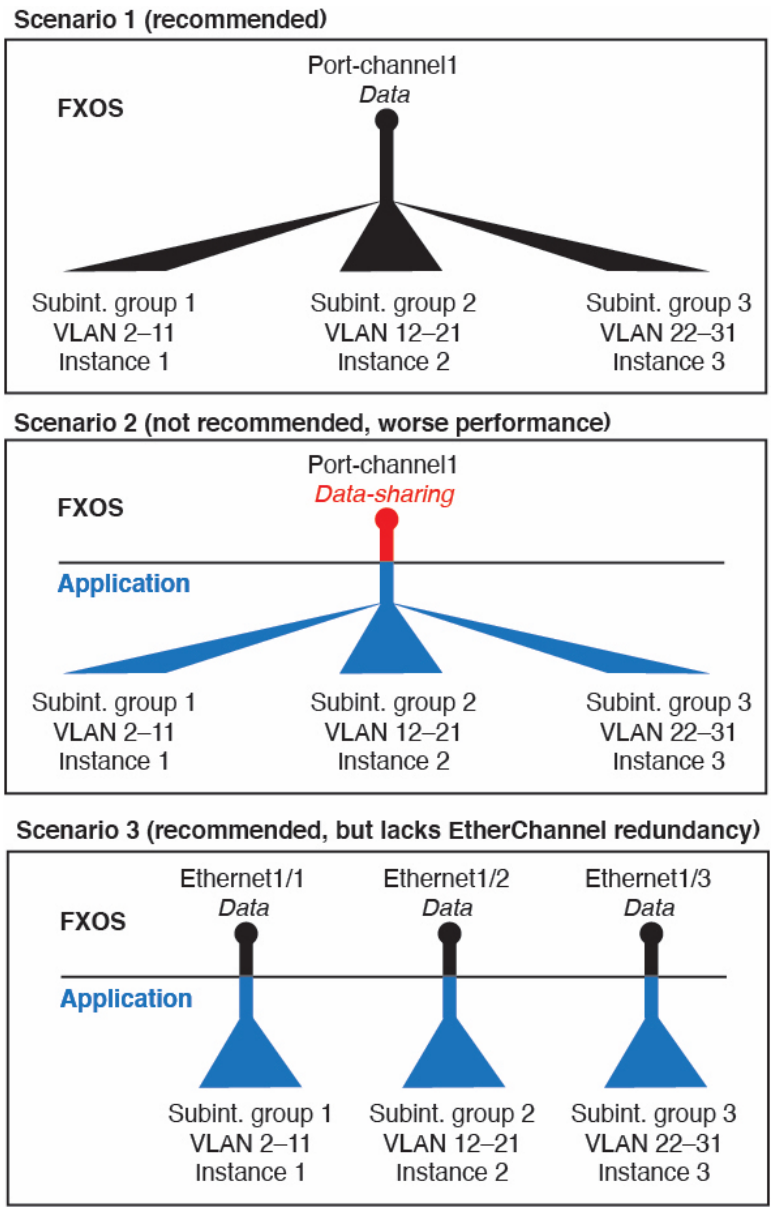
VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

スタンドアロンモードのコンテナインスタンスの場合のみ、FXOS で VLAN サブインターフェイスを作成することもできます。マルチインスタンスクラスタは、クラスタタイプのインターフェイスを除いて、FXOS のサブインターフェイスをサポートしません。アプリケーション定義のサブインターフェイスは、FXOS 制限の対象にはなりません。サブインターフェイスを作成するオペレーティングシステムの選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、FXOS でサブインターフェイスを作成する必要があります。FXOS サブインターフェイスを優先するもう 1 つのシナリオでは、1 つのインターフェイス上の別のサブインターフェイス グループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、イ

ンスタンス C で VLAN 22-31 を使用して Port-Channel1 を使うとします。アプリケーション内でこれらのサブインターフェイスを作成する場合、FXOS 内で親インターフェイスを共有しますが、これはお勧めしません。このシナリオを実現する 3 つの方法については、次の図を参照してください。

図 *84 : FXOS* の *VLAN* とコンテナインスタンスのアプリケーション



シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェ

イスを有効にする必要があります。インターフェイスの状態は個別に制御されるため、シャーシとアプリケーションの間で不一致が発生することがあります。

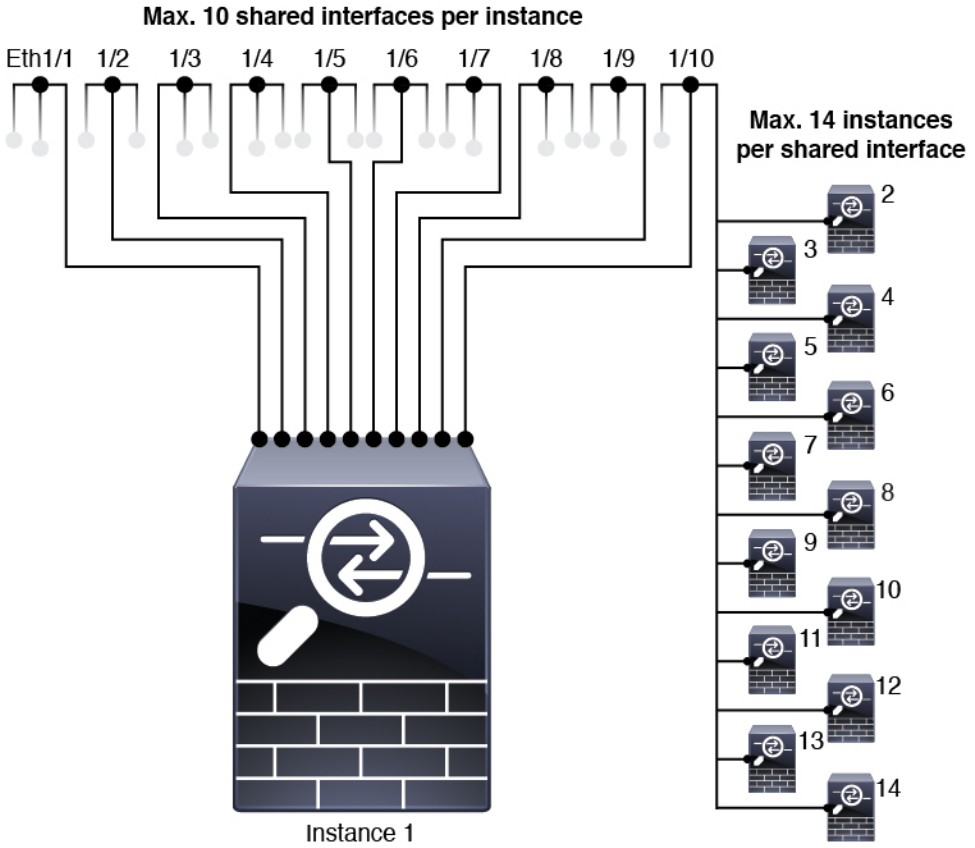
アプリケーション内のインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたはEtherChannelは、アプリケーション内ではデフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

共有インターフェイスの拡張性

インスタンスは、データ共有タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有すると、シャーシは一意のMACアドレスを使用して、正しいインスタンスにトラフィックを転送します。ただし、共有インターフェイスでは、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルが大きくなることがあります（すべてのインスタンスが、同じインターフェイスを共有するその他すべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

転送テーブルに加えて、シャーシはVLANサブインターフェイスの転送用にVLANグループテーブルも保持します。 最大500個のVLANサブインターフェイスを作成できます。

共有インターフェイスの割り当てに次の制限を参照してください。



共有インターフェイスのベスト プラクティス

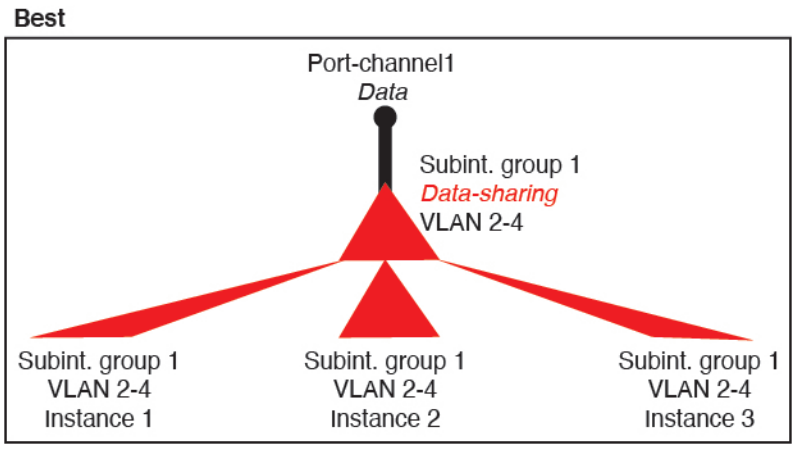
転送テーブルの拡張性を最適にするには、共有するインターフェイスの数をできる限り少なくします。代わりに、1 つまたは複数の物理インターフェイスに最大 500 個の VLAN サブインターフェイスを作成し、コンテナインスタンスで VLAN を分割できます。

インターフェイスを共有する場合は、拡張性の高いものから低いものの順に次の手順を実行します。

1. 最適：単一の親の下のサブインターフェイスを共有し、インスタンスグループと同じサブインターフェイスのセットを使用します。

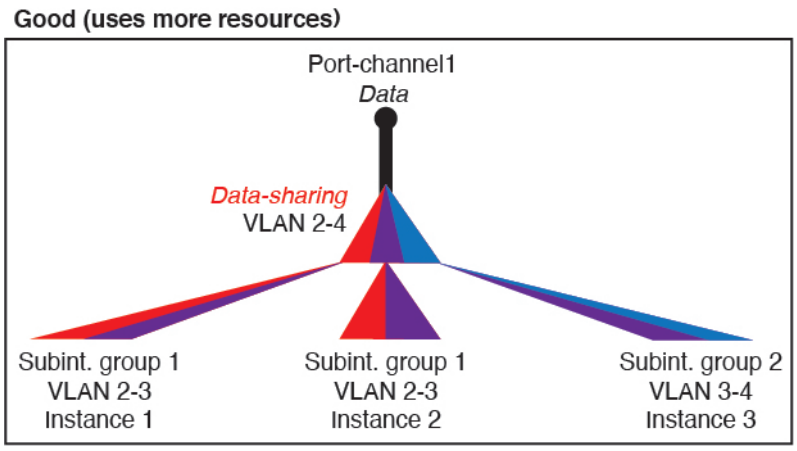
   たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、Port-Channel2、Port-Channel3、Port-Channel4 の代わりに、その EtherChannel のサブインターフェイス（Port-Channel1.2、3、4）を共有します。単一の親のサブインターフェイスを共有する場合、物理/EtherChannel インターフェイスまたは複数の親にわたるサブインターフェイスを共有するときの VLAN グループ テーブルの拡張性は転送テーブルよりも優れています。

   図 *85*：最適：単一の親のサブインターフェイスグループを共有



   インスタンスグループと同じサブインターフェイスのセットを共有しない場合は、（VLAN グループよりも）より多くのリソースを設定で使用することになる可能性があります。たとえば、Port-Channel1.2 および 3 をインスタンス 1 および 2 と共有するとともに Port-Channel1.3 および 4 をインスタンス 3 と共有する（2 つの VLAN グループ）のではなく、Port-Channel1.2、3、および 4 をインスタンス 1、2、および 3 と共有（1 つの VLAN グループ）します。

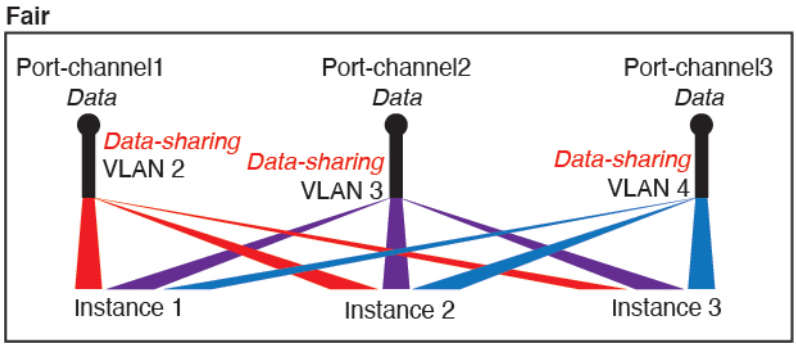
図 *86 :* 良好：単一の親の複数のサブインターフェイスグループを共有



2. 普通：親の間でサブインターフェイスを共有します。

   たとえば、Port-Channel2、Port-Channel4、および Port-Channel4 ではなく、Port-Channel1.2、Port-Channel2.3、および Port-Channel3.4 を共有します。この使用方法は同じ親のサブインターフェイスのみを共有するよりも効率は劣りますが、VLAN グループを利用しています。

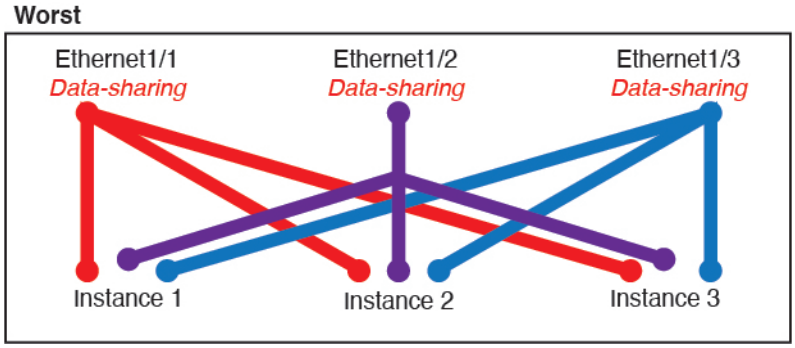
図 *87 :* 普通：個別の親のサブインターフェイスを共有



3. 最悪：個々の親インターフェイス（物理または EtherChannel）を共有します。

   この方法は、最も多くの転送テーブル エントリを使用します。

図 *88 :* 最悪：親インターフェイスを共有



共有インターフェイスの使用状況の例

インターフェイスの共有と拡張性の例について、以下の表を参照してください。以下のシナリオは、すべてのインスタンス間で共有されている管理用の 1 つの物理/EtherChannel インターフェイスと、ハイアベイラビリティで使用する専用のサブインターフェイスを含むもう 1 つの物理/EtherChannel インターフェイスを使用していることを前提としています。

- 表 16 : 3 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス （223 ページ）
- 表 17 : 3 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス （225 ページ）
- 表 18 : 1 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス （227 ページ）
- 表 19 : 1 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス （229 ページ）

3 つの SM-44 と firepower 9300

次の表は、物理インターフェイスまたはEtherchannelのみを使用している9300のSM-44セキュリティモジュールに適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 *16 : 3* つの *SM-44* を備えた *Firepower 9300* の物理/*EtherChannel* インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**0**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30： • 15 • 15	**0**	**2:** • インスタンス 1 • インスタンス 2	14%
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
33： • 11（各 1） • 11（各 1） • 11（各 1）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
33： • *11*（各 *1*） • *11*（各 *1*） • *12*（各 *1*）	***3***： • *1* • *1* • *1*	***34***： • インスタンス *1* - インスタンス *11* • インスタンス *12* - インスタンス *22* • インスタンス *23* - インスタンス *34*	*102 %* 許可しない
30： • 30（各 1）	**1**	**6**： • インスタンス 1 - インスタンス 6	25 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
30： • 10（各 5） • 10（各 5） • 10（各 5）	**3**： • 1 • 1 • 1	**6**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 4 • インスタンス 5 - インスタンス 6	23 %
30： • 30（各 6）	**2**	**5**： • インスタンス 1 - インスタンス 5	28%
30： • 12（各 6） • 18（各 6）	**4**： • 2 • 2	**5**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 5	26 %
24： • 6 • 6 • 6 • 6	**7**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	44 %
24： • 12（各 6） • 12（各 6）	**14**： • 7 • 7	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 4	41%

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 9300 上の 3 つの SM-44 セキュリティ モジュールに適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイスを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 *17 : 3* つの *SM-44* を備えた *Firepower 9300* 上の *1* つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
168： • 168（4 ea.）	**0**	**42**： • インスタンス 1 - インスタンス 42	33%
224： • 224（16 ea.）	**0**	**14**： • インスタンス 1 - インスタンス 14	27 %
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
33： • 11（各 1） • 11（各 1） • 11（各 1）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70： • 70（5 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • 55（5 ea.） • 55（5 ea.） • 55（5 ea.）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
70： • 70（5 ea.）	**2**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • 55（5 ea.） • 55（5 ea.） • 55（5 ea.）	**6**： • 2 • 2 • 2	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70： • 70（5 ea.）	**10**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • *55（5 ea.）* • *55（5 ea.）* • *55（5 ea.）*	***30***： • *10* • *10* • *10*	***33***： • インスタンス *1* - インスタンス *11* • インスタンス *12* - インスタンス *22* • インスタンス *23* - インスタンス *33*	*102 %* 許可しない

1 つの SM 44 を備えた Firepower 9300

次の表は、物理インターフェイスまたは Etherchannel のみを使用している 1 つの SM-44 を備えた Firepower 9300 に適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 *18 : 1* つの *SM-44* を備えた *Firepower 9300* の物理/*EtherChannel* インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**0**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30： • 15 • 15	**0**	**2:** • インスタンス 1 • インスタンス 2	14%
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
14： • 7（各 1） • 7（各 1）	**2:** • **1** • **1**	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
32： • 8 • 8 • 8 • 8	**1**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	21 %
32： • 16（各 8） • 16（各 8）	**2**	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	20 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**2**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	25 %
32： • 16（各 8） • 16（各 8）	**4**： • 2 • 2	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	24 %
24： • 8 • 8 • 8	**8**	**3**： • インスタンス 1 • インスタンス 2 • インスタンス 3	37 %
10： • 10（各 2）	**10**	**5**： • インスタンス 1 - インスタンス 5	69%
10： • 6（各 2） • 4（各 2）	**20**： • 10 • 10	**5**： • インスタンス 1 - インスタンス 3 • インスタンス 4 - インスタンス 5	59%
14： • *12（2 ea.）*	***10***	***7***： • インスタンス *1* - インスタンス *7*	*109%* 許可しない

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 1 つの SM-44 を備えた Firepower 4150 に適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイ

スを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

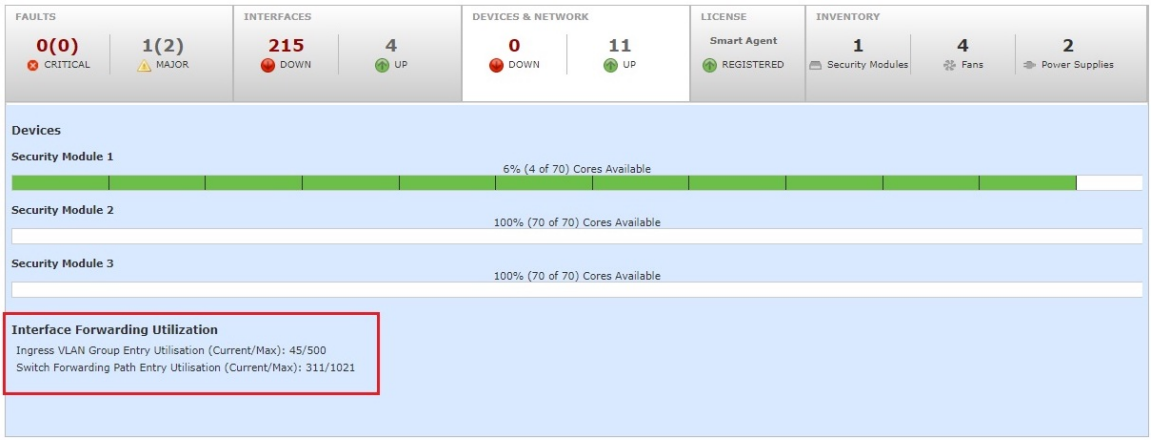
表 *19 : 1* つの *SM-44* を備えた *Firepower 9300* 上の *1* つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
112： • 112（各 8）	**0**	**14**： • インスタンス 1 - インスタンス 14	17%
224： • 224（16 ea.）	**0**	**14**： • インスタンス 1 - インスタンス 14	17%
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
14： • 7（各 1） • 7（各 1）	**2:** • 1 • 1	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
112： • 112（各 8）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
112： • 56（各 8） • 56（各 8）	**2:** • 1 • 1	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
112： • 112（各 8）	**2**	**14**： • インスタンス 1 - インスタンス 14	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
112： • 56（各 8） • 56（各 8）	**4**： • 2 • 2	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
140： • 140（各 10）	**10**	**14**： • インスタンス 1 - インスタンス 14	46 %
140： • 70（各 10） • 70（各 10）	**20**： • 10 • 10	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %

共有インターフェイス リソースの表示

転送テーブルと VLAN グループの使用状況を表示するには、**[デバイスとネットワーク（Devices & Network）]** > **[インターフェイス転送の使用率（Interface Forwarding Utilization）]** エリアを参照し ます。例：



Firewall Threat Defense のインライン セット リンク ステート伝達サポート

インラインセットはワイヤ上のバンプのように動作し、2つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

Firewall Threat Defense アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、Firewall Threat Defense はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンク ステートが変化すると、シャーシはその変化を検知し、その変化に合わせて他のインターフェイスのリンク ステートを更新します。ただし、シャーシからリンク ステートの変更が伝達されるまで最大4秒かかります。障害状態のネットワークデバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。

（注） 同じインラインセットに対して ハードウェア バイパス およびリンクステートの伝達を有効にしないでください。

論理デバイスについて

論理デバイスでは、1 つのアプリケーション インスタンス（ASA または Firewall Threat Defense のいずれか）および 1 つのオプション デコレータ アプリケーション（Radware DefensePro）を実行し、サービスチェーンを形成できます。

論理デバイスを追加する場合は、アプリケーション インスタンス タイプとバージョンを定義し、インターフェイスを割り当て、アプリケーション設定に送信されるブートストラップ設定を構成することもできます。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および Firewall Threat Defense）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- クラスタ：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュール デバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3 つすべてのモジュールがネイティブインスタンスとコンテナインスタンスの両方のクラスタに参加する必要があります。ファイアウォール デバイス マネージャ はクラスタリングをサポートしていません。

論理デバイスのアプリケーションインスタンス：コンテナとネイティブ

アプリケーション インスタンスは次の展開タイプで実行します。

- ネイティブ インスタンス：ネイティブ インスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つだけインストールできます。
- コンテナ インスタンス：コンテナ インスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。マルチインスタンス機能は Firewall Management Center を使用する Firewall Threat Defense でのみサポートされています。ASA またはファイアウォール デバイス マネージャを使用する Firewall Threat Defense ではサポートされていません。

（注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。マルチ コンテキスト モードでは、単一のアプリケーションインスタンスがパーティション化されますが、マルチインスタンス機能では、独立したコンテナインスタンスを使用できます。コンテナインスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェアアップデート、および Firewall Threat Defense のフル機能のサポートが可能です。マルチ コンテキスト モードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。Firewall Threat Defense ではマルチ コンテキストモードは使用できません。

Firepower 9300 の場合、一部のモジュールでネイティブ インスタンスを使用し、他のモジュールではコンテナ インスタンスを使用することができます。

コンテナ インスタンス インターフェイス

コンテナ インターフェイスでの柔軟な物理インターフェイスの使用を可能にするため、FXOSでVLANサブインターフェイスを作成し、複数のインスタンス間でインターフェイス（VLANまたは物理）を共有することができます。ネイティブのインスタンスは、VLANサブインターフェイスまたは共有インターフェイスを使用できません。 マルチインスタンスクラスタは、VLANサブインターフェイスまたは共有インターフェイスを使用できません。クラスタ制御リンクは例外で、クラスタEtherChannelのサブインターフェイスを使用できます。共有インターフェイスの拡張性（219ページ）およびコンテナインスタンスのVLANサブインターフェイスの追加 （258 ページ）を参照してください。

（注） 本書では、*FXOS* VLANサブインターフェイスについてのみ説明します。Firewall Threat Defenseアプリケーション内でサブインターフェイスを個別に作成できます。詳細については、FXOSインターフェイスとアプリケーションインターフェイス（217ページ）を参照してください。

シャーシがパケットを分類する方法

シャーシに入ってくるパケットはいずれも分類する必要があります。その結果、シャーシは、どのインスタンスにパケットを送信するかを決定できます。

- 一意のインターフェイス：1つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。ブリッジグループメンバー インターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意のMACアドレス：シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意のMACアドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイスに割り当てられた固有のMACアドレスが使用されます。固有のMACアドレスがないと、アップストリームルータはインスタンスに直接ルーティングできません。アプリケーション内で各インターフェイスを設定するときに、手動でMACアドレスを設定することもできます。

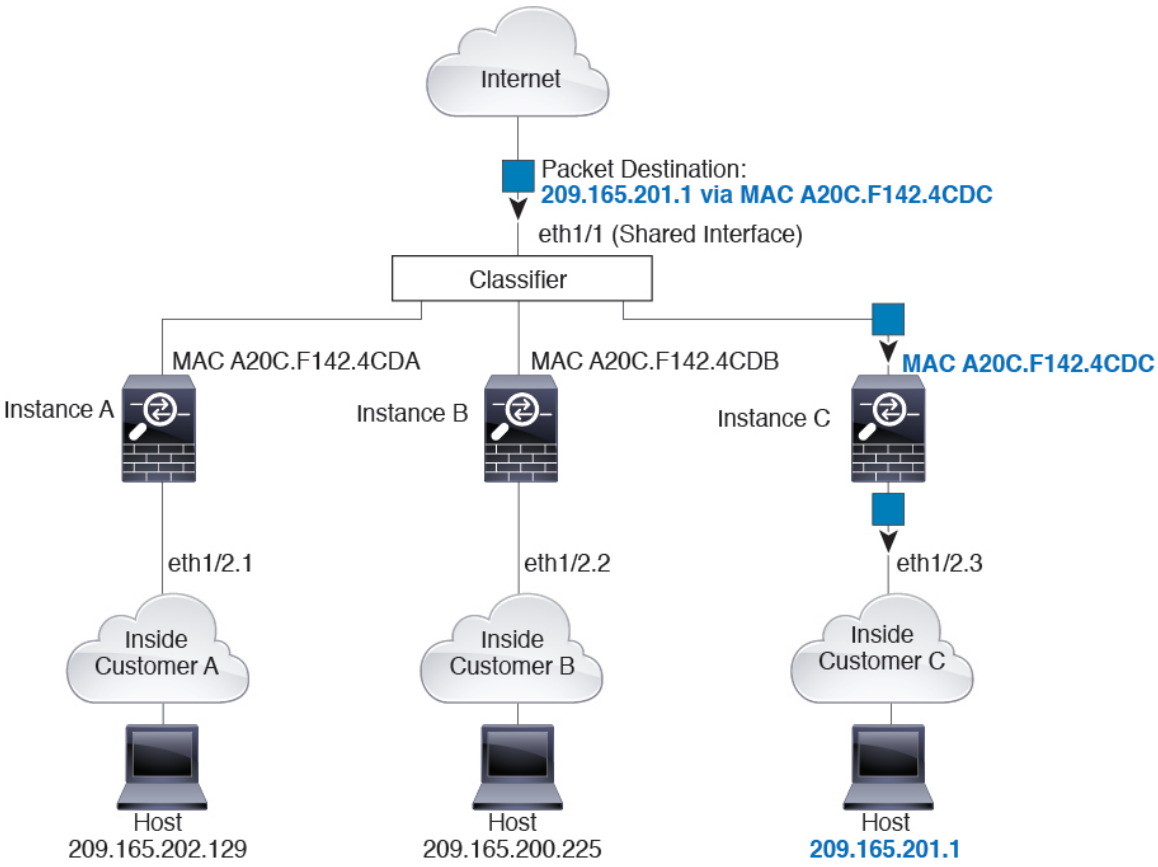
（注） 宛先MACアドレスがマルチキャストまたはブロードキャストMACアドレスの場合、パケットが複製されて各インスタンスに送信されます。

分類例

MAC アドレスを使用した共有インターフェイスのパケット分類

次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンスCにはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをインスタンス C に割り当てます。

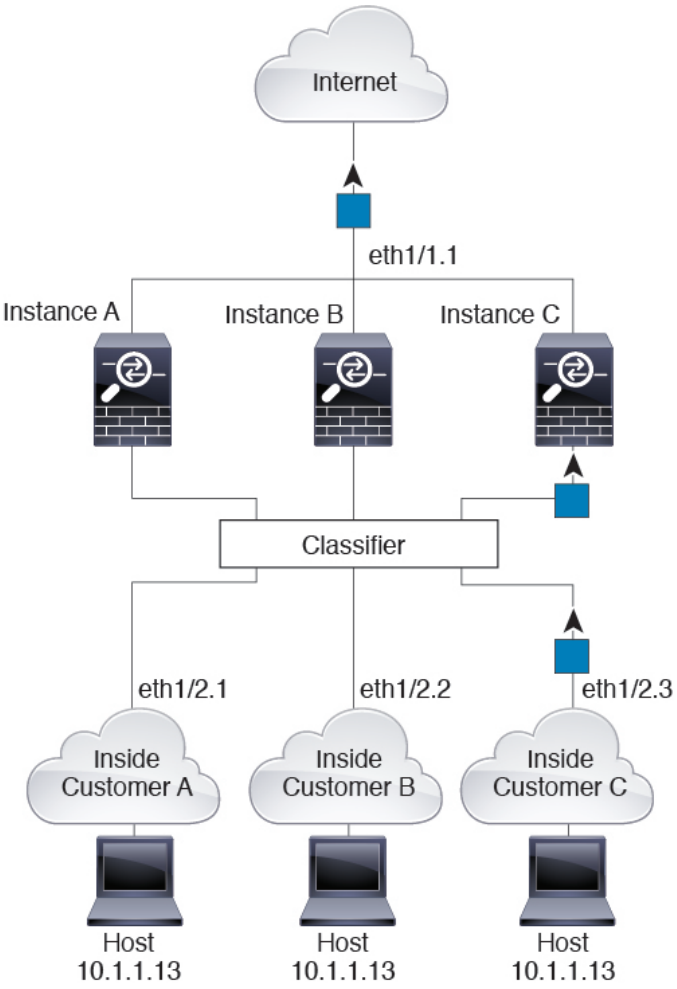
図 *89 : MAC* アドレスを使用した共有インターフェイスのパケット分類



内部ネットワークからの着信トラフィック

内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンスCのホストを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

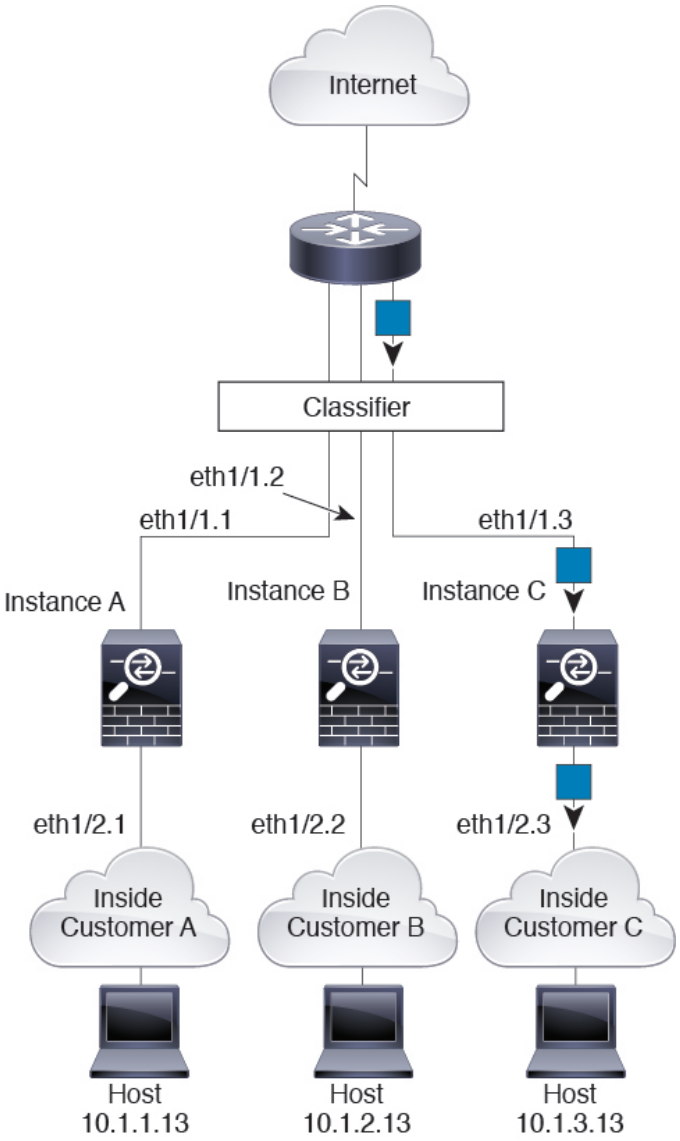
図 *90* : 内部ネットワークからの着信トラフィック



トランスペアレント ファイアウォール インスタンス

トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンス C に割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

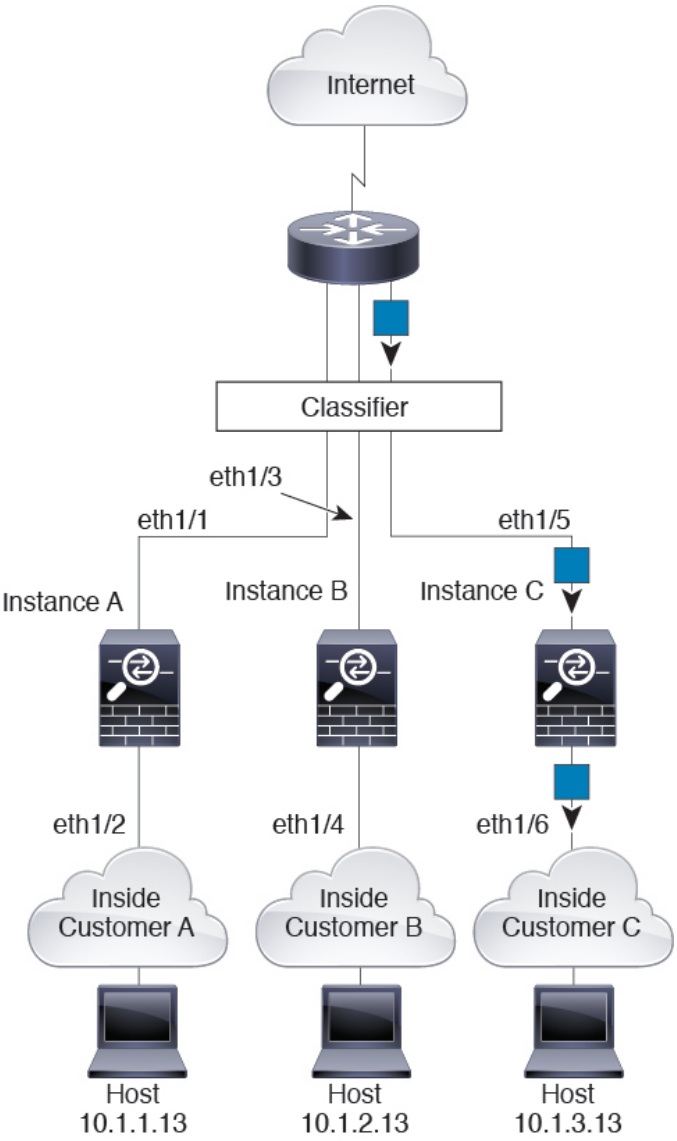
図 *91 :* トランスペアレント ファイアウォール インスタンス



インラインセット

インラインセットの場合は一意のインターフェイスを使用する必要があります。また、それらのセットは物理インターフェイスか、またはEtherChannelである必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/5 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *92* : インラインセット

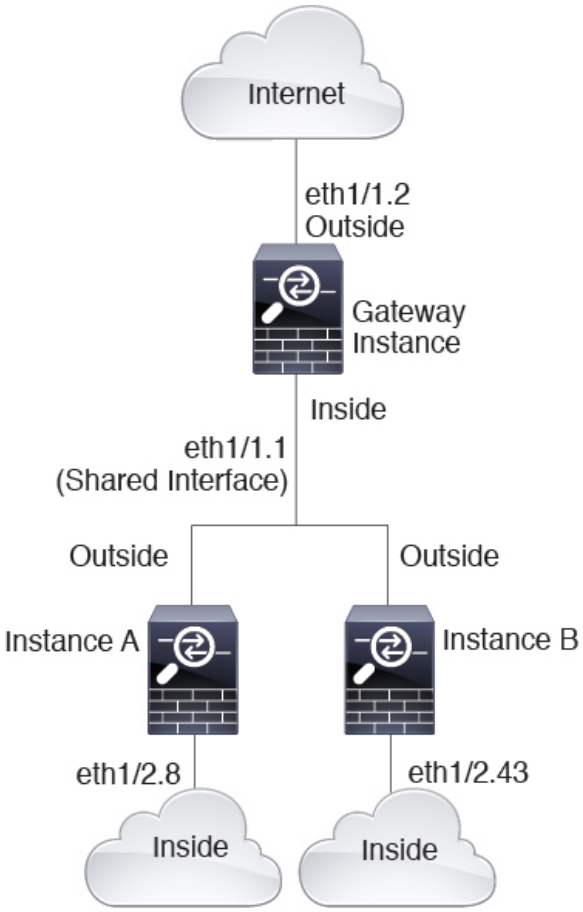


コンテナ インスタンスのカスケード

別のインスタンスの前にインスタンスを直接配置することをインスタンスのカスケードと呼びます。一方のインスタンスの外部インターフェイスは、もう一方のインスタンスの内部インターフェイスと同じインターフェイスです。いくつかのインスタンスのコンフィギュレーションを単純化する場合、最上位インスタンスの共有パラメータを設定することで、インスタンスをカスケード接続できます。

次の図に、ゲートウェイの背後に2つのインスタンスがあるゲートウェイ インスタンスを示します。

図 *93 :* インスタンスのカスケード



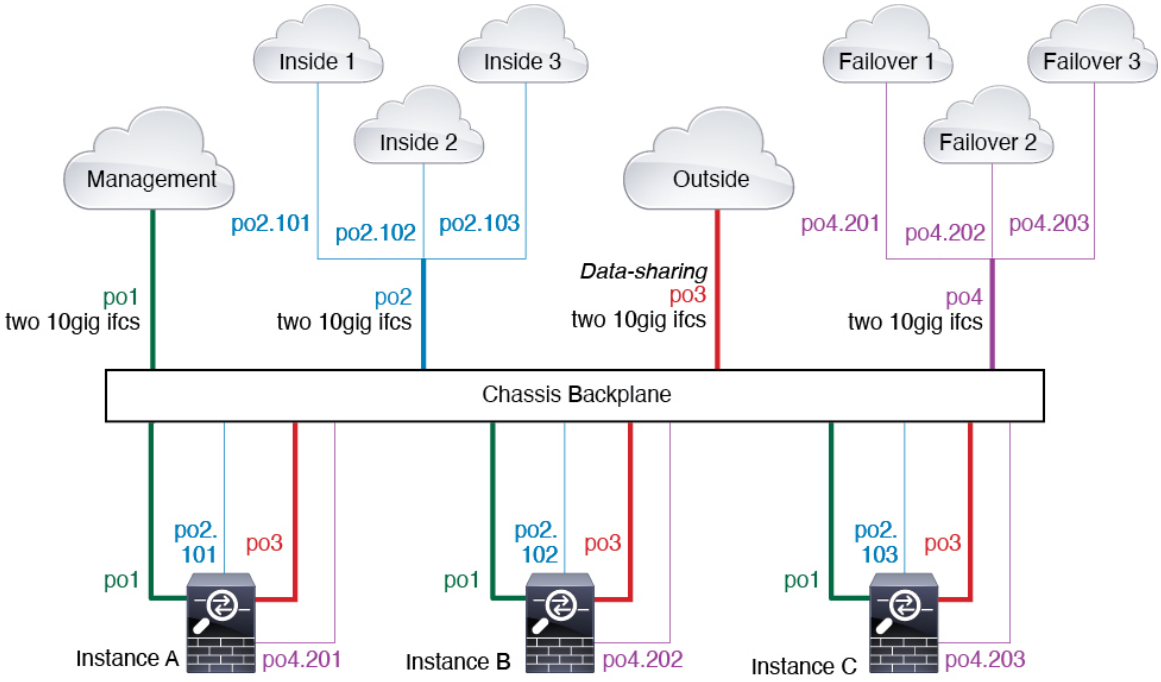
（注） 高可用性を備えたカスケードインスタンス（共有インターフェイスを使用）を使用しないでください。フェールオーバーが発生し、スタンバイユニットが再参加すると、MAC アドレスが一時的に重複し、停止が発生する可能性があります。代わりに、外部スイッチを使用してゲートウェイインスタンスと内部インスタンスに一意のインターフェイスを使用して、それらのインスタンス間でトラフィックを渡す必要があります。

一般的な複数インスタンス展開

次の例には、ルーテッドファイアウォールモードのコンテナインスタンスが3つ含まれます。これらには次のインターフェイスが含まれます。

- 管理：すべてのインスタンスがポートチャネル1インターフェイス（管理タイプ）を使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ管理ネットワークで一意の IP アドレスを使用します。

- 内部：各インスタンスがポートチャネル2（データ タイプ）のサブインターフェイスを使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。
- 外部：すべてのインスタンスがポートチャネル3インターフェイス（データ共有タイプ）を使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ外部ネットワークで一意の IP アドレスを使用します。
- フェールオーバー：各インスタンスがポートチャネル4（データ タイプ）のサブインターフェイスを使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。



コンテナ インスタンス インターフェイスの自動 MAC アドレス

シャーシは、各インスタンスの共有インターフェイスが一意の MAC アドレスを使用するように、インスタンス インターフェイスの MAC アドレスを自動的に生成します。

インスタンス内の共有インターフェイスに MAC アドレスを手動で割り当てると、手動で割り当てられた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インスタンス内のインターフェイスの MAC アドレスを手動で設定してください。

自動生成されたアドレスは A2 で始まり、アドレスが重複するリスクがあるため、手動 MAC アドレスの先頭は A2 にしないでください。

シャーシは、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義のプレフィックスまたはシステム定義のプレフィックスで、*zz.zzzz* はシャーシが生成した内部カウンタです。システム定義のプレフィックスは、IDPROM にプログラムされている Burned-in MAC アドレスプール内の最初の MAC アドレスの下位 2 バイトと一致します。**connect fxos**、**show module** の順に使用して、MAC アドレスプールを表示します。たとえば、モジュール 1 に対して表示される MAC アドレスの範囲が b0aa.772f.f0b0 ～ b0aa.772f.f0bf の場合、システムのプレフィックスは f0b0 になります。

ユーザ定義のプレフィックスは、16進数に変換される整数です。ユーザ定義のプレフィックスの使用方法を示す例としてたとえば、プレフィックス77を設定すると、シャーシは77を16進数値004D (*yyxx*)に変換します。MAC アドレスで使用すると、プレフィックスはシャーシのネイティブ形式に一致するように逆転されます（*xxyy*）。

A2**4D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

コンテナ インスタンスのリソース管理

コンテナ インスタンスごとのリソース使用率を指定するには、FXOS で 1 つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。モデルごとに使用可能なリソースを表示するには、コンテナ インスタンスの要件と前提条件（244 ページ）を参照してください。リソース プロファイルを追加するには、コンテナインスタンスにリソースプロファイルを追加（260 ページ）を参照してください。

マルチインスタンス機能のパフォーマンス スケーリング係数

プラットフォームの最大スループット（接続数、VPN セッション数、および TLS プロキシセッション数）は、ネイティブインスタンスがメモリと CPU を使用するために計算されます（この値は **show resource usage** に示されます）。複数のインスタンスを使用する場合は、インスタンスに割り当てる CPU コアの割合に基づいてスループットを計算する必要があります。たとえば、コアの 50% でコンテナインスタンスを使用する場合は、最初にスループットの 50% を計算する必要があります。さらに、コンテナインスタンスで使用可能なスループットは、ネイティブインスタンスで使用可能なスループットよりも低い場合があります。

インスタンスのスループットを計算する方法の詳細については、https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html を参照してください。

コンテナ インスタンスおよびハイ アベイラビリティ

2 つの個別のシャーシでコンテナインスタンスを使用してハイ アベイラビリティを使用できます。たとえば、それぞれ 10 個のインスタンスを使用する 2 つのシャーシがある場合、10 個の

ハイ アベイラビリティ ペアを作成できます。ハイ アベイラビリティは FXOS で構成されません。各ハイ アベイラビリティ ペアはアプリケーション マネージャで構成します。

詳細な要件については、「ハイアベイラビリティの要件と前提条件 （245 ページ）」と「ハイアベイラビリティ ペアの追加 （268 ページ）」を参照してください。

コンテナインスタンスおよびクラスタリング

セキュリティモジュール/エンジンごとに 1 つのコンテナインスタンスを使用して、コンテナインスタンスのクラスタを作成できます。詳細な要件については、クラスタリングの要件と前提条件 （246 ページ） を参照してください。

コンテナ インスタンスのライセンス

すべてのライセンスがコンテナ インスタンスごとではなく、セキュリティ エンジン/シャーシ（Firepower 4100 の場合）またはセキュリティ モジュール（Firepower 9300 の場合）ごとに使用されます。次の詳細情報を参照してください。

- Essentialsライセンスが セキュリティ モジュール/エンジン ごとに 1 つ自動的に割り当てられます。
- 機能ライセンスは各インスタンスに手動で割り当てますが、セキュリティ モジュール/エンジン につき機能ごとに 1 つのライセンスのみを使用します。たとえば、3 つのセキュリティモジュールを搭載した Firepower 9300 の場合、使用中のインスタンスの数に関係なく、モジュールにつき 1 つの URL フィルタリング ライセンスが必要で、合計 3 つのライセンスが必要になります。

次に例を示します。

表 *20 : Firepower 9300* のコンテナインスタンスのサンプルライセンスの使用状況

Firepower 9300	インスタンス	ライセンス
セキュリティ モジュール 1	インスタンス 1	Essentials、URL フィルタリング、マルウェア防御
	インスタンス 2	Essentials、URL フィルタリング
	インスタンス 3	Essentials、URL フィルタリング
セキュリティ モジュール 2	インスタンス 4	Essentials、IPS
	インスタンス 5	Essentials、URL フィルタリング、マルウェア防御、IPS

Firepower 9300	インスタンス	ライセンス
セキュリティ モジュール 3	インスタンス 6	Essentials、マルウェア防御、IPS
	インスタンス 7	Essentials、IPS

表 *21 :* ライセンスの総数

Essentials	URL フィルタリング	マルウェア防御	IPS
3	2	3	2

論理デバイスの要件と前提条件

要件と前提条件については、次のセクションを参照してください。

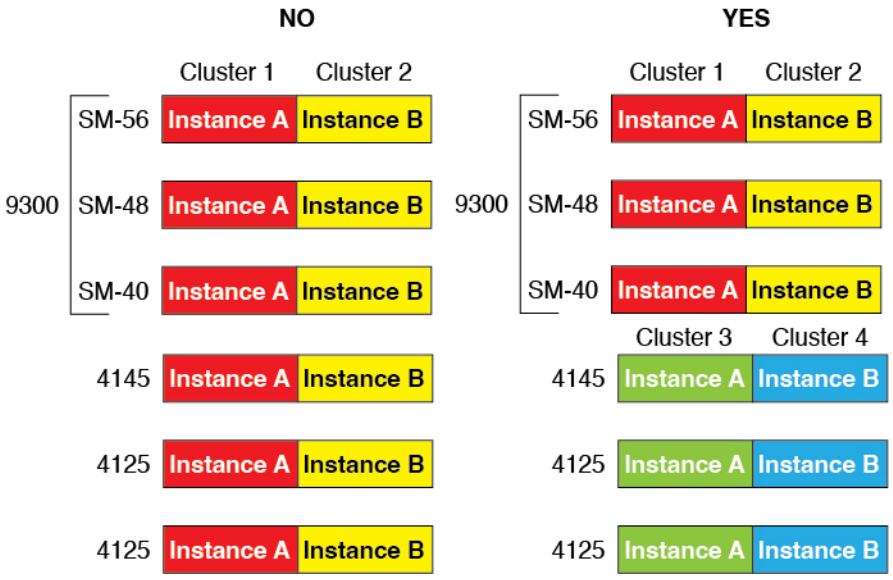
のハードウェアとソフトウェアの要件と前提条件

Firepower 4100/9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。可能な組み合わせについては、次の要件を参照してください。

Firepower 9300の要件

Firepower 9300 には、3 つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を確認します。

- セキュリティモジュール タイプ：Firepower 9300 には、さまざまなタイプのモジュールをインストールできます。たとえば、SM-48 をモジュール 1、SM-40 をモジュール 2、SM-56 をモジュール 3 としてインストールできます。
- ネイティブインスタンスのクラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。空のスロットを含め、シャーシ内にあるすべてのモジュールはクラスタに属している必要がありますが、各シャーシにインストールされているセキュリティモジュールの数はさまざまでかまいません。たとえば、シャーシ 1 に 2 つの SM-40 を、シャーシ 2 に 3 つの SM-40 をインストールできます。 同じシャーシに 1 つの SM-48 および 2 つの SM-40 をインストールする場合、クラスタリングは使用できません。
- コンテナインスタンスのクラスタリング：異なるモデルタイプのインスタンスを使用してクラスタを作成できます。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して1つのクラスタを作成できます。ただし、同じクラスタ内にFirepower 9300 と Firepower 4100 を混在させることはできません。



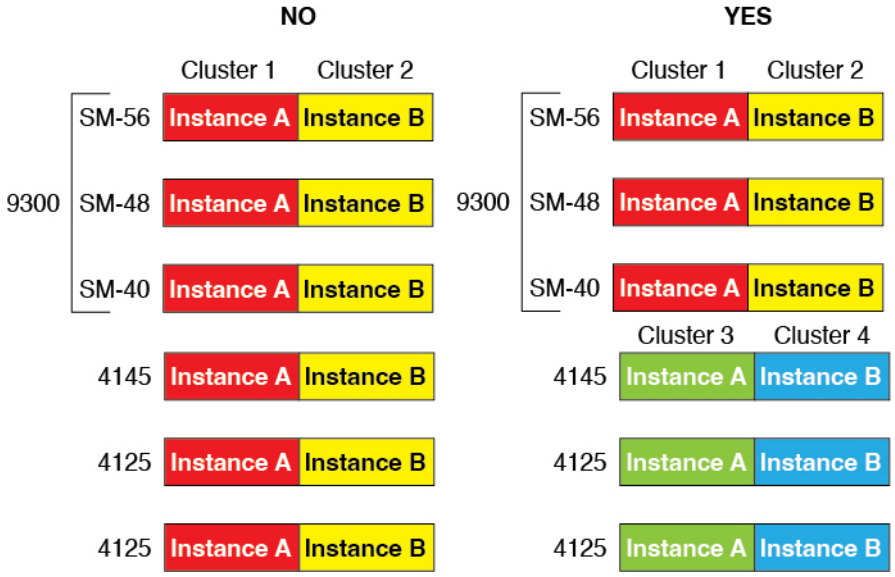
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。ただし、2 つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシには SM-40、SM-48、および SM-56 があります。SM-40 モジュール間、SM-48 モジュール間、および SM-56 モジュール間にハイアベイラビリティペアを作成できます。
- ASA および Firewall Threat Defense のアプリケーションタイプ：異なるアプリケーションタイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール 1 とモジュール 2 に ASA をインストールし、モジュール 3 に Firewall Threat Defense をインストールすることができます。
- ASA または Firewall Threat Defense のバージョン：個別のモジュールで異なるバージョンのアプリケーション インスタンス タイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール 1 に Firewall Threat Defense 6.3 を、モジュール 2 に Firewall Threat Defense 6.4 を、モジュール 3 に Firewall Threat Defense 6.5 をインストールできます。

Firepower 4100の要件

Firepower 4100 には複数のモデルがあります。次の要件を確認します。

- ネイティブインスタンスとコンテナインスタンス：Firepower 4100 にコンテナインスタンスをインストールする場合、そのデバイスは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはデバイスのすべてのリソースを使用するため、デバイスにはネイティブ インスタンスを 1 つのみインストールできます。
- ネイティブインスタンスのクラスタリング：クラスタ内のすべてのシャーシが同じモデルである必要があります。
- コンテナインスタンスのクラスタリング：異なるモデルタイプのインスタンスを使用してクラスタを作成できます。たとえば、Firepower 4145 および 4125 のインスタンスを使用し

て 1 つのクラスタを作成できます。ただし、同じクラスタ内に Firepower 9300 と Firepower 4100 を混在させることはできません。



- 高可用性：高可用性は同じタイプのモデル間でのみサポートされています。
- ASA および Firewall Threat Defense のアプリケーションタイプ：Firepower 4100 は、1 つのアプリケーションタイプのみを実行できます。
- Firewall Threat Defense コンテナインスタンスのバージョン：同じモジュール上で異なるバージョンの Firewall Threat Defense を個別のコンテナインスタンスとして実行できます。

コンテナ インスタンスの要件と前提条件

マルチインスタンスでのハイアベイラビリティまたはクラスタリングの要件については、「ハイアベイラビリティの要件と前提条件 （245 ページ）」および「クラスタリングの要件と前提条件 （246 ページ）」を参照してください。

サポートされるアプリケーション タイプ

- Firewall Threat Defense Firewall Management Center を使用

最大コンテナ インスタンスとモデルあたりのリソース

各コンテナインスタンスに対して、インスタンスに割り当てる CPU コアの数を指定できます。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスあたり 40 GB に設定されます。

表 *22*：モデルごとの最大コンテナ インスタンス数とリソース

モデル	最大コンテナ インスタンス数	使用可能な CPU コア	使用可能な RAM	使用可能なディスクスペース
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 9300 SM-40 セキュリティ モジュール	13	78	334 GB	1359 GB
Firepower 9300 SM-48 セキュリティモジュール	15	94	334 GB	1341 GB
Firepower 9300 SM-56 セキュリティ モジュール	18	110	334 GB	1314 GB

Firewall Management Center の要件

Firepower 4100 シャーシまたは Firepower 9300 モジュール上のすべてのインスタンスに対して、ライセンスの実装のために同じ Firewall Management Center を使用する必要があります。

ハイアベイラビリティの要件と前提条件

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 個別のシャーシ上にあること。Firepower 9300 のシャーシ内ハイアベイラビリティはサポートされません。
  - 同じモデルであること。
  - 高可用性論理デバイスに同じインターフェイスを割り当てること。
  - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- ハイアベイラビリティは Firepower 9300 の同じタイプのモジュール間でのみサポートされますが、2 つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。

- コンテナインスタンスでは、各装置で同じリソースプロファイル属性を使用する必要があります。
- コンテナインスタンス向け：高可用性を備えたカスケードインスタンス（共有インターフェイスを使用）を使用しないでください。フェールオーバーが発生し、スタンバイユニットが再参加すると、MAC アドレスが一時的に重複し、停止が発生する可能性があります。代わりに、外部スイッチを使用してゲートウェイインスタンスと内部インスタンスに一意のインターフェイスを使用して、それらのインスタンス間でトラフィックを渡す必要があります。
- その他のハイアベイラビリティ システム要件については、高可用性のシステム要件（284 ページ）を参照してください。

クラスタリングの要件と前提条件

クラスタ モデルのサポート

Threat Defense は、次のモデルでのクラスタリングをサポートしています。

- Firepower 9300：クラスタには最大 16 ノードを含めることができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。複数のシャーシによるクラスタリングと、1 つのシャーシ内のセキュリティモジュールに分離されたクラスタリングがサポートされます。
- Firepower 4100：複数のシャーシでクラスタリングを使用して、最大 16 ノードがサポートされます。

ユーザの役割

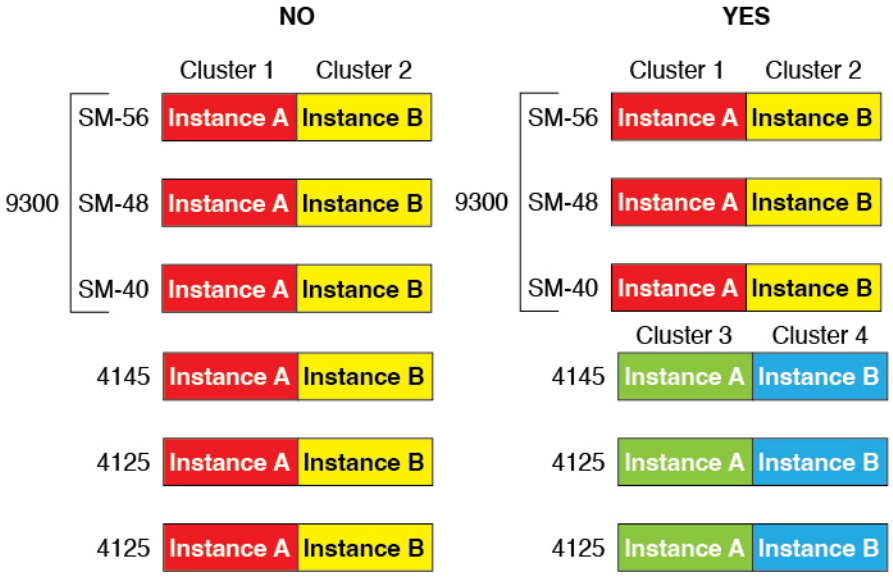
- 管理者
- アクセス管理者
- ネットワーク管理者

クラスタリングハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- ネイティブインスタンスのクラスタリング—Firepower 4100：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。空のスロットを含め、シャーシ内にあるすべてのモジュールはクラスタに属している必要がありますが、各シャーシに設置されているセキュリティ モジュールの数はさまざまでかまいません。

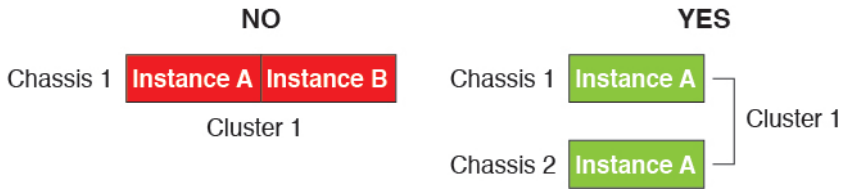
- コンテナインスタンスのクラスタリング—クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することをお勧めします。ただし、必要に応じて、同じクラスタ内に異なるFirepower 9300セキュリティモジュールタイプまたはFirepower 4100モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内でFirepower 9300と4100のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、およびSM-40のインスタンスを使用して1つのクラスタを作成できます。または、Firepower 4145および4125でクラスタを作成できます。



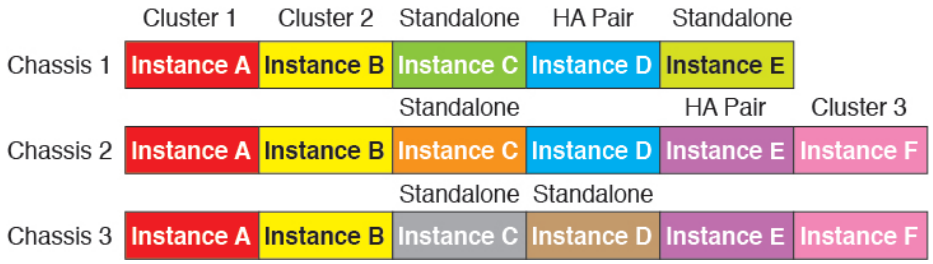
- イメージアップグレード時を除き、同じFXOSおよびアプリケーション ソフトウェアを実行する必要があります。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成を含める必要があります。同じインターフェイスIDの容量が一致し、インターフェイスが同じスパンドEtherChannelに内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワークモジュールを使用できます。複数のシャーシによるクラスタでは、すべてのデータインターフェイスをEtherChannelにする必要があることに注意してください。（インターフェイスモジュールの追加や削除、またはEtherChannelの設定などにより）クラスタリングを有効にした後にFXOSでインターフェイスを変更した場合は、各シャーシで同じ変更を行います（データノードから始めて、制御ノードで終わります）。
- 同じNTPサーバを使用する必要があります。Firewall Threat Defenseでは、Firewall Management Centerも同じNTPサーバーを使用する必要があります。時間を手動で設定しないでください。

マルチインスタンス クラスタリングの要件

- セキュリティモジュール/エンジン間クラスタリングなし：特定のクラスタでは、セキュリティモジュール/エンジンごとに 1 つのコンテナインスタンスのみを使用できます。同じモジュール上で実行されている場合、同じクラスタに2つのコンテナインスタンスを追加することはできません。



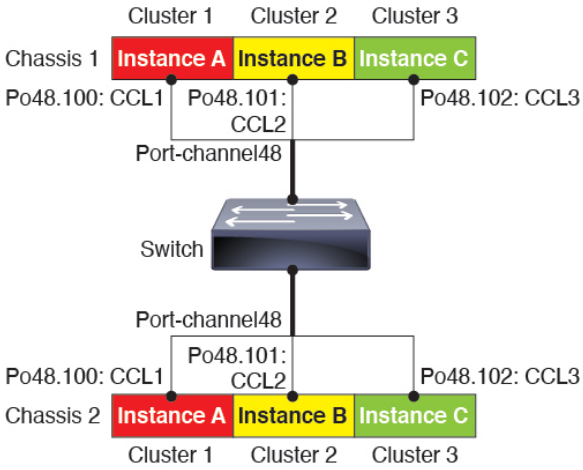
- クラスタとスタンドアロンインスタンスの混在：セキュリティモジュール/エンジン上のすべてのコンテナインスタンスがクラスタに属している必要はありません。一部のインスタンスをスタンドアロンノードまたは高可用性ノードとして使用できます。また、同じセキュリティモジュール/エンジン上で別々のインスタンスを使用して複数のクラスタを作成することもできます。



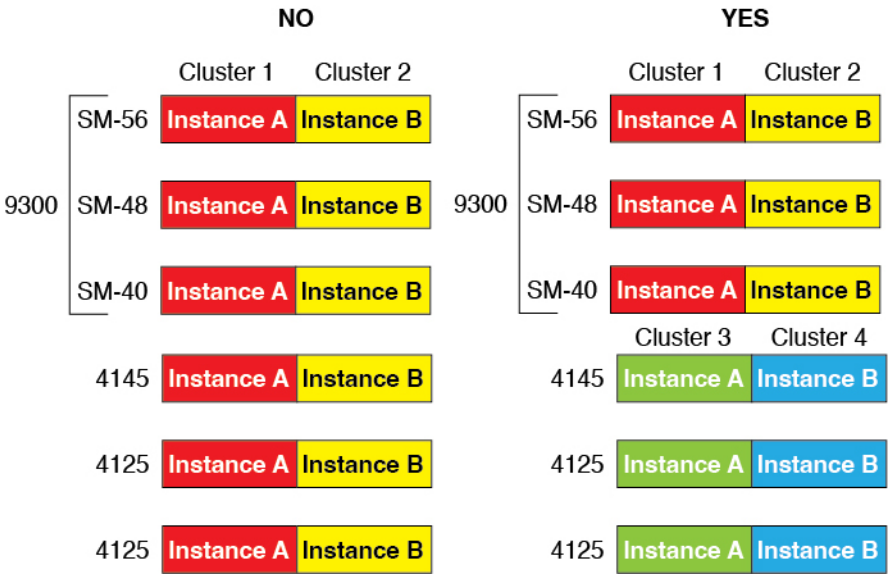
- Firepower 9300 の 3 つすべてのモジュールはクラスタに属している必要があります。Firepower 9300 の場合、クラスタには 3 つすべてのモジュールで 1 つのコンテナインスタンスが必要です。たとえば、モジュール 1 と 2 のインスタンスを使用してクラスタを作成し、モジュール 3 のネイティブインスタンスを使用することはできません。

- リソースプロファイルの一致：クラスタ内の各ノードで同じリソースプロファイル属性を使用することを推奨します。ただし、クラスタノードを別のリソースプロファイルに変更する場合、または異なるモデルを使用する場合は、リソースの不一致が許可されます。

- 専用クラスタ制御リンク：複数のシャーシによるクラスタの場合、各クラスタには専用のクラスタ制御リンクが必要です。たとえば、各クラスタは、同じクラスタタイプの EtherChannel で個別のサブインターフェイスを使用したり、個別の EtherChannel を使用したりできます。



- 共有インターフェイスなし：共有タイプのインターフェイスは、クラスタリングではサポートされません。ただし、同じ管理インターフェイスとイベントインターフェイスを複数のクラスタで使用することはできます。
- サブインターフェイスなし：マルチインスタンスクラスタは、FXOS 定義の VLAN サブインターフェイスを使用できません。クラスタ制御リンクは例外で、クラスタ EtherChannel のサブインターフェイスを使用できます。
- シャーシモデルの混在：クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。または、Firepower 4145 および 4125 でクラスタを作成できます。



- 最大 6 ノード：クラスタ内では最大 6 つのコンテナインスタンスを使用できます。

スイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチの特性については、『Cisco FXOS Compatibility』を参照してください。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

インターフェイスに関する注意事項と制限事項

VLAN サブインターフェイス

- 本書では、*FXOS* VLAN サブインターフェイスについてのみ説明します。Firewall Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。詳細については、FXOS インターフェイスとアプリケーション インターフェイス （217 ページ）を参照してください。
- サブインターフェイス（および親インターフェイス）はコンテナインスタンスにのみ割り当てることができます。

（注） 親インターフェイスをコンテナインスタンスに割り当てると、タグなし（非 VLAN）トラフィックだけが渡されます。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。クラスタタイプのインターフェイスの場合、親インターフェイスを使用することはできません。

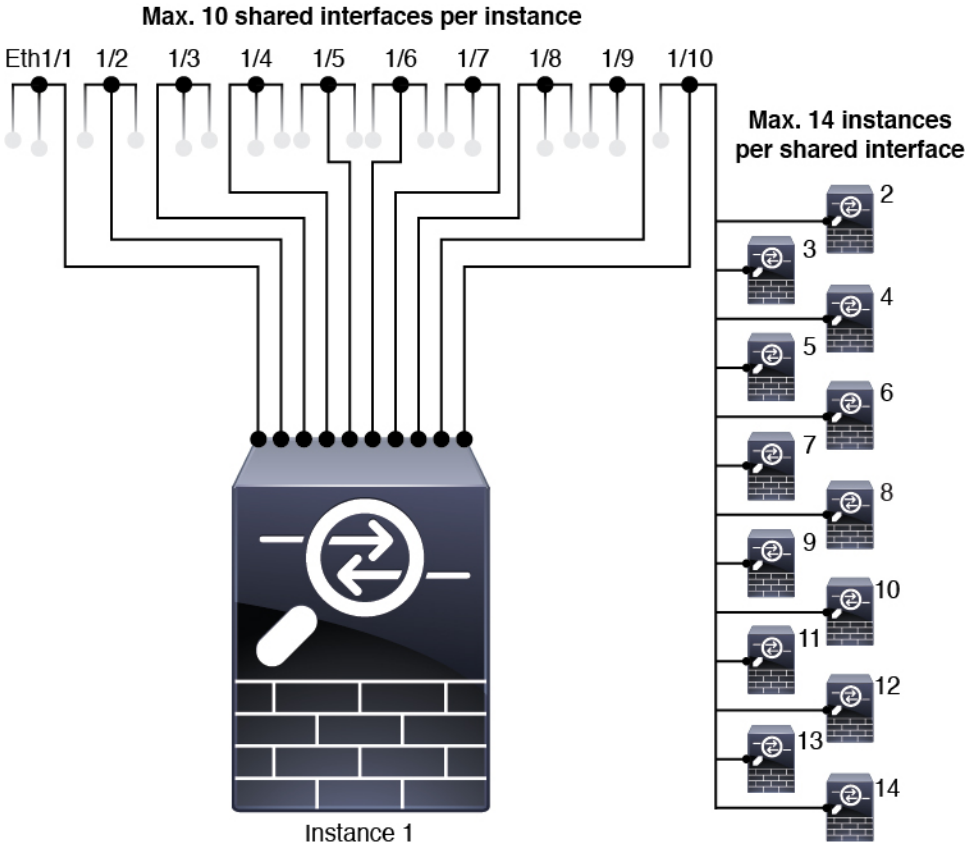
- サブインターフェイスは、データまたはデータ共有タイプのインターフェイス、およびクラスタタイプのインターフェイスでサポートされます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタに使用することはできません。
- マルチインスタンス クラスタリングの場合、データインターフェイス上の FXOS サブインターフェイスはサポートされません。ただし、クラスタ制御リンクではサブインターフェイスがサポートされているため、クラスタ制御リンクには専用の EtherChannel または EtherChannel のサブインターフェイスを使用できます。アプリケーション定義のサブインターフェイスは、データインターフェイスでサポートされていることに注意してください。
- 最大 500 個の VLAN ID を作成できます。

- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
  - Firewall Threat Defense インラインセットまたはパッシブインターフェイスとしてサブインターフェイスを使用することはできません。
  - フェールオーバーリンクにサブインターフェイスを使用すると、その親のすべてのサブインターフェイスおよび親自体の、フェールオーバーリンクとしての使用が制限されます。一部のサブインターフェイスをフェールオーバーリンクとして、一部を通常のデータインターフェイスとして使用することはできません。

データ共有インターフェイス

- ネイティブインスタンスではデータ共有インターフェイスを使用することはできません。
- 共有インターフェイスごとの最大インスタンス数：14。たとえば、Instance14 を介して Instance1 に Ethernet1/1 を割り当てることができます。

  共有インターフェイスごとの最大インスタンス数は 10 です。たとえば、Ethernet1/1.10 を介して Instance1 に Ethernet1/1.1 を割り当てることができます。



- クラスタではデータ共有インターフェイスを使用することはできません。

- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
  - 透過型ファイアウォールモードのデバイスでデータ共有インターフェイスを使用することはできません。
  - Firewall Threat Defenseインラインインセットまたはパッシブインターフェイスでデータ共有インターフェイスを使用することはできません。
  - フェールオーバーリンクにデータ共有インターフェイスを使用することはできません。

次のインラインセット Firewall Threat Defense

- 物理インターフェイス（通常ポートとブレイクアウトポートの両方）および EtherChannel でサポートされます。 サブインターフェイスはサポートされていません。
- リンクステートの伝達はサポートされています。
- 同じインラインセットに対して ハードウェア バイパス およびリンク状態の伝達を有効にしないでください。

ハードウェアバイパス

- Firewall Threat Defense でサポートされています。これらは、ASA の通常のインターフェイスとして使用できます。
- Firewall Threat Defense はインラインセットでのみ ハードウェア バイパス をサポートしています。
- ハードウェアバイパス：対応インターフェイスをブレイクアウトポートに設定することはできません。
- EtherChannel に ハードウェア バイパス インターフェイスを含めて ハードウェア バイパス に使用することはできません。EtherChannel の通常のインターフェイスとして使用できます。
- ハードウェア バイパス はハイ アベイラビリティではサポートされません。
- 同じインラインセットに対して ハードウェア バイパス およびリンク状態の伝達を有効にしないでください。

デフォルトの MAC アドレス

ネイティブインスタンスの場合：

デフォルトのMACアドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスでは、Burned-In MAC Address を使用します。

- EtherChannel: EtherChannelの場合は、そのチャネルグループに含まれるすべてのインターフェイスが同じMACアドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対して透過的になります。ネットワーク アプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャネル インターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。

コンテナインスタンスの場合：

- すべてのインターフェイスのMACアドレスは、MACアドレス プールから取得されます。サブインターフェイスの場合、手動で MAC アドレスを設定する場合は、同じ親インターフェイス上のすべてのサブインターフェイスに一意の MAC アドレスを使用して、正しく分類されるようにしてください。コンテナ インスタンス インターフェイスの自動 MAC アドレス （239 ページ） を参照してください。

一般的なガイドラインと制限事項

ファイアウォール モード

Firewall Threat Defense のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。

ハイ アベイラビリティ

- アプリケーション設定内で高可用性を設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。 データ共有インターフェイスはサポートされていません。

マルチインスタンス

- コンテナインスタンスによる複数インスタンス機能はFirewall Management Center を使用する Firewall Threat Defense に対してのみ使用できます。
- Firewall Threat Defense コンテナ インスタンスの場合、1 つの Firewall Management Center でセキュリティ モジュール/エンジン のすべてのインスタンスを管理する必要があります。
- Firewall Threat Defense コンテナ インスタンスの場合、次の機能はサポートされていません。
  - Radware DefensePro リンク デコレータ
  - Firewall Management Center UCAPL/CC モード
  - ハードウェアへのフローオフロード

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスの有効化、Etherchannel の追加、VLAN サブインターフェイスの追加、インターフェイスプロパティの編集、を実行できます。

インターフェイスの有効化または無効化

各インターフェイスの [管理状態（Admin State）] を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスは無効になっています。 VLANサブインターフェイスの場合、管理状態は親インターフェイスから継承されます。

手順

ステップ 1 [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ページを開きます。

[インターフェイス]ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、下の表にはインストールされているインターフェイスのリストが示されます。

ステップ 2 インターフェイスを有効にするには、 [disabled **Slider disabled**（ ）] をクリックして、[enabled **Slider enabled**（ ）] に変更します。

[はい]をクリックして、変更を確認します。視覚的表現の対応するインターフェイスがグレイから緑に変化します。

ステップ 3 インターフェイスを無効にするには、 [有効なスライダ（enabled **Slider enabled**（ ））] をクリックして、[無効なスライダ（disabled **Slider disabled**（ ））] に変更します。

[はい]をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

（注）
- QSFPH40G-CUxM の場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。
- ポートの SFP を別の SFP モジュールに交換しても、インターフェイスの速度、デュプレックス、および自動ネゴシエーションは自動的に更新されません。インターフェイスを再構成する必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

手順

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

[**All Interfaces**] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 編集するインターフェイスの行の [Edit] をクリックし、[Edit Interface] ダイアログボックスを開きます。

ステップ 3 インターフェイスを有効にするには、[有効（Enable）] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。

ステップ 4 インターフェイスの [タイプ（Type）] を選択します。

インターフェイスタイプの使用方法の詳細については、インターフェイス タイプ （214 ページ）を参照してください。

- **データ**
- [データ共有（Data-sharing）]：コンテナインスタンスのみ。
- **管理**
- [Firepower-eventing]：Firewall Threat Defense のみ。
- [クラスタ（Cluster）]：[クラスタ（Cluster）] タイプは選択しないでください。デフォルトでは、クラスタ制御リンクはポートチャネル 48 に自動的に作成されます。

ステップ 5 （任意） [Speed] ドロップダウン リストからインターフェイスの速度を選択します。

ステップ 6 （任意） インターフェイスで [Auto Negotiation] がサポートされている場合は、[Yes] または [No] オプション ボタンをクリックします。

ステップ 7 （任意） [デュプレックス（Duplex）] ドロップダウン リストからインターフェイスのデュプレックスを選択します。

ステップ 8 （任意） **デバウンス時間（ミリ秒）**を明示的に設定します。0 から 15000 ミリ秒の値を入力します。

（注）
デバウンス時間の設定は、1G インターフェイスではサポートされていません。

ステップ 9 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大 16 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。リンク集約制御プロトコル（LACP）では、2 つのネットワークデバイス間でリンク集約制御プロトコルデータユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データまたはデータ共有インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

（注） モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

非データ インターフェイスのみがアクティブ モードをサポートしています。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [一時停止（Suspended）] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータ インターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止（Suspended）] または [ダウン（Down）] 状態に戻ります。

手順

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

[**All Interfaces**] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 インターフェイス テーブルの上にある [ポート チャネルの追加（Add Port Channel）] をクリックし、[ポート チャネルの追加（Add Port Channel）] ダイアログボックスを開きます。

ステップ 3 [ポート チャネル ID（Port Channel ID）] フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ～ 47 です。

クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、ポートチャネル 48 を削除し、別の ID を使用してクラスタタイプの EtherChannel を設定できます。複数のクラスタタイプの EtherChannel を追加し、マルチインスタンス クラスタリングで使用する VLAN サブインターフェイスを追加できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。

ステップ 4 ポート チャネルを有効にするには、[有効化（Enable）] チェックボックスをオンにします。ポート チャネルをディセーブルにするには、**[Enable]**チェックボックスをオフにします。

ステップ 5 インターフェイスの [タイプ（Type）] を選択します。

インターフェイスタイプの使用方法の詳細については、インターフェイス タイプ （214 ページ）を参照してください。

- **データ**
- [データ共有（Data-sharing）]：コンテナインスタンスのみ。
- **管理**
- [Firepower-eventing]：Firewall Threat Defense のみ。
- **クラスタ**

ステップ 6 ドロップダウン リストでメンバーインターフェイスに適した [管理速度（Admin Speed）] を設定します。

指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。

ステップ 7 データまたはデータ共有インターフェイスに対して、LACP ポート チャネル [Mode]、[Active] または [On] を選択します。

非データまたはデータ共有インターフェイスの場合、モードは常にアクティブです。

ステップ 8 メンバーインターフェイスに適した [管理デュプレックス（Admin Duplex）] を設定します（[全二重（Full Duplex）] または [半二重（Half Duplex）]）。

指定したデュプックスのメンバーインターフェイスを追加すると、ポートチャネルに正常に参加されます。

ステップ 9 ポート チャネルにインターフェイスを追加するには、**[Available Interface]** リストでインターフェイスを選択し、**[Add Interface]** をクリックしてそのインターフェイスを [Member ID] リストに移動します。

同じメディアタイプとキャパシティで最大 16 のインターフェイスを追加できます。メンバーインターフェイスは、同じ速度とデュプレックスに設定する必要があり、このポートチャネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

ヒント
複数のインターフェイスを一度に追加できます。個々のインターフェイスを複数選択するには、**Ctrl** キーを押しながら必要なインターフェイスをクリックします。インターフェイスの範囲を選択するには、範囲の最初にあたるインターフェイスを選択し、次に **Shift** キーを押しながらその範囲の最後にあたるインターフェイスをクリックします。

ステップ 10 ポートチャネルからインターフェイスを削除するには、[Member ID] リストでそのインターフェイスの右側にある **[Delete]** ボタンをクリックします。

ステップ 11 [OK] をクリックします。

コンテナ インスタンスの VLAN サブインターフェイスの追加

ネットワーク配置に応じて、250 ～ 500 の VLAN サブインターフェイスをシャーシに追加できます。シャーシには最大 500 個のサブインターフェイスを追加できます。

マルチインスタンス クラスタリングの場合、クラスタタイプのインターフェイスにサブインターフェイスを追加するだけです。データインターフェイス上のサブインターフェイスはサポートされません。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナ インスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

本書では、*FXOS* VLAN サブインターフェイスについてのみ説明します。Firewall Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。FXOS サブインターフェイスとアプリケーションサブインターフェイスを使用するタイミングの詳細については、FXOS インターフェイスとアプリケーションインターフェイス（217 ページ）を参照してください。

手順

ステップ 1 **[Interfaces]** を選択して **[All Interfaces]** タブを開きます。

[All Interfaces] タブには、ページの上部に現在インストールされているインターフェイスが視覚的に表示され、下の表にはインストールされているインターフェイスのリストが示されています。

ステップ 2 **[Add New]** > **[Subinterface]** をクリックして [Add Subinterface] ダイアログボックスを開きます。

ステップ 3 インターフェイスの [タイプ（Type）] を選択します。

インターフェイスタイプの使用方法の詳細については、インターフェイス タイプ （214 ページ）を参照してください。

- **データ**
- **データ共有**
- [クラスタ（Cluster）]：クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタに使用することはできません。

データインターフェイスおよびデータ共有インターフェイスの場合：タイプは、親インターフェイスのタイプに依存しません。たとえば、データ共有の親とデータサブインターフェイスを設定できます。

ステップ 4 ドロップダウン リストから親**インターフェイス**を選択します。

現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合、その親インターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できます。

ステップ 5 [Subinterface ID] を 1 ～ 4294967295 で入力します。

この ID は、*interface_id.subinterface_id* のように親インターフェイスの ID に追加されます。たとえば、サブインターフェイスを ID 100 でイーサネット 1/1 に追加する場合、そのサブインターフェイス ID はイーサネット 1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。

ステップ 6 1 ～ 4095 の間で [VLAN ID] を設定します。

ステップ 7 [OK] をクリックします。

親インターフェイスを展開し、その下にあるすべてのサブインターフェイスを表示します。

論理デバイスの設定

Firepower 4100/9300に、スタンドアロン論理デバイスまたはハイアベイラビリティペアを追加します。

クラスタリングについては、Firepower 4100/9300 のクラスタリング （543 ページ）を参照してください。

コンテナインスタンスにリソースプロファイルを追加

コンテナインスタンスごとにリソース使用率を指定するには、1つまたは複数のリソースプロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。

- コアの最小数は 6 です。

（注） コア数が少ないインスタンスは、コア数が多いインスタンスよりも、CPU使用率が比較的高くなる場合があります。コア数が少ないインスタンスは、トラフィック負荷の変化の影響を受けやすくなります。トラフィックのドロップが発生した場合には、より多くのコアを割り当ててください。

- コアは偶数（6、8、10、12、14 など）で最大値まで割り当てることができます。
- 使用可能なコアの最大数は、セキュリティモジュール/シャーシモデルによって異なります。コンテナ インスタンスの要件と前提条件 （244 ページ） を参照してください。

シャーシには、「Default-Small」と呼ばれるデフォルトリソース プロファイルが含まれています。このコア数は最小です。このプロファイルの定義を変更したり、使用されていない場合には削除することもできます。シャーシをリロードし、システムに他のプロファイルが存在しない場合は、このプロファイルが作成されます。

リソースプロファイルを割り当て後に変更すると、問題が発生します。次のガイドラインを参照してください。

- 使用中のリソースプロファイルの設定を変更することはできません。そのリソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。
- Firewall Threat Defense インスタンスを Firewall Management Center に追加した後にリソースプロファイルの設定を変更する場合は、Firewall Management Center の [デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [システム（System）] > [インベントリ（Inventory）] ダイアログボックスで各ユニットのインベントリを更新します。
- インスタンスに別のプロファイルを割り当てると、再起動します。
- 両方のユニットでプロファイルを同じにする必要がある確立されたハイアベイラビリティペアのインスタンスに異なるプロファイルを割り当てる場合、次の手順を実行する必要があります。
  1. ハイ アベイラビリティを解除します。
  2. 両方のユニットに新しいプロファイルを割り当てます。
  3. ハイアベイラビリティを再確立します。
- 確立されたクラスタ内のインスタンスに異なるプロファイルを割り当てる場合は、プロファイルが一致する必要がないため、最初に新しいプロファイルをデータノードに適用します。すべてが復帰したら、新しいプロファイルを制御ノードに適用できます。

手順

ステップ 1 **[Platform Settings]** > **[Resource Profiles]** を選択し、[Add] をクリックします。

[リソースプロファイルの追加（Add Resource Profile）] ダイアログボックスが表示されます。

ステップ 2 次のパラメータを設定します。

- [名前（Name）]：プロファイルの名前を 1 ～ 64 文字で設定します。追加後にこのプロファイルの名前を変更することはできません。
- [説明（Description）]：プロファイルの説明を最大 510 文字で設定します。
- [コア数（Number of Cores）]：プロファイルのコア数を 6 ～ 最大数（偶数）で設定します。最大数はシャーシによって異なります。

ステップ 3 **[OK]** をクリックします。

スタンドアロン Firewall Threat Defense の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2モジュール クラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用できます。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードし、そのイメージを Firepower 4100/9300 シャーシ。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および Firewall Threat Defense）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（また、[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示されます）。
- 後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。詳細については、FTD コマンドリファレンスの **configure network management-data-interface** コマンドを参照してください。
- また、少なくとも1つのデータ タイプのインターフェイスを設定する必要があります。必要に応じて、すべてのイベントのトラフィック（Web イベントなど）を運ぶ firepower-eventing インターフェイスも作成できます。詳細については、「インターフェイス タイプ （214 ページ）」を参照してください。
- コンテナインスタンスに対して、デフォルトのプロファイルを使用しない場合は、コンテナインスタンスにリソースプロファイルを追加 （260 ページ）に従ってリソース プロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティ モジュール/エンジン を再度初期化する必要があります。[セキュリティモジュール（Security Modules）] または [セキュリティエンジン（Security Engine）] を選択し、[再初期化（Reinitialize）] をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテ

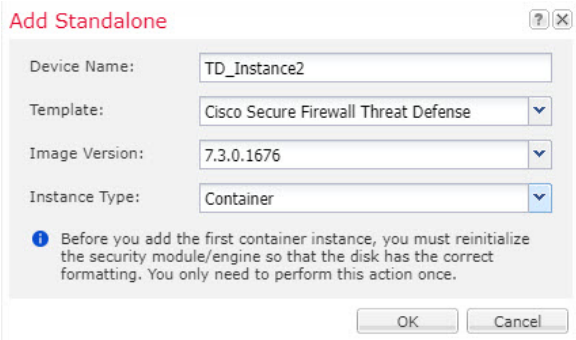
ナインスタンスに置き換える場合は、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。

- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス
  - Firewall Management Center 選択した IP アドレス/NAT ID
  - DNS サーバの IP アドレス
  - Firewall Threat Defense ホスト名とドメイン名

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

（注）
論理デバイスの追加後にこの名前を変更することはできません。

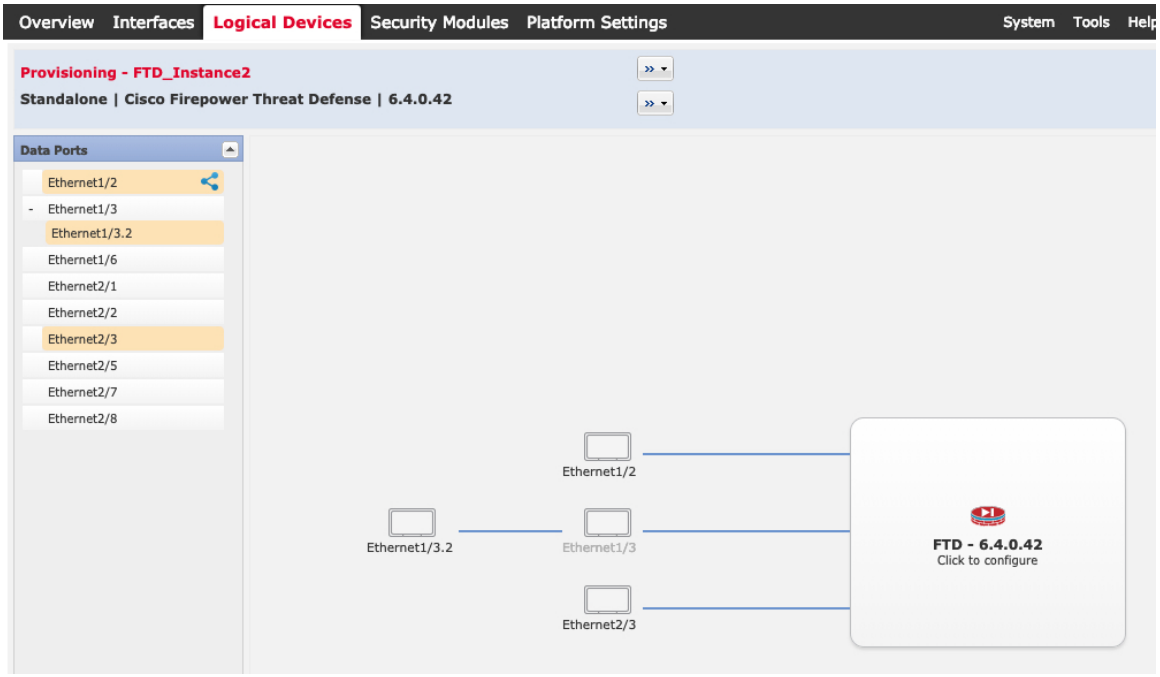
b) [Template] では、[Cisco Firepower Threat Defense] を選択します。
c) [Image Version] を選択します。
d) [インスタンスタイプ（Instance Type）] : [コンテナ（Container）] または [ネイティブ（Native）] を選択します。

ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。コンテナ インスタンスでは、セキュリティ モジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

e) [OK] をクリックします。

[プロビジョニング - デバイス名（Provisioning - device name）] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。



[Interfaces] ページでは、以前に有効にしたデータとデータ共有インターフェイスのみを割り当てることができます。後で Firewall Management Center のこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

コンテナ インスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナインスタンスに割り当てることができます。データ共有インターフェイスは [Sharing] アイコン（）で示されます。

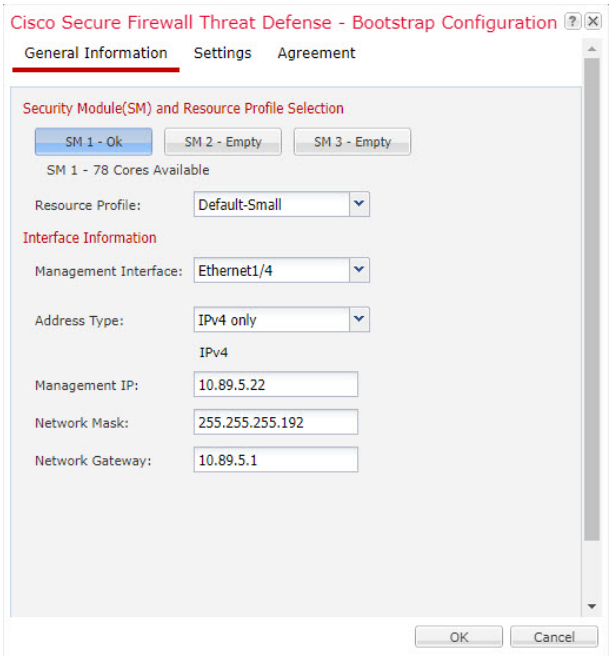
ハードウェア バイパス 対応のポートは次のアイコンで表示されます：。特定のインターフェイス モジュールでは、インライン セット インターフェイスに対してのみハードウェア バイパス機能を有効にできます（Firewall Management Center設定ガイドを参照）。ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。ハードウェア バイパス ペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示

されます。ハードウェア バイパス 機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。



a) （Firepower 9300 の場合）[セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。

b) コンテナのインスタンスでは、**リソースのプロファイル**を指定します。

後でさまざまなリソースプロファイルを割り当てると、インスタンスがリロードされ、この操作に約 5 分かかることがあります。

（注）
両方のユニットでプロファイルを同じにする必要がある確立されたハイアベイラビリティペアのインスタンスに異なるプロファイルを後で割り当てる場合、次の手順を実行する必要があります。

1. ハイ アベイラビリティを解除します。
2. 両方のユニットに新しいプロファイルを割り当てます。
3. ハイアベイラビリティを再確立します。

c) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

d) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

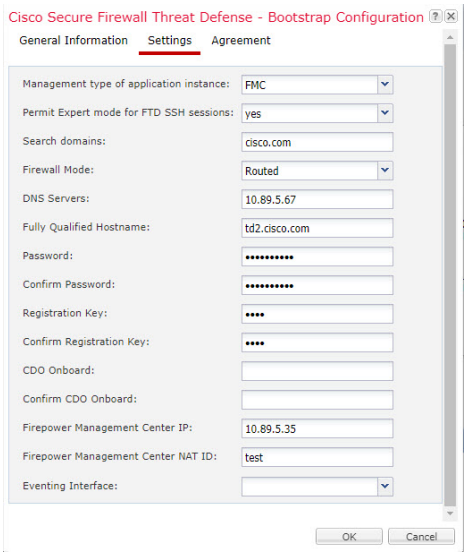
e) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

f) [Network Mask] または [Prefix Length] に入力します。

g) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] タブで、次の項目を入力します。



a) ネイティブ インスタンスの場合は、[アプリケーションインスタンスの管理タイプ（Management type of application instance）] ドロップダウン リストで [FMC] を選択します。

ネイティブインスタンスは、マネージャとしてのファイアウォールデバイスマネージャもサポートしています。論理デバイスを展開した後にマネージャタイプを変更することはできません。

b) 管理 Firewall Management Center の [Firepower Management Center IP] を入力します。Firewall Management Center の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

c) **FTD SSH セッションからエキスパート モード**、[**Yes**]、または [**No**] を許可します。エキスパート モードでは、高度なトラブルシューティングに Firewall Threat Defense シェルからアクセスできます。

このオプションで [Yes] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザがエキスパートモードを開始できます。[いいえ（No）] を選択した場合、FXOS CLI からコンテナインスタンスにアクセスするユーザのみがエキスパー

トモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパートモードを使用します。このモードを開始するには、Firewall Threat Defense CLI で **expert** コマンドを使用します。

d) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。

e) [Firewall Mode] を [Transparen] または [Routed] に選択します。

ルーテッドモードでは、Firewall Threat Defenseはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォールモードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

f) [DNS Servers] をカンマ区切りのリストとして入力します。

たとえば、Firewall Management Centerのホスト名を指定する場合、Firewall Threat Defense は DNS を使用します。

g) Firewall Threat Defense の [Fully Qualified Hostname] を入力します。

h) 登録時に Firewall Management Center とデバイス間で共有する [Registration Key] を入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。Firewall Threat Defense を追加するときに、Firewall Management Center に同じキーを入力します。

i) CLI アクセス用の Firewall Threat Defense 管理ユーザの [Password] を入力します。

j) イベントの送信に使用する [イベンティングインターフェイス（Eventing Interface）] を選択します。指定しない場合は、管理インターフェイスが使用されます。

このインターフェイスは、Firepower-eventing インターフェイスとして定義する必要があります。

k) コンテナインスタンスの場合は、[ハードウェア暗号化（Hardware Crypto）] を [有効（Enabled）] または [無効（Disabled）] に設定します。

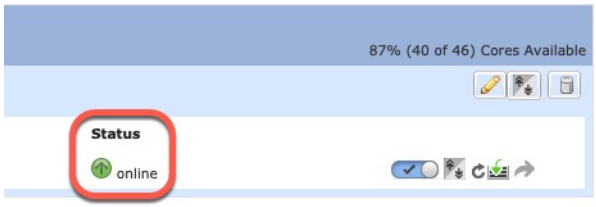
この設定により、ハードウェアの TLS 暗号化アクセラレーションが有効になり、特定タイプのトラフィックのパフォーマンスが向上します。この機能はデフォルトでイネーブルになっています。セキュリティ モジュールごとに最大 16 個のインスタンスについて TLS 暗号化アクセラレーションをイネーブルにすることができます。この機能は、ネイティブインスタンスでは常に有効になっています。このインスタンスに割り当てられているハードウェア暗号化リソースの割合を表示するには、**show hw-crypto** コマンドを入力します。

ステップ 7 [Agreement] タブで、エンド ユーザ ライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 **[保存（Save）]** をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**[論理デバイス（Logical Devices）]** ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 10 Firewall Threat Defense を管理対象デバイスとして追加し、セキュリティ ポリシーの設定を開始するには、Firewall Management Center コンフィギュレーション ガイドを参照してください。

ハイ アベイラビリティ ペアの追加

Firewall Threat Defenseハイ アベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイ アベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

ハイアベイラビリティの要件と前提条件 （245 ページ）を参照してください。

手順

ステップ 1 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 2 フェールオーバーリンクとステートリンクに 1 つまたは 2 つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間で高可用性トラフィックを交換します。フェールオーバーリンクとステートリンクの組み合わせには、10 GB のデータインターフェイスを使用することを推奨します。使用可能なインターフェイスがある場合は、別のフェールオーバーリンクとステートリンクを使用できます。ステートリンクには、最も多くの帯域幅が必要です。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用す

ることはできません。シャーシ間でスイッチを使用することをお勧めします。この場合、フェールオーバーインターフェイスと同じネットワークセグメント上に他のデバイスを配置できません。

コンテナインスタンスの場合、データ共有インターフェイスはフェールオーバーリンクではサポートされていません。親インターフェイスまたはEtherChannelにサブインターフェイスを作成し、各インスタンスのサブインターフェイスを割り当てて、フェールオーバーリンクとして使用することを推奨します。フェールオーバーリンクと同じ親上のすべてのサブインターフェイスを使用する必要があることに注意してください。1 つのサブインターフェイスをフェールオーバーリンクとして使用し、他のサブインターフェイス（または親インターフェイス）を通常のデータインターフェイスとして使用することはできません。

ステップ 3 論理デバイスで高可用性を有効にします。高可用性 （283 ページ）を参照してください。

ステップ 4 高可用性を有効にした後にインターフェイスを変更する必要がある場合は、最初にスタンバイユニットで変更を実行してから、アクティブユニットで変更を実行します。

Firewall Threat Defense 論理デバイスのインターフェイスの変更

Firewall Threat Defense 論理デバイスでは、インターフェイスの割り当てや割り当て解除、または管理インターフェイスの置き換えを行うことができます。その後、Firewall Management Center でインターフェイス設定を同期できます。

新しいインターフェイスの追加や未使用のインターフェイスの削除が、Firewall Threat Defense の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバなど、Firewall Threat Defense の設定における多くの場所で直接参照されている可能性があります。セキュリティゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつFirewall Management Center での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。

始める前に

- 物理インターフェイスの設定 （254 ページ）およびEtherChannel（ポート チャネル）の追加 （256 ページ） に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスをEtherChannelに追加する場合(たとえば、すべてのインターフェイスがデフォルトでクラスタに割り当てられる場合)、最初にそのインターフェイスを論理デバイスから割り当て解除してから、EtherChannelに追加する必要があります。新しいEtherChannelの場合、EtherChannelをデバイスに割り当てることができます。
- 管理インターフェイスまたはイベントインターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバー インターフェイスが少なくとも 1 つある EtherChannel

を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。Firewall Threat Defense デバイスの再起動（管理インターフェイスの変更により再起動）後、Firewall Management Center で設定を同期すると、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。

- クラスタリングやハイアベイラビリティのため、Firewall Management Center で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にデータ/スタンバイユニットでインターフェイスを変更してから、制御/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼさないことに注意してください。
- マルチインスタンスモードでは、サブインターフェイスを同じ VLAN タグを持つ別のサブインターフェイスと変更するには、最初にインターフェイスのすべての設定（nameif config を含む）を削除してから、Firewall シャーシ マネージャ からインターフェイスの割り当てを解除する必要があります。割り当てが解除されたら、新しいインターフェイスを追加し、Firewall Management Center からインターフェイスの同期を使用します。

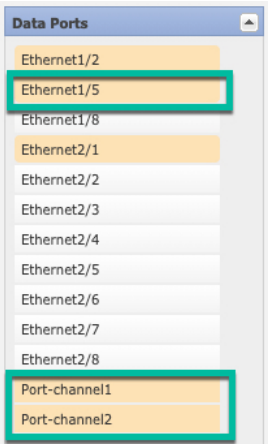
手順

ステップ 1 Firewall シャーシ マネージャで、[論理デバイス]を選択します。

ステップ 2 右上にある [編集（Edit）] アイコンをクリックし、その論理デバイスを編集します。

ステップ 3 [データポート（Data Ports）] 領域で新しいデータインターフェイスを選択し、そのインターフェイスを割り当てます。

まだインターフェイスを削除しないでください。



ステップ 4 次のように、管理インターフェイスまたはイベントインターフェイスを置き換えます。

これらのタイプのインターフェイスでは、変更を保存するとデバイスが再起動します。

a) ページ中央のデバイスアイコンをクリックします。

b) [一般（General）] または [クラスタ情報（Cluster Information）] タブで、ドロップダウン リストから新しい [管理インターフェイス（Management Interface）] を選択します。
c) [設定（Settings）] タブで、ドロップダウンリストから新しい [イベントインターフェース（Eventing Interface）] を選択します。
d) [OK]をクリックします。

管理インターフェイスの IP アドレスを変更した場合は、Firewall Management Center でデバイスの IP アドレスを変更する必要もあります。**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス/クラスタ（Device/Cluster）]** と移動します。[管理]領域で、ブートストラップ設定アドレスと一致するようにIPアドレスを設定します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 Firewall Management Center でインターフェイスを同期します。

a) Firewall Management Center にログインします。
b) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defenseデバイス[編集（Edit）]（） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。
c) [インターフェイス（Interfaces）] タブの左上にある [デバイスの同期（Sync Device）] ボタンをクリックします。
d) 変更が検出されると、インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス（Interfaces）] ページに表示されます。インターフェイスの変更を表示するには、[クリックして詳細を表示]リンクをクリックします。
e) インターフェイスを削除する場合は、古いインターフェイスから新しいインターフェイスにインターフェイス設定を手動で転送します。

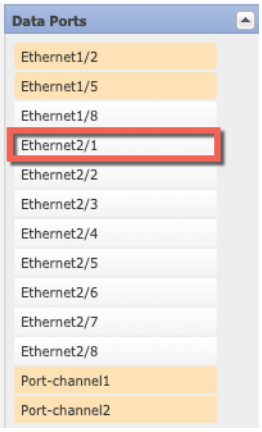
   インターフェイスはまだ削除していないため、既存の設定を参照できます。古いインターフェイスを削除して検証を再実行した後も、さらに設定を修正する機会があります。検証を実行すると、古いインターフェイスがまだ使用されているすべての場所が表示されます。

f) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

   エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

g) [Save] をクリックします。
h) **[展開（Deploy）] > [展開（Deployment）]**をクリックします。
i) デバイスを選択して [展開（Deploy）] をクリックし、割り当てられたデバイスにポリシーを展開します。変更内容は導入するまで適用されません。

ステップ 7 Firewall シャーシ マネージャ でデータインターフェイスの割り当てを解除するには、[データポート（Data Ports）] 領域でそのインターフェイスの選択を解除します。



ステップ 8 [保存（Save）] をクリックします。

ステップ 9 Firewall Management Center でインターフェイスを再度同期します。

アプリケーションのコンソールへの接続

アプリケーションのコンソールに接続するには、次の手順を使用します。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect ftd *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- Firewall Threat Defense：「**exit**」と入力します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

論理デバイスの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firewall Threat Defense 動作リンク状態と物理リンク状態の同期	6.7	いずれか	シャーシでは、Firewall Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Firewall Threat Defense アプリケーション インターフェイスの管理状態は考慮されません。Firewall Threat Defense からの同期がない場合は、たとえば、Firewall Threat Defenseアプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、Firewall Threat Defense のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、Firewall Threat Defense が処理できるようになる前に外部ルータが Firewall Threat Defense へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、またはRadware vDP デコレータを使用する Firewall Threat Defense ではサポートされていません。ASA ではサポートされていません。 新規/変更された [Firepower Chassis Manager] 画面：**[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）]** 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail**
コンテナインスタンス向けの Firewall Management Center を使用した Firewall Threat Defense 設定のバックアップと復元	6.7	いずれか	Firewall Threat Defense コンテナインスタンスで Firewall Management Center バックアップ/復元ツールを使用できるようになりました。 新規/変更された Firewall Management Center 画面：**[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）]** 新規/変更された Firewall Threat Defense CLI コマンド：**restore** サポートされるプラットフォーム：Firepower 4100/9300 （注） FXOS 2.9 が必要です。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタ タイプ インターフェイスでの VLAN サブインターフェイスのサポート（マルチインスタンス使用のみ）	6.6	任意（Any）	マルチインスタンスクラスタで使用するために、クラスタタイプのインターフェイスでVLANサブインターフェイスを作成できるようになりました。各クラスタには一意のクラスタ制御リンクが必要であるため、VLANサブインターフェイスはこの要件を満たすための簡単な方法を提供します。または、クラスタごとに専用の EtherChannel を割り当てることもできます。複数のクラスタインターフェイスが許可されるようになりました。 新規/変更された [Firepower Chassis Manager] 画面： **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）]** ドロップダウンメニュー **[サブインターフェイス（Subinterface）] > [タイプ（Type）]**フィールド 新規/変更された FXOS コマンド：**set port-type cluster** （注） FXOS 2.8.1 が必要です。
Firepower 4112 上の Firewall Threat Defense	6.6	任意（Any）	Firepower 4112 を導入しました。 （注） FXOS 2.8.1 が必要です。
複数のコンテナインスタンスのTLS暗号化アクセラレーション	6.5	任意（Any）	Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス（最大 16 個）で TLS 暗号化アクセラレーションがサポートされるようになりました。以前は、モジュール/セキュリティエンジンごとに1つのコンテナインスタンスに対してのみTLS暗号化アクセラレーションを有効にすることができました。 新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、**enter hw-crypto** 次に **set admin-state enabled** FXOS コマンドを使用します。 新規/変更された [Firepower Chassis Manager] 画面： **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）] > [設定（Settings）] >** の [ハードウェア暗号化（Hardware Crypto）] ドロップダウンメニュー （注） FXOS 2.7.1 が必要です。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firewall Threat Defense Firepower 4115、4125、および 4145	6.4	任意（Any）	Firepower 4115、4125、および 4145 が導入されました。 （注） FXOS 2.6.1.157 が必要です。
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	6.4	任意（Any）	3 つのセキュリティ モジュール、SM-40、SM-48、および SM-56 が導入されました。 （注） FXOS 2.6.1.157 が必要です。
ASA および Firewall Threat Defense を同じ Firepower 9300 の別のモジュールでサポート	6.4	任意（Any）	ASA および Firewall Threat Defense 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1.157 が必要です。
モジュール/セキュリティエンジンのいずれかの Firewall Threat Defense コンテナインスタンスでの SSL ハードウェアアクセラレーションのサポート	6.4	任意（Any）	これで、モジュール/セキュリティ エンジンのいずれかのコンテナ インスタンスに対して SSL ハードウェア アクセラレーションを有効にすることができるようになりました。他のコンテナインスタンスに対して SSL ハードウェアアクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。 新規/変更された FXOS コマンド： **config hwCrypto enable** 変更された画面はありません。 （注） FXOS 2.6.1.157 が必要です。

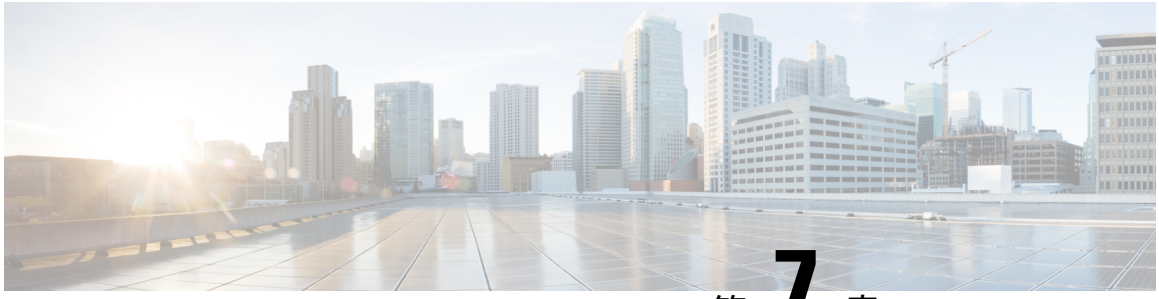
機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firepower 4100/9300 の Firewall Threat Defense のマルチインスタンス機能	6.3	任意（Any）	

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
			単一のセキュリティエンジンまたはモジュールに、それぞれ Firewall Threat Defense コンテナインスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブアプリケーション インスタンスを展開できるだけでした。 柔軟な物理インターフェイスの使用を可能にするため、FXOS でVLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。リソース管理では、各インスタンスのパフォーマンス機能をカスタマイズできます。 2 台の個別のシャーシ上でコンテナ インスタンスを使用して高可用性を使用できます。クラスタリングはサポートされません。 （注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。Firewall Threat Defense ではマルチコンテキストモードは使用できません。 新規/変更された Firewall Management Center 画面： • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** アイコン **[インターフェイス（Interfaces）]** タブ 新規/変更された [Firepower Chassis Manager] 画面： • **[概要（Overview）]** > **[デバイス（Devices）]** • **[インターフェイス（Interfaces）]** > **[すべてのインターフェイス（All Interfaces）]** > **[新規追加（Add New）]** ドロップダウン メニュー **[サブインターフェイス（Subinterface）]** • **[インターフェイス（Interfaces）]** > **[すべてのインターフェイス（All Interfaces）]** > **[タイプ（Type）]** • **[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]** • **[プラットフォームの設定（Platform Settings）]** > **[Macプール（Mac Pool）]** • **[プラットフォームの設定（Platform Settings）]** > **[リソースのプロファイル（Resource Profiles）]** 新規/変更された FXOS コマンド：**connect ftd** *name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**createresource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
			set resource-profile-name、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** サポートされるプラットフォーム：Firepower 4100/9300
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	6.3	任意（Any）	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）] > [クラスタ情報（Cluster Information）] > [CCL サブネット IP（CCL Subnet IP）]**フィールド 新規/変更された FXOS コマンド： **set cluster-control-link network** サポートされるプラットフォーム：Firepower 4100/9300
オンモードでのデータ EtherChannel のサポート	6.3	任意（Any）	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 新規/変更された [Firepower Chassis Manager] 画面： • **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [ポートチャネルの編集（Edit Port Channel）] > [モード（Mode）]** 新規/変更された FXOS コマンド：**set port-channel-mode** サポートされるプラットフォーム：Firepower 4100/9300
Firewall Threat Defense インラインセットでの EtherChannel のサポート	6.2	任意（Any）	Firewall Threat Defense インライン セットで Etherchannel を使用できるようになりました。 サポートされるプラットフォーム：Firepower 4100/9300

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
6 つの Firewall Threat Defense モジュールのシャーシ間クラスタリング	6.2	任意（Any）	Firewall Threat Defense のシャーシ間クラスタリングが実現されました。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [構成（Configuration）]** サポートされるプラットフォーム：Firepower 4100/9300
サポート対象ネットワーク モジュールに対する Firepower 4100/9300 でのハードウェア バイパス サポート	6.1	いずれか	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Firepower 4100/9300
Firewall Threat Defense のインライン セット リンク ステート伝達サポート	6.1	いずれか	Firewall Threat Defense アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、Firewall Threat Defense はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。 新規/変更された FXOS コマンド：**show fault |grep link-down**、**show interface detail** サポートされるプラットフォーム：Firepower 4100/9300

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firepower 9300 の Firewall Threat Defense でのシャーシ内クラスタリング サポート	6.0.1	いずれか	Firepower 9300 が Firewall Threat Defense アプリケーションでシャーシ内クラスタリングをサポートするようになりました。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [構成（Configuration）]** 新規/変更された FXOS コマンド：**enter mgmt-bootstrap ftd, enter bootstrap-key FIREPOWER_MANAGER_IP, enter bootstrap-key FIREWALL_MODE, enter bootstrap-key-secret REGISTRATION_KEY, enter bootstrap-key-secret PASSWORD, enter bootstrap-key FQDN, enter bootstrap-key DNS_SERVERS, enter bootstrap-key SEARCH_DOMAINS, enter ipv4 firepower, enter ipv6 firepower, set value, set gateway, set ip, accept-license-agreement** サポートされるプラットフォーム：Firepower 4100/9300



第 7 章

高可用性

ここでは、アクティブ/スタンバイフェールオーバーを設定して、Firewall Threat Defense システムのハイアベイラビリティを実現する方法について説明します。

- Secure Firewall Threat Defense のハイ アベイラビリティについて （283 ページ）
- 設定同期の最適化 （301 ページ）
- ハイアベイラビリティの要件と前提条件 （302 ページ）
- 高可用性 のガイドライン （302 ページ）
- ハイ アベイラビリティ ペアの追加 （305 ページ）
- オプションの高可用性パラメータの設定 （308 ページ）
- 高可用性 の管理 （311 ページ）
- 高可用性のモニタリング （318 ページ）
- 高可用性の履歴 （319 ページ）

Secure Firewall Threat Defense のハイ アベイラビリティについて

フェールオーバーとも呼ばれるハイアベイラビリティを設定するには、専用フェールオーバーリンク（および任意でステート リンク）を介して相互に接続された 2 台の同じ Firewall Threat Defense デバイスが必要です。Firewall Threat Defense はアクティブ/スタンバイ フェールオーバーをサポートしています。つまり 1 台のユニットがアクティブなユニットとなりトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニターされます。所定の条件に一致すると、フェールオーバーが行われます。

（注） ハイ アベイラビリティは、パブリック クラウドで実行される Firewall Threat Defense Virtual ではサポートされていません。Firewall Threat Defense Virtual デバイスの高可用性設定の詳細については、Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。

高可用性 のシステム要件

この項では、高可用性 コンフィギュレーションにある Firewall Threat Defense デバイスのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

高可用性コンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。 さらに、コンテナ インスタンスでは、同じリソース プロファイル属性を使用する必要があります。

  Firepower 9300 の場合、高可用性は同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。

  ハイアベイラビリティペアを Firewall Management Center に追加した後にリソースプロファイルを変更する場合は、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[システム（System）]** > **[インベントリ（Inventory）]**ダイアログボックスで各ユニットのインベントリを更新します。

  両方のユニットでプロファイルを同じにする必要がある確立されたハイアベイラビリティペアのインスタンスに異なるプロファイルを割り当てる場合、次の手順を実行する必要があります。

  1. ハイ アベイラビリティを解除します。
  2. 両方のユニットに新しいプロファイルを割り当てます。
  3. ハイアベイラビリティを再確立します。

- インターフェイスの数とタイプが同じであること。

  プラットフォーム モード では、高可用性 を有効にする前に、すべてのインターフェイスが FXOS で同一に事前構成されている必要があります。高可用性を有効にした後でインターフェイスを変更する場合は、スタンバイユニットの FXOS でそのインターフェイスを変更してから、アクティブユニットで同じ変更を行います。

高可用性 コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージ ファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してくださ

い。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

高可用性コンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- 同じファイアウォール モードにあること（ルーテッドまたはトランスペアレント）。
- ソフトウェア バージョンが同じであること。
- Firewall Management Center 上で、同じドメインまたはグループに入っていること。
- 同じ NTP コンフィギュレーションであること。脅威に対する防御のための NTP 時刻同期の設定を参照してください。
- 非コミットの変更で、Firewall Management Center 上で完全に展開していること。
- どのインターフェイスでも、DHCP または PPPoE は変更していないこと。
- （Firepower 4100/9300）同じフローオフロードモードを使用し、両方とも有効または無効になっている。

高可用性ペアでの Firewall Threat Defense デバイスのライセンス要件

高可用性構成の両方の Firewall Threat Defense ユニットは、ライセンスが同じである必要があります。

高可用性構成には 2 つのライセンス資格（ペアの各デバイスに 1 つずつ）が必要です。

高可用性を確立する前に、どのライセンスがセカンダリ/スタンバイデバイスに割り当てられているかどうかは問題にはなりません。高可用性の設定中に、Firewall Management Center はスタンバイユニットに割り当てられている不要なライセンスをすべて削除し、プライマリ/アクティブユニットに割り当てられているのと同じライセンスで置き換えます。たとえば、アクティブユニットに Essentials ライセンスと IPS ライセンスが割り当てられており、スタンバイユニットに Essentials ライセンスのみが割り当てられている場合、Firewall Management Center は Cisco Smart Software Manager と通信して、アカウントからスタンバイユニット用に使用可能な IPS ラインセンスを取得します。ライセンスアカウントで十分な数の資格が購入されていなければ、正しい数のライセンスを購入するまで、アカウントは非準拠の状態になります。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。シスコでは、フェールオーバー リンクまたはステートフル フェールオーバー リンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス（eth0）を使用します。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータインターフェイス（物理、または EtherChannel）はいずれもフェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。サブインターフェイスを使用することもできませんマルチインスタンスモードのシャーシで定義されたサブインターフェイスを除きます。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。

Firewall Threat Defense は、ユーザー データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバーリンクやデータのために使用することもできません（マルチインスタンスシャーシのサブインターフェイスのみ）。フェールオーバーリンクに対してシャーシのサブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと親自体のフェールオーバーリンクとしての使用が制限されます。

（注） フェールオーバーまたはステートリンクとして EtherChannel を使用している場合、ハイアベイラビリティを確立する前に、両方のデバイスで同じメンバインターフェイスを備えた同じ EtherChannel が存在していることを確認する必要があります。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- Firepower 4100/9300：フェールオーバー リンクに管理タイプのインターフェイスを使用することはできません。
- リンクのサイジングについては、次のガイドラインを参照してください。

表 *23 :* フェールオーバー リンクのサイズ

モデル	結合フェールオーバー リンクとステート リンクのインターフェイス サイズ
Firepower 1010	1 Gbps
Firepower 1100	1 Gbps
Firepower 2100	1 Gbps
Cisco Secure Firewall 3100	Cisco Secure Firewall 3105：1 Gbps Cisco Secure Firewall 3110：1 Gbps Cisco Secure Firewall 3120：1 Gbps Cisco Secure Firewall 3130：10 Gbps Cisco Secure Firewall 3140：10 Gbps
Firepower 4100	10 Gbps
Firepower 9300	10 Gbps

交替頻度は、ユニットのホールド時間と同じです。

（注） 設定が大きく、ユニットのホールド時間が短い場合、メンバーインターフェイスを交互に切り替えると、セカンダリユニットの参加/再参加を防止できます。この場合、セカンダリユニットが参加するまで、メンバーインターフェイスの 1 つを無効にします。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- Firewall Threat Defense デバイスのフェールオーバーインターフェイスと同じネットワークセグメント（ブロードキャストドメインまたは VLAN）に他のデバイスのないスイッチを使用する。
- イーサネット ケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因に

なったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。ただし、大規模な構成とトラフィックの多いネットワークを使用する場合は、ステート リンクとフェールオーバー リンクに専用のインターフェイスを使用することを検討する必要があります。

ステートフル フェールオーバー リンク専用のインターフェイス

ステートリンク専用のデータインターフェイス（物理、またはEtherChannel）を使用できます。専用のステートリンクの要件についてはフェールオーバー リンクのインターフェイス （286 ページ）、ステートリンクの接続についてはフェールオーバー リンクの接続 （287 ページ）を参照してください。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンしている場合、フェールオーバー動作は、フェールオーバー リンクが正常化するまで停止されます。

耐障害性のあるフェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

単一のスイッチまたはスイッチ セットが 2 つの Firewall Threat Defense デバイス間のフェールオーバーインターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたは Inter-Switch Link（ISL）がダウンすると、両方の Firewall Threat Defense デバイスがアクティブになります。したがって、次の図で示されている 2 つの接続方式は推奨**しません**。

図 *94 :* 単一のスイッチを使用した接続 ◆◆◆ 非推奨

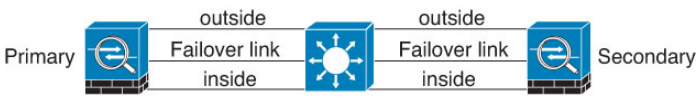
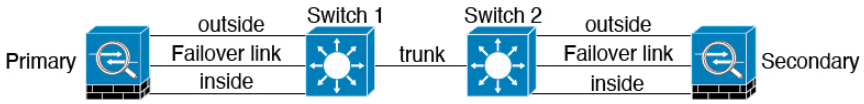


図 *95 : 2* つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、異なるスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *96 :* 異なるスイッチを使用した接続

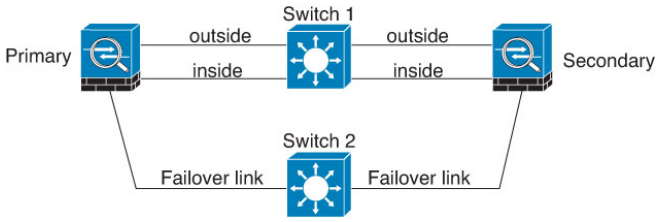
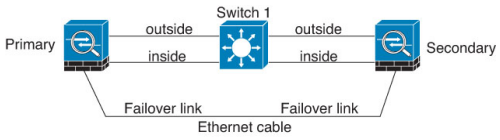


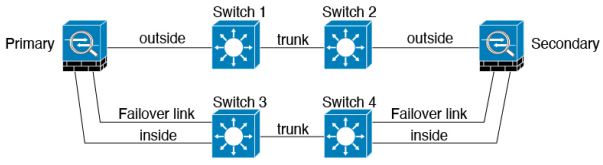
図 *97 :* ケーブルを使用した接続



シナリオ 3：推奨

Firewall Threat Defense データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *98 :* セキュアなスイッチを使用した接続



高可用性 の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上にアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。通常、フェールオーバーが発生すると、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワークデバイスは、MAC と IP アドレスのペアリングの変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注） 推奨されてはいますが、スタンバイアドレスは必須ではありません。スタンバイ IP アドレスがなければ、アクティブ装置はネットワーク テストを実行してスタンバイ インターフェイスの状態を確認することはできません。できることはリンク ステートの追跡のみです。また、管理目的でそのインターフェイス上のスタンバイ装置に接続することもできません。

ステートリンクのIPアドレスおよびMACアドレスは、フェールオーバー時に変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ 高可用性 の場合、フェールオーバーイベント中の IP アドレスと MAC アドレスの使用方法については、次を参照してください。

1. アクティブ装置は常に、プライマリ装置のIPアドレスとMACアドレスを使用します。
2. アクティブ装置がフェールオーバーすると、スタンバイ装置は障害が発生した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
3. 障害が発生した装置がオンライン状態に戻ると、スタンバイ状態になり、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずに起動した場合、プライマリ装置のMAC アドレスを認識していないため、セカンダリ装置がアクティブ装置になり、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。このため、ネットワーク トラフィックが中断することがあります。同様に、新しいハードウェアでプライマリ装置をスワップ アウトすると新しい MAC アドレスが使用されます。

高可用性を無効にし、フェールオーバー設定を無効状態に設定した場合は、高可用性を手動で再開するか、デバイスを再起動する必要があります。デバイスを再起動するのではなく、コマンド **configure high-availability resume** を使用して高可用性を再開することをお勧めします。フェールオーバー設定が無効なスタンバイ装置をリロードすると、スタンバイ装置はアクティブ装置として起動し、プライマリ装置の IP アドレスと MAC アドレスを使用します。これにより、IP アドレスが重複し、ネットワークトラフィックが中断されます。**configure high-availability resume** コマンドを使用してフェールオーバーを有効にし、トラフィックフローを復元します。

（注） スタンドアロンデバイスでフェールオーバーを有効にすると、データインターフェイスがフェールオーバーのネゴシエーション状態でダウンし、トラフィックが中断されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。セカンダリ装置がプライマリ装置より先にオンラインになった場合でも、セカンダリ装置がアクティブ装置であるときに正しい MAC アドレスを使用するように、プライマリ装置とセカンダリ装置の両方で仮想MACアドレスを設定することをお勧めします。仮想MAC アドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの

ARPテーブルをクリアする必要がある場合があります。MACアドレスが変わった場合、Firewall Threat Defense デバイスはスタティックNATアドレスに対してGratuitous ARPを送信しません。そのため、接続されたルータはこれらのアドレスのMACアドレス変更を認識できません。

仮想 MAC アドレス

Firewall Threat Defense デバイス には仮想 MAC アドレスを設定する複数の方法があります。1 つの方法だけ使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合、使用される MAC アドレスは多くの変数によって決まるため、予測できないことがあります。

マルチインスタンス機能の場合、FXOS シャーシはすべてのインターフェイスに対してプライマリ MAC アドレスのみ自動生成します。プライマリおよびセカンダリ MAC アドレスの両方で、生成された MAC アドレスを仮想 MAC アドレスで上書きすることができますが、セカンダリ MAC アドレスを事前に定義することは必須ではありません。セカンダリ MAC アドレスを設定すると、セカンダリ装置のハードウェアが新しい場合に、to-the-box 管理トラフィックが中断されないようになります。

フェールオーバーでの MAC アドレス テーブルの更新

フェールオーバー時、新しいアクティブ デバイスとして指定されたデバイスは、MAC テーブル内の各 MAC アドレス エントリに対してマルチキャスト パケットを生成し、それをすべてのブリッジグループインターフェイスに送信します。このアクションにより、ブリッジグループ内の上流スイッチは、新しいアクティブデバイスのインターフェイスでルーティングテーブルを更新し、正確なトラフィック転送を保証します。

マルチキャストパケットの生成および上流スイッチのルーティングテーブルを更新するのにかかる時間は、MACアドレステーブルのエントリ数とブリッジ グループ インターフェイスの数によって異なります。フェールオーバーイベント中に発生した遅延に関連する統計を表示するには、コマンド **show failover statistics state-switch-delay** を使用します。

ステートフル フェールオーバー

ステートフェールオーバー中にアクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

サポートされる機能

ステートフル フェールオーバーでは、次のステート情報がスタンバイ Firewall Threat Defense デバイス に渡されます。

- NAT 変換テーブル
- TCP 接続状態と UDP 接続状態（HTTP 接続状態を含む）。その他の IP プロトコル タイプとICMPは、新しいパケットが到着すると新しいアクティブデバイスで確立されるため、アクティブ装置によって解析されません。

- Snort 接続状態、インスペクションの結果、およびピン ホールに関する情報（TCP の厳密な適用を含む）。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションおよびピン ホール。
- スタティック/ダイナミック ルーティング テーブル：ステートフル フェールオーバーは OSPF や EIGRP などのダイナミック ルーティング プロトコルに参加します。そのため、アクティブ装置上のダイナミック ルーティング プロトコルを介して学習されたルートは、スタンバイ装置のルーティング情報ベース（RIB）テーブルに保持されます。フェールオーバーイベントが発生した場合、最初はアクティブなセカンダリ装置にプライマリ装置をミラーリングするルールがあるため、パケットは通常は最小限の切断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルート エントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれます。

（注） ルートは、アクティブ装置上のリンクアップまたはリンクダウンイベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイス上に構成された DHCP サーバは DHCP クライアントにアドレスを付与する前に ping を送信してアドレスが使用されていないことを確認するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS には関係ありません。
- アクセス コントロール ポリシーの決定：トラフィックの一致（URL、URL カテゴリ、地理位置情報などを含む）、侵入検知、マルウェア、およびファイル タイプに関する決定は、フェールオーバー時に維持されます。ただし、フェールオーバー時に評価される接続には、次の注意事項があります。
  - AVC：App-ID 判定は複製されますが、検出状態は複製されません。フェールオーバーが発生する前に App-ID 判定が完了および同期していれば、同期は正常に行われます。
  - 侵入検知状態：フェールオーバーの途中でピックアップが発生すると、新しいインスペクションは完了しますが古い状態は失われます。

- ファイル マルウェア ブロッキング：フェールオーバーの前にファイルの判定結果を利用できるようにする必要があります。
- ファイル タイプの検出およびブロッキング：フェールオーバーの前にファイル タイプを特定する必要があります。元のアクティブデバイスでファイルを特定しているときにフェールオーバーが発生すると、ファイル タイプは同期されません。ファイル ポリシーでそのファイル タイプがブロックされていても、新しいアクティブ デバイスはファイルをダウンロードします。

- アイデンティティポリシーによるユーザアイデンティティの決定。ISE セッションディレクトリを介して受動的に収集されたユーザと IP アドレスのマッピングや、キャプティブポータル経由のアクティブ認証が含まれます。フェールオーバー時にアクティブに認証されるユーザは、再認証を要求されることがあります。
- ネットワーク AMP：クラウド ルックアップは各デバイスに依存していないため、通常、フェールオーバーはこの機能に影響しません。詳細：
  - 署名ルックアップ：ファイルの送信中にフェールオーバーが発生すると、ファイルイベントは生成されず、検出は行われません。
  - ファイルストレージ：ファイルの保存中にフェールオーバーが発生した場合、元のアクティブデバイスに保存されます。ファイルの保存中に元のアクティブなデバイスがダウンした場合、ファイルは保存されません。
  - ファイルの事前分類（ローカル分析）：事前分類の途中でフェールオーバーが発生すると、検出は失敗します。
  - ファイルの動的分析（クラウドへの接続）：フェールオーバーが発生すると、システムがクラウドにファイルを送信する場合があります。
  - アーカイブ ファイル サポート：分析中にフェールオーバーが発生すると、システムはファイル/アーカイブを表示できなくなります。
  - カスタムブラックリスト：フェールオーバーが発生すると、イベントは生成されません。
- セキュリティインテリジェンスの決定。ただし、フェールオーバー時に進行中の DNS ベースの決定は完了しません。
- RA VPN：リモート アクセス VPN のエンド ユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバープロセス中にパケットを失って、パケット損失から回復できない可能性があります。
- すべての接続から、確立された接続だけがスタンバイ デバイスに複製されます。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ Firewall Threat Defense デバイス に渡されません。

- GREv0 および IPv4-in-IP 以外のプレーンテキストトンネル内のセッション。トンネル内のセッションは複製されません。新しいアクティブ ノードでは、正しいポリシー ルールを照合するために既存のインスペクション判定を再利用することはできません。
- 復号された TLS/SSL 接続：復号状態は同期されず、アクティブユニットに障害が発生すると、復号された接続がリセットされます。新しいアクティブユニットへの新しい接続を確立する必要があります。復号されていない接続（つまり、TLS/SSL[復号しない（Do Not Decrypt）] ルールアクションに一致する）は影響を受けず、正しく複製されます。
- TCP ステート バイパス接続。
- マルチキャスト ルーティング。

ハイ アベイラビリティのためのブリッジ グループの要件

ブリッジ グループを使用する場合は、ハイ アベイラビリティに関して特別な考慮事項があります。

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行しているスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング状態に移行できます。ポートがブロッキング状態の間のブリッジ グループ メンバーインターフェイスでのトラフィックの損失を回避するために、次の回避策のいずれかを設定できます。

- アクセス モードのスイッチ ポート：スイッチで STP PortFast 機能を有効にします。

```
interface interface_id
  spanning-tree portfast
```

  PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは STP に参加し続けます。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- スイッチ ポートがトランク モードになっている場合、または STP PortFast を有効にできない場合は、フェールオーバー機能または STP の安定性に影響を与える、次のあまり望ましくない回避策のいずれかを使用できます。
  - ブリッジ グループおよびメンバー インターフェイスでインターフェイス モニタリングを無効にします。
  - フェールオーバー基準のインターフェイス保留時間を、ユニットがフェールオーバーする前に STP が収束できる大きな値に増やします。
  - スイッチの STP タイマーを短くして、STP がインターフェイス保留時間よりも早く収束できるようにします。

フェールオーバーのヘルス モニタリング

Firewall Threat Defenseデバイスは、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニターします。この項では、各装置の状態を判断するために、Firewall Threat Defense デバイスがテストを実行する方法について説明します。

装置のヘルス モニターリング

Firewall Threat Defense デバイスは、hello メッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、フェールオーバー リンクを含む各データインターフェイスでLANTEST メッセージを送信し、ピアが応答するかどうかを確認します。Firewall Threat Defense デバイスが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- Firewall Threat Defenseデバイスがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- Firewall Threat Defense デバイスがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- Firewall Threat Defense デバイスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイス モニタリング

ユニットは、モニター対象のインターフェイス上で 15 秒間 hello メッセージを受信しなかった場合に、インターフェイス テストを実行します。1 つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、デバイスはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）] > [フェールオーバートリガー条件（Failover Trigger Criteria）]** を参照）、さらに、アクティブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したデバイスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

インターフェイスにIPv4およびIPv6アドレスが設定されている場合、デバイスはIPv4を使用してヘルス モニタリングを実行します。インターフェイスにIPv6アドレスだけが設定されている場合、デバイスはARPではなくIPv6ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャストpingテストの場合、デバイスはIPv6全ノード アドレス（FE02::1）を使用します。

インターフェイス テスト

Firewall Threat Defenseデバイスでは、次のインターフェイス テストが使用されます。各テストの時間は約1.5秒。

1. リンクアップ/ダウンテスト：インターフェイス ステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、デバイスは障害が発生し、テストが停止したと見なします。ステータスがアップの場合、デバイスはネットワーク アクティビティを実行します。

2. ネットワーク アクティビティ テスト：ネットワークの受信アクティビティのテストです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスはARPテストを開始します。

3. ARPテスト：ARPが正しく応答するかどうかをテストします。各ユニットは、ARPテーブル内の最新のエントリのIPアドレスに対して単一のARP要求を送信します。ユニットがテスト中にARP応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。ユニットがARP応答を受信しない場合、デバイスは、ARPテーブル内の「次の」エントリのIPアドレスに対して単一のARP要求を送信します。ユニットがテスト中にARP応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスはブートストラップpingテストを開始します。

4. ブロードキャストPingテスト：ping応答が正しいかどうかをテストします。各ユニットがブロードキャストpingを送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARPテストを使用してテストが再開されます。両方の装置がARPおよびブロードキャストpingテストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

インターフェイス ステータス

モニタ対象のインターフェイスには、次のステータスがあります。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Normal (Waiting)：インターフェイスは起動していますが、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- Normal (Not-Monitored)：インターフェイスは動作中ですが、フェールオーバー プロセスによってモニタされていません。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- Link Down (Waiting)：インターフェイスまたは VLAN は管理上ダウンしており、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- Link Down (Not-Monitored)：インターフェイスまたは VLAN は管理上ダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- No Link：インターフェイスの物理リンクがダウンしています。
- No Link (Waiting)：インターフェイスの物理リンクがダウンしており、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。
- No Link (Not-Monitored)：インターフェイスの物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

フェールオーバー トリガーおよび検出タイミング

Firepower ハイアベイラビリティペアでは、次のイベントでフェールオーバーがトリガーされます。

- アクティブユニットの 50% を超える Snort インスタンスがダウンした場合
- アクティブユニットのディスク容量使用率が 90% を超えた場合
- アクティブユニットで **no failover active** コマンドが実行された場合、またはスタンバイユニットで **failover active** コマンドが実行された場合
- アクティブユニットで障害が発生したインターフェイスの数がスタンバイユニットよりも多くなった場合
- アクティブデバイスのインターフェイス障害が設定されたしきい値を超えた場合

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。デフォルト値を変更するには、フェールオーバーが発生するしきい値として、障害が発生したインターフェイスの数またはモニター対象インターフェイスの割合を設定します。アクティブデバイスでしきい値を超えると、フェールオーバーが発生します。スタンバイデバイスでしきい値を超えると、ユニットが **Fail** 状態に移行します。

デフォルトのフェールオーバー条件を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

表 *24 :*

コマンド	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	デフォルトのフェールオーバー基準を変更します。 インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 250 を設定できます。 インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

次の表に、フェールオーバー トリガー イベントと、関連する障害検出のタイミングを示します。フェールオーバーが発生した場合、フェールオーバーの理由およびその他のハイ アベイラビリティ ペアに関するさまざまな作業をメッセージ センターで表示できます。これらのしきい値は、指定した最小値と最大値の範囲内の値に設定できます。

表 *25 : Firewall Threat Defense* フェールオーバー時間

フェールオーバートリガー イベント	最小	デフォルト	最大数
アクティブユニットの電源の喪失、ハードウェアのダウン、ソフトウェアのリロードまたはクラッシュにより、モニター対象インターフェイスまたはフェールオーバーリンクでhelloメッセージを受信しなくなる。	800 ミリ秒	15 秒	45 秒
アクティブユニットインターフェイス物理リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ ユニットのインターフェイスは実行されているが、接続の問題によりインターフェイステストを行っている。	5 秒	25 秒	75 秒

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Firewall Threat Defense デバイスに引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーを設定する場合は、一つの装置をプライマリに設定し、もう一つの装置をセカンダリに設定します。設定時に、プライマリ装置のポリシーがセカンダリ装置に同期されます。この時点で、2 つの装置は、デバイスおよびポリシー設定用の単一のデバイスとして機能します。ただし、イベント、ダッシュボード、レポート、およびヘルス モニタリングについては、引き続き個別のデバイスとして表示されます。

フェールオーバーペアの2つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がスタンバイであるか、つまりどちらの IP アドレスを使用し、どちらの装置でアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリ装置の MAC アドレスは常にアクティブ IP アドレスと組み合わされます。このルールの例外は、セカンダリ装置がアクティブになり、フェールオーバー リンク経由でプライマリ装置の MAC アドレスを取得できない場合に発生します。この場合、セカンダリ装置の MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイフェールオーバーでは、フェールオーバーは装置ごとに行われます。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *26 :* フェールオーバー イベント

障害イベント	ポリシー	アクティブユニットのアクション	スタンバイユニットのアクション	注記
アクティブユニットが故障(電源またはハードウェア)	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする	モニタ対象インターフェイスまたはフェールオーバーリンクでhelloメッセージが受信されることはありません。
以前にアクティブだったユニットが復旧	フェールオーバーなし	スタンバイになる	なし	なし。
スタンバイユニットが故障(電源またはハードウェア)	フェールオーバーなし	スタンバイに故障とマークする	該当なし	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる フェールオーバーリンクに故障とマークする	アクティブになる フェールオーバーリンクに故障とマークする	スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置がアクティブになります。
ステート リンクの障害	フェールオーバーなし	なし	なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
しきい値を超えたアクティブユニットでインターフェイスに障害が発生	フェールオーバー	アクティブを障害としてマークする	アクティブになる	なし。
しきい値を超えたスタンバイユニットでインターフェイスに障害が発生	フェールオーバーなし	なし	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

設定同期の最適化

デバイスが一時停止後に再起動するか、高可用性を再開する場合、参加するデバイスは実行中の設定をクリアします。次に、アクティブデバイスが、設定全体を参加デバイスに送信して完全に同期します。アクティブデバイスの設定が大規模な場合、このプロセスには数分かかることがあります。

設定同期最適化機能により、設定ハッシュ値を交換して、参加ユニットとアクティブユニットの設定を比較できます。アクティブデバイスと参加デバイスの両方で計算されたハッシュが一致する場合、参加デバイスは完全な設定同期をスキップし、高可用性設定に再参加します。この機能により、さらに迅速なピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。

設定同期の最適化のガイドラインと制限事項

- 設定同期最適化機能は、デフォルトで有効になっています。
- Firewall Threat Defense のマルチコンテキストモードは、完全な設定同期中にコンテキストの順序を共有することによって設定同期最適化をサポートし、後続のノード再参加中にコンテキストの順序を比較できるようにします。
- パスフレーズとフェールオーバー IPsec キーを設定すると、アクティブユニットとスタンバイユニットで計算されたハッシュ値が異なるため、設定同期の最適化で効果を得られません。
- ダイナミック ACL または SNMPv3 を使用してデバイスを設定すると、設定同期最適化は効果を発揮しません。
- アクティブデバイスは、デフォルトの動作として、LAN リンクのフラッピングによって完全な設定を同期します。アクティブデバイスとスタンバイデバイス間のフェールオーバーフラッピングの間、設定同期最適化はトリガーされず、デバイスによって完全な設定同期が実行されます。
- 高可用性設定が中断やアクティブデバイスとスタンバイデバイス間のネットワーク通信の切断から復旧する際に、設定同期最適化がトリガーされます。

設定同期の監視

設定同期最適化機能が有効になっている場合、syslog メッセージが生成され、アクティブユニットと参加ユニットで計算されたハッシュ値が一致するか、一致しないか、または操作がタイムアウトになったかどうかが表示されます。また、ハッシュ要求を送信してからハッシュ応答を取得して比較するまでの経過時間も表示されます。

ハイアベイラビリティの要件と前提条件

モデルのサポート

Secure Firewall Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

高可用性 のガイドライン

モデルのサポート

- Firepower 1010：
  - 高可用性を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性は、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の 高可用性 のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLANインターフェイスはフェールオーバーによってモニタできますが、スイッチポートはモニタできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、高可用性 を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。
  - ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。
- Firepower 9300：シャーシ内ハイ アベイラビリティはサポートされません。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の Firewall Threat Defense Virtual では、レイヤ 2 接続が必要なため、高可用性 はサポートされません。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行している接続済みスイッチ ポートが、トポロジの変化を検出すると 30 ～ 50 秒間ブロッキング状態になる可能性があります。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチで STP PortFast 機能を有効にすることができます。

  interface *interface_id* **spanning-tree portfast**

  この回避策は、ルーテッド モード インターフェイスとブリッジ グループ インターフェイスの両方に接続されたスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは STP に参加し続けます。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- Firewall Threat Defense デバイス フェールオーバーペアに接続されたスイッチ上でポート セキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポート セキュリティ機能によって違反フラグが付けられた場合に発生します。

- アクティブ/スタンバイ 高可用性 と VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニターすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

- 高可用性ペアの作成中にピアデバイスのいずれかで clish を実行すると、両方のピアデバイスが不明状態になり、高可用性設定が失敗します。

- フェールオーバーの直後に、syslog メッセージの送信元アドレスが数秒間フェールオーバー インターフェイス アドレスになります。

- （フェールオーバー中に）コンバージェンスを向上させるには、どの設定やインスタンスにも関連付けられていない HA ペアのインターフェイスをシャットダウンする必要があります。

- 評価モードでフェールオーバー暗号化を設定すると、システムは暗号化に DES を使用します。エクスポート準拠アカウントを使用してデバイスを登録すると、デバイスはリブート後に AES を使用します。したがって、アップグレードのインストール後など、何らかの理由でシステムがリブートすると、ピアは通信できなくなり、両方のユニットがアクティブユニットになります。デバイスを登録するまで、暗号化を設定しないことを推奨します。評価モードで暗号化を設定する場合は、デバイスを登録する前に暗号化を削除することを推奨します。

- フェールオーバーで SNMPv3 を使用する場合、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットにレプリケートされません。ユーザーを削除して再追加し、設定を再展開して、ユーザーを新しいユニットに強制的にレプリケートする必要があります。

- デバイスは、SNMP クライアントのエンジンデータをピアと共有しません。
- 非常に多数のアクセスコントロールルールとNATルールがある場合、設定のサイズによって効率的な設定のレプリケーションが妨げられる可能性があり、その結果、スタンバイユニットがスタンバイ準備完了状態に達するまでの時間が長くなります。これは、コンソールまたは SSH セッションを介したレプリケーション中にスタンバイユニットに接続する機能にも影響を与える可能性があります。設定のレプリケーションのパフォーマンスを向上させるには、**asp rule-engine transactional-commit access-group** および **asp rule-engine transactional-commit nat** コマンドを使用して、アクセスルールと NAT の両方でトランザクションコミットを有効にします。
- スタンバイロールに移行する 高可用性 ペアのユニットは、アクティブユニットとクロックを同期します。

  例：

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- 高可用性のユニットは、クロックを動的に同期しません。同期が行われるときのイベントの例を次に示します。
  - 新しい 高可用性 ペアが作成される。
  - 高可用性 が中断されて再作成される。
  - フェールオーバーリンクを介した通信が中断され、再確立される。
  - **no failover/failover** または **configure high-availability suspend/resume**（Firewall Threat Defense）コマンドを使用して、フェールオーバーステータスが CLI で手動で変更された。
- 高可用性 を有効にすると、すべてのルートが強制的に削除され、高可用性 の進行がアクティブ状態に変わった後に再度追加されます。このフェーズ中に接続が失われる可能性があります。
- プライマリユニットを置き換える場合は、高可用性を再作成するときに、交換ユニットをセカンダリユニットとして設定し、以前のセカンダリユニットから交換ユニットに設定が複製されるようにする必要があります。交換ユニットをプライマリとして設定すると、運用中ユニットの設定が誤って上書きされます。
- Firepower 1100 および 2100 デバイスが高可用性で展開されており、それらのデバイスで何百ものインターフェイスが設定されている場合、フェールオーバー時間の遅延（秒単位）が増加する可能性があります。

- 高可用性 設定では、一般にポート 53 を使用する短時間の接続はすぐに閉じられ、それらの接続がアクティブからスタンバイに転送または同期されることはありません。そのため、両方の 高可用性 デバイスの接続数に違いが生じる可能性があります。これは、短時間の接続の予期される動作です。長時間（たとえば、30 ～ 60 秒を超える）の接続の比較を試みることができます。
- 高可用性 設定では、初期接続（3 ウェイ ハンドシェイク プロセスがまだ完了していない接続要求）はすぐに閉じられ、アクティブデバイスとスタンバイデバイス間で同期されません。この設計により、HA システムの効率とセキュリティが確保されます。このため、両方の 高可用性 デバイスで接続数に違いが生じる可能性がありますが、これは予想されることです。
- フェールオーバー LAN リンクがバックツーバックで接続されておらず、代わりに 1 つ以上のスイッチを介して接続されている場合、中間経路内の障害によってアクティブユニットとスタンバイユニットの接続が失われ、アクティブ/スタンバイ状態の一貫性が失われる可能性があります。これは 高可用性 機能には影響しませんが、アクティブユニットとスタンバイユニット間のフェールオーバーリンク経路を確認して回復することをお勧めします。

  フェールオーバー LAN リンクがダウンしている場合、設定はピアユニットに複製されない可能性があるため、設定を展開することは推奨されません。
- Cisco Secure Firewall Threat Defense Virtual スタートアップガイド を参照し、Firewall Threat Defense Virtual のデバイス設定で高可用性を確認してください。
- トランスペアレント モードにおいて、アクティブ ユニットでホットスタンバイ ルータ（HSRP）の MAC アドレスが失われるという問題が発生した場合は、MAC アドレスのスタティック マッピングを作成します。
- 脅威防御デバイス が高可用性の場合、UCAPL または CC コンプライアンスモードは変更できません。高可用性ペアを形成する前に、コンプライアンス モードを変更します。

ハイ アベイラビリティ ペアの追加

アクティブ/スタンバイのハイアベイラビリティペアを確立するには、一方のデバイスをプライマリ、他方をセカンダリとして指定します。Firewall Management Center は、マージした設定をペア内のデバイスに展開します。競合がある場合は、プライマリデバイスの設定が使用されます。

マルチドメイン展開では、ハイ アベイラビリティ ペアのデバイスは同じドメインに属している必要があります。

（注） フェールオーバーリンクとステートフル フェールオーバー リンクはプライベート IP スペースにあり、ハイアベイラビリティペアのピア間の通信にのみ使用されます。ハイアベイラビリティが確立された後に、選択したインターフェイスリンクと暗号化設定の変更を行うと、ハイアベイラビリティペアが壊れ、再設定が必要になります。

注意 ハイアベイラビリティペアを作成または破棄すると、プライマリデバイスとセカンダリデバイスで Snort プロセスがただちに再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。ハイアベイラビリティペアの作成を続けると、プライマリデバイスとセカンダリデバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

始める前に

以下の点について両方のデバイスを確認してください。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。
- ドメインおよびグループが同じであること。
- 通常のヘルス ステータスであり、同じソフトウェアを実行していること。
- ルーティングされているか、またはトランスペアレント モードであること。
- 同じ NTP コンフィギュレーションであること。時刻の同期（890 ページ）を参照してください。
- 未確定の変更がない状態で、完全に展開されていること。
- すべてのインターフェイスで DHCP または PPPoE が設定されていないこと。

（注） プライマリデバイスで利用可能な証明書がセカンダリデバイスに存在しない場合は、2 台の Firewall Threat Defense デバイス間でハイアベイラビリティを構成することができます。ハイアベイラビリティが構成されると、証明書がセカンダリデバイス上で同期されます。

手順

ステップ 1 デバイスの追加 （34 ページ） に従って、両方のデバイスを Firewall Management Center に追加します。

ステップ 2 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

ステップ 3 [追加（Add）] ドロップダウンメニューから、[高可用性（High Availability）] を選択します。

ステップ 4 ハイアベイラビリティペアの表示用の [名前（Name）] を入力してください。

ステップ 5 [デバイス タイプ（Device Type）] では、[Firepower Threat Defense] を選択します。

ステップ 6 ハイアベイラビリティペアの [プライマリピア（Primary Peer）] デバイスを選択します。

ステップ 7 ハイアベイラビリティペアの [セカンダリピア（Secondary Peer）] デバイスを選択します。

ステップ 8 [続行（Continue）] をクリックします。

ステップ 9 [LANフェールオーバーリンク（LAN Failover Link）] では、フェールオーバーの通信のための十分な帯域幅の [インターフェイス（Interface）] を選択します。

（注）
論理名がなくセキュリティゾーンに属さないインターフェイスのみが、[ハイアベイラビリティペアの追加（Add High Availability Pair）] ダイアログの [インターフェイス（Interface）] ドロップダウンに一覧表示されます。

ステップ 10 識別するための任意の [論理名（Logical Name）] を入力します。

ステップ 11 アクティブなユニットの、フェールオーバー リンクの [プライマリ IP（Primary IP）] アドレスを指定します。

このアドレスは、未使用のサブネット上になければなりません。このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254 または /31）にすることができます。

（注）
169.254.1.0/24 や fd00:0:0:*::/64 は内部で使用されるサブネットです。フェールオーバーやステートリンクには使用できません。

ステップ 12 必要に応じて、[IPv6 アドレスを使用（Use IPv6 Address）] を選択します。

ステップ 13 スタンバイ ユニットのフェールオーバー リンクの [セカンダリ IP（Secondary IP）] アドレスを指定します。この IP アドレスはプライマリ IP アドレスのように、同じサブネット内になければなりません。

ステップ 14 IPv4 アドレスを使用する場合、プライマリとセカンダリの IP アドレス両方に適用されるサブネットマスクを入力します。

ステップ 15 必要に応じて、[ステートフルフェールオーバーリンク（Stateful Failover Link）] では、同じ**インターフェイス**を選択するか、または別のインターフェイスを選択し、ハイアベイラビリティの設定情報を入力します。

このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254 または /31）にすることができます。

（注）
169.254.1.0/24 や fd00:0:0:*::/64 は内部で使用されるサブネットです。フェールオーバーやステートリンクには使用できません。

ステップ 16 必要に応じて、フェールオーバー リンク間の IPsec 暗号化について、[有効（Enabled）] を選択し、さらに [キー生成（key generate）] メソッドを選択します。

ステップ 17 [OK] をクリックします。システム データの同期が行われるため、このプロセスが完了するまでに数分かかります。

次のタスク

デバイスをバックアップします。バックアップを使用することで、障害が発生したデバイスを迅速に交換し、Firewall Management Center からリンク解除せずにハイ アベイラビリティ サービスを復旧できます。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

オプションの高可用性パラメータの設定

最初の高可用性構成を Firewall Management Center で確認できます。高可用性ペアを解除して再設定しないと、これらの設定を編集することはできません。

フェールオーバーの結果を改善するために、フェールオーバー トリガー条件を編集できます。インターフェイス モニタリングでは、どのインタフェースがフェイルオーバーに適しているかを判断できます。

スタンバイ IP アドレスとインターフェイス モニタリングの設定

各インターフェイスにスタンバイ IP アドレスを設定します。推奨されてはいますが、スタンバイアドレスは必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。

デフォルトでは、論理名が設定されているすべての物理インターフェイス、Firepower 1010、のすべての VLAN インターフェイスでモニタリングが有効になっています。重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。 インターフェイス モニタリングの場合、Firepower 1010 スイッチポートが対象です。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [High Availability] タブをクリックします

ステップ 4 [モニタ対象インターフェイス（Monitored Interfaces）] エリアで、編集するインターフェイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 5 [このインターフェイスの障害をモニタする（Monitor this interface for failures）] チェック ボックスをオンにします。

ステップ 6 [IPv4] タブで、[スタンバイIPアドレス（Standby IP Address）] を入力します。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリー アドレスである必要があります。

ステップ 7 IPv6 アドレスを手動で設定した場合、[IPv6] タブでアクティブ IP アドレスの横にある [編集（Edit）]（✎） をクリックして、[スタンバイIPアドレス（Standby IP Address）] を入力し、[OK] をクリックします。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリー アドレスである必要があります。自動生成 [EUI 64の適用（Enforce EUI 64）] アドレスの場合、スタンバイ アドレスは自動的に生成されます。

ステップ 8 **[OK]** をクリックします。

ハイ アベイラビリティ フェールオーバー条件の編集

ネットワーク配置に基づいてフェールオーバー条件をカスタマイズできます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [ハイアベイラビリティ（High Availability）] を選択します。

ステップ 4 [フェールオーバートリガー条件（Failover Trigger Criteria）] の横にある [編集（Edit）]（✎） をクリックします。

ステップ 5 [インターフェイス障害しきい値（Interface Failure Threshold）] で、デバイスがフェールオーバーする条件となるインターフェイスの失敗の数または割合を選択します。

ステップ 6 [helloパケット間隔（Hello packet Intervals）] で、フェールオーバー リンクを介して送信される hello パケットの頻度を選択します。

（注）

Firepower 2100 でリモートアクセス VPN を使用する場合は、デフォルトの hello パケット間隔を使用します。使用しない場合は、CPU 使用率が高くなる場合があり、フェールオーバーを発生させる可能性があります。

ステップ 7 **[OK]** をクリックします。

仮想 MAC アドレスを設定します。

フェールオーバーのため、Secure Firewall Management Center で以下の方法を使用して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定できます。

- インターフェイスの設定中に、[インターフェイスの編集（Edit Interface）] ページの [詳細（Advanced）] タブ。MAC アドレスの設定 （749 ページ） を参照してください。
- [高可用性（High Availability）] ページからアクセスする [インターフェイスMACアドレスの追加（Add Interface MAC Address）] ダイアログボックス。この手順を参照してください。

（注） （MAC アドレスが両方の高可用性ユニットへのすべてのサブインターフェイスに転送されるように）プライマリユニットとセカンダリユニットの両方で MAC アドレスを設定する場合に推奨されるアプローチは、[インターフェイス（Interfaces）] タブを使用して、アクティブおよびスタンバイの両方の高可用性ユニットのサブインターフェイスに MAC アドレスを複製することです。

両方の場所でアクティブ MAC アドレスとスタンバイ MAC アドレスを設定した場合、フェイルオーバーではインターフェイス設定で定義されたアドレスが優先されます。

物理インターフェイスにアクティブ MAC アドレスとスタンバイ MAC アドレスを指定することでフェールオーバー中のトラフィック喪失を最低に抑えることができます。この機能は、フェールオーバーのための IP アドレスのマッピングに冗長性を提供します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある [編集（Edit）]（ ） をクリックします。

ステップ 3 [ハイ アベイラビリティ（High Availability）] をクリックします。

ステップ 4 インターフェイス MAC アドレスの横にある [追加（Add）] ( ) アイコンを選択します。

ステップ 5 [物理インターフェイス（Physical Interface）] を選択します。

ステップ 6 [アクティブインターフェイスMACアドレス（Active Interface Mac Address）] を入力します。

ステップ 7 [スタンバイインターフェイスMACアドレス（Standby Interface Mac Address）] を入力します。

ステップ 8 [OK] をクリックします。

（注）
詳細については、「Firepower アプライアンスでの FTD 高可用性の設定」の タスク 2、手順 10 ～ 14 を参照してください。

。

高可用性 の管理

この項では、高可用性 の設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、高可用性 を有効化した後に 高可用性 装置を管理する方法について説明します。

Firewall Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替え

Firewall Threat Defense ハイアベイラビリティペアを確立した後、アクティブユニットとスタンバイユニットを手動で切り替えることができます。そうすることで、現在のアクティブユニットにおける持続的な障害やヘルスイベントなどに起因するフェールオーバーを効果的に実施できます。この手順を実行する前に、両方のユニットを完全に展開しておく必要があります。

始める前に

単一の Firewall Threat Defense 高可用性ペアのノードステータスの更新 （312 ページ）。これにより、Firewall Threat Defense ハイ アベイラビリティ デバイス ペアのステータスと Firewall Management Center のステータスが同期されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 アクティブピアを変更するハイアベイラビリティペアの横にある [アクティブピアの切り替え（Switch Active Peer）] をクリックします。

ステップ 3 次の操作を実行できます。

- ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

- キャンセルして[デバイス管理（Device Management）]ページに戻る場合は、[いいえ（No）]をクリックします。

単一の Firewall Threat Defense 高可用性ペアのノードステータスの更新

Firewall Threat Defense 高可用性ペアのアクティブデバイスまたはスタンバイデバイスが再起動されると、いずれのデバイスについても、Firewall Management Center に正確な高可用性ステータスが表示されない場合があります。これは、デバイスが再起動すると、高可用性ステータスがデバイス上でただちに更新され、対応するイベントが Firewall Management Center に送信されるためです。ただし、デバイスと Firewall Management Center 間の通信がまだ確立されていないため、ステータスが Firewall Management Center で更新されないことがあります。

Firewall Management Center とデバイスの間で通信障害が発生したり、通信チャネルが不安定になったりすると、データの同期が失われる可能性があります。ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスを切り替えると、かなりの時間が経過しても変更が Firewall Management Center に反映されないことがあります。

これらのシナリオでは、ハイ アベイラビリティ ノードのステータスを更新して、ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスに関する正確な情報を取得できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 ノードステータスを更新するハイアベイラビリティペアの横にある [HA ノードのステータス更新（Refresh HA Node Status）] をクリックします。

ステップ 3 [はい（Yes）] をクリックすると、ノードのステータスが更新されます。

ハイ アベイラビリティの中断と再開

高可用性ペアの 1 つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状況で、フェールオーバーリンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイ ユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。

高可用性を中断する場合、現在アクティブなデバイスはアクティブなままで、すべてのユーザー接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の擬似-スタンバイ デバイスにフェールオーバーされることはなくなります。

高可用性の中断と高可用性の無効化の主な違いは、中断された高可用性デバイスでは高可用性設定が保持されることです。高可用性を無効化すると、設定は消去されます。そのため、中断されたシステムで高可用性を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバーペアとして再び機能します。

高可用性を中断するには、**configure high-availability suspend** コマンドを使用します。

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

アクティブ装置から高可用性を中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置のインターフェイス設定も消去されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

フェールオーバーを再開するには、**configure high-availability resume** コマンドを使用します。

```
> configure high-availability resume
Successfully resumed high-availablity.
```

ユニットが中断状態の場合にのみ、ユニットを再開できます。ユニットは、ピアユニットとアクティブ/スタンバイ ステータスをネゴシエートします。

（注） ハイ アベイラビリティの中断は一時的な状態です。ユニットをリロードすると、ハイ アベイラビリティ設定が自動的に再開され、ピアとアクティブ/スタンバイ ステータスがネゴシエートされます。

Firewall Threat Defense ハイアベイラビリティペアでのユニット交換

バックアップファイルを使用して Firewall Threat Defense 高可用性ペアの障害が発生したユニットを交換するには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Restoring Firewall Management Centers and Managed Devices*」を参照してください。

障害が発生したデバイスのバックアップがない場合は、ハイアベイラビリティを解除する必要があります。その後に、交換用デバイスを Secure Firewall Management Center に登録し、ハイアベイラビリティを再確立します。このプロセスは、デバイスがプライマリかセカンダリかによって異なります。

- バックアップなしでのプライマリ Firewall Threat Defense HA ユニットの交換（314 ページ）
- バックアップなしでのセカンダリ Firewall Threat Defense HA ユニットの交換（315 ページ）

バックアップなしでのプライマリ Firewall Threat Defense HA ユニットの交換

次に示す手順に従って、Firewall Threat Defense の高可用性ペアで障害が発生したプライマリユニットを交換します。ここに示した手順に従わないと、既存の高可用性設定を上書きする可能性があります。

注意 Firewall Threat Defense の高可用性ペアを作成または分断すると、プライマリおよびセカンダリデバイスの Snort プロセスがすぐに再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

注意 ディスクのイメージを再作成せずに、センサーまたは Firewall Management Center から別のデバイスにディスクを移動しないでください。これはサポートされていない構成であり、機能が損なわれる可能性があります。

手順

ステップ 1 [強制切断（Force Break）] を選択して、高可用性ペアを分離します。高可用性ペアの解除（315 ページ）を参照してください。

（注）
切断操作により、Firewall Threat Defense と Firewall Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。

ステップ 2 障害が発生したプライマリ Firewall Threat Defense デバイスの登録を Firewall Management Center から解除します。「Firewall Management Center からのデバイスの削除（登録解除）（39 ページ）」を参照してください。

ステップ 3 交換用の Firewall Threat Defense を Firewall Management Center に登録します。「デバイスの追加（34 ページ）」を参照してください。

ステップ 4 登録時には、既存のセカンダリ/アクティブ ユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。ハイ アベイラビリティ ペアの追加（305 ページ）を参照してください。

バックアップなしでのセカンダリ Firewall Threat Defense HA ユニットの交換

次に示す手順に従って、Firewall Threat Defense の高可用性ペアで障害が発生したセカンダリユニットを交換します。

注意 Firewall Threat Defense の高可用性ペアを作成または分断すると、プライマリおよびセカンダリデバイスの Snort プロセスがすぐに再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

手順

ステップ 1 [強制切断（Force Break）] を選択して、高可用性ペアを分離します。高可用性ペアの解除（315 ページ）を参照してください。

（注）
切断操作により、Firewall Threat Defense と Firewall Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。

ステップ 2 セカンダリ Firewall Threat Defense デバイスの登録を Firewall Management Center から解除します。「Firewall Management Center からのデバイスの削除（登録解除） （39 ページ）」を参照してください。

ステップ 3 交換用の Firewall Threat Defense を Firewall Management Center に登録します。「デバイスの追加 （34 ページ）」を参照してください。

ステップ 4 登録時には、既存のプライマリ/アクティブ ユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。ハイ アベイラビリティ ペアの追加 （305 ページ）を参照してください。

高可用性ペアの解除

高可用性ペアを解除すると、高可用性設定が両方のユニットから削除されます。

アクティブユニットは稼働状態を維持し、トラフィックを転送します。スタンバイユニットのインターフェイス設定は消去されます。

解除操作の前にアクティブユニットに展開されていなかったポリシーは、解除操作が完了しても引き続き展開されないままになります。解除操作が完了した後に、スタンドアロンデバイスにポリシーを展開してください。

（注）

- Firewall Threat Defense デバイスの高可用性インターフェイスで IPsec が有効になっている場合、デバイスは、暗号化されたパケットを優先順位の高い受信キューに入れることができません。その結果、大量のデータトラフィックのシナリオでは、デバイスが多数の暗号化された接続を効率的に管理および優先順位付けできないため、高可用性を解除しようとしても失敗する可能性があります。デバイスのリソース使用率と最大スループットを表示するには、`show resource usage` コマンドを使用します。
- Firewall Management Center を使用して高可用性ペアに到達できない場合、手動で高可用性を解除するには、各デバイスの CLI に接続し、**configure high-availability disable** を入力します。削除（登録解除）高可用性ペアのと新しい Firewall Management Center への登録（317 ページ）も参照してください。

注意 Firewall Threat Defense の高可用性ペアを解除すると、プライマリユニットとセカンダリユニットの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。

始める前に

- 単一の Firewall Threat Defense 高可用性ペアのノードステータスの更新（312 ページ）。これにより、高可用性ペアのステータスと Firewall Management Center のステータスが同期されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 解除する高可用性ペアの横にある [HAの解除（Break HA）] をクリックします。

ステップ 3 スタンバイピアが応答しない場合は、[強制解除（Force Break）] をオンにします。

ステップ 4 [はい（Yes）] をクリックします。

解除操作によって、アクティブおよびスタンバイユニットから高可用性設定が削除されます。

アクティブユニットに展開されている FlexConfig ポリシーでは、高可用性解除操作後に展開の失敗が表示される場合があります。FlexConfig ポリシーを変更してアクティブユニット上に再展開する必要があります。

次のタスク

アクティブユニット上で FlexConfig ポリシーを使用している場合は、FlexConfig ポリシーを変更して再展開して展開エラーを解消します。

（注） 高可用性を解除した後も、アクティブユニットとして動作していた Firewall Threat Defense デバイスには、スタンバイユニットの IP アドレスが設定されたままになります。これを解決するには、以前アクティブであった Firewall Threat Defense デバイスで追加の展開を実行し、スタンバイユニットの IP アドレスを設定から削除します。

削除（登録解除）高可用性ペアのと新しい Firewall Management Center への登録

Firewall Management Center からペアを登録解除できます。その場合、高可用性ペアはそのまま維持されます。ペアを新しい Firewall Management Center に登録する場合または Firewall Management Center がペアに到達できなくなった場合は、ペアを登録解除できます。

高可用性ペアを登録解除すると、次のようになります。

- Firewall Management Center とペアとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからペアが削除されます。
- ペアのプラットフォーム設定ポリシーで、NTP を使用して Firewall Management Center から時間を受信するように設定されている場合は、ペアがローカル時間管理に戻されます。
- 設定はそのままになるため、ペアはトラフィックの処理を続行します。

  NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Firewall Management Center にペアを再登録すると、設定が削除されるため、ペアはその時点でトラフィックの処理を停止します。高可用性設定はそのまま維持されるため、ペア全体を追加できます。登録時にアクセス コントロール ポリシーを選択できますが、トラフィックを再度処理する前に、登録後に他のポリシーを再適用してから設定を展開する必要があります。

始める前に

- この手順では、プライマリユニットへの CLI アクセスが必要です。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 登録解除する高可用性ペアの横にあるを[その他（More）] クリックし、**[削除（Delete）]** を選択します。

ステップ 3 [はい（Yes）] をクリックします。デバイス高可用性ペアが登録解除されます。

ステップ 4 プライマリユニットを新しいデバイスとして追加することで、新しい（または同じ）Firewall Management Center にペアを登録できます。

a) 一方のユニットの CLI に接続して、**show failover** コマンドを入力することにより、プライマリユニットを確認します。

出力の最初の行に、このユニットがプライマリかセカンダリかが示されます。

```
> show failover
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On

[...]
```

b) プライマリユニットの CLI で、**configure manager add** コマンドを使用して新しい Firewall Management Center を特定します。Firewall Threat Defense 管理インターフェイスの CLI での変更 （72 ページ）を参照してください。

c) **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、**[追加（Add）]**> **[デバイス（Device）]** をクリックします。

プライマリユニットをデバイスとして追加するだけで、Firewall Management Center がセカンダリユニットを検出します。

高可用性のモニタリング

このセクションの手順に従うことで、高可用性のステータスをモニターできます。

フェールオーバー履歴の表示

ハイアベイラビリティの両方のデバイスに関するフェールオーバーの履歴を 1 つのビューに表示できます。履歴は古いものから順番に表示され、すべてのフェールオーバーの理由が示されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [サマリー（Summary）] を選択します。

ステップ 4 [一般（General）] で、[表示（View）]（👁）をクリックします。

ステートフル フェールオーバーの統計情報の表示

ハイ アベイラビリティ ペアのプライマリとセカンダリ デバイス両方のステートフル フェールオーバー リンク統計情報を表示できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 ステートフル フェールオーバー リンクの下にある[表示（View）]（👁）をクリックします。

ステップ 5 統計情報を表示するデバイスを選択します。

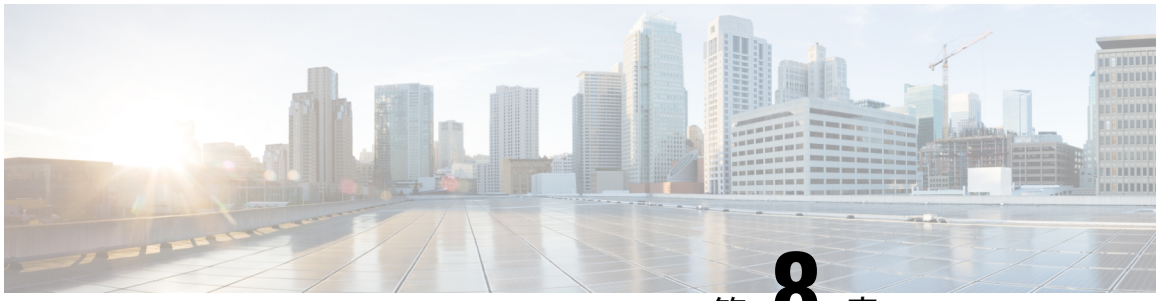
高可用性の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
高可用性ペアの登録解除により、ペアを解除せずに再登録できるようになりました。	7.3	任意（Any）	高可用性ペアを削除（登録解除）する場合、CLI でペアを手動で解除し、スタンドアロンデバイスを再登録する必要がなくなりました。プライマリユニットを新しい Firewall Management Center に追加できるようになり、スタンバイユニットが自動的に検出されます。ペアを再登録すると設定が消去されるため、ポリシーを再適用する必要があります。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ポリシーのロールバックは高可用性でサポートされています	7.2	任意（Any）	**configure policy rollback** コマンドは高可用性でサポートされています。
HA ピアリングを高速化する設定同期最適化機能	7.2	任意（Any）	設定同期最適化機能により、config-hash 値を交換して参加ユニットとアクティブユニットの設定を比較できます。アクティブユニットと参加ユニットの両方で計算されたハッシュが一致する場合、参加ユニットは完全な設定同期をスキップして HA に再参加します。この機能により、さらに迅速な HA ピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	7.1	任意（Any）	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。
高可用性グループまたはクラスタ内のルートをクリアします。	7.1	任意（Any）	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在は、高可用性グループまたはクラスタで動作している場合、このコマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループやクラスタ内のすべてのユニットのルーティングテーブルをクリアします。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細

FTD のハイアベイラビリティのハードニング	6.2.3	いずれか	バージョン 6.2.3 では、ハイアベイラビリティの FTD デバイスに関する次の機能が導入されています。
			• 高可用性ペアのアクティブまたはスタンバイ FTD デバイスが再起動されると、いずれの管理対象デバイスについても正確な高可用性ステータスが FMC に表示されない可能性があります。ただし、デバイスと FMC の間の通信がまだ確立されていないため、ステータスが FMC でアップグレードされないことがあります。[デバイス（Devices）] > [デバイス管理（Device Management）] ページの [ノードステータスの更新（Refresh Node Status）] オプションを使用すると、高可用性ユニットのステータスを更新して、高可用性ペアのアクティブデバイスとスタンバイデバイスに関する正確な情報を取得できます。
			• FMC UI の [デバイス（Devices）] > [デバイス管理（Device Management）] ページには、新しい [アクティブピアの切り替え（Switch Active Peer）] アイコンがあります。
			• バージョン 6.2.3 には、新しい REST API オブジェクト **Device High Availability Pair Services** が含まれており、次の 4 つの機能を備えています。
			  • **DELETE ftddevicehapairs**
			  • **PUT ftddevicehapairs**
			  • **POST ftddevicehapairs**
			  • **GET ftddevicehapairs**



第 8 章

における Firewall Threat Defense のクラスタの展開Cisco Secure Firewall 3100 のクラスタリング

クラスタリングを利用すると、複数の Firewall Threat Defense 装置をグループ化して 1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「クラスタリングでサポートされない機能 （374 ページ）」を参照してください。

- Cisco Secure Firewall 3100 のクラスタリングについて （323 ページ）
- クラスタリングのライセンス （325 ページ）
- クラスタリングの要件と前提条件 （325 ページ）
- クラスタリングに関するガイドライン （326 ページ）
- クラスタリングの設定 （331 ページ）
- クラスタノードの管理 （354 ページ）
- クラスタのモニタリング （366 ページ）
- クラスタリングの例 （372 ページ）
- クラスタリングの参考資料 （373 ページ）
- クラスタリングの履歴 （388 ページ）

Cisco Secure Firewall 3100 のクラスタリングについて

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは 1 つのユニットとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離された高速バックプレーン ネットワーク。クラスタ制御リンクと呼ばれます。
- 各ファイアウォールへの管理アクセス（コンフィギュレーションおよびモニタリングのため）。

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロードバランシングを、アップストリームおよびダウンストリームのルータがスパンド EtherChannel。クラスタ内の複数のメンバのインターフェイスをグループ化して 1 つの EtherChannel とします。この EtherChannel がユニット間のロードバランシングを実行します。

制御ノードとデータノードの役割

クラスタ内のメンバーの 1 つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、プライオリティ設定によって決まります。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバーはデータノードです。 最初にクラスタを作成するときに、制御ノードにするノードを指定します。これは、クラスタに追加された最初のノードであるため、制御ノードになります。

クラスタ内のすべてのノードは、同一の設定を共有します。最初に制御ノードとして指定したノードは、データノードがクラスタに参加するときにその設定を上書きします。そのため、クラスタを形成する前に制御ノードで初期設定を実行するだけで済みます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

クラスタ インターフェイス

データインターフェイスは、スパンドEtherChannel。詳細については、クラスタインターフェイスについて （331 ページ）を参照してください。

通常のファイアウォールインターフェイスまたはIPS専用インターフェイス（インラインセットまたはパッシブインターフェイス）を使用できます。

（注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。詳細については、クラスタ制御リンク （331ページ）を参照してください。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

管理ネットワーク

管理インターフェイスを使用して各ノードを管理する必要があります。クラスタリングでは、データインターフェイスからの管理はサポートされていません。

クラスタリングのライセンス

個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。

制御ノードをFirewall Management Centerに追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタを作成する前に、データノードにどのライセンスが割り当てられているのかは問題になりません。制御ノードのライセンス設定は、各データノードに複製されます。クラスタのライセンスは、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[ライセンス（License）]** エリアで変更できます。

（注） Firewall Management Centerにライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、Firewall Management Centerにライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのデータユニットがクラスタをいったん離れてから再参加することになります。

クラスタリングの要件と前提条件

モデルの要件

- Secure Firewall 3100：最大 8 ユニット

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

ハードウェアおよびソフトウェアの要件

クラスタ内のすべてのユニット：

- 同じモデルである必要があります。
- 同じインターフェイスを含めること。
- Firewall Management Center へのアクセスは管理インターフェイスから行うこと。データインターフェイスの管理はサポートされていません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレス アップグレードがサポートされます。
- ファイアウォールモードが同じであること（ルーテッドまたは透過）。
- 同じドメインに属していること。
- 同じグループに属していること。
- 保留中または進行中の展開がないこと。
- 制御ノードにサポート対象外の機能が設定されていないこと（「クラスタリングでサポートされない機能 （374 ページ）」を参照）。
- データノードに VPN が設定されていないこと。制御ノードにはサイト間 VPN を設定できます。

スイッチ要件

- クラスタリングの設定前にスイッチの設定を完了していること。クラスタ制御リンクに接続されているポートに適切な MTU 値（高い値） が設定されていること。デフォルトでは、クラスタ制御リンクの MTU は、データインターフェイスよりも 100 バイト大きく設定されています。スイッチで MTU が一致しない場合、クラスタの形成に失敗します。

クラスタリングに関するガイドライン

ファイアウォール モード

ファイアウォールモードは、すべてのユニットで一致する必要があります。

ハイ アベイラビリティ

クラスタリングでは、高可用性はサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

スイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンクインターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンクインターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。さらに、クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。
- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS XR インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタデバイス MTU は、IOS XR *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **src-dst-mixed-ip-port** を使用することをお勧めします（Cisco Nexus OS および Cisco IOS-XE の **port-channel load-balance** コマンドを参照）。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリープロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。

- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

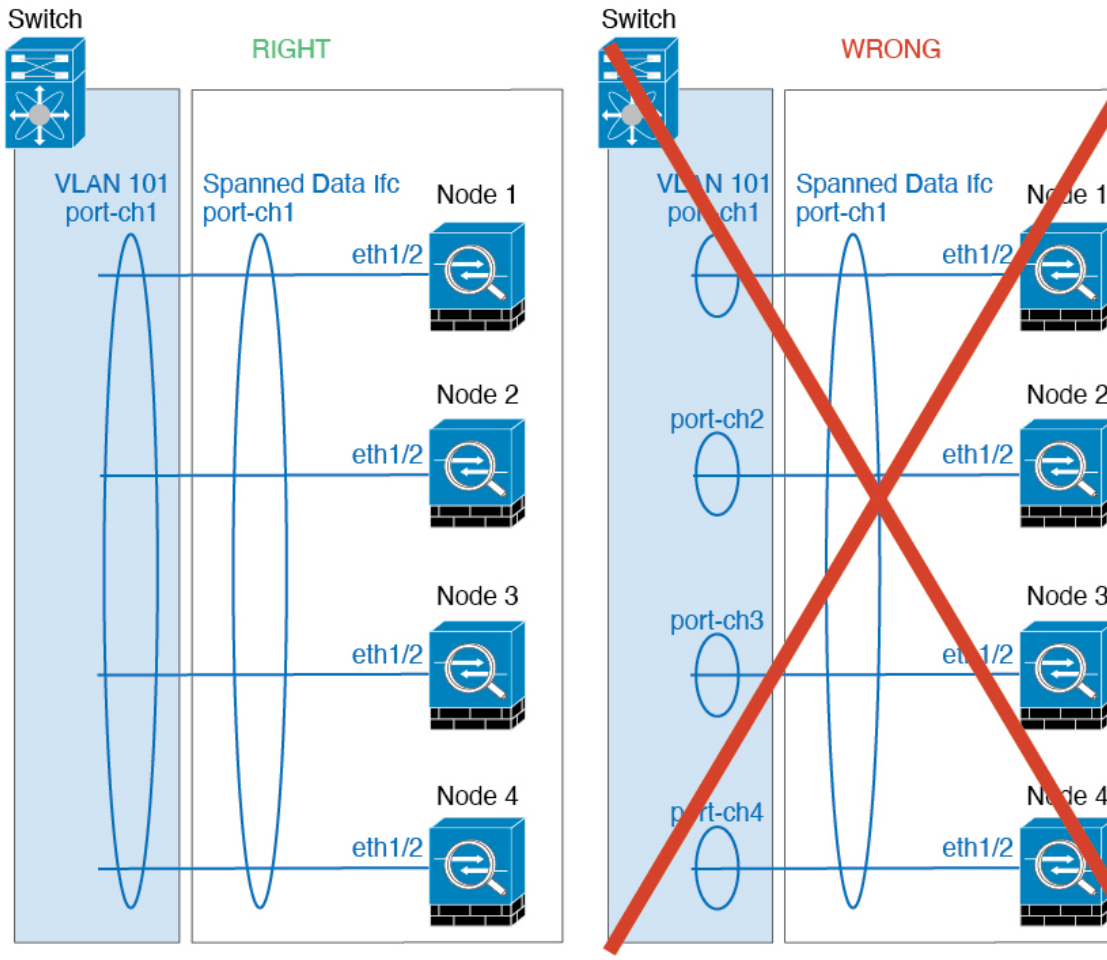
  router(config)# **port-channel** *id* **hash-distribution fixed**

  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

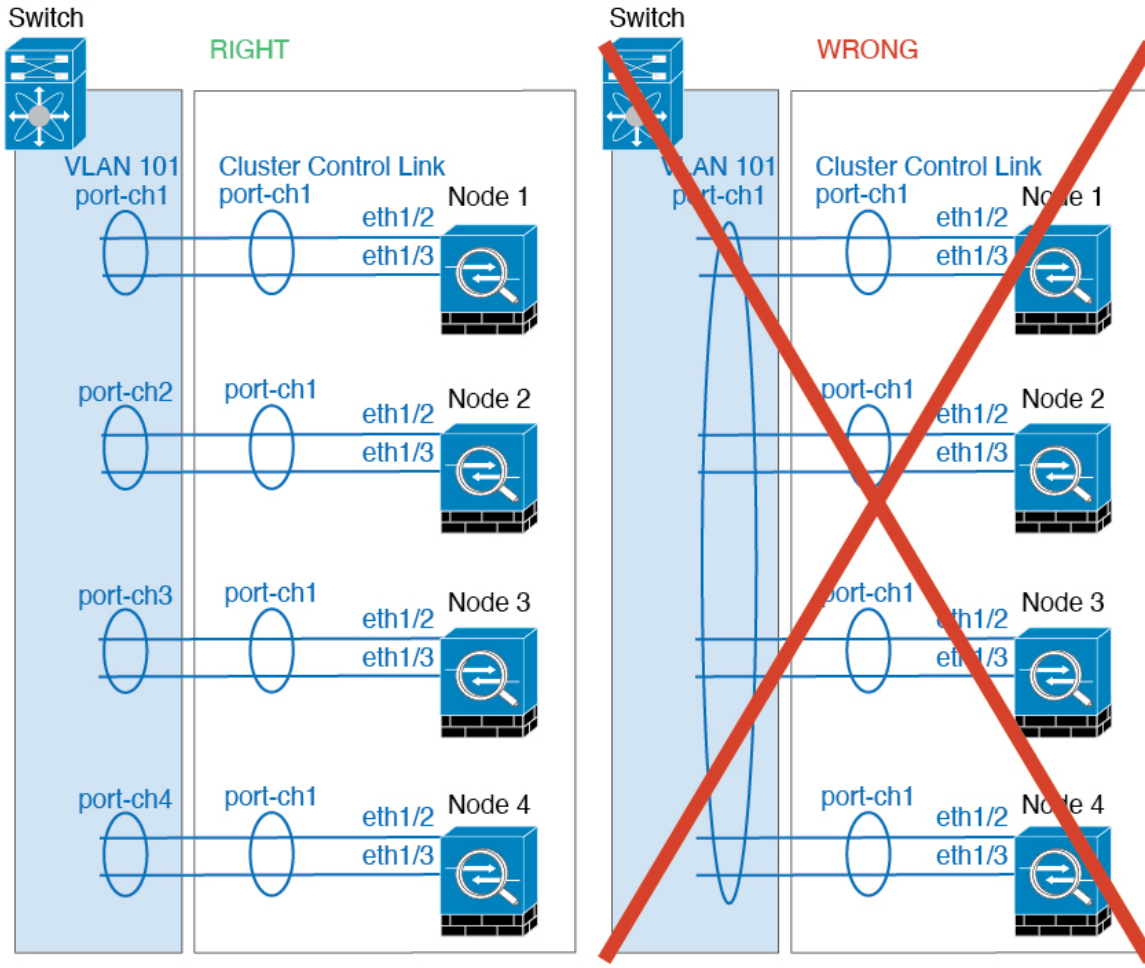
- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能を無効化する必要があります。

EtherChannel

- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



- デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



その他のガイドライン

- 重要なトポロジの変更（EtherChannel インターフェイスの追加や削除、Firewall Threat Defense またはスイッチのインターフェイスの有効化や無効化、VSS または vPC を形成するスイッチの追加など）が発生した場合は、ヘルスチェック機能を無効にし、無効になっているインターフェイスのインターフェイスモニタリングも無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバー ポートがダウンし、サーバーが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージが ASA クラスタに送信されます。このようなメッセージにより、ASA

クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。

- 復号された TLS/SSL 接続の場合、復号状態は同期されず、接続オーナーに障害が発生すると、復号された接続がリセットされます。新しいユニットへの新しい接続を確立する必要があります。復号されていない接続（復号しないルールに一致）は影響を受けず、正しく複製されます。

クラスタリングのデフォルト

- cLACP システム ID は自動生成され、システムの優先順位はデフォルトでは 1 になっています。
- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が 5 分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

クラスタリングの設定

Firewall Management Center にクラスタを追加するには、各ノードをスタンドアロンユニットとして Firewall Management Center に追加し、制御ノードにするユニットでインターフェイスを設定してからクラスタを形成します。

クラスタ インターフェイスについて

データインターフェイスは、スパンド EtherChannel など）として設定することはできません。

通常のファイアウォールインターフェイスまたは IPS 専用インターフェイス（インラインセットまたはパッシブインターフェイス）を使用できます。

また、各ユニットの、少なくとも 1 つのハードウェア インターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンク

各ユニットの、少なくとも 1 つのハードウェア インターフェイスをクラスタ制御リンク専用とする必要があります。可能な場合は、クラスタ制御リンクに EtherChannel を使用することを推奨します。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク インターフェイスとネットワーク

クラスタ制御リンクには、任意の物理インターフェイスまたはEtherChannelを使用できます。VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。管理/診断インターフェイスも使用できません。

各クラスタ制御リンクは、同じサブネット上の IP アドレスを持ちます。このサブネットは、他のすべてのトラフィックからは隔離し、クラスタ制御リンクインターフェイスだけが含まれるようにしてください。

（注） 2 メンバークラスタの場合、ノード間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。（テスト目的などで）ユニットを直接接続する必要がある場合は、クラスタを形成する前に、両方のノードでクラスタ制御リンクインターフェイスを設定して有効にする必要があります。

クラスタ制御リンクのサイジング

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。

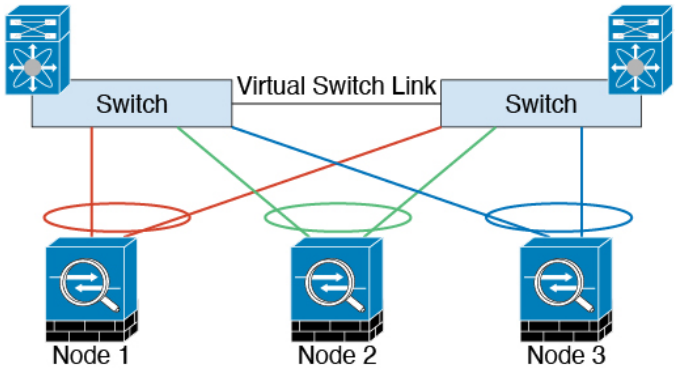
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンクの冗長性

次の図は、仮想スイッチングシステム（VSS）、仮想ポートチャネル（vPC）、StackWise、または StackWise Virtual 環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが冗長システムの一部である場合は、同じ EtherChannel 内のファイアウォールインターフェイスをそれぞれ、冗長システム内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

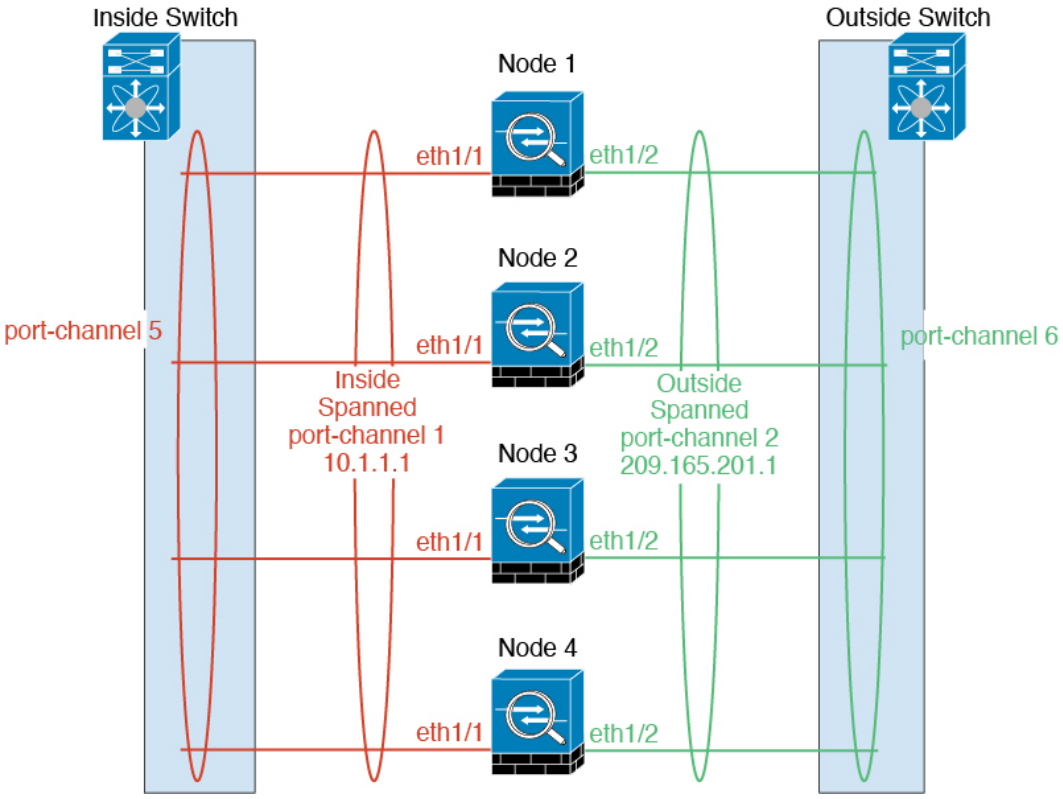
クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。

通常のファイアウォール インターフェイスの場合：スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジグループ メンバーではなく BVI に割り当てられます。

EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

- 使用するロード バランシング ハッシュ アルゴリズムは「対称」であるようにします。つまり、どちらの方向からのパケットも同じハッシュを持たせて、スパンド EtherChannel 内の同じ Firewall Threat Defense に送信します。送信元と宛先の IP アドレス（デフォルト）または送信元と宛先のポートをハッシュ アルゴリズムとして使用することを推奨します。
- Firewall Threat Defense をスイッチに接続するときは、同じタイプのラインカードを使用します。すべてのパケットに同じハッシュ アルゴリズムが適用されるようにするためです。

ロード バランシング

EtherChannel リンクは、送信元または宛先 IP アドレス、TCP ポートおよび UDP ポート番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

（注） スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのノードにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。

EtherChannel 内のリンク数はロード バランシングに影響を及ぼします。

対称ロード バランシングは常に可能とは限りません。NAT を設定する場合は、フォワード パケットとリターン パケットとで IP アドレスやポートが異なります。リターン トラフィックはハッシュに基づいて別のユニットに送信されるため、クラスタはほとんどのリターン トラフィックを正しいユニットにリダイレクトする必要があります。

EtherChannel の冗長性

EtherChannel には、冗長性機能が組み込まれています。これは、すべてのリンクの回線プロトコル ステータスをモニターします。リンクの 1 つで障害が発生すると、トラフィックは残りのリンク間で再分散されます。EtherChannel のすべてのリンクが特定のユニット上で停止したが、他方のユニットがまだアクティブである場合は、そのユニットはクラスタから削除されます。

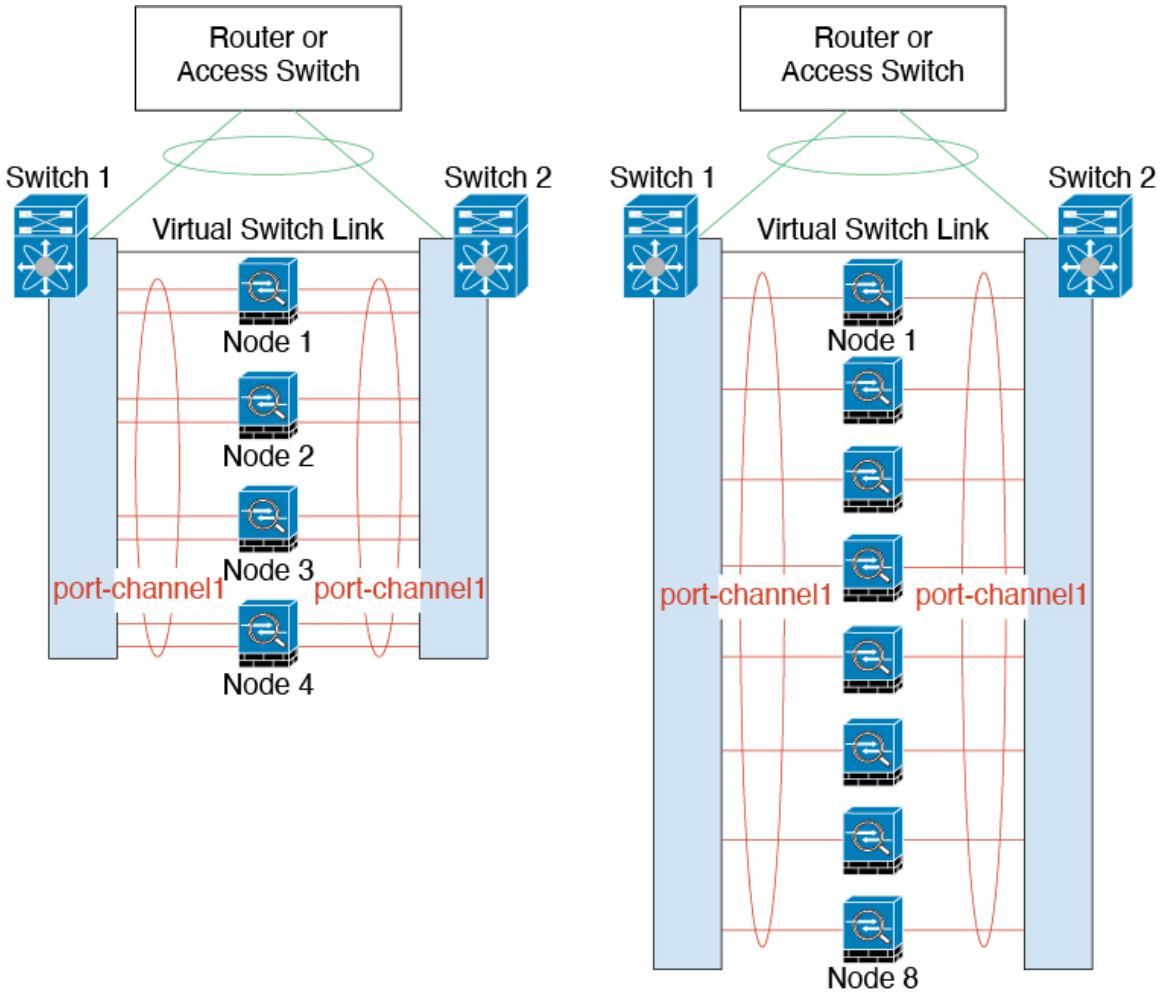
冗長スイッチシステムへの接続

1 つの Firewall Threat Defense につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの Firewall Threat Defense につき複数のインターフェイスが特に役立つのは、VSS、vPC、StackWise、または StackWise Virtual の両方のスイッチに接続するときです。

スイッチによっては、スパンド EtherChannel に最大 32 個のアクティブ リンクを設定できます。この機能では、vPC 内の両方のスイッチが、それぞれ 16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

EtherChannel で 8 個のアクティブリンクをサポートするスイッチの場合、冗長システムで 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブリンクを設定できます。

次の図では、4 ノードクラスタおよび 8 ノードクラスタでの 16 アクティブリンクのスパンド EtherChannel を示します。



Firewall Management Center へのデバイスのケーブル接続と追加

クラスタリングを設定する前に、デバイスを準備する必要があります。具体的には、すべてのノードがクラスタ制御リンクを介して通信できない限り、クラスタは起動しません。したがって、クラスタを形成する前に、クラスタ制御リンクの準備ができている必要があります。

手順

ステップ 1 クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

ステップ 2 アップストリームとダウンストリームの機器を設定します。

a) クラスタ制御リンクのネットワークに、データインターフェイスの最大 MTU より少なくとも 100 バイト高くなるように MTU を設定します。

デフォルトでは、クラスタ制御リンクの MTU は 1500 バイトです。そのため、クラスタノードのクラスタ制御リンクの MTU は 1600 バイトに設定されます。データインターフェイスにより高い MTU を使用する場合は、それに応じて接続スイッチのクラスタ制御リンクの MTU を増やしてください。

b) オプションの EtherChannel を含め、アップストリームおよびダウンストリーム機器でクラスタ制御リンクインターフェイスを設定します。

クラスタ制御リンクの要件については、「クラスタ制御リンクインターフェイスとネットワーク （332 ページ）」を参照してください。

c) スパンド EtherChannel を含むアップストリームおよびダウンストリーム機器のデータインターフェイスを設定します。

スパンド EtherChannel のケーブル接続の方法については、「クラスタ インターフェイスについて （331 ページ）」を参照してください。

ステップ 3 同じドメインおよびグループ内のスタンドアロンデバイスとして、各ノードを Firewall Management Center に追加します。

デバイスの追加 （34 ページ）を参照してください。単一のデバイスでクラスタを作成し、後からノードを追加できます。デバイスを追加したときに行った初期設定（ライセンス、アクセス コントロール ポリシー）は、制御ノードからすべてのクラスタノードに継承されます。クラスタを形成するときに制御ノードを選択します。

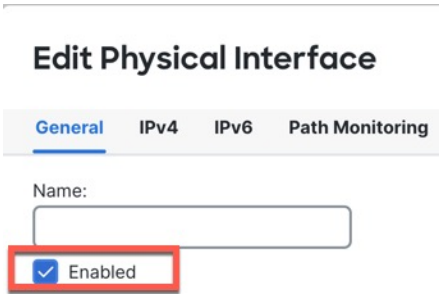
ステップ 4 制御ノードにするデバイスでクラスタ制御リンクを有効にします。

他のノードを追加すると、それらのノードはクラスタ制御リンク設定を継承します。

（注）
クラスタ制御リンクの名前、または IP アドレスを設定しないでください。クラスタの形成時に、クラスタ制御リンクインターフェイスの MTU が最も高いデータインターフェイス MTU よりも 100 バイト多い値に自動的に設定されるため、設定が必要なくなりました。ただし、クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。クラスタを追加するときに MTU がこの範囲に設定されている場合は、[インターフェイス（Interfaces）] ページに戻り、手動で 8362 よりも大きくすることをお勧めします。

a) 制御ノードにするデバイスで、[デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択し、[編集（Edit）]（ ） をクリックします。
b) [インターフェイス（Interfaces）] をクリックします。
c) インターフェイスをイネーブルにします。クラスタ制御リンクに EtherChannel を使用する場合は、すべてのメンバーをイネーブルにします。物理インターフェイスの有効化およびイーサネット設定の構成 （635 ページ）を参照してください。

図 *99* : クラスタ制御リンクインターフェイスの有効化



d) （任意） EtherChannel を追加します。 EtherChannel の設定 （644 ページ）を参照してください。

クラスタ制御リンクで不要なトラフィックを削減できるように、クラスタ制御リンクのメンバーインターフェイスに対しては On モードを使用することをお勧めします（デフォルトはアクティブモードです）。クラスタ制御リンクは LACP トラフィックのオーバーヘッドを必要としません。これは隔離された、安定したネットワークであるからです。**注**：データ EtherChannel を Active モードに設定することをお勧めします。

e) [保存（Save）] > [展開（Deploy）] の順にクリックして、インターフェイスの変更を制御ノードに展開します。

クラスタの作成

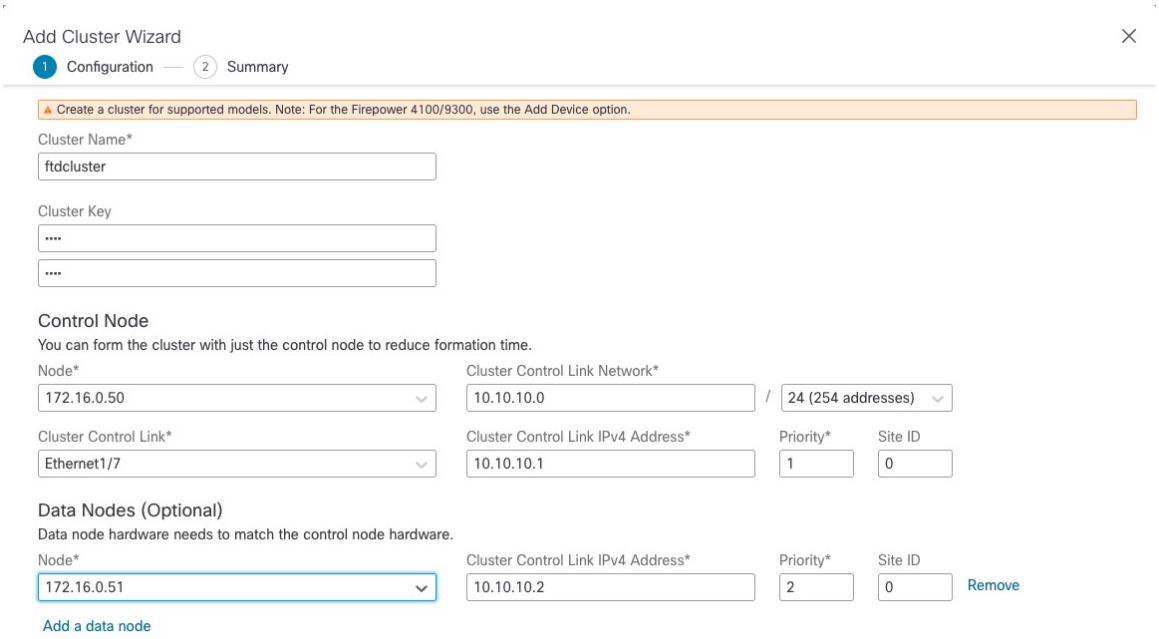
Firewall Management Center 内の 1 台以上のデバイスでクラスタを形成します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択してから、[追加（Add）] > [クラスタ（Cluster）] の順に選択します。 > >

[クラスタの追加（Add Cluster）] ウィザードが表示されます。

図 *100 : [*クラスタの追加（***Add Cluster***）*]*ウィザード



ステップ 2 制御トラフィックの [クラスタ名（Cluster Name）] と認証用の [クラスタキー（Cluster Key）] を指定します。

- [クラスタ名（Cluster Name）] : 1 ～ 38 文字の ASCII 文字列。
- [クラスタキー（Cluster Key）] : 1 ～ 63 文字の ASCII 文字列。[クラスタキー（Cluster Key）]の値は暗号キーを生成するために使用されます。この暗号は、データパストラフィック（接続状態の更新や転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。

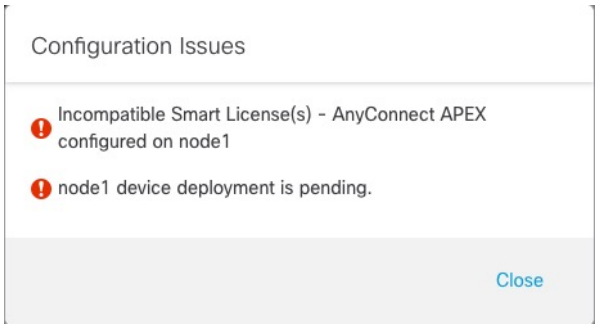
ステップ 3 [制御ノード（Control Node）] については、次のように設定します。

- [ノード（Node）] : 最初に制御ノードにするデバイスを選択します。Firewall Management Centerがクラスタを形成すると、このノードが最初にクラスタに追加されて制御ノードになります。

（注）

ノード名の横に **エラー**（） アイコンが表示されている場合は、そのアイコンをクリックして設定の問題を表示します。クラスタの形成をキャンセルし、問題を解決してからクラスタの形成に戻る必要があります。次に例を示します。

図 *101* : 設定の問題



上記の問題を解決するには、サポート対象外の VPN ライセンスを削除し、保留中の設定の変更をデバイスに展開します。

- [クラスタ制御リンクネットワーク（Cluster Control Link Network）]：IPv4 サブネットを指定します。このインターフェイスではIPv6はサポートされていません。[24]、[25]、[26]、または [27] サブネットを指定します。
- [クラスタ制御リンク（Cluster Control Link）]：クラスタ制御リンクに使用する物理インターフェイスまたは EtherChannel を選択します。

  （注）
  クラスタ制御リンクインターフェイスのMTUは、最も高いデータインターフェイスMTUよりも100バイト多い値に自動的に設定されます。デフォルトでは、MTUは1,600バイトです。クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。クラスタを追加するときに MTU がこの範囲に設定されている場合は、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** ページで MTU を 8362 よりも大きくすることをお勧めします。

  クラスタ制御リンクに接続されているスイッチの MTU を適切な値（高い値）に設定してください。そうしないと、クラスタ形成に失敗します。

- [クラスタ制御リンクIPv4アドレス（Cluster Control Link IPv4 Address）]：このフィールドには、クラスタ制御リンクネットワークの最初のアドレスが自動的に入力されます。必要に応じてホストアドレスを編集できます。
- [プライオリティ（Priority）]：制御ノードの選択に対するこのノードのプライオリティを設定します。プライオリティは1～100であり、1が最高のプライオリティです。他のノードよりプライオリティを低く設定しても、クラスタが最初に形成されたときは、このノードが引き続き制御ノードになります。
- [サイトID（Site ID）]：（FlexConfig 機能）このノードのサイト ID を 1 ～ 8 の間で入力します。値を0に設定するとサイト間クラスタリングが無効になります。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加のカスタマイズは、FlexConfig 機能を使用した場合にのみ設定できます。

ステップ 4 [データノード（Data Nodes）]（オプション）で、[データノードを追加（Add a data node）] をクリックしてクラスタにノードを追加します。

クラスタの形成を高速化するために制御ノードのみでクラスタを形成することも、すべてのノードをここで追加することも可能です。各データノードで以下を設定します。

- [ノード（Node）]：追加するデバイスを選択します。

  （注）

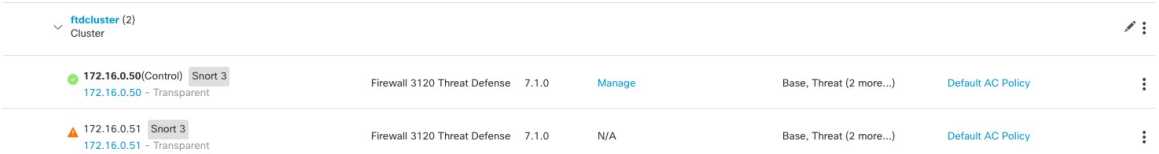
  ノード名の横に **エラー**（） アイコンが表示されている場合は、そのアイコンをクリックして設定の問題を表示します。クラスタの形成をキャンセルし、問題を解決してからクラスタの形成に戻る必要があります。

- [クラスタ制御リンクIPv4アドレス（Cluster Control Link IPv4 Address）]：このフィールドには、クラスタ制御リンクネットワークの次のアドレスが自動的に入力されます。必要に応じてホストアドレスを編集できます。
- [プライオリティ（Priority）]：制御ノードの選択に対するこのノードのプライオリティを設定します。プライオリティは 1 ～ 100 であり、1 が最高のプライオリティです。
- [サイトID（Site ID）]：（FlexConfig 機能）このノードのサイト ID を 1 ～ 8 の間で入力します。値を 0 に設定するとサイト間クラスタリングが無効になります。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加のカスタマイズは、FlexConfig 機能を使用した場合にのみ設定できます。

ステップ 5 [続行（Continue）] をクリックします。[概要（Summary）] を確認し、[保存（Save）] をクリックします。

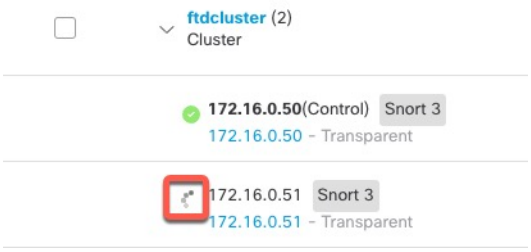
[デバイス（Devices）]>[デバイス管理（Device Management）] ページにクラスタ名が表示されます。クラスタを展開して、クラスタノードを表示します。

図 *102*：クラスタの管理

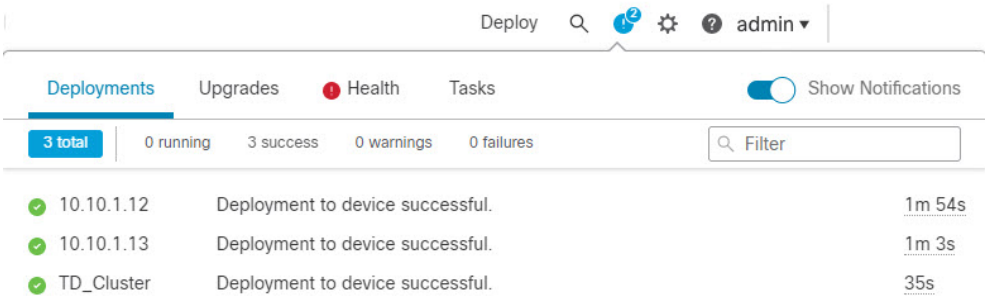


現在登録中のノードには、ロードアイコンが表示されます。

図 *103 :* ノードの登録



クラスタノードの登録をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。Firewall Management Center は、ノードの登録ごとにクラスタ登録タスクを更新します。

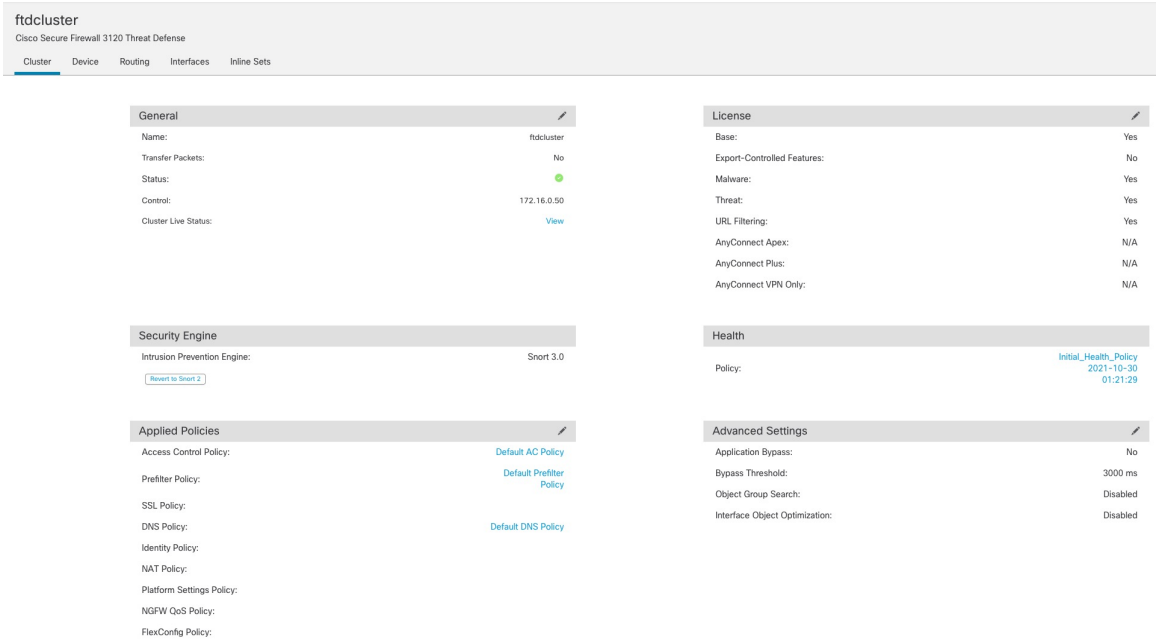


ステップ 6 クラスタの [編集（Edit）]（✎）をクリックして、デバイス固有の設定を指定します。

ほとんどの設定は、クラスタ内のノードではなく、クラスタ全体に適用できます。たとえば、ノードごとに表示名を変更できますが、インターフェイスはクラスタ全体についてのみ設定できます。

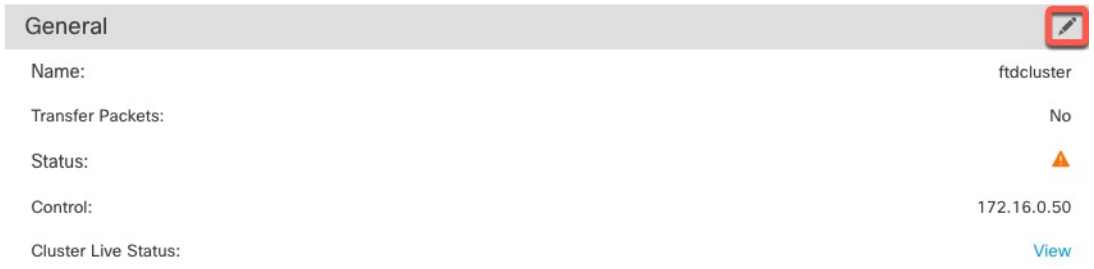
ステップ 7 [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] 画面に、クラスタの [全般（General）] などの設定が表示されます。

図 *104* : クラスタ設定

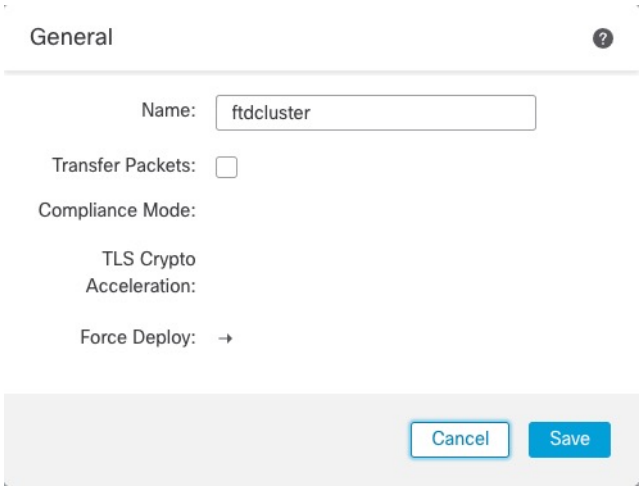


[全般（General）] 領域には、次のクラスタに固有の項目が表示されます。

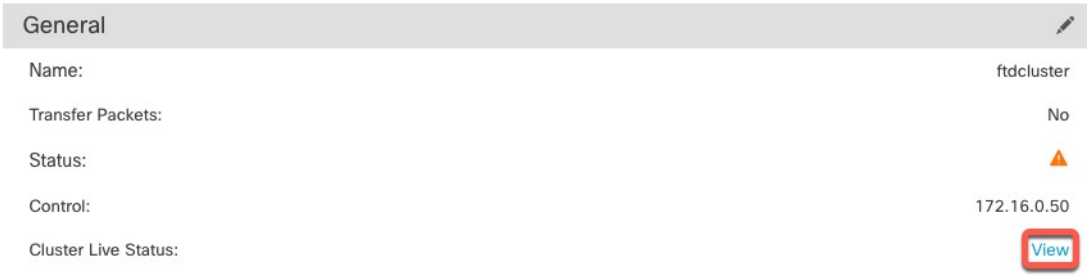
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタの表示名を変更します。



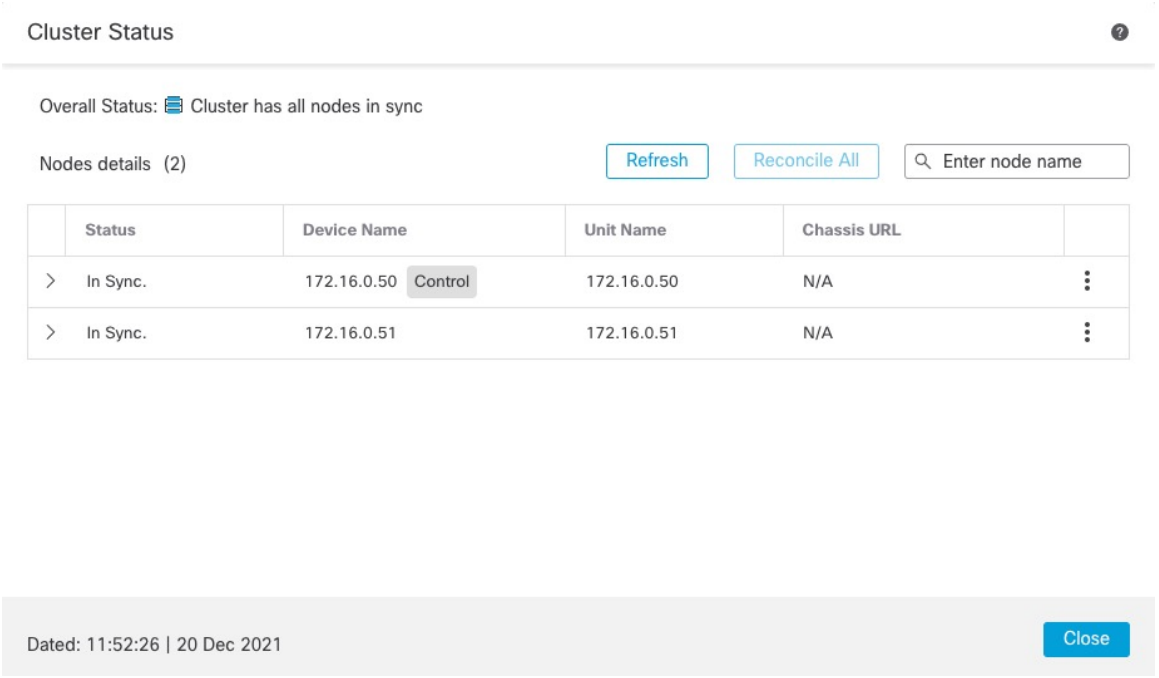
その後に、[名前（Name）] フィールドを設定します。



- [全般（General）] > [クラスタステータスの表示（View cluster status）] : [クラスタステータスの表示（View cluster status）] リンクをクリックして [クラスタステータス（Cluster Status）] ダイアログボックスを開きます。



[クラスタステータス（Cluster Status）] ダイアログボックスでは、[すべて照合（Reconcile All）] をクリックしてデータユニットの登録を再試行することもできます。



ステップ 8 **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）]** の右上のドロップダウンメニューで、クラスタ内の各メンバーを選択し、次の設定を指定することができます。

図 *105* : デバイス設定

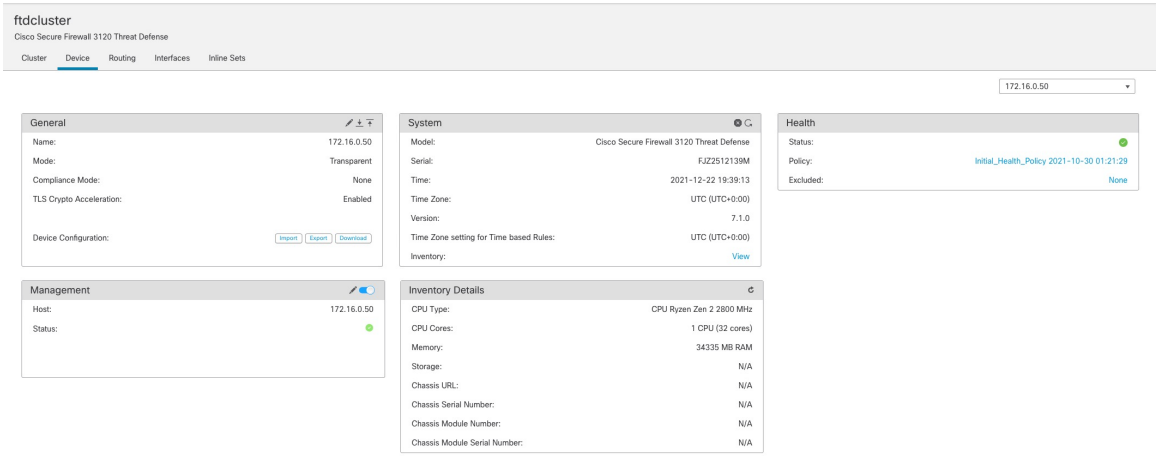
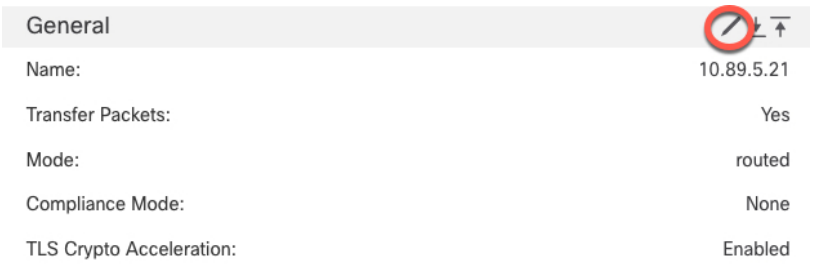
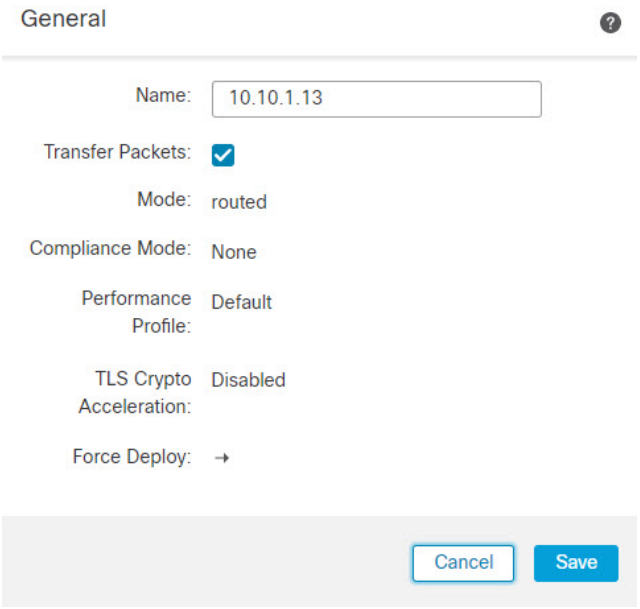


図 *106* : ノードの選択

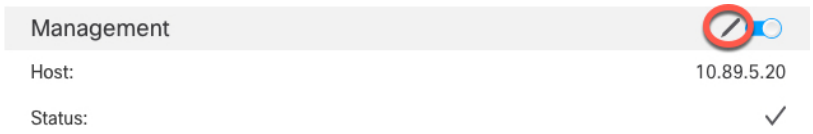
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタメンバーの表示名を変更します。



その後に、[名前（Name）] フィールドを設定します。



- [管理（Management）] > [ホスト（Host）] : デバイス設定で管理 IP アドレスを変更する場合は、Firewall Management Center で新しいアドレスを一致させてネットワーク上のデバイスに到達できるようにする必要があります。最初に接続を無効にし、[管理（Management）] 領域で [ホスト（Host）] のアドレスを編集してから、接続を再度有効にします。



インターフェイスの設定

データインターフェイスをスパンドEtherChannelとして設定します。 個別インターフェイスとして実行できる唯一のインターフェイスである診断インターフェイスを設定することもできます。

手順

ステップ1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、クラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ2 [インターフェイス（Interfaces）] をクリックします。

ステップ3 スパンド EtherChannel データインターフェイスを設定します。

a) EtherChannelは1つ以上設定します。EtherChannelの設定 （644ページ）を参照してください。

EtherChannelには1つ以上のメンバーインターフェイスを含めることができます。このEtherChannelはすべてのノードにまたがっているため、各ノードに必要なメンバーインターフェイスは1つだけです。ただし、スループットと冗長性を向上させるために、メンバーを複数にすることをお勧めします。

b) （任意） 通常のファイアウォール インターフェイスの場合は、EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。サブインターフェイスの追加 （694 ページ）を参照してください。

c) EtherChannel インターフェイスの [編集（Edit）]（✎） をクリックします。

d) 名前とその他のパラメータを設定します。通常のファイアウォールインターフェイスについては、ルーテッドモードのインターフェイスの設定（717ページ）を参照してください。また、トランスペアレントモードについては、ブリッジ グループ インターフェイスの設定（724ページ）を参照してください。IPS専用インターフェイスについては、インラインセットとパッシブインターフェイス （763 ページ）を参照してください。

- クラスタ制御リンクインターフェイスのMTUがデータインターフェイスのMTUより100バイト以上大きくない場合、データインターフェイスのMTUを減らす必要があるというエラーが表示されます。デフォルトでは、クラスタ制御リンクのMTUは1,600バイトです。データインターフェイスの MTU を増やす場合は、まずクラスタ制御リンクの MTU を増やしてください。クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されないことに注意してください。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。

- ルーテッドモードの場合、DHCP、PPPoE、IPv6 自動設定、および手動リンクローカルアドレスはサポートされません。ポイントツーポイント接続の場合、31 ビットのサブネット マスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。

e) EtherChannel に、一意の手動グローバル MAC アドレスを設定します。[詳細設定（Advanced）] をクリックし、[アクティブなMACアドレス（Active MAC Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

[スタンバイMACアドレス（Standby MAC Address）] は設定しないでください。無視されます。

潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel には、現在ネットワークで使用されていない、一意のMACアドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在の制御ユニットに留まります。MAC アドレスを設定していない場合に、制御ユニットが変更された場合、新しい制御ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

f) [OK] をクリックします。他のデータ インターフェイスについても前述の手順を繰り返します。

ステップ 4 （任意） 診断インターフェイスを設定します。

診断インターフェイスは、個別インターフェイス モードで実行できる唯一のインターフェイスです。syslog メッセージや SNMP などに、このインターフェイスを使用できます。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）]** を選択して、IPv4 または IPv6 アドレス プールを追加します。アドレス プール （1323 ページ）を参照してください。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。仮想 IP アドレスはこのプールには含まれませんが、同一ネットワーク上に存在している必要があります。各ユニットに割り当てられる正確なローカルアドレスを事前に決定することはできません。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** で、診断インターフェイスの [編集（Edit）]（✎） をクリックします。

c) [IPv4] で [IPアドレス（IP Address）] とマスクを入力します。この IP アドレスは、そのクラスタの固定アドレスで、常に現在の制御ユニットに属します。

d) 作成したアドレス プールを [IPv4 アドレス プール（IPv4 Address Pool）] ドロップダウンリストから選択します。

e) [IPv6] > [基本（Basic）] で、[IPv6アドレスプール（IPv6 Address Pool）] ドロップダウンリストから、作成したアドレスプールを選択します。

f) 通常どおり、他のインターフェイス設定を行います。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）] > [展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

クラスタのヘルスモニターの設定

[クラスタ（Cluster）]ページの[クラスタヘルスモニターの設定（Cluster Health Monitor Settings）]セクションには、次の表で説明されている設定が表示されます。

図 *107* : クラスタのヘルスモニターの設定

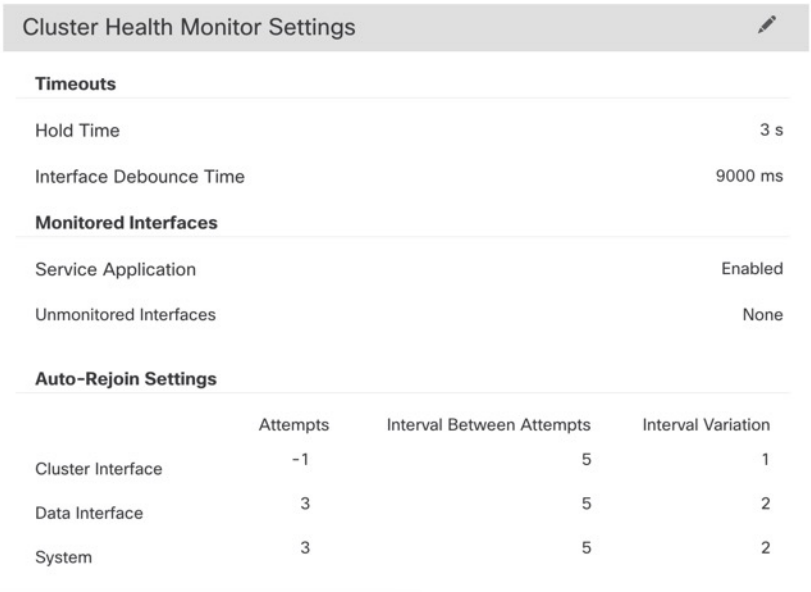


表 *27* : [クラスタヘルスモニターの設定（*Cluster Health Monitor Settings*）]セクションテーブルのフィールド

フィールド	説明
タイムアウト（Timeouts）	
保留時間（Hold Time）	指定できる範囲は0.3～45秒です。デフォルトは3秒です。ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間（Interface Debounce Time）	指定できる範囲は300～9000ミリ秒です。デフォルトは500 msです。インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると見なされ、クラスタからノードが削除されるまでの時間です。

フィールド	説明
Monitored Interfaces（モニタリング対象インターフェイス）	インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。
サービスアプリケーション（Service Application）	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。
モニタリング対象外のインターフェイス（Unmonitored Interfaces）	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定（Auto-Rejoin Settings）	
クラスタインターフェイス（Cluster Interface）	クラスタ制御リンクに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは -1（無制限）です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 1 倍です。試行ごとに間隔を長くするかどうかを定義します。
データインターフェイス（Data Interfaces）	データインターフェイスに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。
システム（System）	内部エラーが発生した後に自動再結合の設定を表示します。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。

フィールド	説明
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。

（注） システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

これらの設定は、このセクションから変更できます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI やBVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

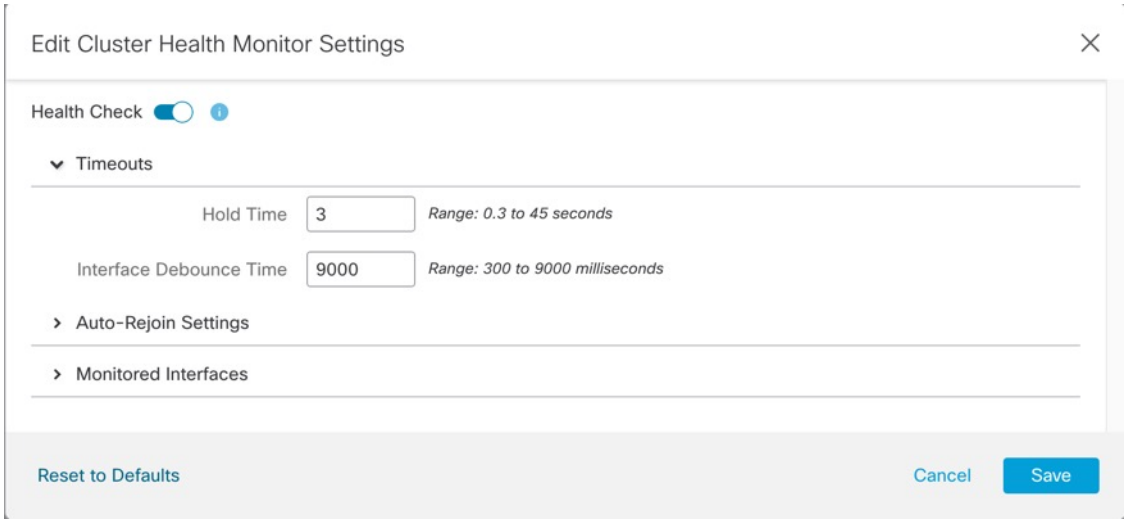
ステップ 2 変更するクラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [クラスタ（Cluster）] をクリックします。

ステップ 4 [クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）] セクションで、[編集（Edit）]（✎） をクリックします。

ステップ 5 [ヘルスチェック（Health Check）] スライダをクリックして、システムのヘルスチェックを無効にします。

図 *108 :* システムヘルスチェックの無効化



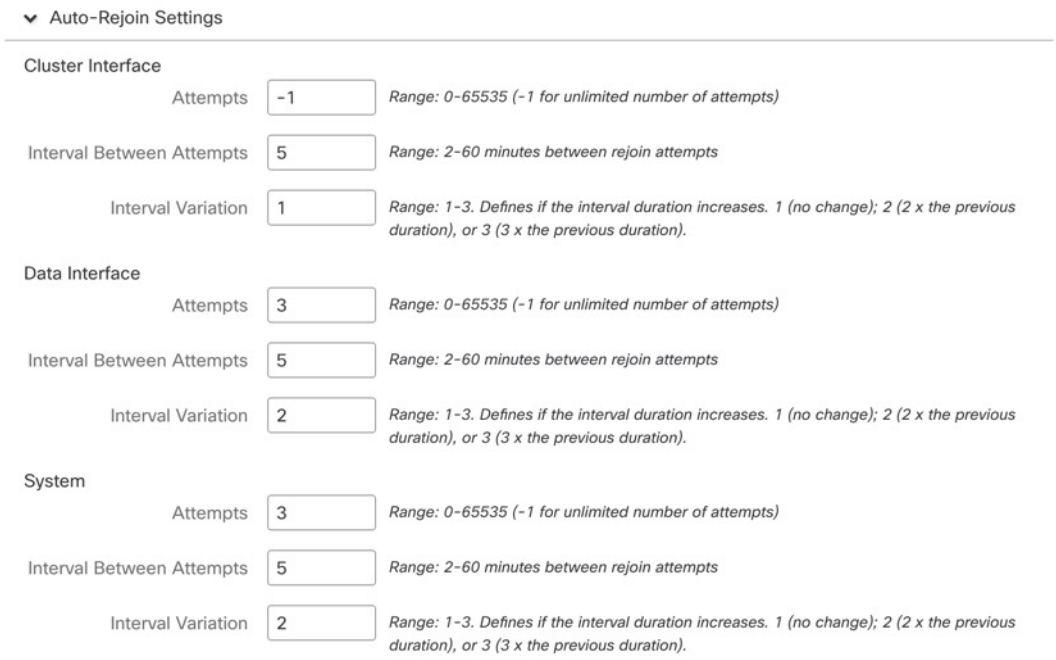
何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間（Hold Time）]：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ～ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間（Interface Debounce Time）]：デバウンス時間は 300 ～ 9000 ms の範囲で値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 *109* : 自動再結合の設定

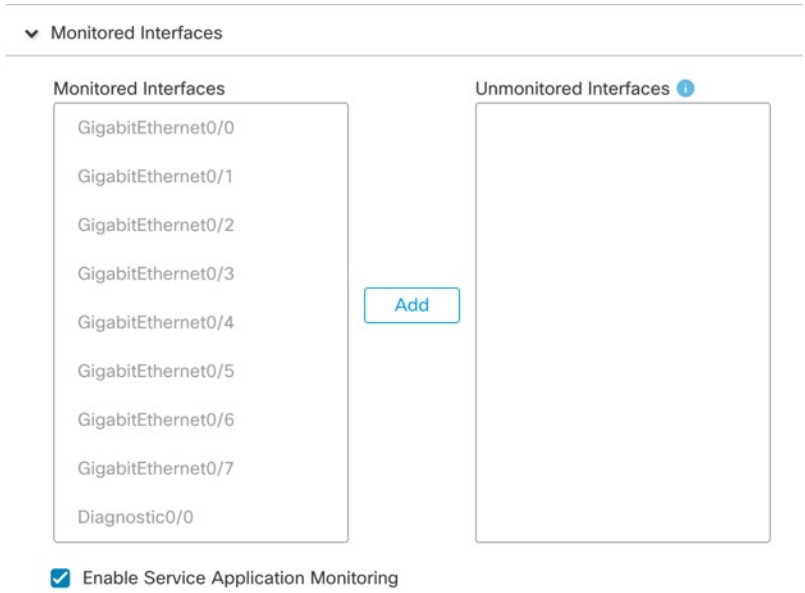


[クラスタインターフェイス（Cluster Interface）]、[データインターフェイス（Data Interface）]、および[システム（System）]に次の値を設定します（内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります）。

- [試行数（Attempts）]：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。[クラスタインターフェイス（Cluster Interface）] のデフォルト値は -1（無制限）です。[データインターフェイス（Data Interface）] と [システム（System）] のデフォルト値は 3 です。
- [試行の間隔（Interval Between Attempts）]：再結合試行の間隔を 2 ～ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [間隔のバリエーション（Interval Variation）]：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、[クラスタインターフェイス（Cluster Interface）] の場合は **1**、[データインターフェイス（Data Interface）] および [システム（System）] の場合は **2** です。

ステップ 8 [モニタリング対象のインターフェイス（Monitored Interfaces）] または [モニタリング対象外のインターフェイス（Unmonitored Interfaces）] ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリングを有効にする（Enable Service Application Monitoring）] をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 *110* : モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングを無効にできます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

クラスタノードの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタノードを管理できます。

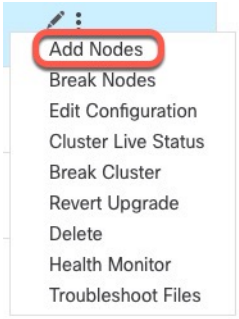
新しいクラスタノードの追加

1 つ以上の新しいクラスタノードを既存のクラスタに追加できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、クラスタの [その他（More）] (⋮) をクリックして [ノードを追加（Add Nodes）] を選択します。 >

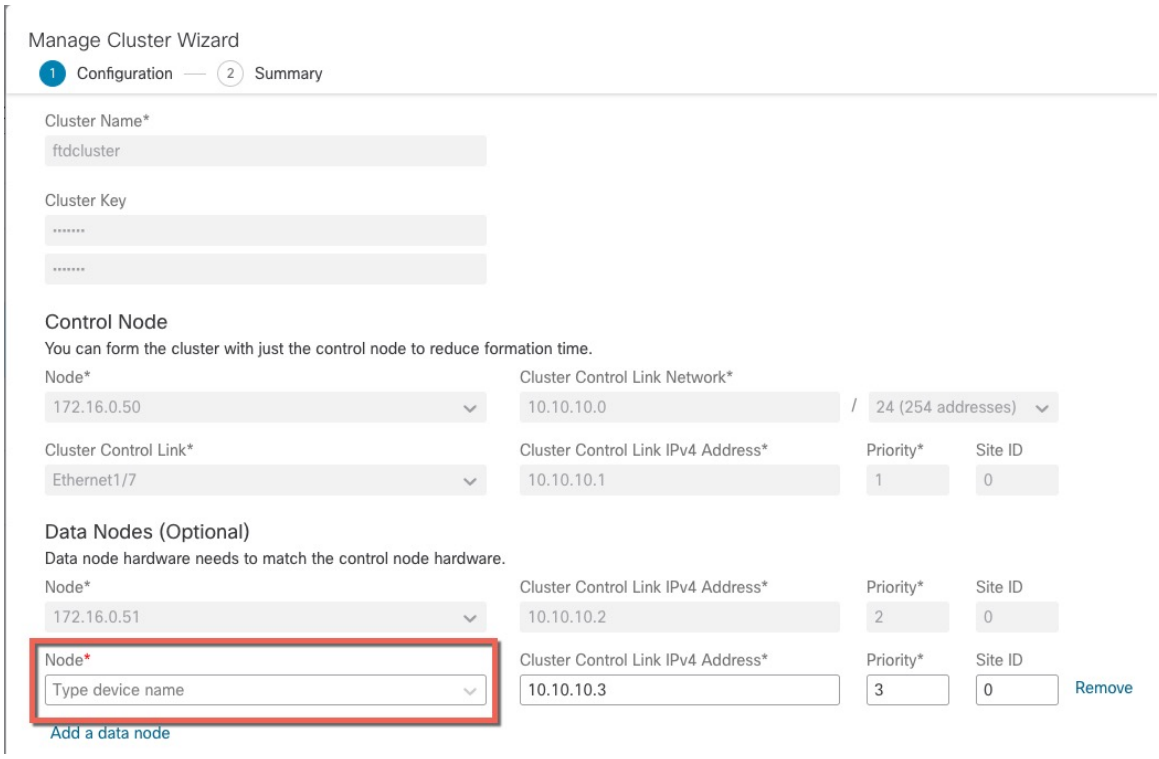
図 *111* : ノードの追加



[クラスタの管理（Manage Cluster）] ウィザードが表示されます。

ステップ 2 [ノード（Node）] メニューからデバイスを選択し、必要に応じて IP アドレス、優先順位、およびサイト ID を調整します。

図 *112 : [*クラスタの管理（***Manage Cluster***）*]*ウィザード

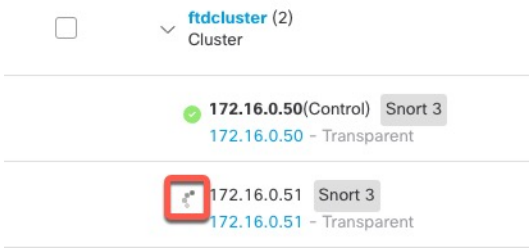


ステップ 3 さらにノードを追加するには、[データノードを追加（Add a data node）] をクリックします。

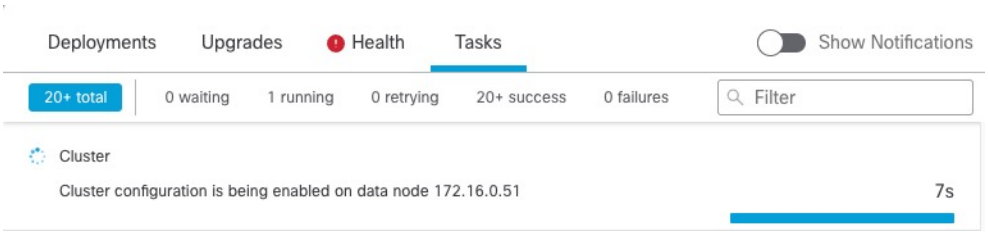
ステップ 4 [続行（Continue）] をクリックします。[概要（Summary）] を確認し、[保存（Save）] をクリックします。

現在登録されているノードには、ロードアイコンが表示されます。

図 *113 : ノードの登録*



クラスタノードの登録をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。



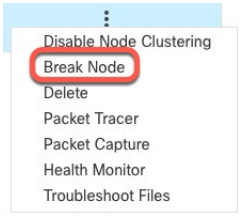
ノードの除外

ノードがスタンドアロンデバイスになるように、クラスからノードを削除できます。クラスタ全体を解除しない限り、制御ノードを除外することはできません。データノードの設定は消去されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、除外するノードの [その他（More）] (⋮) をクリックして [ノードを除外（Break Node）] を選択します。

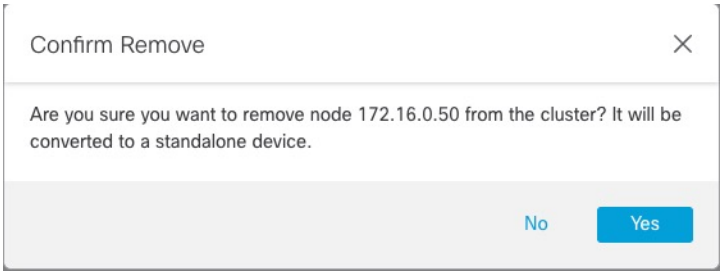
図 *114* : ノードの除外



オプションで、クラスタの [詳細（More）] メニューから [ノードを除外（Break Nodes）] を選択して 1 つ以上のノードを除外できます。

ステップ 2 除外の確定を求められたら、[はい（Yes）] をクリックします。

図 *115* : 解除の確定



クラスタノードの除外をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。

クラスタの解除

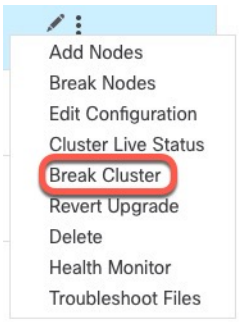
クラスタを解除し、すべてのノードをスタンドアロンデバイスに変換できます。制御ノードはインターフェイスとセキュリティポリシーの設定を保持しますが、データノードでは設定が消去されます。

手順

ステップ 1 ノードを照合することにより、すべてのクラスタノードが Firewall Management Center で管理されていることを確認します。クラスタノードの照合 （363 ページ）を参照してください。

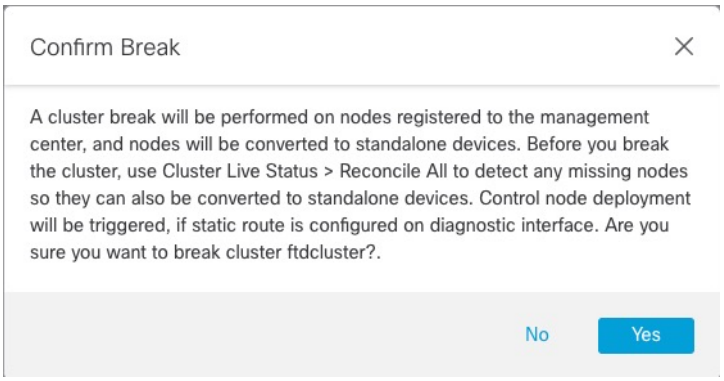
ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、クラスタの [その他（More）] (⋮) をクリックして [クラスタを解除（Break Cluster）] を選択します。

図 *116* : クラスタの解除



ステップ 3 クラスタを解除するよう求められたら、[はい（Yes）] をクリックします。

図 *117* : 解除の確定



クラスタの解除をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。

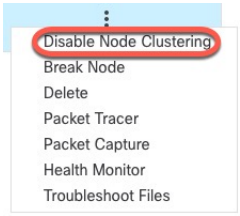
クラスタリングを無効にする

ノードの削除に備えて、またはメンテナンスのために一時的にノードを非アクティブ化する場合があります。この手順は、ノードを一時的に非アクティブ化するためのものです。ノードは引き続き Firewall Management Center のデバイスリストに表示されます。ノードが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。

手順

ステップ 1 無効にするユニットに対して、**[デバイス（Devices）]>[デバイス管理（Device Management）]** の順に選択して [その他（More）] (⋮) をクリックし、[ノードのクラスタリングを無効にする（Disable Node Clustering）] を選択します。

図 *118*: クラスタリングを無効にする



制御ノードでクラスタリングを無効にすると、データノードの 1 つが新しい制御ノードになります。なお、中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるため、新しい制御ノード上で接続を再確立する必要があります。制御ノードがクラスタ内の唯一のノードである場合、そのノードでクラスタリングを無効にすることはできません。

ステップ 2 ノードのクラスタリングを無効にすることを確認します。

ノードは、[デバイス（Devices）]>[デバイス管理（Device Management）] リストの名前の横に [（無効（Disabled））] と表示されます。

ステップ 3 クラスタリングを再び有効にするには、クラスタへの再参加（359 ページ）を参照してください。

クラスタへの再参加

（たとえば、インターフェイスで障害が発生したために）ノードがクラスタから削除された場合、または手動でクラスタリングを無効にした場合は、クラスタに手動で再参加する必要があ

ります。クラスタへの再参加を試行する前に、障害が解決されていることを確認します。ノードをクラスタから削除できる理由の詳細については、「クラスタへの再参加（382ページ）」を参照してください。

手順

ステップ1 再度有効にするユニットに対して、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択して [その他（More）] (⋮) をクリックし、[ノードのクラスタリングを有効にする（Enable Node Clustering）] を選択します。

ステップ2 ユニットでクラスタリングを有効にすることを確認します。

制御ノードの変更

⚠

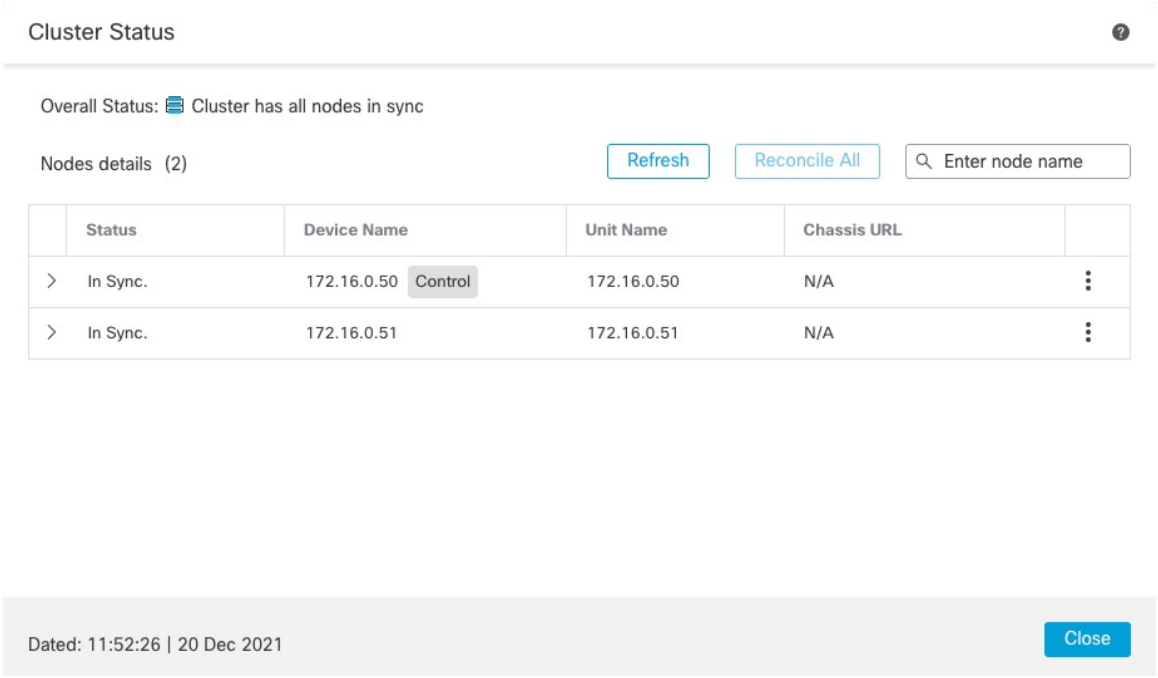
注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするユニットを厳密に指定する必要がある場合は、このセクションの手順を使用します。なお、中央集中型機能については、いずれかの方法で制御ノード変更を強制するとすべての接続がドロップされるため、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

手順

ステップ1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [その他（More）] (⋮) > [クラスタのライブステータス（Cluster Live Status）] を選択して [クラスタステータス（Cluster Status）] ダイアログボックスを開きます。

図 *119*: クラスタのステータス



ステップ 2 制御ユニットにしたいユニットについて、[その他（More）] (⋮) >[ロールを制御に変更（Change Role to Control）] を選択します。

ステップ 3 ロールの変更を確認するように求められます。チェックボックスをオンにして [OK] をクリックします。

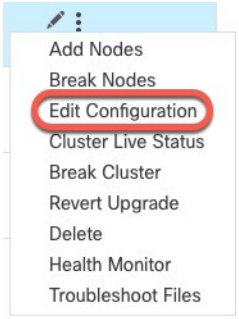
クラスタ設定の編集

クラスタ設定を編集できます。クラスタキー、クラスタ制御リンクインターフェイス、またはクラスタ制御リンクネットワークを変更すると、クラスタは自動的に解除されて再形成されます。クラスタが再形成されるまで、トラフィックの中断が発生する可能性があります。ノードのクラスタ制御リンクの IP アドレス、ノードの優先順位、またはサイト ID を変更すると、影響を受けるノードのみが除外されてクラスタに再追加されます。

手順

ステップ 1 **[デバイス（Devices）]>[デバイス管理（Device Management）]** の順に選択し、クラスタの [その他（More）] (⋮) をクリックして [設定を編集（Edit Configuration）] を選択します。

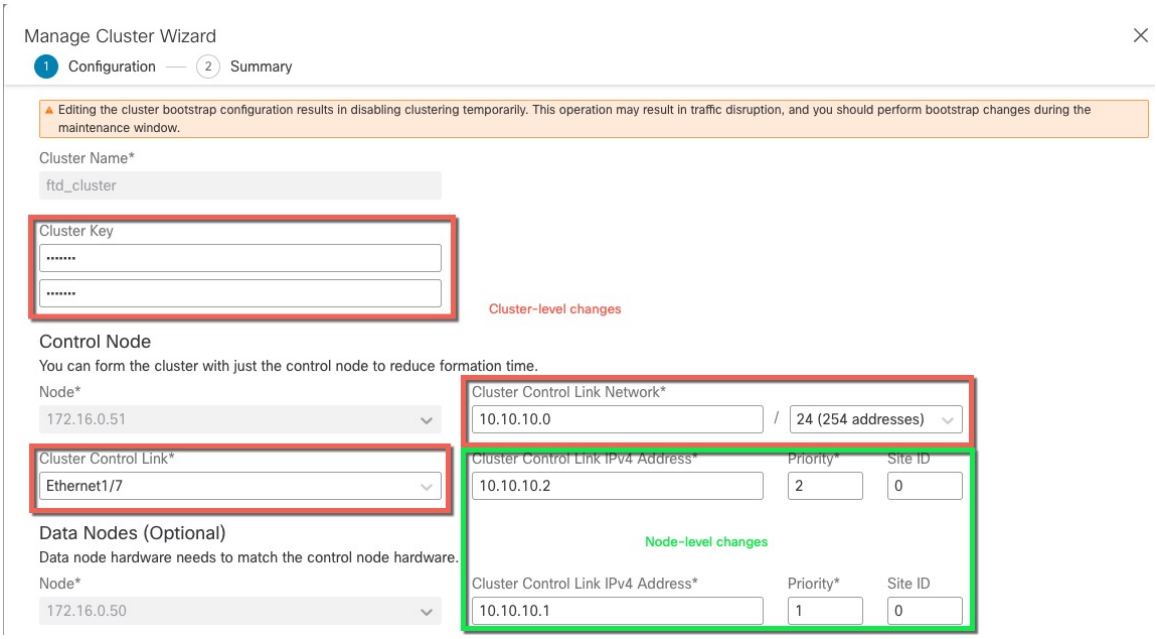
図 *120 :* 設定の編集



[クラスタの管理（Manage Cluster）] ウィザードが表示されます。

ステップ 2 クラスタ設定を更新します。

図 *121 : [*クラスタの管理（***Manage Cluster***）*]*ウィザード



クラスタ制御リンクが EtherChannel の場合、インターフェイスのドロップダウンメニューの横にある [編集（Edit）]（✎）をクリックして、インターフェイスのメンバーシップと LACP の設定を編集できます。

ステップ 3 [続行（Continue）] をクリックします。[概要（Summary）] を確認し、[保存（Save）] をクリックします。

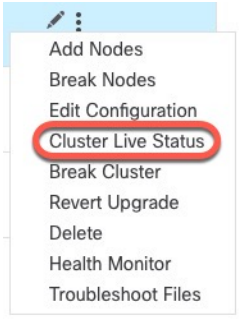
クラスタノードの照合

クラスタノードの登録に失敗した場合は、デバイスからFirewall Management Centerに対してクラスタメンバーシップを照合できます。たとえば、Firewall Management Centerが特定のプロセスで占領されているか、ネットワークに問題がある場合、データノードの登録に失敗することがあります。

手順

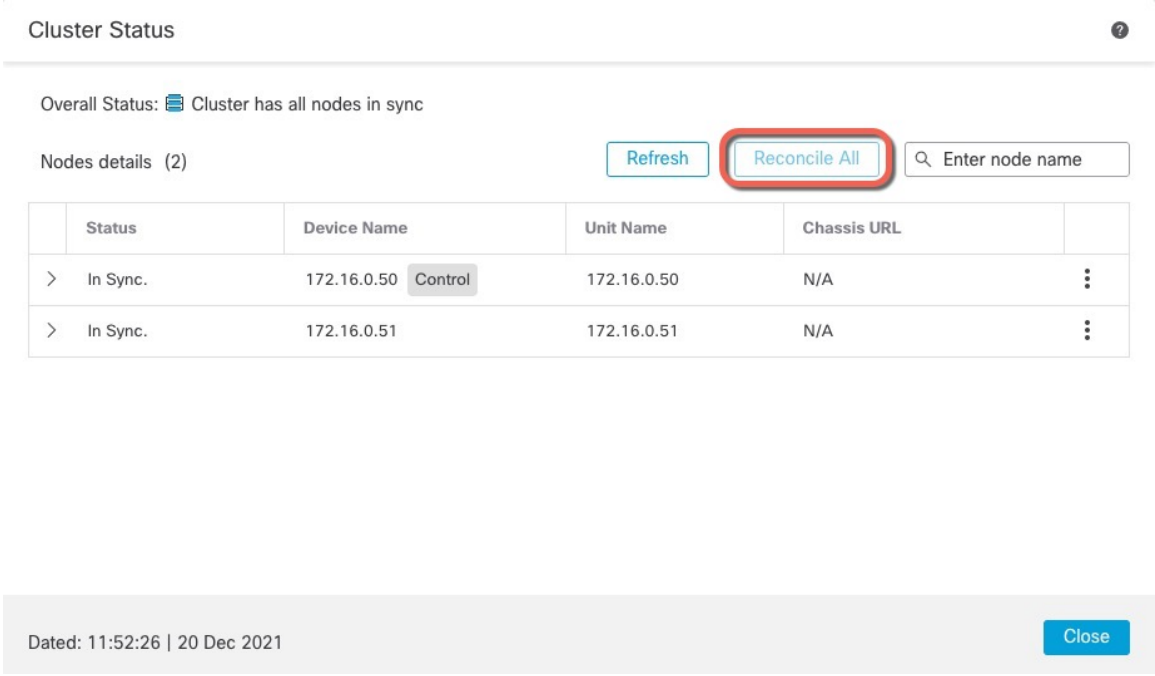
ステップ1 クラスタの **[Devices]** > **[Device Management]** > [その他（More）] (⋮) を選択し、次に [Cluster Live Status] を選択して [Cluster Status] ダイアログボックスを開きます。

図 *122*：クラスタのライブステータス



ステップ2 [すべてを照合（Reconcile All）] をクリックします。

図 *123 :* すべてを照合



クラスタ ステータスの詳細については、クラスタのモニタリング （366ページ）を参照してください。

クラスタまたはノードの削除（登録解除）と新しいFirewaManagement Center への登録

Firewall Management Center からクラスタを登録解除できます。これにより、クラスタはそのまま維持されます。クラスタを新しい Firewall Management Center に追加する場合は、クラスタを登録解除することができます。

クラスタからノードを除外することなく、Firewall Management Center からノードを登録解除することもできます。ノードは Firewall Management Center に表示されていませんが、まだクラスタの一部であり、引き続きトラフィックを渡して制御ノードになることも可能です。現在動作している制御ノードを登録解除することはできません。Firewall Management Center から到達不可能になったノードは登録解除してもかまいませんが、管理接続をトラブルシューティングする間、クラスタの一部として残しておくことも可能です。

クラスタの登録解除：

- Firewall Management Center とクラスタとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからクラスタが削除されます。

- クラスタのプラットフォーム設定ポリシーで、NTP を使用して Firewall Management Center から時間を受信するように設定されている場合は、クラスタがローカル時間管理に戻されます。
- 設定はそのままになるため、クラスタはトラフィックの処理を続行します。

  NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Firewall Management Center にクラスタを再登録すると、設定が削除されるため、クラスタはその時点でトラフィックの処理を停止します。クラスタ設定はそのまま維持されるため、クラスタ全体を追加できます。登録時にアクセス コントロール ポリシーを選択できますが、トラフィックを再度処理する前に、登録後に他のポリシーを再適用してから設定を展開する必要があります。

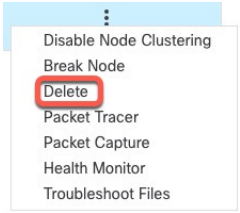
始める前に

この手順では、いずれかのノードへの CLI アクセスが必要です。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、クラスタかノードの [その他（More）] (⋮) をクリックして [登録解除] **[削除（Delete）]** を選択します。

図 *124* : クラスタまたはノードの削除



ステップ 2 クラスタかノードを削除するよう求められたら、[はい（Yes）] をクリックします。

ステップ 3 クラスタメンバーの 1 つを新しいデバイスとして追加することにより、クラスタを新しい（または同じ）Firewall Management Center に登録できます。

クラスタノードの 1 つをデバイスとして追加するだけで、残りのクラスタノードが検出されます。

a) 1 つのクラスタノードの CLI に接続し、**configure manager add** コマンドを使用して新しい Firewall Management Center を識別します。 Firewall Threat Defense 管理インターフェイスの CLI での変更 （72 ページ）を参照してください。

b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、**[追加（Add）]** > **[デバイス（Device）]** をクリックします。

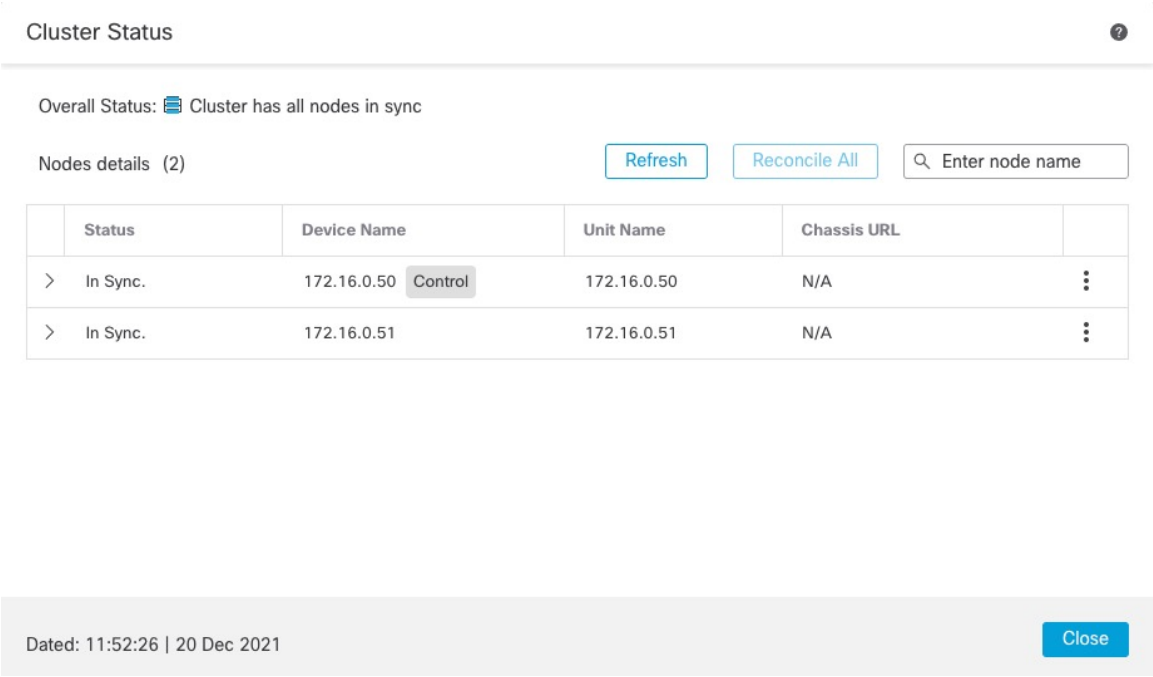
ステップ 4 未登録のノードを再度追加するには、クラスタノードの照合（363 ページ）を参照してください。

クラスタのモニタリング

クラスタは、Firewall Management Center と Firewall Threat Defense の CLI でモニターできます。

- [クラスタステータス（Cluster Status）] ダイアログボックスには、[デバイス（Devices）] > [デバイス管理（Device Management）] > [その他（More）] アイコンから、または [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] ページ > [全般（General）] 領域 > [クラスタのライブステータス（Cluster Live Status）] リンクからアクセスできます。 > > >

図 *125* : クラスタのステータス



制御ノードには、そのロールを示すグラフィックインジケータがあります。

クラスタメンバーステータスには、次の状態が含まれます。

- 同期中（In Sync）：ノードは Firewall Management Center に登録されています。
- 登録の保留中（Pending Registration）：ノードはクラスタの一部ですが、まだ Firewall Management Center に登録されていません。ノードの登録に失敗した場合は、[すべてを照合（Reconcile All）] をクリックして登録を再試行できます。
- クラスタリングが無効（Clustering is disabled）：ノードは Firewall Management Center に登録されていますが、クラスタの非アクティブなメンバーです。クラスタリング設

定は、後で再有効化する予定がある場合は変更せずに維持できます。また、ノードをクラスタから削除することも可能です。

- クラスタに参加中...（Joining cluster...）：ノードがシャーシ上でクラスタに参加していますが、参加は完了していません。参加後にFirewall Management Centerに登録されます。

ノードごとに [概要（Summary）] と [履歴（History）] を表示できます。

図 *126 : ノードの [概要（Summary）]*

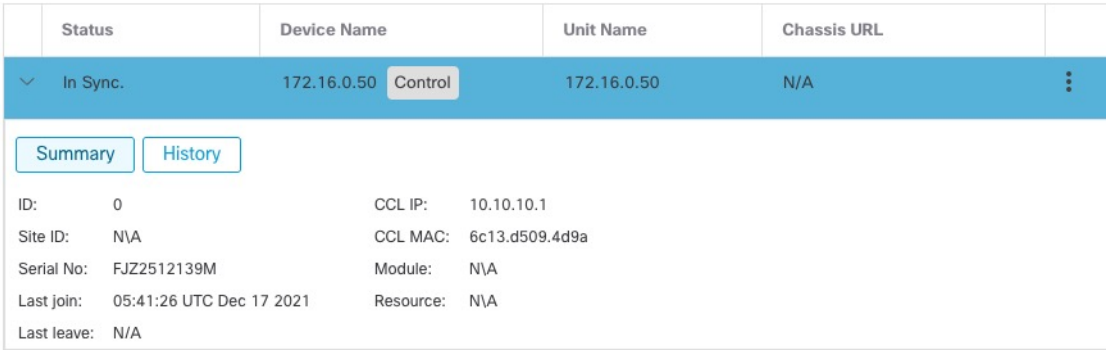
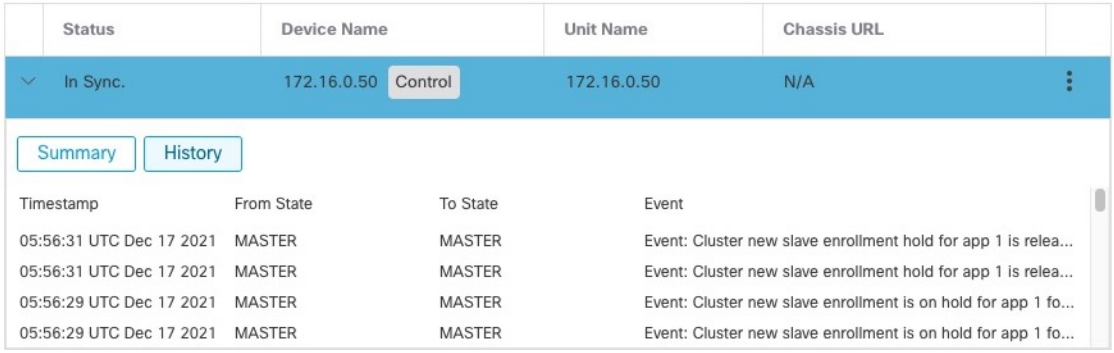


図 *127 : ノードの [履歴（History）]*



- [システム（System）]（⚙）> [Tasks] ページ。

  [タスク（Tasks）]ページには、ノードが登録されるたびにクラスタ登録タスクの最新情報が表示されます。

- [デバイス（Devices）] > [デバイス管理（Device Management）] > cluster_name。 >

  デバイスの一覧表示ページでクラスタを展開すると、IPアドレスの横にそのロールが表示されている制御ノードを含む、すべてのメンバーノードを表示できます。登録中のノードには、ロード中のアイコンが表示されます。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

クラスタ ヘルス モニター ダッシュボード

クラスタのヘルスモニター

Firewall Threat Defense がクラスタの制御ノードである場合、Firewall Management Center はデバイス メトリック データ コレクタからさまざまなメトリックを定期的に収集します。クラスタの ヘルスモニターは、次のコンポーネントで構成されています。

- 概要ダッシュボード：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。
  - トポロジセクションには、クラスタのライブステータス、個々の脅威防御の状態、脅威防御ノードのタイプ（制御ノードまたはデータノード）、およびデバイスの状態が表示されます。デバイスの状態は、[無効（Disabled）]（デバイスがクラスタを離れたとき）、[初期状態で追加（Added out of box）]（パブリッククラウドクラスタでFirewall Management Center に属していない追加ノード）、または [標準（Normal）]（ノードの理想的な状態）のいずれかです。
  - クラスタの統計セクションには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するクラスタの現在のメトリックが表示されます。

（注） CPU とメモリのメトリックは、データプレーンと Snort の使用量の個々の平均を示します。

  - メトリックチャート、つまり、CPU使用率、メモリ使用率、スループット、および接続数は、指定された期間におけるクラスタの統計を図表で示します。
- 負荷分散ダッシュボード：2 つのウィジェットでクラスタノード全体の負荷分散を表示します。
  - 分布ウィジェットには、クラスタノード全体の時間範囲における平均パケットおよび接続分布が表示されます。このデータは、ノードによって負荷がどのように分散されているかを示します。このウィジェットを使用すると、負荷分散の異常を簡単に特定して修正できます。
  - ノード統計ウィジェットには、ノードレベルのメトリックが表形式で表示されます。クラスタノード全体の CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するメトリックデータが表示されます。このテーブルビューでは、データを関連付けて、不一致を簡単に特定できます。

- メンバー パフォーマンス ダッシュボード：クラスタノードの現在のメトリックを表示します。セレクタを使用してノードをフィルタリングし、特定ノードの詳細を表示できます。メトリックデータには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、およびNAT変換数が含まれます。
- CCLダッシュボード：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- 時間範囲：さまざまなクラスタ メトリック ダッシュボードやウィジェットに表示される情報を制限するための調整可能な時間枠。
- カスタムダッシュボード：クラスタ全体のメトリックとノードレベルのメトリックの両方に関するデータを表示します。ただし、ノードの選択は脅威防御メトリックにのみ適用され、ノードが属するクラスタ全体には適用されません。

クラスタ ヘルスの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

クラスタヘルスモニターは、クラスタとそのノードのヘルスステータスの詳細なビューを提供します。このクラスタヘルスモニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

- Firewall Management Centerの1つ以上のデバイスからクラスタを作成しているかを確認します。

手順

ステップ1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]**を選択します。

[モニタリング（Monitoring）]ナビゲーションウィンドウを使用して、ノード固有のヘルスモニターにアクセスします。

ステップ2 デバイスリストで[展開（Expand）]（>）と[折りたたみ（Collapse）]（⌄）をクリックして、管理対象のクラスタデバイスのリストを展開または折りたたみます。

ステップ3 クラスタのヘルス統計を表示するには、クラスタ名をクリックします。デフォルトでは、クラスタモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- [概要（Overview）]：他の事前定義されたダッシュボードからの主要なメトリックを表示します。ノード、CPU、メモリ、入力レート、出力レート、接続統計情報、NAT変換情報などが含まれます。
- [負荷分散（Load Distribution）]：クラスタノード間のトラフィックとパケットの分散。
- [メンバーパフォーマンス（Member Performance）]：CPU 使用率、メモリ使用率、入力スループット、出力スループット、アクティブな接続、および NAT 変換に関するノードレベルの統計情報。
- [CCL]：インターフェイスのステータスおよび集約トラフィックの統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているクラスタメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で1時間前（デフォルト）から、最長では 2 週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を 5 分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの展開アイコンをクリックします。

展開アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されます。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 （ノード固有のヘルスモニターの場合）ページ上部のデバイス名の右側にあるアラート通知で、ノードの正常性アラートを確認します。

正常性アラートにポインタを合わせると、ノードの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 7 （ノード固有のヘルスモニターの場合）デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。

- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- [Snort]：Snort プロセスに関連する統計情報。
- [ASP ドロップ（ASP drops）]：さまざまな理由でドロップされたパケットに関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 正常性モニターの右上隅にあるプラス記号[新しいダッシュボードの追加（Add New Dashboard）]（＋）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタムダッシュボードを作成します。

クラスタ全体のダッシュボードの場合は、クラスタのメトリックグループを選択してから、メトリックを選択します。

クラスタメトリック

クラスタのヘルスモニターは、クラスタとそのノードに関連する統計情報と、負荷分散、パフォーマンス、および CCL トラフィックの統計データの集約結果を追跡します。

表 *28*：クラスタメトリック

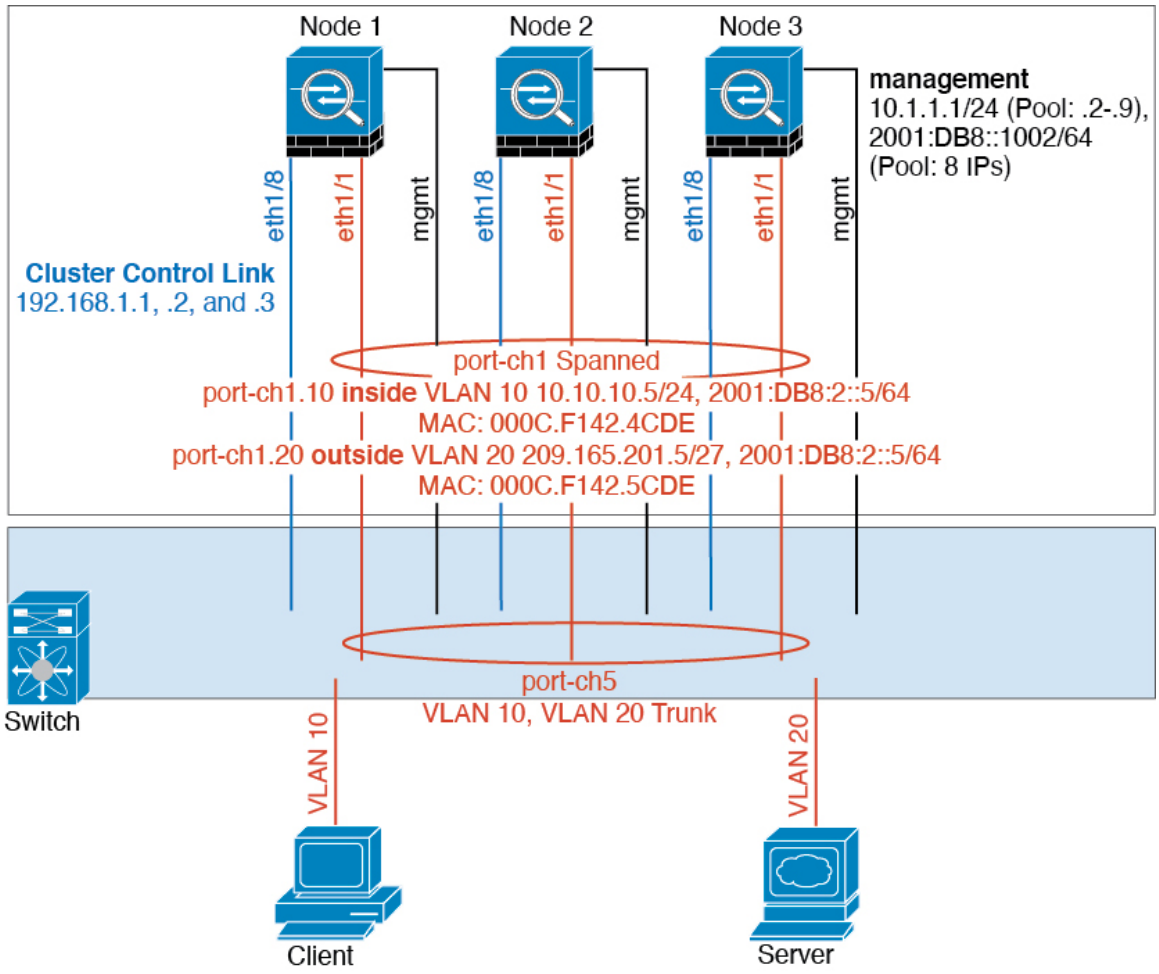
メトリック	説明	フォーマット（Format）
CPU	クラスタノード上の CPU メトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
メモリ	クラスタノード上のメモリメトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
データスループット	クラスタの着信および発信データトラフィックの統計。	バイト
CCL スループット	クラスタの着信および発信 CCL トラフィックの統計。	バイト
接続	クラスタ内のアクティブな接続数。	番号
NAT 変換数	クラスタの NAT 変換数。	番号
分布	1 秒ごとのクラスタ内の接続分布数。	番号

メトリック	説明	フォーマット（Format）
パケット	クラスタ内の1秒ごとのパケット配信の件数。	番号

クラスタリングの例

これらの例には、一般的な展開の例が含まれます。

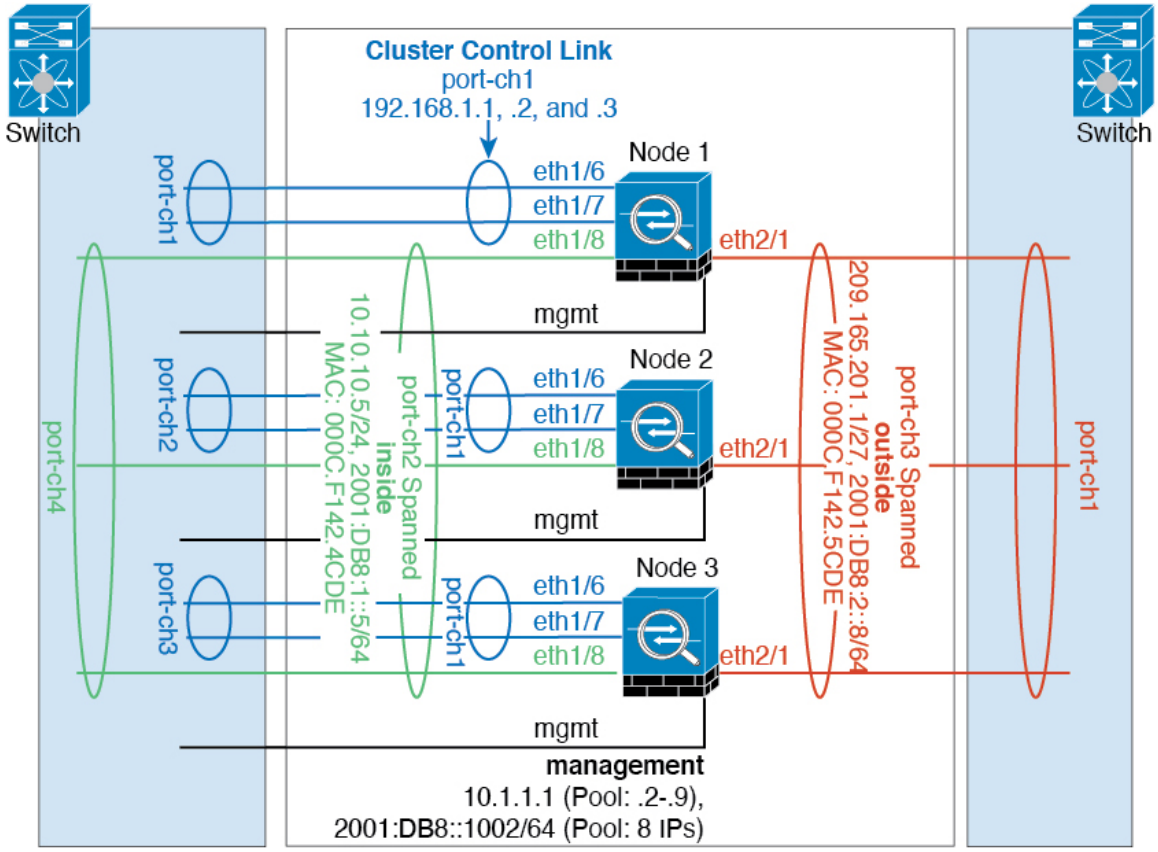
スティック上のファイアウォール



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンドEtherChannelを使用するときは、スイッチ側ですべてのデータリンクがグループ化されて1つのEtherChannelとなります。が使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

Firewall Threat Defense の機能とクラスタリング

Firewall Threat Defense の一部の機能はクラスタリングではサポートされず、一部は制御ユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

（注） クラスタリングでもサポートされていないFlexConfig機能（WCCPインスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーション ガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- リモート アクセス VPN（SSL VPN および IPsec VPN）
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- 仮想トンネルインターフェイス（VTI）
- 高可用性
- 統合ルーティングおよびブリッジング
- Firewall Management Center UCAPL/CC モード
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

（注） クラスタリングでも一元化されている FlexConfig 機能（RADIUS インスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーションガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- スタティック ルート モニタリング
- サイト間 VPN
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ダイナミックルーティング

接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバによって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を

更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

個別インターフェイス モードでのマルチキャスト ルーティング

個別インターフェイスモードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべて制御ユニットで処理されて転送されるので、パケットレプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の Firewall Threat Defense に送信されることがあります。ロードバランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない Firewall Threat Defense に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

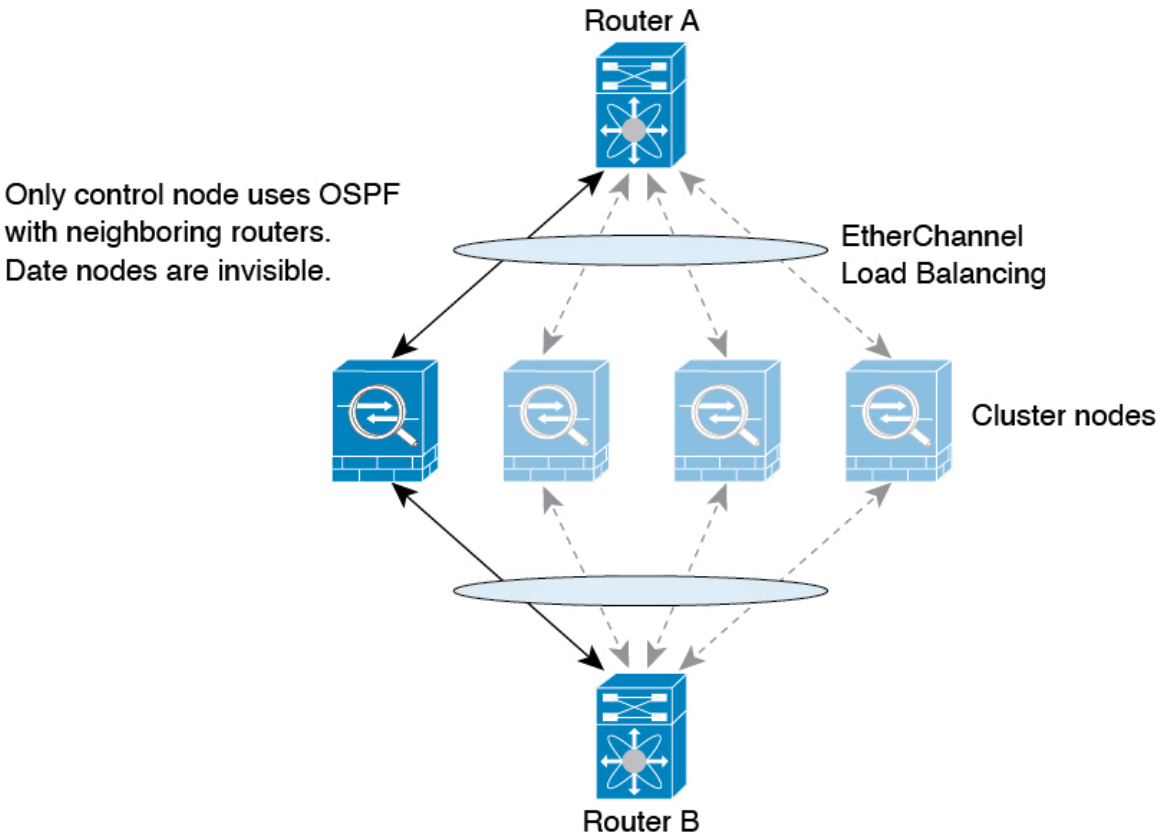
- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
  - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。

- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

でのダイナミック ルーティング

ルーティングプロセスは制御ノード上だけで実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 *128 :* スパンド *EtherChannel* モードでのダイナミック ルーティング



データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバールータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

SNMP とクラスタリング

SNMP エージェントは、個々の Firewall Threat Defense を、その [診断（Diagnostic）] 診断インターフェイスのローカルIPアドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザは新しいノードに複製されません。SNMPv3ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

syslog とクラスタリング

- クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ノードのみが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノードが選定されたときに、VPN接続を再確立する必要があります。

VPN トンネルをスパンドEtherChannelアドレスに接続すると、接続が自動的に制御ノードに転送されます。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80%になります。

たとえば、モデルが単独稼働で約 10 Gbps のトラフィックを処理できる場合、8 ユニットのクラスタでは、最大合計スループットは 80 Gbps（8 ユニット x 10 Gbps）の約 80% で 64 Gbps になります。

制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。

（注） 最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままです。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。
5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。

（注） ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、ノードとインターフェイスの正常性をモニターし、ノード間で接続状態を複製することにより、ハイアベイラビリティを実現します。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからハートビートパケットまたはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション 2 のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。

詳細については、制御ノードの選定 （380 ページ）を参照してください。

インターフェイス モニタリング

各ノードは、使用中のすべての指名されたハードウェア インターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

- スパンド EtherChannel：クラスタ Link Aggregation Control Protocol（cLACP）を使用します。各ノードは、リンクステータスおよび cLACP プロトコルメッセージをモニタして、ポートがまだ EtherChannel でアクティブであるかどうかを判断します。ステータスが制御ノードに報告されます。

ヘルスモニタリングを有効にすると、（主要な EtherChannel を含む）すべての物理インターフェイスがデフォルトでモニタされます。オプションでインターフェイスごとにモニタリングを無効にできます。指名されたインターフェイスのみモニターできます。たとえば、指名された EtherChannel に障害が発生している状態と判断されてはなりません。つまり、EtherChannel のすべてのメンバーポートはクラスタ削除のトリガーに失敗する必要があります。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。Firewall Threat Defense がメンバーをクラスタから削除するまでの時間は、そのノードが確立済みメンバーであるかクラスタに参加しようとしているかによって異なります。確立済みメンバーのインターフェイスがダウン状態の場合、Firewall Threat Defense はそのメンバーを 9 秒後に削除します。Firewall Threat Defense は、ノードがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、

Firewall Threat Defense はクラスタから削除されません。EtherChannel 以外の場合は、メンバー状態に関係なく、ノードは 500 ミリ秒後に削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、Firewall Threat Defense は自動的にクラスタへの再参加を試みます。

（注） Firewall Threat Defenseが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理/診断インターフェイスのみがトラフィックを送受信できます。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- 最初に参加するときに障害が発生したクラスタ制御リンク：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：FTDは、無限に5分ごとに自動的に再参加を試みます。
- データ インターフェイスの障害：Firewall Threat Defense は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、Firewall Threat Defense アプリケーションはクラスタリングを無効にします。データ インターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ノードは再起動するとクラスタに再参加します。Firewall Threat Defense アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。
- 障害が発生した設定の展開：FMC から新しい設定を展開し、展開が一部のクラスタメンバーでは失敗したものの、他のメンバーでは成功した場合、失敗したノードはクラスタから削除されます。クラスタリングを再度有効にして手動でクラスタに再参加する必要があります。制御ノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除さ

れません。すべてのデータノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *29*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システムアップタイムをトラッキングします。
ARP Table	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	Yes	—
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—

クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップ

オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  ICMP/ICMPv6 ハッシュの詳細：

  - エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
  - 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
  - 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

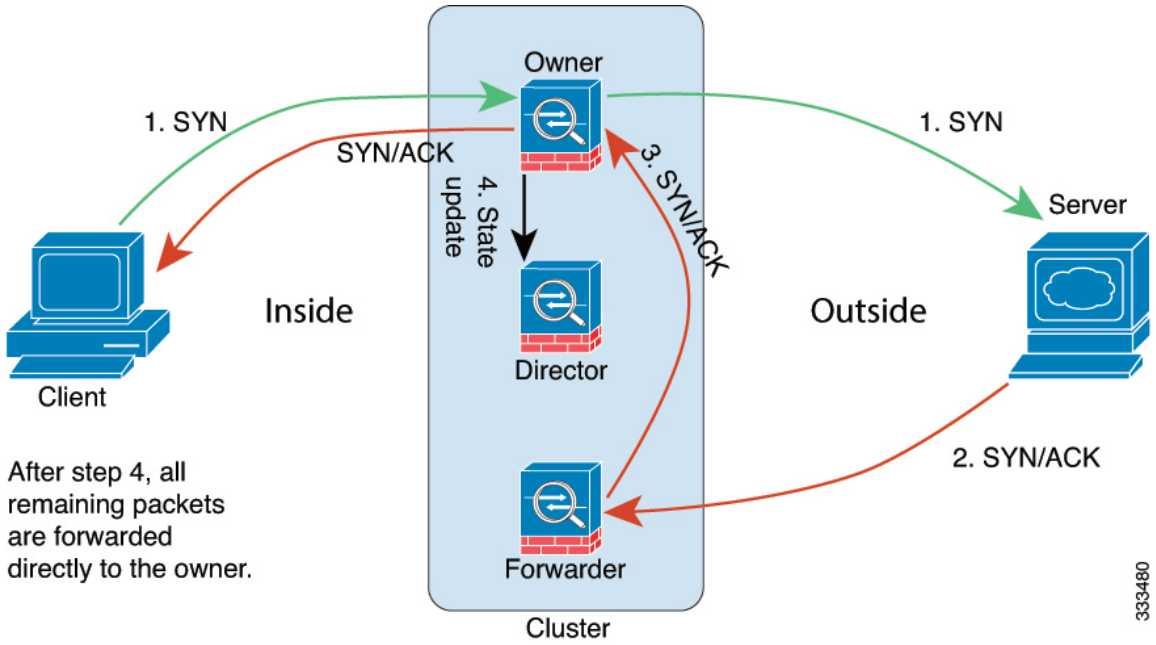
- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータフロー

次の例は、新しい接続の確立を示します。

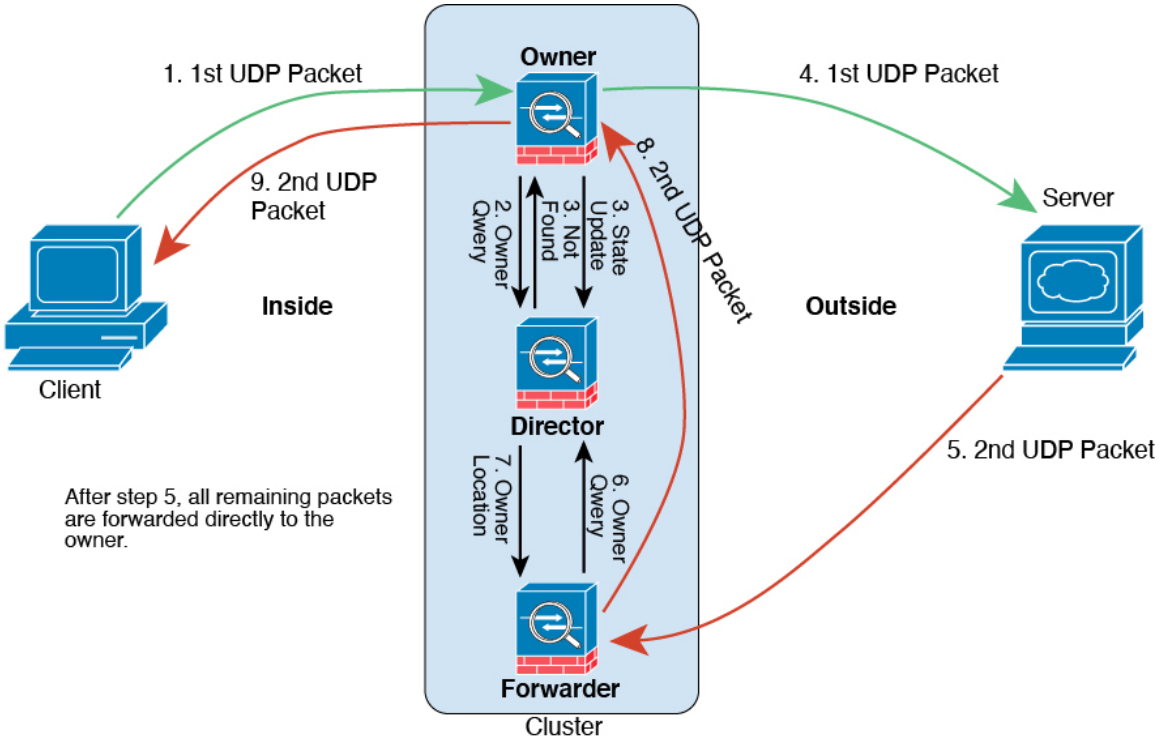


1. SYN パケットがクライアントから発信され、Firewall Threat Defense の 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firewall Threat Defense（ロード バランシング方法に基づく）に配信されます。この Firewall Threat Defense はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータフロー

次の例は、新しい接続の確立を示します。

1. 図 *129 : ICMP* および *UDP* データ フロー

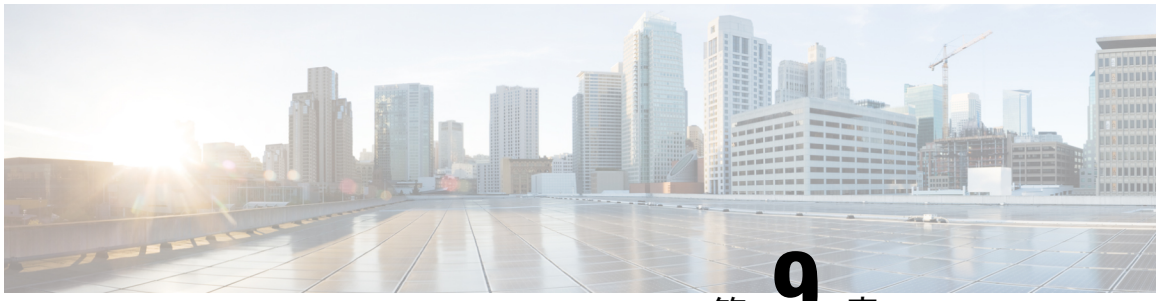


UDP パケットがクライアントから発信され、1 つの Firewall Threat Defense（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

クラスタリングの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタのヘルスモニターの設定	7.3.0	いずれか	クラスタのヘルスモニター設定を編集できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）]** （注） 以前にFlexConfigを使用してこれらの設定を行った場合は、展開前に必ずFlexConfigの設定を削除してください。削除しなかった場合は、FlexConfigの設定によってManagement Centerの設定が上書きされます。
クラスタ ヘルス モニター ダッシュボード	7.3.0	いずれか	クラスタのヘルス モニター ダッシュボードでクラスタの状態を表示できるようになりました。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]**
クラスタ制御リンクMTUの自動構成	7.2.0	7.2.0	クラスタ制御リンクインターフェイスのMTUが、最も高いデータインターフェイスMTUよりも100バイト多い値に自動的に設定されるようになりました。デフォルトでは、MTUは1,600バイトです。
Cisco Secure Firewall 3100のクラスタリング	7.1.0	7.1.0	Cisco Secure Firewall 3100は、最大8ノードのスパンドEtherChannelクラスタリングをサポートします。 新規/変更された画面： • [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタの追加（Add Cluster）] • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[詳細（More）]**メニュー • **[Devices]** > **[Device Management]** > **[Cluster]** サポートされるプラットフォーム：Cisco Secure Firewall 3100



第 9 章

プライベートクラウドでの Threat Defense Virtual のクラスタリング

クラスタリングを利用すると、複数の Firewall Threat Defense Virtual をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。VMware と KVM を使用して、プライベートクラウドに Firewall Threat Defense Virtual クラスタを導入できます。ルーテッド ファイアウォール モードのみがサポートされます。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「サポートされていない機能とクラスタリング （429 ページ）」を参照してください。

- プライベートクラウドでの Threat Defense Virtual のクラスタリングについて （389 ページ）
- Threat Defense Virtual クラスタリングのライセンス （394 ページ）
- Threat Defense Virtual クラスタリングの要件および前提条件 （394 ページ）
- Threat Defense Virtual クラスタリングのガイドライン （396 ページ）
- Threat Defense Virtual クラスタリングの設定 （397 ページ）
- クラスタノードの管理 （412 ページ）
- クラスタのモニタリング （423 ページ）
- クラスタリングの参考資料 （429 ページ）
- プライベートクラウドでの Threat Defense Virtual のクラスタリング履歴 （443 ページ）

プライベートクラウドでの Threat Defense Virtual のクラスタリングについて

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは 1 つのデバイスとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離されたネットワーク。VXLAN インターフェイスを使用したクラスタ制御リンクと呼ばれます。レイヤ 3 物理ネットワーク上でレイヤ 2 仮想ネットワークとして機能する VXLAN により、Firewall Threat Defense Virtual はクラスタ制御リンクを介してブロードキャスト/マルチキャストメッセージを送信できます。
- 各ファイアウォールへの管理アクセス（コンフィギュレーションおよびモニタリングのため）。Firewall Threat Defense Virtual 導入には、クラスタノードの管理に使用するManagement 0/0 インターフェイスが含まれています。

クラスタをネットワーク内に配置するときは、アップストリームおよびダウンストリームのルータは、レイヤ3の個別インターフェイスおよび次のいずれかの方法を使用して、クラスタとの間で送受信されるデータをロードバランシングできる必要があります。

- ポリシーベースルーティング：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してノード間のロードバランシングを実行します。
- 等コスト マルチパス ルーティング：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミック ルートを使用してノード間のロードバランシングを実行します。

（注） レイヤ 2 スパンド EtherChannels はサポートされません。

制御ノードとデータノードの役割

クラスタ内のメンバーの1つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、プライオリティ設定によって決まります。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバーはデータノードです。 最初にクラスタを作成するときに、制御ノードにするノードを指定します。これは、クラスタに追加された最初のノードであるため、制御ノードになります。

クラスタ内のすべてのノードは、同一の設定を共有します。最初に制御ノードとして指定したノードは、データノードがクラスタに参加するときにその設定を上書きします。そのため、クラスタを形成する前に制御ノードで初期設定を実行するだけで済みます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

個々のインターフェイス

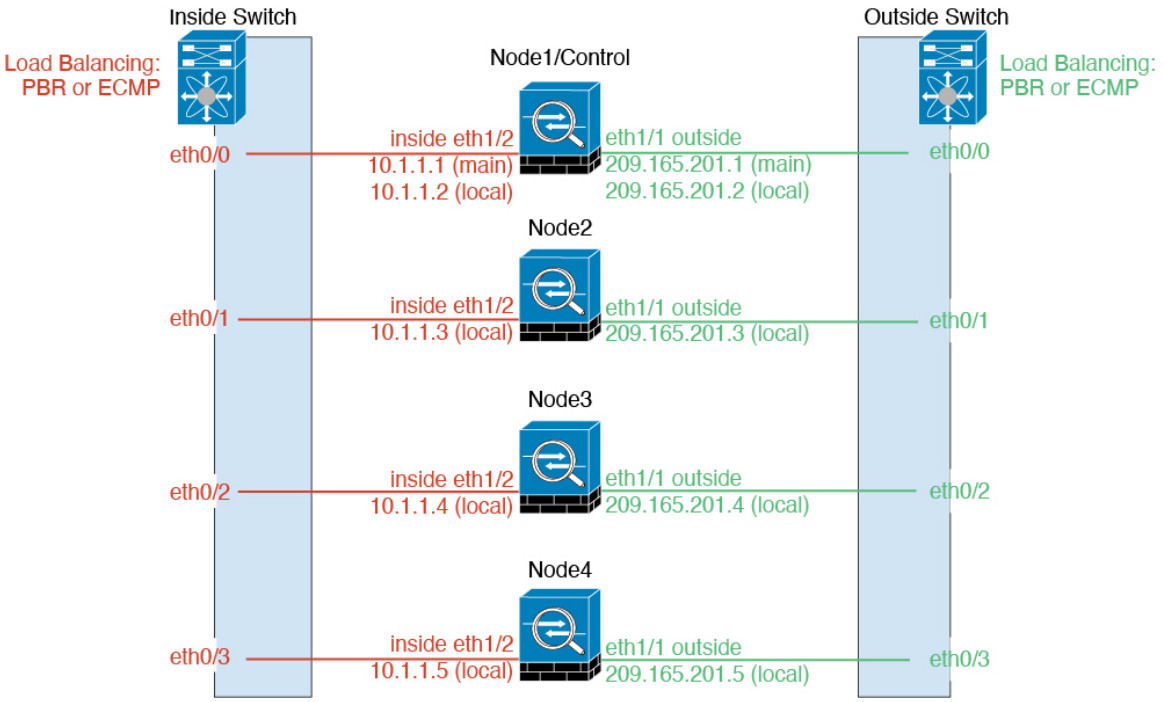
クラスターフェイスを個々のインターフェイスとして設定できます。

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル *IP* アドレスを持ちます。各インターフェイスのメインクラスタ *IP* アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。

IPS 専用インターフェイス（インラインセットとパッシブインターフェイス）は、個別インターフェイスとしてサポートされません。

インターフェイス コンフィギュレーションは制御ノード上だけで行う必要があるため、IP アドレスプールを設定して、このプールのアドレスがクラスタノード（制御ノード用を含む）の特定のインターフェイスに使用されるようにします。

アップストリームスイッチ上でロードバランシングを別途する必要があります。



（注） レイヤ 2 スパンド EtherChannels はサポートされません。

ポリシーベース ルーティング

個別インターフェイスを使用するときは、各 Firewall Threat Defense インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロードバランシング方法の 1 つが、ポリシーベース ルーティング（PBR）です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての Firewall Threat Defense に分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ Firewall Threat Defense に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクト トラッキングとともに使用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 Firewall Threat Defense をモニタします。これで、PBR は、特定の Firewall Threat Defense の到達可能性に基づいてルート マップを有効化または無効化できます。詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

等コスト マルチパス ルーティング

個別インターフェイスを使用するときは、各 Firewall Threat Defense インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロード バランシング方法の 1 つが、等コスト マルチパス（ECMP）ルーティングです。

この方法が推奨されるのは、すでに ECMP を使用しており、既存のインフラストラクチャを活用したい場合です。

ECMP ルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannel のように、送信元および宛先の IP アドレスや送信元および宛先のポートのハッシュを使用してネクスト ホップの 1 つにパケットを送信できます。ECMP ルーティングにスタティック ルートを使用する場合は、Firewall Threat Defense の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した Firewall Threat Defense へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 Firewall Threat Defense を設定する必要があります。

クラスタ制御リンク

ノードごとに 1 つのインターフェイスをクラスタ制御リンク専用の VXLAN（VTEP）インターフェイスにする必要があります。VXLAN の詳細については、「VXLAN インターフェイスの設定 （707 ページ）」を参照してください。

VXLAN トンネル エンドポイント

VXLAN トンネル エンドポイント（VTEP）デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイス タイプ（VXLAN Network Identifier（VNI）インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、 VTEP 間に VNI を

トンネリングするVTEP送信元インターフェイスと呼ばれる通常のインターフェイス）がありますVTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

VTEP 送信元インターフェイス

VTEP送信元インターフェイスは、VNIインターフェイスに関連付けられる予定の標準のFirewall Threat Defense Virtualインターフェイスです。1 つの VTEP ソースインターフェイスをクラスタ制御リンクとして機能するように設定できます。ソースインターフェイスは、クラスタ制御リンクの使用専用に予約されています。各VTEP ソースインターフェイスには、同じサブネット上の IP アドレスがあります。このサブネットは、他のすべてのトラフィックからは隔離し、クラスタ制御リンクインターフェイスだけが含まれるようにしてください。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。設定できる VNI インターフェイスは 1 つだけです。各 VNI インターフェイスは、同じサブネット上の IP アドレスを持ちます。

ピア VTEP

単一のVTEP ピアを許可するデータインターフェイス用の通常のVXLANとは異なり、Firewall Threat Defense Virtual クラスタリングでは複数のピアを設定できます。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

管理ネットワーク

管理インターフェイスを使用して各ノードを管理する必要があります。クラスタリングでは、データインターフェイスからの管理はサポートされていません。

Threat Defense Virtual クラスタリングのライセンス

各 Firewall Threat Defense Virtual クラスタノードには、同じパフォーマンス階層ライセンスが必要です。すべてのメンバーに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のメンバーに一致するようにすべてのノードで制限されます。スループットレベルは、一致するように制御ノードから各データノードに複製されます。

個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。

制御ノードを Firewall Management Center に追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタを作成する前に、データノードにどのライセンスが割り当てられているのかは問題になりません。制御ノードのライセンス設定は、各データノードに複製されます。クラスタのライセンスは、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [ライセンス（License）]** エリアで変更できます。

（注） Firewall Management Center にライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、Firewall Management Center にライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのデータユニットがクラスタをいったん離れてから再参加することになります。

Threat Defense Virtual クラスタリングの要件および前提条件

モデルの要件

- FTDv5、FTDv10、FTDv20、FTDv30、FTDv50、FTDv100
- VMware または KVM
- 2x2 構成のクラスタで最大 4 つのノードがサポートされます。最大 2 つのホストを設定し、各ホストに最大 2 つの Threat Defense 仮想インスタンスを設定できます。

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

ハードウェアおよびソフトウェアの要件

クラスタ内のすべてのユニット：

- クラスタ制御リンクでジャンボフレーム予約を有効にする必要があります。`"DeploymentType": "Cluster"` を設定して Firewall Threat Defense Virtual を展開するときに、Day 0 構成でこれを実行します。それ以外の場合は、クラスタが形成されて正常な状態になった後で、各ノードを再起動してジャンボフレームを有効にする必要があります。
- （KVM のみ）KVM ホスト上のすべての VM に CPU ハードパーティショニング（CPU ピン留め）を使用する必要があります。
- 同じパフォーマンス層である必要があります。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のノードに一致するようにすべてのノードで制限されます。
- Firewall Management Center 通信の管理インターフェイスを指定する必要があります。データインターフェイス管理はサポートされていません。
- アップグレード時を除き、同じバージョンを実行する必要があります。ヒットレスアップグレードがサポートされます。
- 同じドメインに属していること。
- 同じグループに属していること。
- 保留中または進行中の展開がないこと。
- 制御ノードにサポート対象外の機能が設定されていないこと：サポートされていない機能とクラスタリング （429 ページ）。
- データノードに VPN が設定されていないこと。制御ノードにはサイト間 VPN を設定できます。

Firewall Management Center の要件

Firewall Management Center NTP サーバーをすべてのクラスタノードから到達可能な信頼できるサーバーに設定し、適切にクロックを同期できるようにします。デフォルトでは、デバイスは Firewall Management Center と同じ NTP サーバーが使用されます。すべてのクラスタノードの時刻が同じ時刻に設定されていない場合は、クラスタから自動で削除されます。

スイッチ要件

クラスタリングの設定前にスイッチの設定を完了していること。クラスタ制御リンクに接続されているポートに適切なMTU値（高い値）が設定されていること。デフォルトでは、クラスタ制御リンクのMTUは、データインターフェイスよりも154バイト大きく設定されています。スイッチでMTUが一致しない場合、クラスタの形成に失敗します。

Threat Defense Virtual クラスタリングのガイドライン

ハイ アベイラビリティ

クラスタリングでは、高可用性はサポートされません。

IPv6

クラスタ制御リンクは、IPv4のみを使用してサポートされます。

その他のガイドライン

- 重要なトポロジの変更（EtherChannelインターフェイスの追加や削除、Firewall Threat Defense Virtualのインターフェイスの有効化や無効化、VSSまたはvPCを形成するスイッチの追加、など）が発生した場合は、ヘルスチェック機能を無効にし、トポロジ変更の影響を受けるインターフェイスのインターフェイスモニタリングも無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP接続のFIN/ACKパケットがドロップされると、FTPクライアントがハングします。この場合は、FTP接続を再確立する必要があります。
- 復号されたTLS/SSL接続の場合、復号状態は同期されず、接続オーナーに障害が発生すると、復号された接続がリセットされます。新しいユニットへの新しい接続を確立する必要があります。復号されていない接続（復号しないルールに一致）は影響を受けず、正しく複製されます。
- データインターフェイスのVXLANはサポートしていません。クラスタ制御リンクのみがVXLANをサポートします。

クラスタリングのデフォルト

- cLACPシステムIDは自動生成され、システムの優先順位はデフォルトでは1になっています。

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が5分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

Threat Defense Virtual クラスタリングの設定

Firewall Threat Defense Virtual の展開後にクラスタリングを設定するには、次のタスクを実行します。

Management Center へのデバイスの追加

クラスタリングを構成する前に、各クラスタノードを展開してから、Firewall Management Center でデバイスをスタンドアロンユニットとして追加します。

手順

ステップ 1 『Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』[英語] に従って各クラスタノードを展開します。

クラスタ内のすべてのユニット：

- クラスタ制御リンクでジャンボフレーム予約を有効にする必要があります。`"DeploymentType": "Cluster"` を設定して Firewall Threat Defense Virtual を展開するときに、Day 0 構成でこれを実行します。それ以外の場合は、クラスタが形成されて正常な状態になった後で、各ノードを再起動してジャンボフレームを有効にする必要があります。
- （KVM のみ）KVM ホスト上のすべての VM に CPU ハードパーティショニング（CPU ピン留め）を使用する必要があります。

ステップ 2 同じドメインおよびグループ内のスタンドアロンデバイスとして、各ノードを Firewall Management Center に追加します。

デバイスの追加 （34 ページ）を参照してください。単一のデバイスでクラスタを作成し、後からノードを追加できます。デバイスを追加したときに行った初期設定（ライセンス、アクセ

ス コントロール ポリシー）は、制御ノードからすべてのクラスタノードに継承されます。クラスタを形成するときに制御ノードを選択します。

クラスタの作成

Firewall Management Center 内の 1 台以上のデバイスでクラスタを形成します。

始める前に

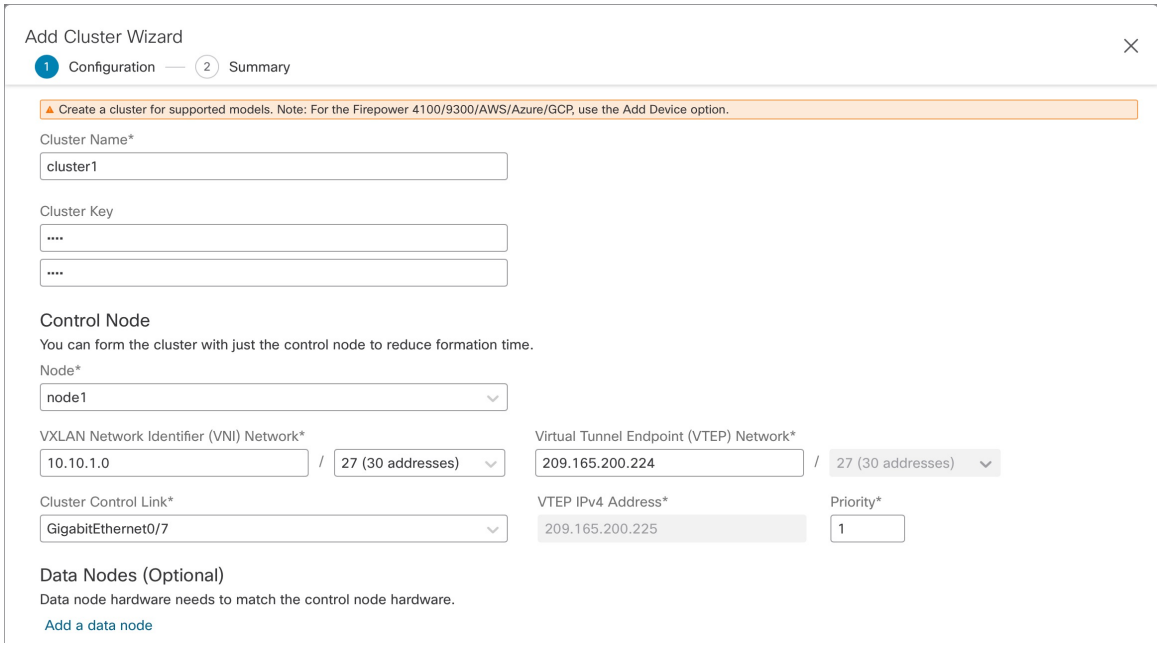
一部の機能はクラスタリングに対応していません。そのため、クラスタリングを有効にしてから、設定を行う必要があります。一部の機能は、設定してしまうとクラスタの作成をブロックします。たとえば、インターフェイスに IP アドレスを設定したり、BVI などのサポート対象外のインターフェイスタイプを設定したりしないでください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択してから、[追加（Add）] > [クラスタ（Cluster）] の順に選択します。 > >

[クラスタの追加（Add Cluster）] ウィザードが表示されます。

図 *130 : [クラスタの追加（Add Cluster）] ウィザード*



ステップ 2 制御トラフィックの [クラスタ名（Cluster Name）] と認証用の [クラスタキー（Cluster Key）] を指定します。

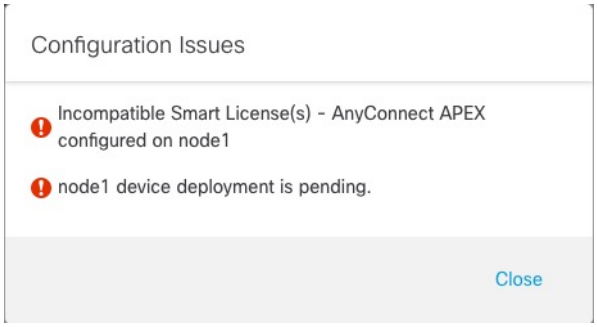
- [クラスタ名（Cluster Name）]：1 ～ 38 文字の ASCII 文字列。
- [クラスタキー（Cluster Key）]：1 ～ 63 文字の ASCII 文字列。[クラスタキー（Cluster Key）]の値は暗号キーを生成するために使用されます。この暗号は、データパストラフィック（接続状態の更新や転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。

ステップ 3 [制御ノード（Control Node）] については、次のように設定します。

- [ノード（Node）]：最初に制御ノードにするデバイスを選択します。Firewall Management Centerがクラスタを形成すると、このノードが最初にクラスタに追加されて制御ノードになります。

（注）
ノード名の横に **エラー**（ ）アイコンが表示されている場合は、そのアイコンをクリックして設定の問題を表示します。クラスタの形成をキャンセルし、問題を解決してからクラスタの形成に戻る必要があります。次に例を示します。

図 *131*：設定の問題



上記の問題を解決するには、サポート対象外の VPN ライセンスを削除し、保留中の設定の変更をデバイスに展開します。

- [VXLANネットワーク識別子(VNI)ネットワーク（VXLAN Network Identifier (VNI) Network）]：VNI ネットワークの IPv4 サブネットを指定します。このネットワークでは IPv6 はサポートされていません。[24]、[25]、[26]、または [27] サブネットを指定します。IP アドレスは、このネットワーク上の各ノードに自動的に割り当てられます。VNI ネットワークは、物理 VTEP ネットワーク上で稼働する暗号化された仮想ネットワークです。
- [クラスタ制御リンク（Cluster Control Link）]：クラスタ制御リンクに使用する物理インターフェイスを選択します。
- [仮想トンネルエンドポイント(VTEP)ネットワーク（Virtual Tunnel Endpoint (VTEP) Network）]：物理インターフェイス ネットワークの IPv4 サブネットを指定します。このネットワークでは IPv6 はサポートされていません。VTEP ネットワークは VNI ネットワークとは別のネットワークであり、物理クラスタ制御リンクに使用されます。
- [VTEP IPv4 アドレス（VTEP IPv4 Address）]：このフィールドには、VTEP ネットワークの最初のアドレスが自動的に入力されます。

- [プライオリティ（Priority）]：制御ノードの選択に対するこのノードのプライオリティを設定します。プライオリティは1～100であり、1が最高のプライオリティです。他のノードよりプライオリティを低く設定しても、クラスタが最初に形成されたときは、このノードが引き続き制御ノードになります。

ステップ4 [データノード（Data Nodes）]（オプション）で、[データノードを追加（Add a data node）]をクリックしてクラスタにノードを追加します。

クラスタの形成を高速化するために制御ノードのみでクラスタを形成することも、すべてのノードをここで追加することも可能です。各データノードで以下を設定します。

- [ノード（Node）]：追加するデバイスを選択します。

  （注）

  ノード名の横に **エラー**（ ）アイコンが表示されている場合は、そのアイコンをクリックして設定の問題を表示します。クラスタの形成をキャンセルし、問題を解決してからクラスタの形成に戻る必要があります。

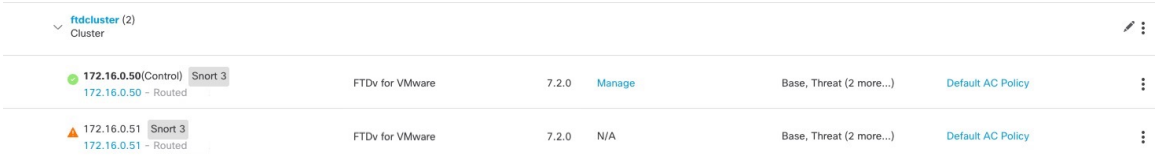
- [VTEP IPv4 アドレス（VTEP IPv4 Address）]：このフィールドには、VTEP ネットワークの次のアドレスが自動的に入力されます。
- [プライオリティ（Priority）]：制御ノードの選択に対するこのノードのプライオリティを設定します。プライオリティは 1 ～ 100 であり、1 が最高のプライオリティです。

ステップ5 [続行（Continue）]をクリックします。[概要（Summary）]を確認し、[保存（Save）]をクリックします。

クラスタブートストラップ構成は、クラスタノードに保存されます。ブートストラップ構成には、クラスタ制御リンクに使用される VXLAN インターフェイスが含まれています。

[デバイス（Devices）]>[デバイス管理（Device Management）]ページにクラスタ名が表示されます。クラスタを展開して、クラスタノードを表示します。

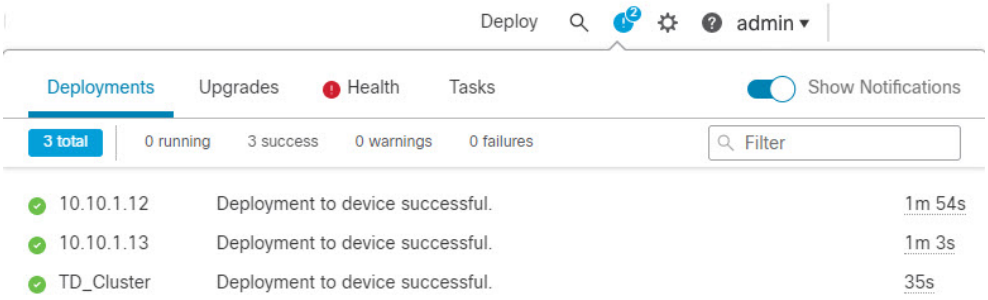
図 *132*：クラスタの管理



現在登録中のノードには、ロードアイコンが表示されます。

図 *133* : ノードの登録

クラスタノードの登録をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。Firewall Management Center は、ノードの登録ごとにクラスタ登録タスクを更新します。

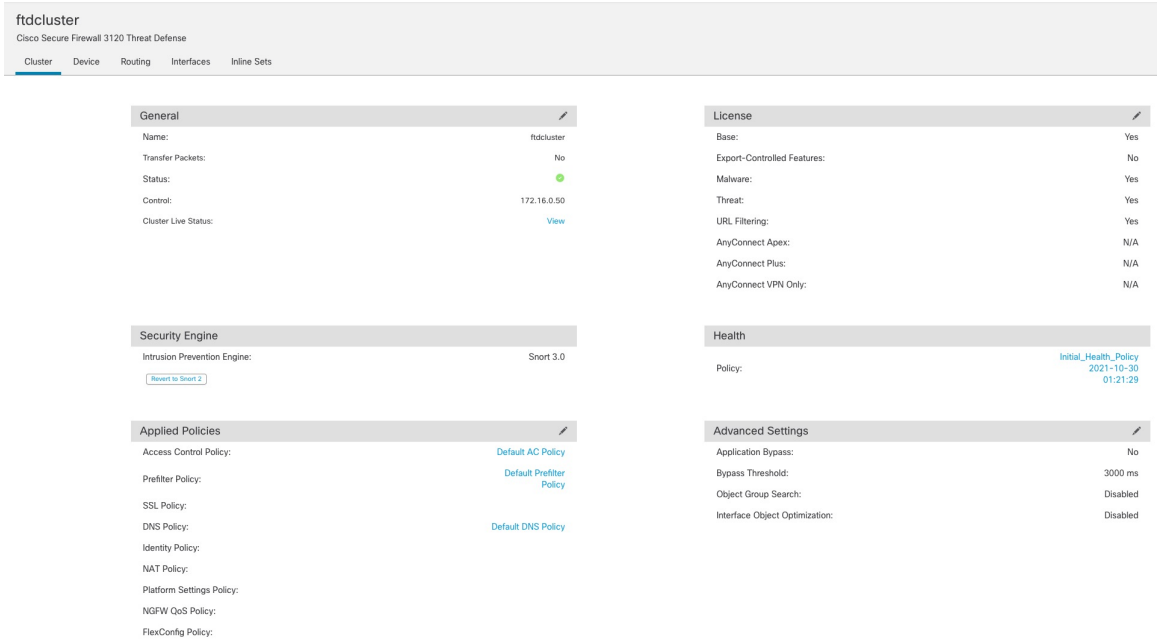


ステップ 6 クラスタの [編集（Edit）]（✎） をクリックして、デバイス固有の設定を指定します。

ほとんどの設定は、クラスタ内のノードではなく、クラスタ全体に適用できます。たとえば、ノードごとに表示名を変更できますが、インターフェイスはクラスタ全体についてのみ設定できます。

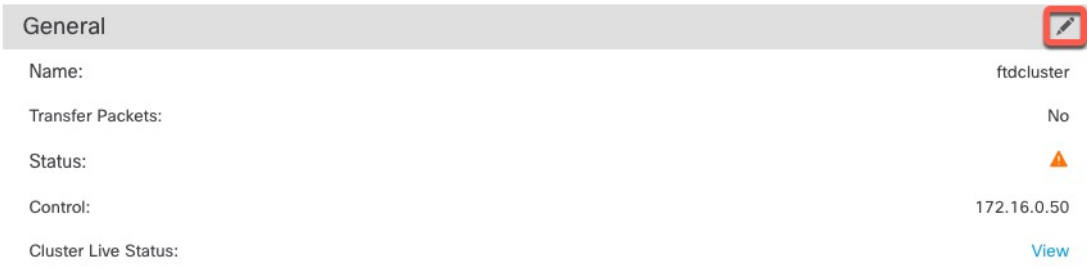
ステップ 7 [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] 画面に、クラスタの [全般（General）] などの設定が表示されます。

図 *134* : クラスタ設定

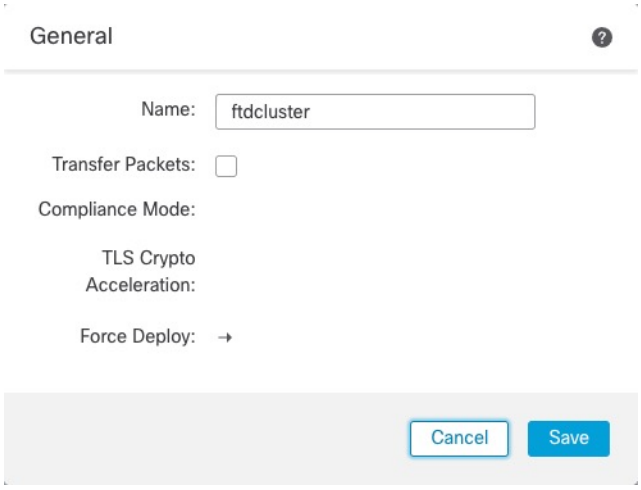


[全般（General）] 領域には、次のクラスタに固有の項目が表示されます。

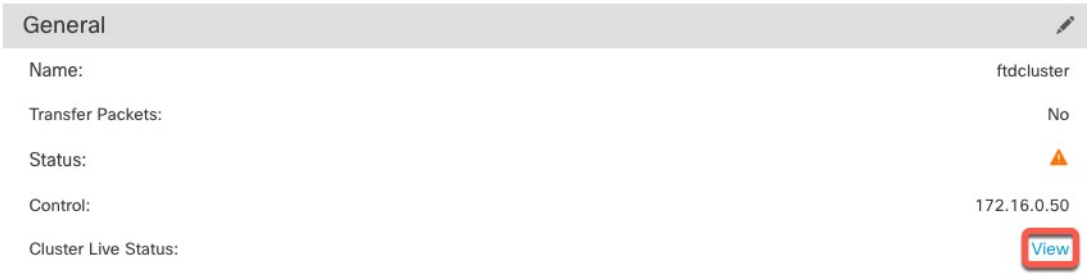
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタの表示名を変更します。



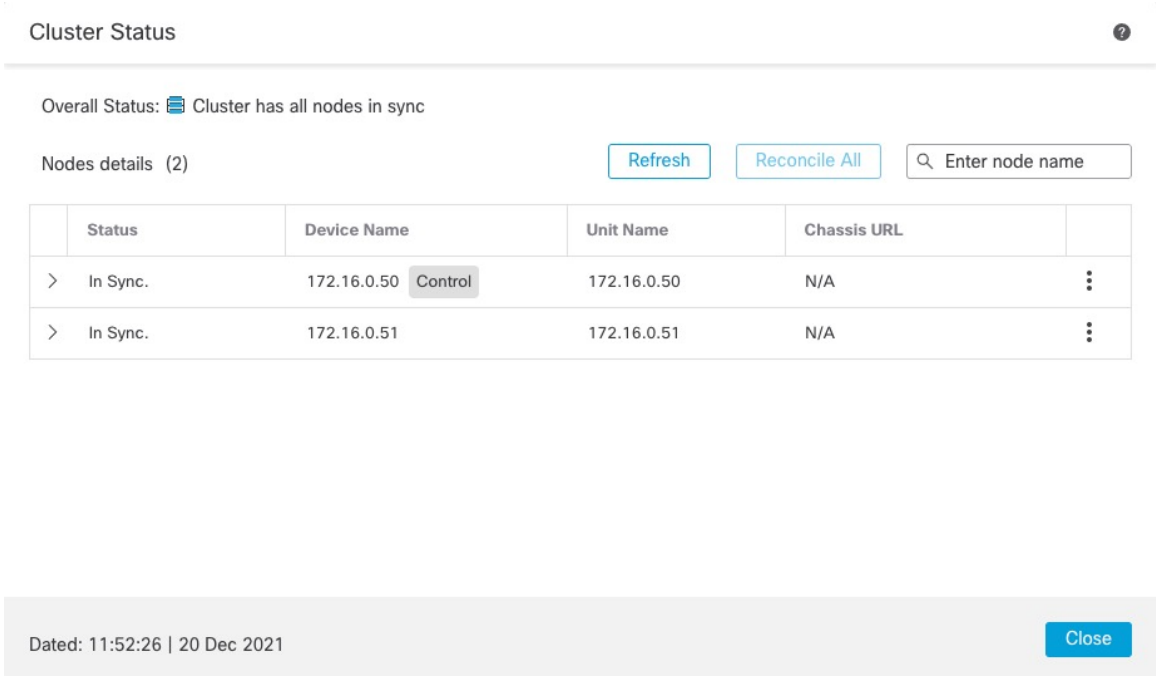
その後に、[名前（Name）] フィールドを設定します。



- [全般（General）] > [表示（View）] : [表示（View）] リンクをクリックして [クラスタステータス（Cluster Status）] ダイアログボックスを開きます。



[クラスタステータス（Cluster Status）] ダイアログボックスでは、[すべて照合（Reconcile All）] をクリックしてデータユニットの登録を再試行することもできます。



ステップ 8 **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）]** の右上のドロップダウンメニューで、クラスタ内の各メンバーを選択し、次の設定を指定することができます。

図 *135* : デバイス設定

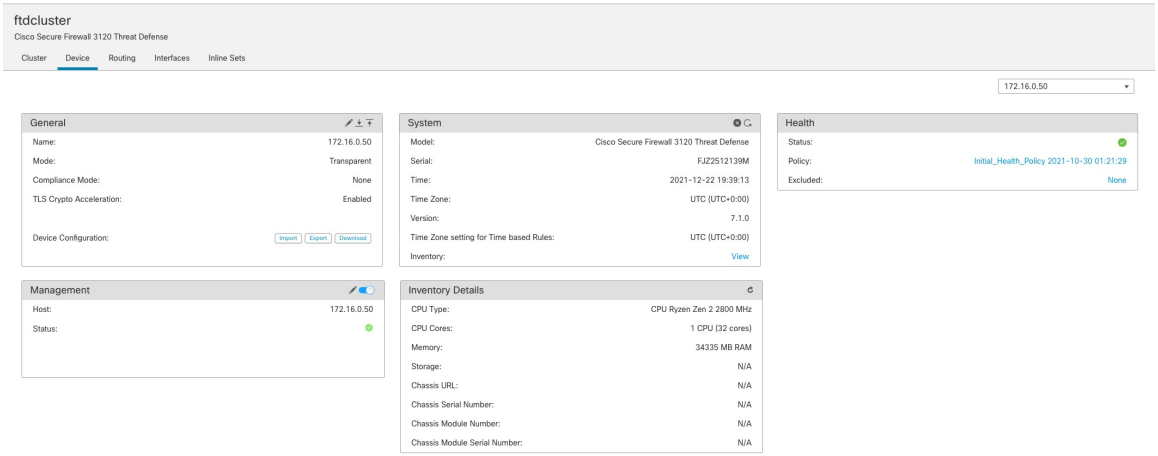
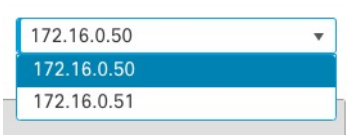
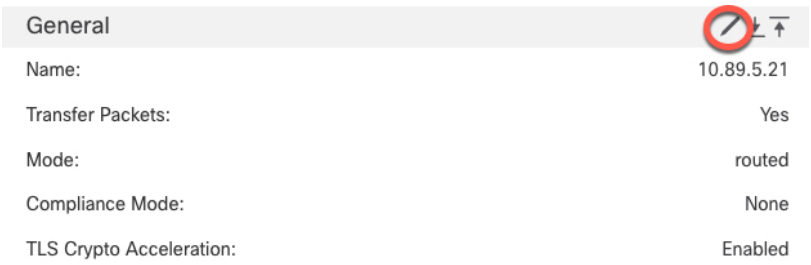


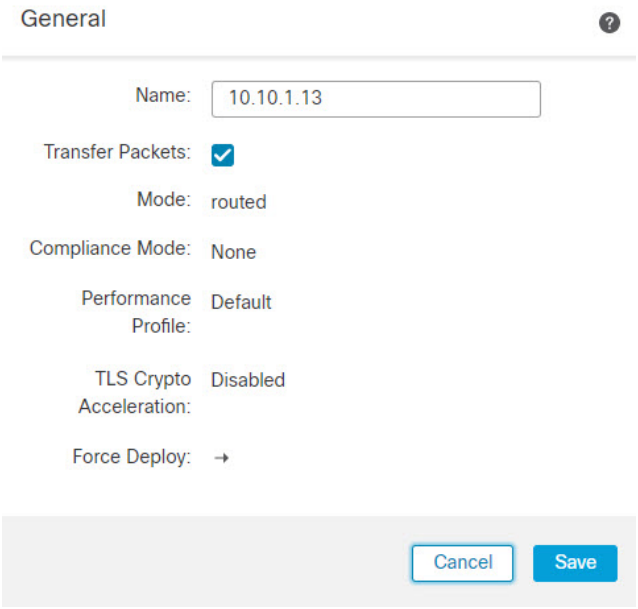
図 *136* : ノードの選択



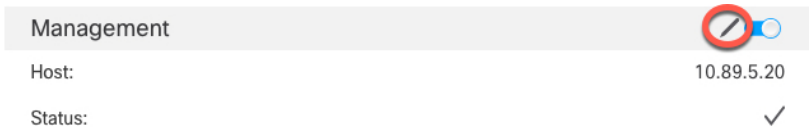
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタメンバーの表示名を変更します。



その後に、[名前（Name）] フィールドを設定します。



- [管理（Management）] > [ホスト（Host）] : デバイス設定で管理 IP アドレスを変更する場合は、Firewall Management Center で新しいアドレスを一致させてネットワーク上のデバイスに到達できるようにする必要があります。最初に接続を無効にし、[管理（Management）] 領域で [ホスト（Host）] のアドレスを編集してから、接続を再度有効にします。



ステップ 9 ジャンボフレームの予約を有効にせずにクラスタノードを展開した場合は、すべてのクラスタノードを再起動して、クラスタ制御リンクに必要なジャンボフレームを有効にします。デバイスのシャットダウンまたは再起動 （41 ページ）を参照してください。

事前にジャンボフレームの予約を有効にした場合は、この手順をスキップできます。

クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッド（100 バイト）およびVXLANのオーバーヘッド（54バイト）にも対応する必要があります。クラスタを作成すると、MTU はデータインターフェイスの最大 MTU（デフォルトでは 1654）よりも 154 バイト大きい値が設定されます。後でデータインターフェイスの MTU を増やす場合は、クラスタ制御リンクの MTU も増やすようにしてください。たとえば、最大 MTU は 9198 バイトであるため、データインターフェイスの最大 MTU は 9044 になり、クラスタ制御リンクは 9198 に設定できます。 MTU の設定 （747 ページ）を参照してください。

（注）
クラスタ制御リンクに接続されているスイッチの MTU を適切な値（高い値）に設定してください。そうしないと、クラスタ形成に失敗します。

インターフェイスの設定

ここでは、個々のインターフェイスがクラスタリング互換となるようにインターフェイスを設定する方法について説明します。個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在の制御ノードに属します。すべてのデータインターフェイスは個別インターフェイスである必要があります。

診断インターフェイスでは、IPアドレスプールを設定するか、DHCPを使用できます。診断インターフェイスのみがDHCPからのアドレスの取得をサポートしています。DHCPを使用する場合は、この手順を使用しないでください。代わりに、通常どおりに設定します（ルーテッドモードのインターフェイスの設定 （717 ページ）を参照）。

（注） サブインターフェイスは使用できません。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[アドレスプール（Address Pools）]** を選択して、IPv4 または IPv6 アドレスプールを追加します。 アドレス プール （1323 ページ）を参照してください。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。仮想IPアドレスはこのプールには含まれませんが、同一ネットワーク上に存在している必要があります。各ユニットに割り当てられる正確なローカルアドレスを事前に決定することはできません。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、クラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [インターフェイス（Interfaces）] をクリックし、データインターフェイスの [編集（Edit）]（✎） をクリックします。

ステップ 4 [IPv4] で [IPアドレス（IP Address）] とマスクを入力します。この IP アドレスは、そのクラスタの固定アドレスで、常に現在の制御ユニットに属します。

ステップ 5 作成したアドレスプールを [IPv4アドレスプール（IPv4 Address Pool）] ドロップダウンリストから選択します。

（注）
このインターフェイスに MAC アドレスを手動で割り当てる場合は、FlexConfig を使用して **mac-address pool** を作成する必要があります。

ステップ 6 [IPv6] > [基本（Basic）] で、[IPv6アドレスプール（IPv6 Address Pool）] ドロップダウンリストから、作成したアドレスプールを選択します。

ステップ 7 通常どおり、他のインターフェイス設定を行います。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

クラスタのヘルスモニターの設定

[クラスタ（Cluster）]ページの [クラスタヘルスモニターの設定（Cluster Health Monitor Settings）] セクションには、次の表で説明されている設定が表示されます。

図 *137* : クラスタのヘルスモニターの設定

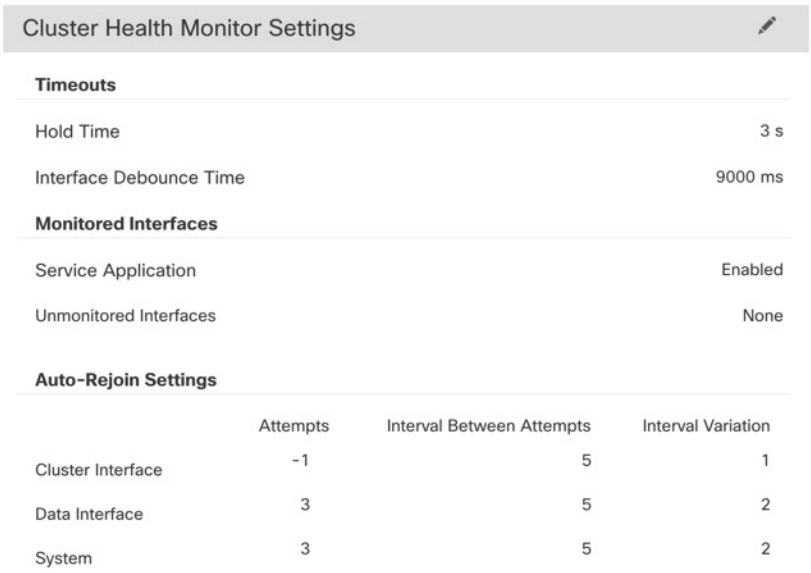


表 *30 : [*クラスタヘルスモニターの設定（***Cluster Health Monitor Settings***）*]* セクションテーブルのフィールド

フィールド	説明
タイムアウト（Timeouts）	
保留時間（Hold Time）	指定できる範囲は 0.3 ～ 45 秒です。デフォルトは 3 秒です。ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間（Interface Debounce Time）	指定できる範囲は 300 ～ 9000 ミリ秒です。デフォルトは 500 ms です。インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると見なされ、クラスタからノードが削除されるまでの時間です。
Monitored Interfaces（モニタリング対象インターフェイス）	インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。
サービスアプリケーション（Service Application）	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。
モニタリング対象外のインターフェイス（Unmonitored Interfaces）	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定（Auto-Rejoin Settings）	
クラスタインターフェイス（Cluster Interface）	クラスタ制御リンクに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは -1（無制限）です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 1 倍です。試行ごとに間隔を長くするかどうかを定義します。

フィールド	説明
データインターフェイス（Data Interfaces）	データインターフェイスに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。
システム（System）	内部エラーが発生した後に自動再結合の設定を表示します。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。

（注） システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

これらの設定は、このセクションから変更できます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI やBVIなどの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

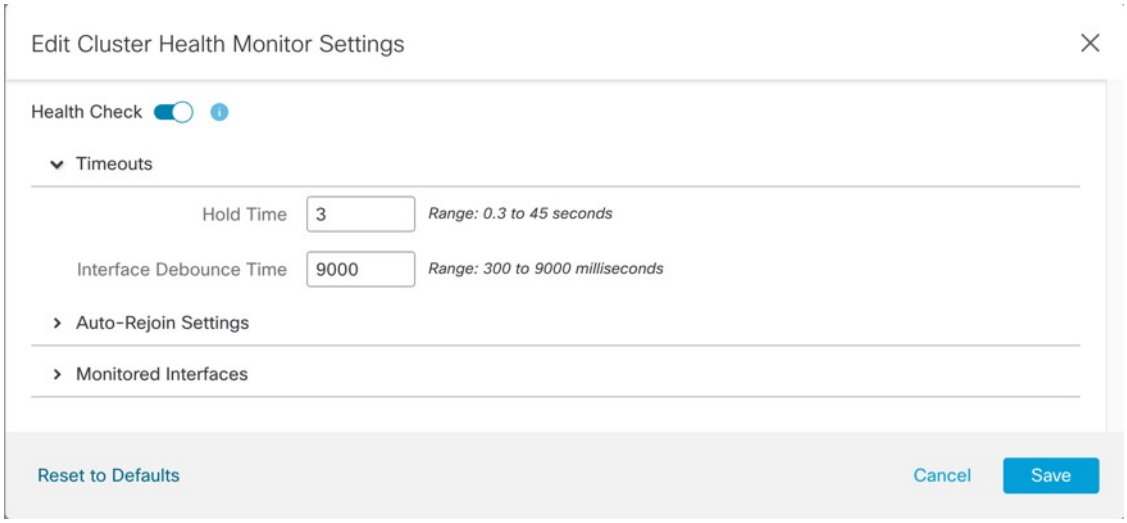
ステップ 2 変更するクラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [クラスタ（Cluster）] をクリックします。

ステップ 4 [クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）] セクションで、[編集（Edit）]（✎） をクリックします。

ステップ 5 [ヘルスチェック（Health Check）] スライダをクリックして、システムのヘルスチェックを無効にします。

図 *138* : システムヘルスチェックの無効化



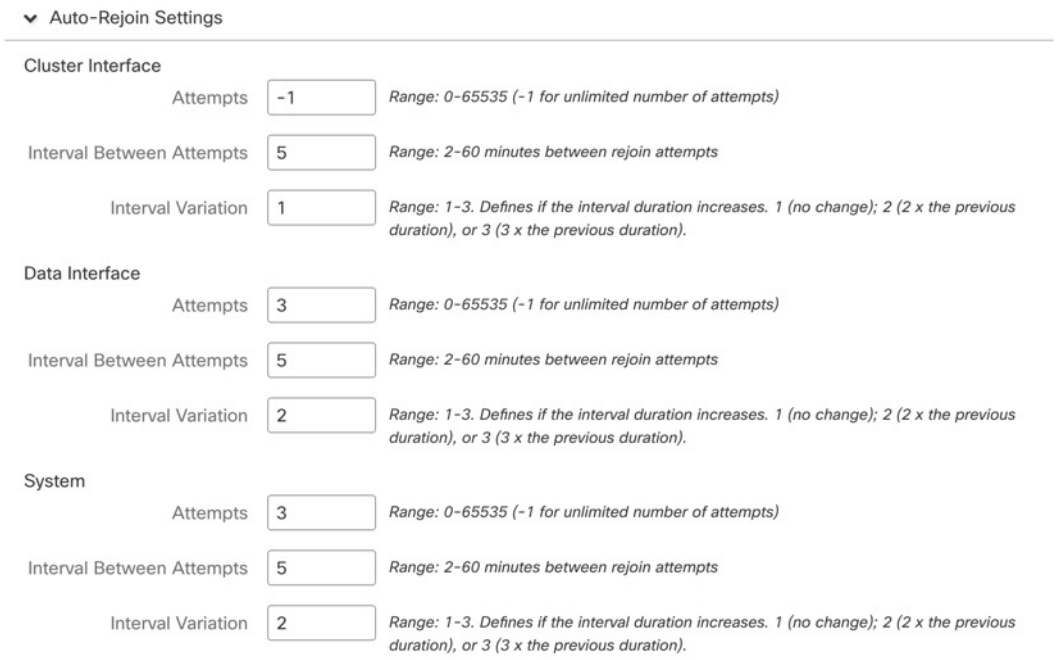
何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間（Hold Time）]：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ～ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間（Interface Debounce Time）]：デバウンス時間は 300 ～ 9000 ms の範囲で値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 *139* : 自動再結合の設定

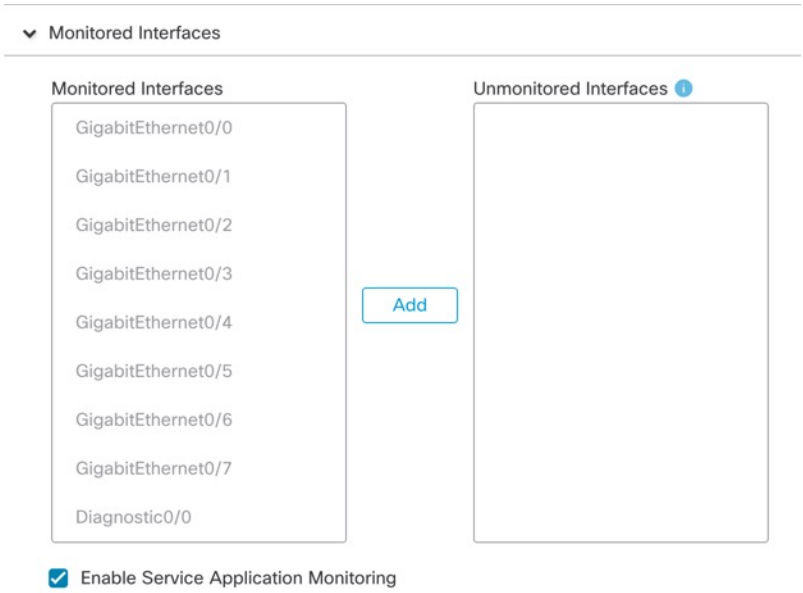


[クラスタインターフェイス（Cluster Interface）]、[データインターフェイス（Data Interface）]、および[システム（System）]に次の値を設定します（内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります）。

- [試行数（Attempts）]：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。[クラスタインターフェイス（Cluster Interface）] のデフォルト値は -1（無制限）です。[データインターフェイス（Data Interface）] と [システム（System）] のデフォルト値は 3 です。
- [試行の間隔（Interval Between Attempts）]：再結合試行の間隔を 2 ～ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [間隔のバリエーション（Interval Variation）]：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、[クラスタインターフェイス（Cluster Interface）] の場合は **1**、[データインターフェイス（Data Interface）] および [システム（System）] の場合は **2** です。

ステップ 8 [モニタリング対象のインターフェイス（Monitored Interfaces）] または [モニタリング対象外のインターフェイス（Unmonitored Interfaces）] ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリングを有効にする（Enable Service Application Monitoring）] をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 *140 :* モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングを無効にできます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

クラスタノードの管理

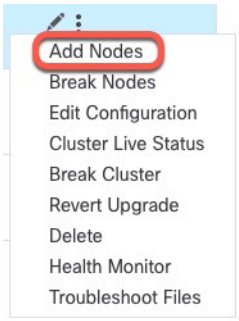
新しいクラスタノードの追加

1 つ以上の新しいクラスタノードを既存のクラスタに追加できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、クラスタの [その他（More）] (⋮) をクリックして [ノードを追加（Add Nodes）] を選択します。

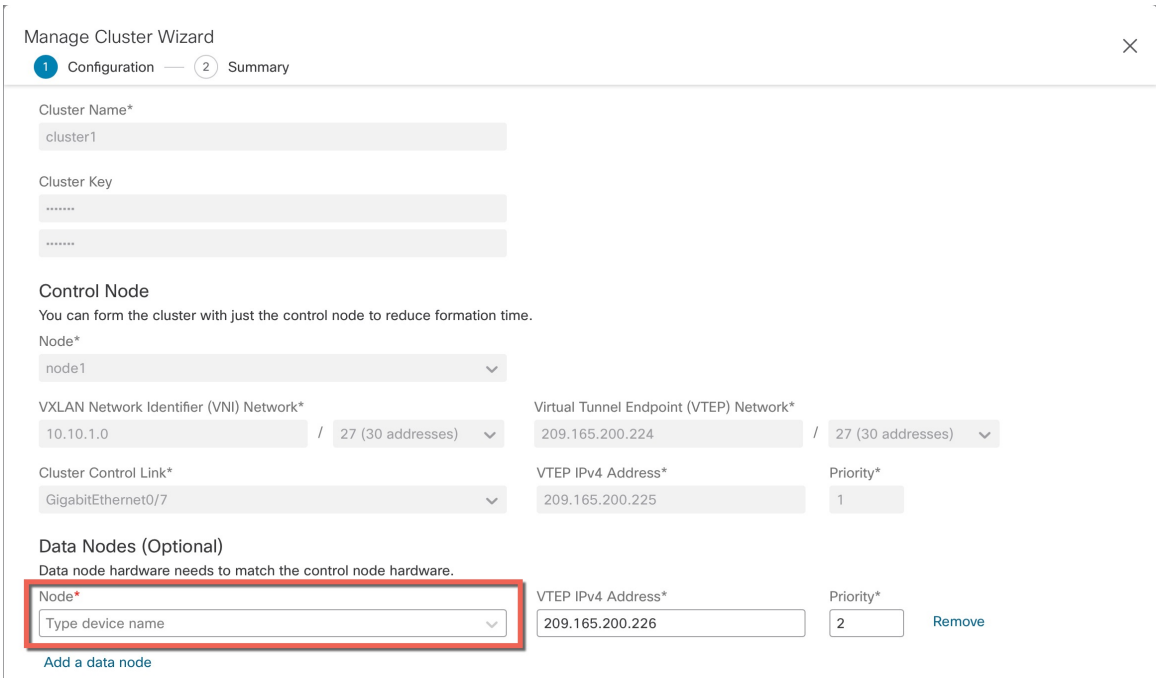
図 *141 : ノードの追加*



[クラスタの管理（Manage Cluster）] ウィザードが表示されます。

ステップ 2 [ノード（Node）] メニューからデバイスを選択し、必要に応じて IP アドレスと優先順位を調整します。

図 *142 : [クラスタの管理（Manage Cluster）] ウィザード*

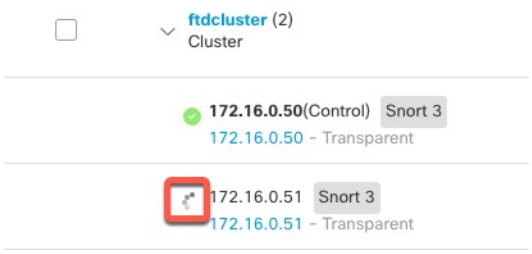


ステップ 3 さらにノードを追加するには、[データノードを追加（Add a data node）] をクリックします。

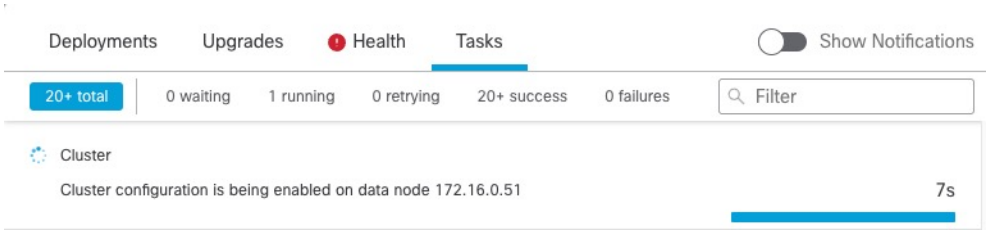
ステップ 4 [続行（Continue）] をクリックします。[概要（Summary）] を確認し、[保存（Save）] をクリックします。

現在登録されているノードには、ロードアイコンが表示されます。

図 *143* : ノードの登録



クラスタノードの登録をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。



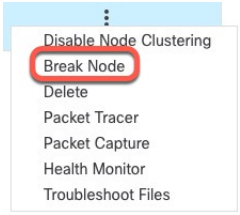
ノードの除外

ノードがスタンドアロンデバイスになるように、クラスからノードを削除できます。クラスタ全体を解除しない限り、制御ノードを除外することはできません。データノードの設定は消去されます。

手順

ステップ 1 [デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択し、除外するノードの [その他（More）] (⋮) をクリックして [ノードを除外（Break Node）] を選択します。

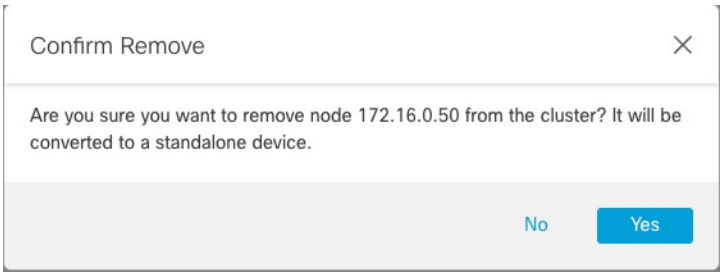
図 *144* : ノードの除外



オプションで、クラスタの [詳細（More）] メニューから [ノードを除外（Break Nodes）] を選択して 1 つ以上のノードを除外できます。

ステップ 2 除外の確定を求められたら、[はい（Yes）] をクリックします。

図 *145* : 解除の確定



クラスタノードの除外をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。

クラスタの解除

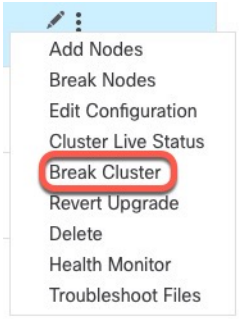
クラスタを解除し、すべてのノードをスタンドアロンデバイスに変換できます。制御ノードはインターフェイスとセキュリティポリシーの設定を保持しますが、データノードでは設定が消去されます。

手順

ステップ 1 ノードを照合することにより、すべてのクラスタノードが Firewall Management Center で管理されていることを確認します。クラスタノードの照合 （420 ページ）を参照してください。

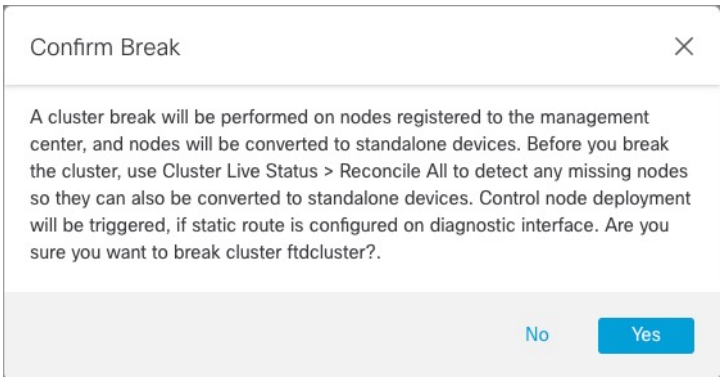
ステップ 2 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、クラスタの [その他（More）] (⋮) をクリックして [クラスタを解除（Break Cluster）] を選択します。

図 *146* : クラスタの解除



ステップ 3 クラスタを解除するよう求められたら、[はい（Yes）] をクリックします。

図 *147* : 解除の確定



クラスタの解除をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。

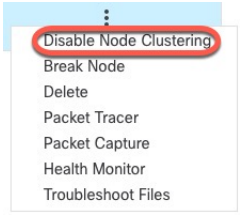
クラスタリングを無効にする

ノードの削除に備えて、またはメンテナンスのために一時的にノードを非アクティブ化する場合があります。この手順は、ノードを一時的に非アクティブ化するためのものです。ノードは引き続き Firewall Management Center のデバイスリストに表示されます。ノードが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。

手順

ステップ 1 無効にするユニットに対して、[デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択して [その他（More）] をクリックし、[ノードのクラスタリングを無効にする（Disable Node Clustering）] を選択します。

図 *148* : クラスタリングを無効にする



制御ノードでクラスタリングを無効にすると、データノードの1つが新しい制御ノードになります。なお、中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるため、新しい制御ノード上で接続を再確立する必要があります。制御ノードがクラスタ内の唯一のノードである場合、そのノードでクラスタリングを無効にすることはできません。

ステップ 2 ノードのクラスタリングを無効にすることを確認します。

ノードは、[デバイス（Devices）]>[デバイス管理（Device Management）] リストの名前の横に [（無効（Disabled））] と表示されます。

ステップ 3 クラスタリングを再び有効にするには、クラスタへの再参加（417ページ）を参照してください。

クラスタへの再参加

（たとえば、インターフェイスで障害が発生したために）ノードがクラスタから削除された場合、または手動でクラスタリングを無効にした場合は、クラスタに手動で再参加する必要があります。クラスタへの再参加を試行する前に、障害が解決されていることを確認します。ノードをクラスタから削除できる理由の詳細については、「クラスタへの再参加（437ページ）」を参照してください。

手順

ステップ 1 再度有効にするユニットに対して、[デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択して [その他（More）] (⋮) をクリックし、[ノードのクラスタリングを有効にする（Enable Node Clustering）] を選択します。>

ステップ 2 ノードのクラスタリングを有効にすることを確認します。

制御ノードの変更

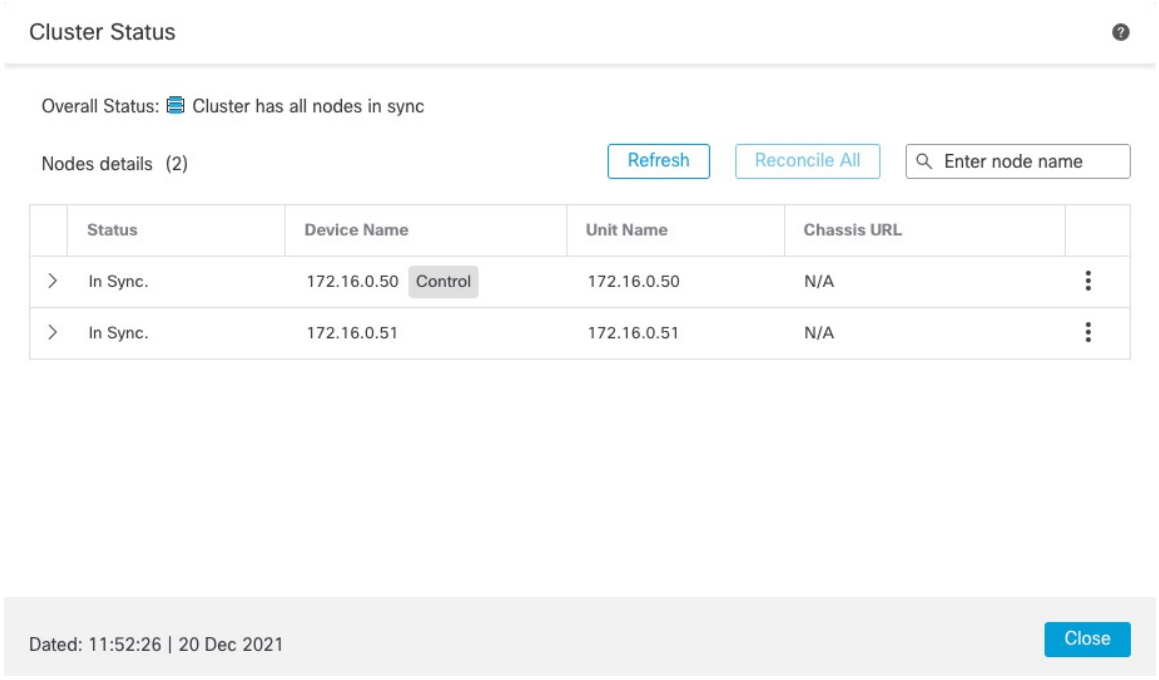
注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするユニットを厳密に指定する必要がある場合は、このセクションの手順を使用します。なお、中央集中型機能については、いずれかの方法で制御ノード変更を強制するとすべての接続がドロップされるため、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [その他（More）] > [クラスタのライブステータス（Cluster Live Status）] を選択して [クラスタステータス（Cluster Status）] ダイアログボックスを開きます。

図 *149*：クラスタのステータス



ステップ 2 制御ユニットにしたいユニットについて、[その他（More）] >[ロールを制御に変更（Change Role to Control）] を選択します。

ステップ 3 ロールの変更を確認するように求められます。チェックボックスをオンにして [OK] をクリックします。

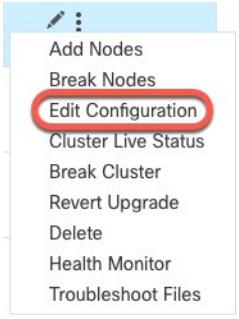
クラスタ設定の編集

クラスタ設定を編集できます。ノードのVTEP IPアドレスまたはノードの優先順位以外の値を変更すると、クラスタは自動的に失われて再構築されます。クラスタが再形成されるまで、トラフィックの中断が発生する可能性があります。ノードのVTEP IPアドレスやノードの優先順位を変更すると、影響を受けるノードのみが除外されてクラスタに再追加されます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、クラスタの [その他（More）] (⋮) をクリックして [設定を編集（Edit Configuration）] を選択します。

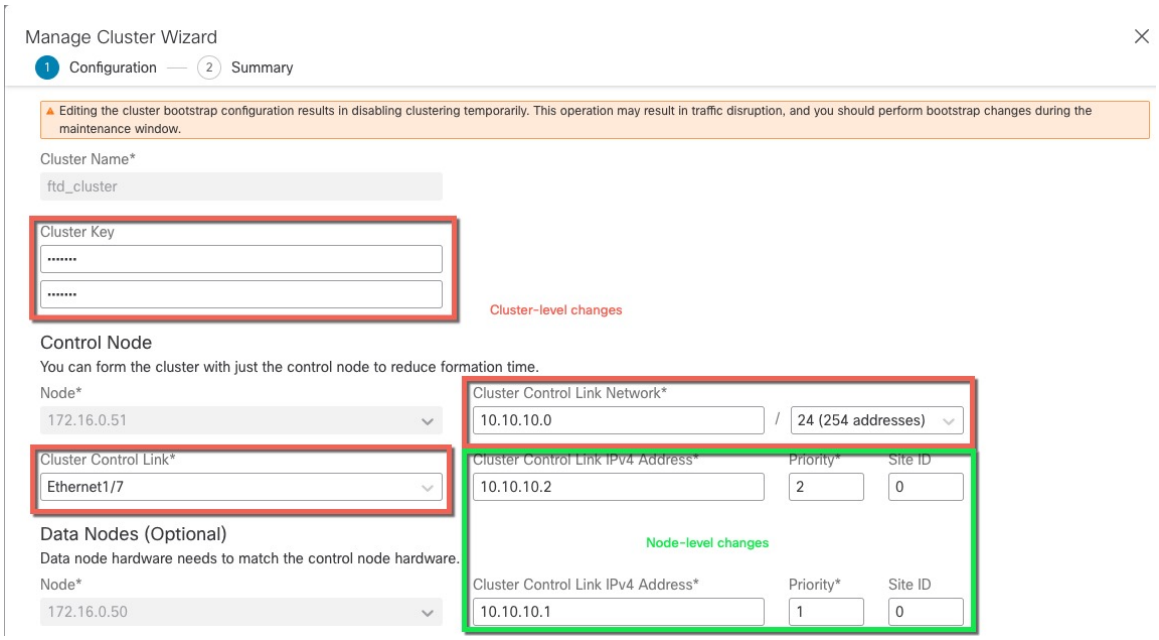
図 *150* : 設定の編集



[クラスタの管理（Manage Cluster）] ウィザードが表示されます。

ステップ 2 クラスタ設定を更新します。

図 *151 : [*クラスタの管理（***Manage Cluster***）*]*ウィザード



ステップ 3 [続行（Continue）] をクリックします。[概要（Summary）] を確認し、[保存（Save）] をクリックします。

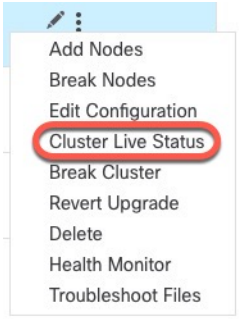
クラスタノードの照合

クラスタノードの登録に失敗した場合は、デバイスから Firewall Management Center に対してクラスタメンバーシップを照合できます。たとえば、Firewall Management Center が特定のプロセスで占領されているか、ネットワークに問題がある場合、データノードの登録に失敗することがあります。

手順

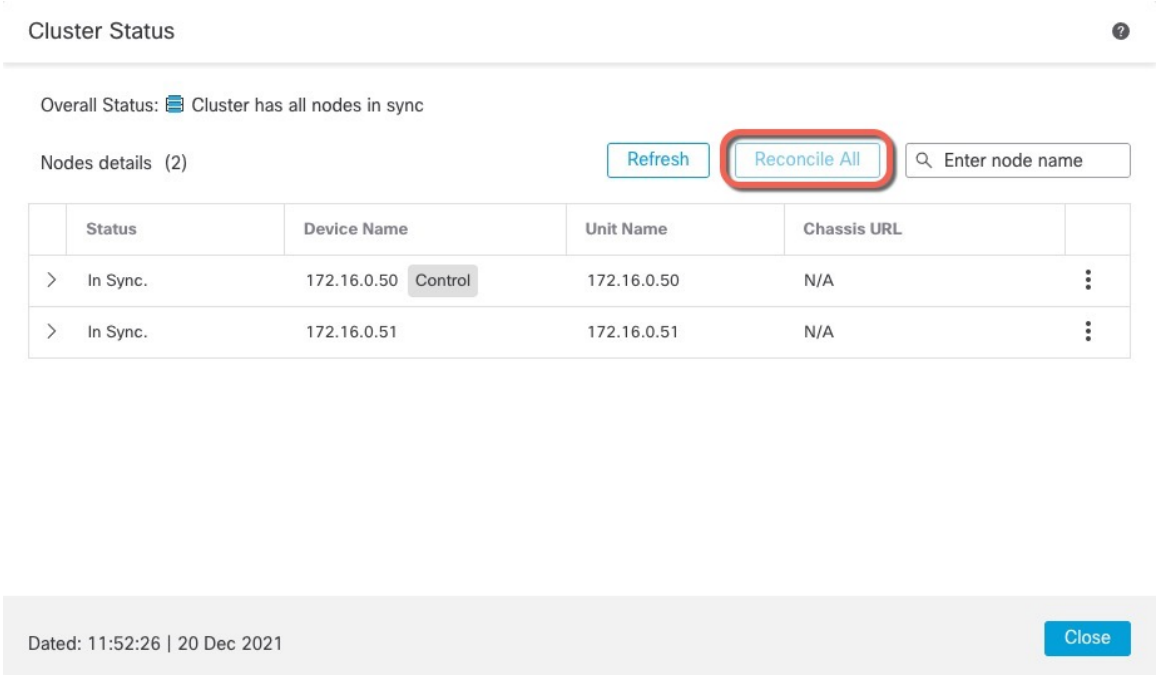
ステップ 1 クラスタの **[Devices]** > **[Device Management]** > [その他（More）] (⋮) を選択し、次に [Cluster Live Status] を選択して [Cluster Status] ダイアログボックスを開きます。

図 *152 :* クラスタのライブステータス



ステップ 2 [すべてを照合（Reconcile All）] をクリックします。

図 *153 :* すべてを照合



クラスタ ステータスの詳細については、クラスタのモニタリング（423 ページ）を参照してください。

クラスタまたはノードの削除（登録解除）と新しいFirewall Management Center への登録

Firewall Management Center からクラスタを登録解除できます。これにより、クラスタはそのまま維持されます。クラスタを新しい Firewall Management Center に追加する場合は、クラスタを登録解除することができます。

クラスタからノードを除外することなく、Firewall Management Center からノードを登録解除することもできます。ノードは Firewall Management Center に表示されていませんが、まだクラスタの一部であり、引き続きトラフィックを渡して制御ノードになることも可能です。現在動作している制御ノードを登録解除することはできません。Firewall Management Center から到達不可能になったノードは登録解除してもかまいませんが、管理接続をトラブルシューティングする間、クラスタの一部として残しておくことも可能です。

クラスタの登録解除：

- Firewall Management Center とクラスタとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからクラスタが削除されます。
- クラスタのプラットフォーム設定ポリシーで、NTP を使用して Firewall Management Center から時間を受信するように設定されている場合は、クラスタがローカル時間管理に戻されます。
- 設定はそのままになるため、クラスタはトラフィックの処理を続行します。

  NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Firewall Management Center にクラスタを再登録すると、設定が削除されるため、クラスタはその時点でトラフィックの処理を停止します。クラスタ設定はそのまま維持されるため、クラスタ全体を追加できます。登録時にアクセス コントロール ポリシーを選択できますが、トラフィックを再度処理する前に、登録後に他のポリシーを再適用してから設定を展開する必要があります。

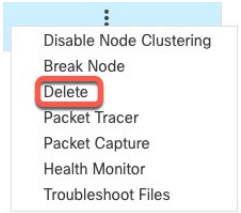
始める前に

この手順では、いずれかのノードへの CLI アクセスが必要です。

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** の順に選択し、クラスタかノードの [その他（More）] (⋮) をクリックして [登録解除] **[削除（Delete）]** を選択します。

図 *154* : クラスタまたはノードの削除



ステップ 2 クラスタかノードを削除するよう求められたら、[はい（Yes）] をクリックします。

ステップ 3 クラスタメンバーの 1 つを新しいデバイスとして追加することにより、クラスタを新しい（または同じ）Firewall Management Center に登録できます。

a) 1 つのクラスタノードの CLI に接続し、**configure manager add** コマンドを使用して新しい Firewall Management Center を識別します。「Threat Defense 管理インターフェイスの CLI での変更」を参照してください。

b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、[デバイスの追加（Add Device）] をクリックします。

クラスタノードの 1 つをデバイスとして追加するだけで、残りのクラスタノードが検出されます。

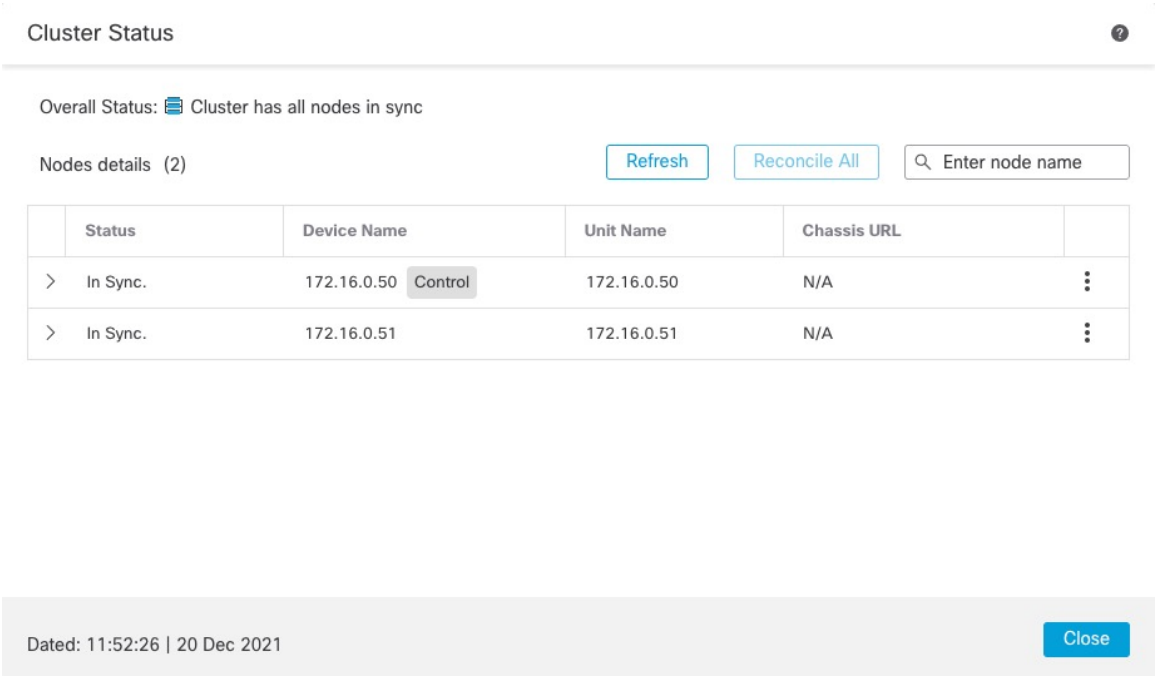
ステップ 4 削除したノードを再度追加する方法については、「クラスタノードの照合（420 ページ）」を参照してください。

クラスタのモニタリング

クラスタは、Firewall Management Center と Firewall Threat Defense の CLI でモニターできます。

- [クラスタステータス（Cluster Status）] ダイアログボックスには、[デバイス（Devices）] > [デバイス管理（Device Management）] > [その他（More）] (⋮) アイコンから、または [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] ページ > [全般（General）] 領域 > [クラスタのライブステータス（Cluster Live Status）] リンクからアクセスできます。 > > >

図 155 : クラスタのステータス



制御ノードには、そのロールを示すグラフィックインジケータがあります。

クラスタメンバーステータスには、次の状態が含まれます。

- 同期中（In Sync）：ノードは Firewall Management Center に登録されています。
- 登録の保留中（Pending Registration）：ノードはクラスタの一部ですが、まだ Firewall Management Center に登録されていません。ノードの登録に失敗した場合は、[すべてを照合（Reconcile All）] をクリックして登録を再試行できます。
- クラスタリングが無効（Clustering is disabled）：ノードは Firewall Management Center に登録されていますが、クラスタの非アクティブなメンバーです。クラスタリング設定は、後で再有効化する予定がある場合は変更せずに維持できます。また、ノードをクラスタから削除することも可能です。
- クラスタに参加中...（Joining cluster...）：ノードがシャーシ上でクラスタに参加していますが、参加は完了していません。参加後に Firewall Management Center に登録されます。

ノードごとに [概要（Summary）] と [履歴（History）] を表示できます。

図 *156* : ノードの *[*概要（*Summary***）*]***

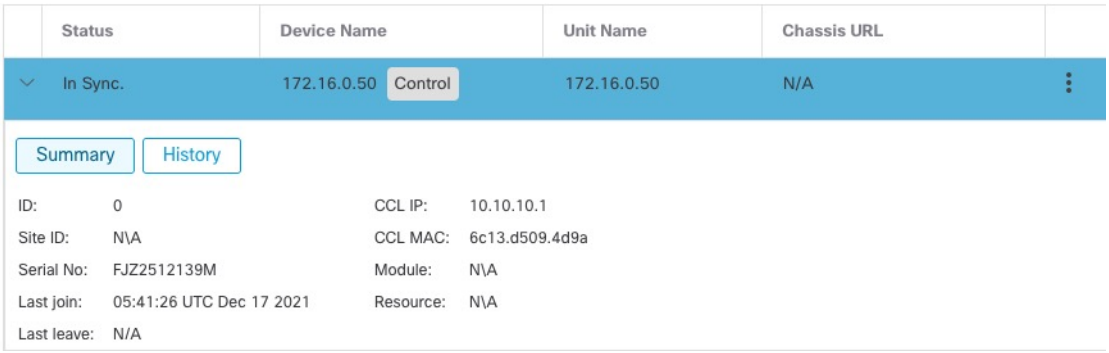
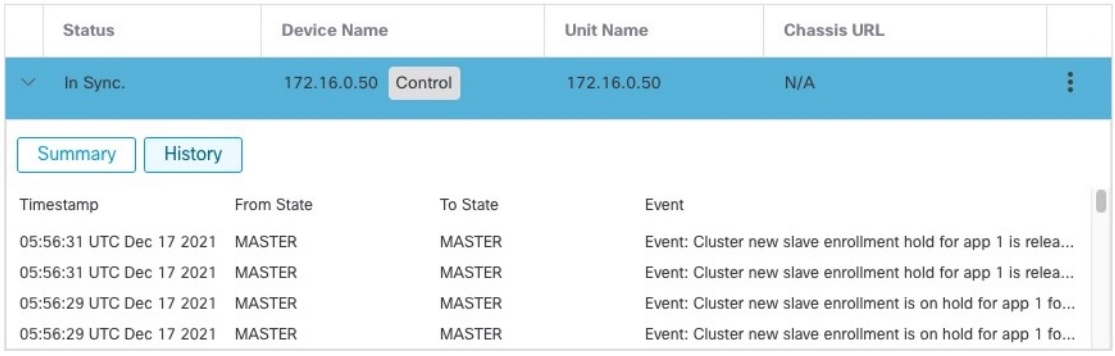


図 *157* : ノードの *[*履歴（*History***）*]***



- [システム（System）]（⚙）> [Tasks] ページ。

  [タスク（Tasks）]ページには、ノードが登録されるたびにクラスタ登録タスクの最新情報が表示されます。

- [デバイス（Devices）] > [デバイス管理（Device Management）] > cluster_name。 >

デバイスの一覧表示ページでクラスタを展開すると、IPアドレスの横にそのロールが表示されている制御ノードを含む、すべてのメンバーノードを表示できます。登録中のノードには、ロード中のアイコンが表示されます。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

クラスタ ヘルス モニター ダッシュボード

クラスタのヘルスモニター

Firewall Threat Defense がクラスタの制御ノードである場合、Firewall Management Center はデバイス メトリック データ コレクタからさまざまなメトリックを定期的に収集します。クラスタの ヘルスモニターは、次のコンポーネントで構成されています。

- 概要ダッシュボード：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。
  - トポロジセクションには、クラスタのライブステータス、個々の脅威防御の状態、脅威防御ノードのタイプ（制御ノードまたはデータノード）、およびデバイスの状態が表示されます。デバイスの状態は、[無効（Disabled）]（デバイスがクラスタを離れたとき）、[初期状態で追加（Added out of box）]（パブリッククラウドクラスタでFirewall Management Center に属していない追加ノード）、または [標準（Normal）]（ノードの理想的な状態）のいずれかです。
  - クラスタの統計セクションには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するクラスタの現在のメトリックが表示されます。

（注） CPU とメモリのメトリックは、データプレーンと Snort の使用量の個々の平均を示します。

  - メトリックチャート、つまり、CPU使用率、メモリ使用率、スループット、および接続数は、指定された期間におけるクラスタの統計を図表で示します。

- 負荷分散ダッシュボード：2 つのウィジェットでクラスタノード全体の負荷分散を表示します。

- 分布ウィジェットには、クラスタノード全体の時間範囲における平均パケットおよび接続分布が表示されます。このデータは、ノードによって負荷がどのように分散されているかを示します。このウィジェットを使用すると、負荷分散の異常を簡単に特定して修正できます。
- ノード統計ウィジェットには、ノードレベルのメトリックが表形式で表示されます。クラスタノード全体の CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するメトリックデータが表示されます。このテーブルビューでは、データを関連付けて、不一致を簡単に特定できます。

- メンバー パフォーマンス ダッシュボード：クラスタノードの現在のメトリックを表示します。セレクタを使用してノードをフィルタリングし、特定ノードの詳細を表示できます。メトリックデータには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数が含まれます。
- CCL ダッシュボード：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- 時間範囲：さまざまなクラスタ メトリック ダッシュボードやウィジェットに表示される情報を制限するための調整可能な時間枠。
- カスタムダッシュボード：クラスタ全体のメトリックとノードレベルのメトリックの両方に関するデータを表示します。ただし、ノードの選択は脅威防御メトリックにのみ適用され、ノードが属するクラスタ全体には適用されません。

クラスタ ヘルスの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

クラスタヘルスモニターは、クラスタとそのノードのヘルスステータスの詳細なビューを提供します。このクラスタヘルスモニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

- Firewall Management Center の 1 つ以上のデバイスからクラスタを作成しているかを確認します。

手順

ステップ 1 [システム（System）]（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択します。

[モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、ノード固有のヘルスモニターにアクセスします。

ステップ 2 デバイスリストで [展開（Expand）]（ > ）と [折りたたみ（Collapse）]（ ⌄ ）をクリックして、管理対象のクラスタデバイスのリストを展開または折りたたみます。

ステップ 3 クラスタのヘルス統計を表示するには、クラスタ名をクリックします。デフォルトでは、クラスタモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- [概要（Overview）]：他の事前定義されたダッシュボードからの主要なメトリックを表示します。ノード、CPU、メモリ、入力レート、出力レート、接続統計情報、NAT 変換情報などが含まれます。
- [負荷分散（Load Distribution）]：クラスタノード間のトラフィックとパケットの分散。
- [メンバーパフォーマンス（Member Performance）]：CPU 使用率、メモリ使用率、入力スループット、出力スループット、アクティブな接続、および NAT 変換に関するノードレベルの統計情報。
- [CCL]：インターフェイスのステータスおよび集約トラフィックの統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているクラスタメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で 1 時間前（デフォルト）から、最長では 2 週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を 5 分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの展開アイコンをクリックします。

展開アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されます。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 （ノード固有のヘルスモニターの場合）ページ上部のデバイス名の右側にあるアラート通知で、ノードの正常性アラートを確認します。

正常性アラートにポインタを合わせると、ノードの正常性の概要が表示されます。ポップアップウィンドウに、上位 5 つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 7 （ノード固有のヘルスモニターの場合）デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- [Snort]：Snort プロセスに関連する統計情報。
- [ASP ドロップ（ASP drops）]：さまざまな理由でドロップされたパケットに関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 正常性モニターの右上隅にあるプラス記号[新しいダッシュボードの追加（Add New Dashboard）]（＋）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタムダッシュボードを作成します。

クラスタ全体のダッシュボードの場合は、クラスタのメトリックグループを選択してから、メトリックを選択します。

クラスタメトリック

クラスタのヘルスモニターは、クラスタとそのノードに関連する統計情報と、負荷分散、パフォーマンス、および CCL トラフィックの統計データの集約結果を追跡します。

表 *31* : クラスタメトリック

メトリック	説明	フォーマット（Format）
CPU	クラスタノード上の CPU メトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
メモリ	クラスタノード上のメモリメトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
データスループット	クラスタの着信および発信データトラフィックの統計。	バイト

メトリック	説明	フォーマット（Format）
CCL スループット	クラスタの着信および発信 CCL トラフィックの統計。	バイト
接続	クラスタ内のアクティブな接続数。	番号
NAT 変換数	クラスタの NAT 変換数。	番号
分布	1 秒ごとのクラスタ内の接続分布数。	番号
パケット	クラスタ内の1秒ごとのパケット配信の件数。	番号

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

Threat Defense の機能とクラスタリング

Firewall Threat Defense の一部の機能はクラスタリングではサポートされず、一部は制御ユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

サポートされていない機能とクラスタリング

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

（注） クラスタリングでもサポートされていない FlexConfig 機能（WCCP インスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーション ガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- リモート アクセス VPN（SSL VPN および IPsec VPN）
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- 仮想トンネルインターフェイス（VTI）
- 高可用性
- 統合ルーティングおよびブリッジング
- Firewall Management Center UCAPL/CC モード

- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

（注） クラスタリングでも一元化されている FlexConfig 機能（RADIUS インスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーションガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- スタティック ルート モニタリング

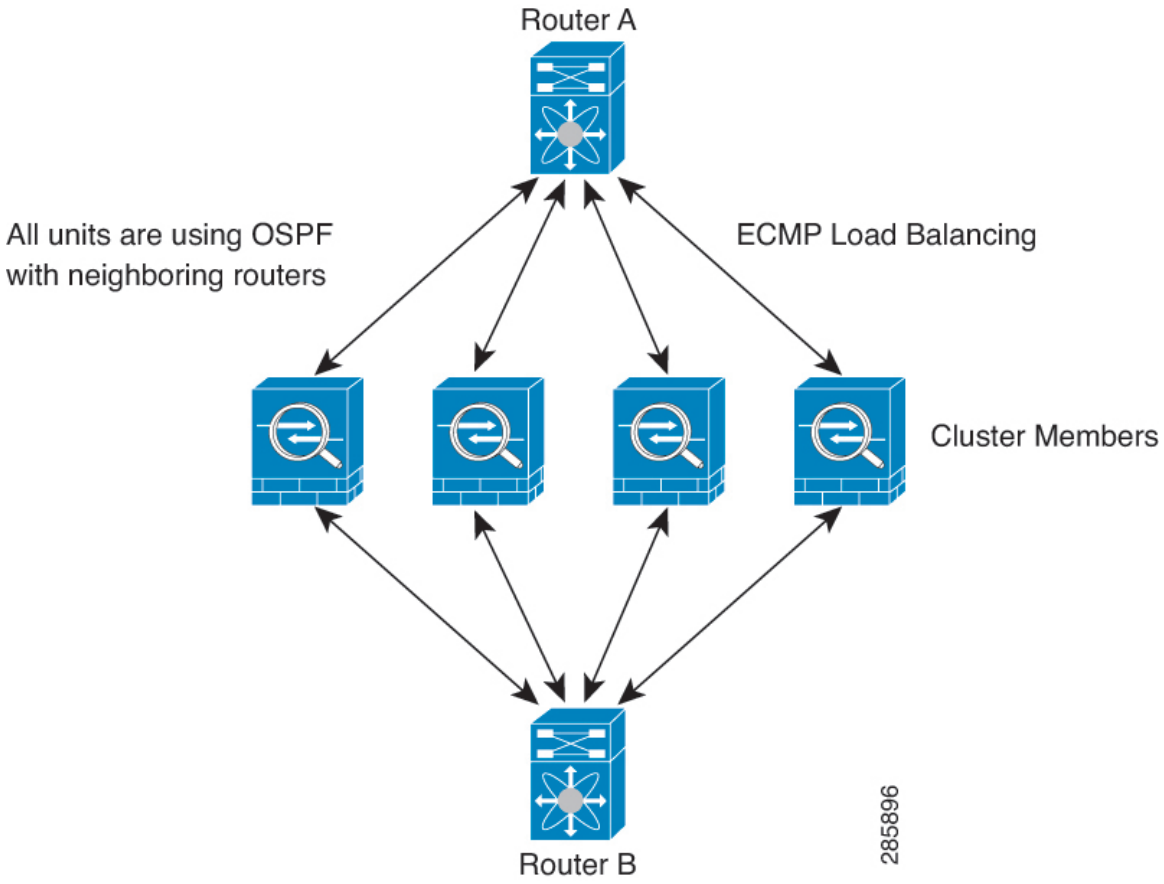
接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

ダイナミック ルーティングおよびクラスタリング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *158 :* 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタプールを設定する必要があります。

FTP とクラスタリング

- FTPデータ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の Firewall Threat Defense に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない Firewall Threat Defense に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NATオーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。
- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。
- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード

間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。

- クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。

- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET

- TFTP
- XDMCP
- SIP

- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

SNMP とクラスタリング

SNMP エージェントは、個々の Firewall Threat Defense を、その [診断（Diagnostic）] 診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングで SNMPv3 を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3 ユーザは新しいノードに複製されません。SNMPv3 ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

syslog とクラスタリング

- クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

VPN とクラスタリング

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノードが選定されたときに、VPN接続を再確立する必要があります。

PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80%になります。

たとえば、モデルが単独稼働で約 10 Gbps のトラフィックを処理できる場合、8 ユニットのクラスタでは、最大合計スループットは 80 Gbps（8 ユニット x 10 Gbps）の約 80% で 64 Gbps になります。

制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。

（注） 最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままで

す。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。

5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。

（注） ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

クラスタ内のハイアベイラビリティ

クラスタリングは、ノードとインターフェイスの正常性をモニターし、ノード間で接続状態を複製することにより、ハイアベイラビリティを実現します。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからハートビートパケットまたはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション2のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。

インターフェイス モニタリング

各ノードは、使用中のすべての指名されたハードウェアインターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

すべての物理インターフェイスがモニタリングされます。ただし、モニタリングできるのは、名前付きインターフェイスのみです。ヘルスチェックは、インターフェイスごとに、モニターリングをオプションで無効にすることができます。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。ノードは 500 ミリ秒後に削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、Firewall Threat Defense は自動的にクラスタへの再参加を試みます。

（注） Firewall Threat Defenseが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理/診断インターフェイスのみがトラフィックを送受信できます。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- 最初に参加するときに障害が発生したクラスタ制御リンク：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：FTDは、無限に5分ごとに自動的に再参加を試みます。
- データ インターフェイスの障害：Firewall Threat Defense は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、Firewall Threat Defense アプリケーションはクラスタリングを無効にします。データ インターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ノードは再起動するとクラスタに再参加します。Firewall Threat Defense アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。
- 障害が発生した設定の展開：FMC から新しい設定を展開し、展開が一部のクラスタメンバーでは失敗したものの、他のメンバーでは成功した場合、失敗したノードはクラスタから削除されます。クラスタリングを再度有効にして手動でクラスタに再参加する必要があります。制御ノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。すべてのデータノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *32*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システムアップタイムをトラッキングします。
ARP Table	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	Yes	—
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—

クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- バックアップオーナー：オーナーから受信した TCP/UDP ステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバッ

クアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  ICMP/ICMPv6 ハッシュの詳細：

  - エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
  - 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
  - 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

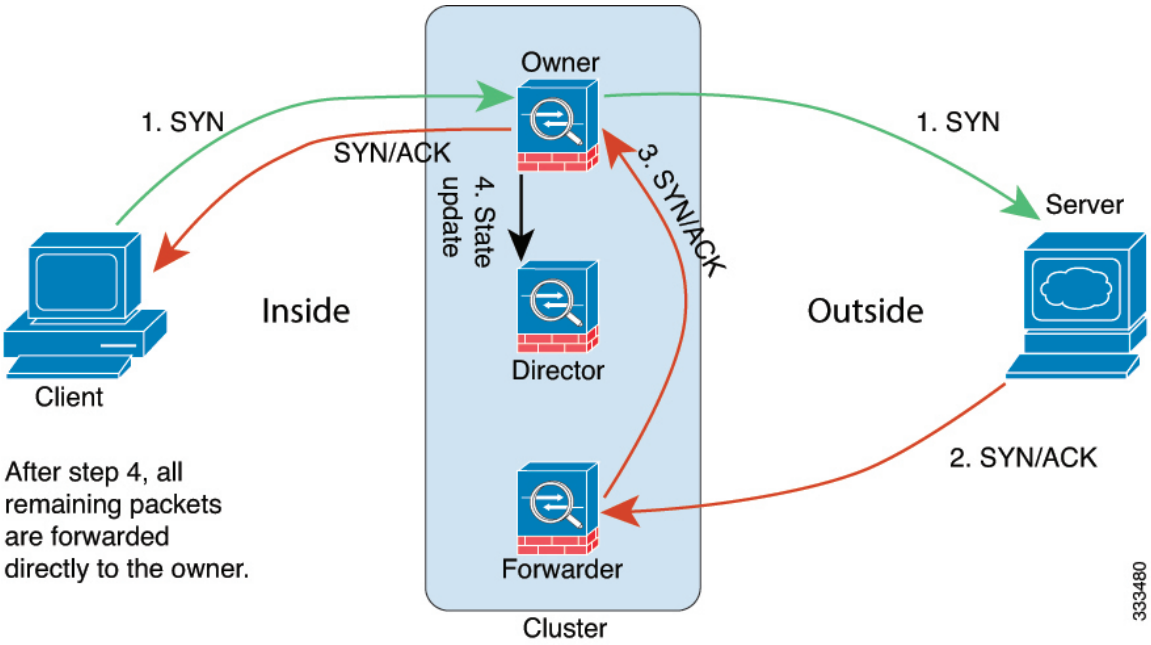
- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

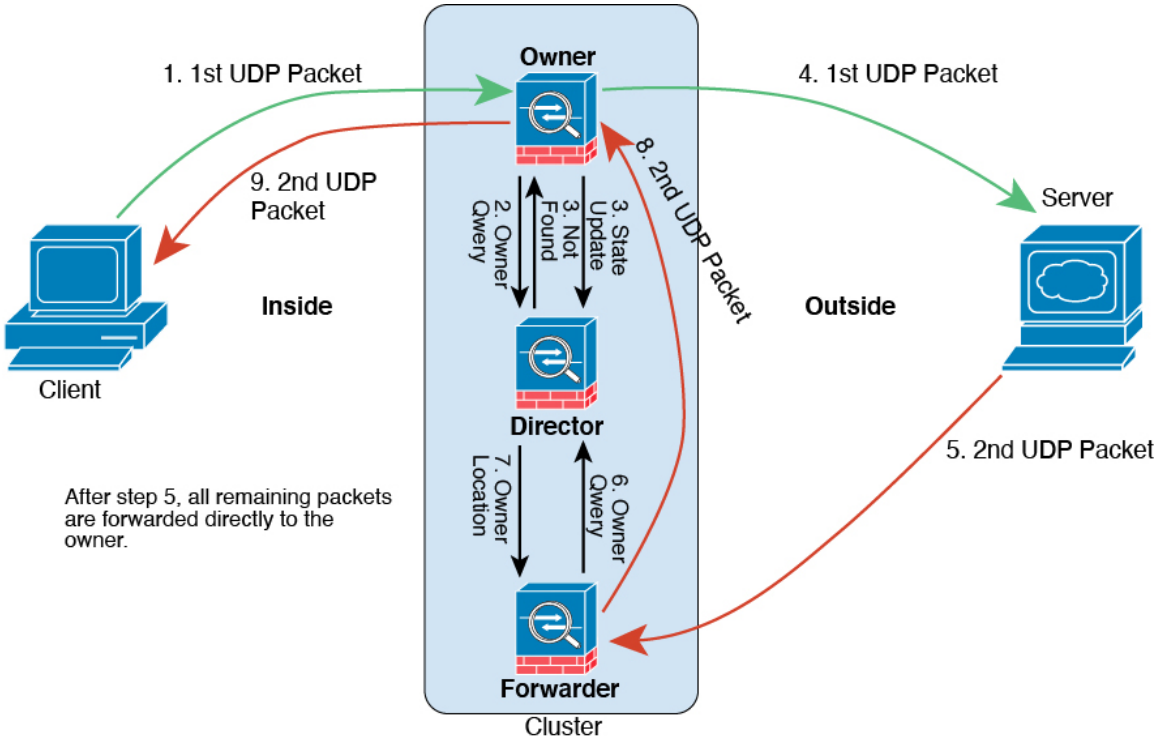


1. SYN パケットがクライアントから発信され、Firewall Threat Defense の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firewall Threat Defense（ロード バランシング方法に基づく）に配信されます。この Firewall Threat Defense はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

1. 図 *159 : ICMP* および *UDP* データフロー

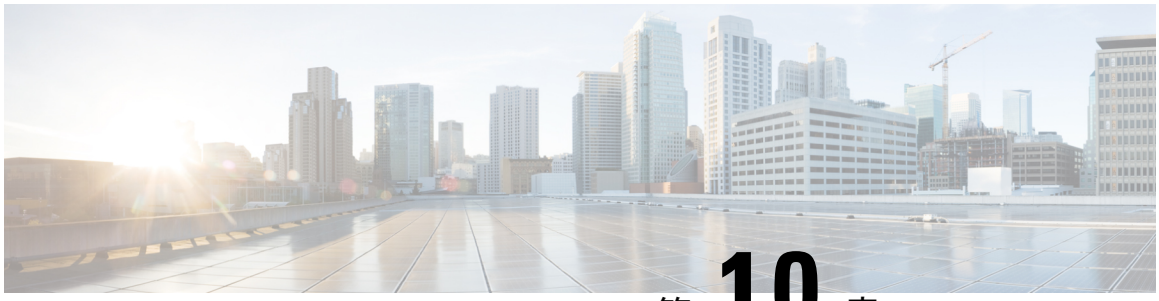


UDP パケットがクライアントから発信され、1 つの Firewall Threat Defense（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

プライベートクラウドでの Threat Defense Virtual のクラスタリング履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタのヘルスモニターの設定	7.3.0	いずれか	クラスタのヘルスモニター設定を編集できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **クラスタ（Cluster）** > **[クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）]** （注） 以前に FlexConfig を使用してこれらの設定を行った場合は、展開前に必ず FlexConfig の設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。
クラスタ ヘルス モニター ダッシュボード	7.3.0	いずれか	クラスタのヘルス モニター ダッシュボードでクラスタの状態を表示できるようになりました。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]**
VMware および KVM の Firewall Threat Defense Virtual のクラスタリング	7.2.0	7.2.0	Firewall Threat Defense Virtual は VMware および KVM で最大 4 ノードの個別インターフェイスのクラスタリングをサポートします。 新規/変更された画面： • [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタの追加（Add Cluster）] • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[詳細（More）]**メニュー • **[Devices]** > **[Device Management]** > **[Cluster]** サポートされているプラットフォーム：VMware および KVM 上の Firewall Threat Defense Virtual



第 10 章

パブリッククラウドでの Threat Defense Virtual のクラスタリング

クラスタリングを利用すると、複数の Firewall Threat Defense Virtual をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。以下のパブリック クラウド プラットフォームを使用して、パブリッククラウドに Firewall Threat Defense Virtual クラスタを展開できます。

- Amazon Web Services（AWS）
- Microsoft Azure
- Google Cloud Platform（GCP）

現在は、ルーテッド ファイアウォール モードのみがサポートされます。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「サポートされていない機能とクラスタリング （528 ページ）」を参照してください。

- パブリッククラウドにおける Threat Defense Virtual クラスタリングについて （446 ページ）
- Threat Defense Virtual クラスタリングのライセンス （449 ページ）
- Threat Defense Virtual クラスタリングの要件および前提条件 （449 ページ）
- Threat Defense Virtual クラスタリングのガイドライン （451 ページ）
- AWS でクラスタを展開する （453 ページ）
- Azure でクラスタを展開する （474 ページ）
- GCP でのクラスタの展開 （494 ページ）
- Management Center へのクラスタの追加（手動展開） （504 ページ）
- クラスタのヘルスモニターの設定 （511 ページ）
- クラスタノードの管理 （517 ページ）
- クラスタのモニタリング （520 ページ）
- クラスタのアップグレード （526 ページ）

• クラスタリングの参考資料 （527 ページ）
• パブリッククラウドの Threat Defense Virtual クラスタリングの履歴 （541 ページ）

パブリッククラウドにおける Threat Defense Virtual クラスタリングについて

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは 1 つのデバイスとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離されたネットワーク。VXLAN インターフェイスを使用したクラスタ制御リンクと呼ばれます。レイヤ 3 物理ネットワーク上でレイヤ 2 仮想ネットワークとして機能する VXLAN により、Firewall Threat Defense Virtual はクラスタ制御リンクを介してブロードキャスト/マルチキャストメッセージを送信できます。
- ロードバランサ：パブリッククラウドに応じて、外部ロードバランシングには次のオプションがあります。
  - AWS Gateway Load Balancer

    AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。Firewall Threat Defense Virtual は、Geneve インターフェイスのシングルアームプロキシを使用して分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。
  - Azure ゲートウェイロードバランサ

    Azure サービスチェーンでは、Firewall Threat Defense Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。Firewall Threat Defense Virtual は、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。
  - 内部および外部のネイティブ GCP ロードバランサ
  - シスコ クラウド サービス ルータなどの内部および外部ルータを使用した等コスト マルチパス ルーティング（ECMP）

    ECMP ルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannel のように、送信元および宛先の IP アドレスや送信元および宛先のポートのハッシュを使用してネクスト ホップの

1 つにパケットを送信できます。ECMP ルーティングにスタティックルートを使用する場合は、Firewall Threat Defense の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した Firewall Threat Defense へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 Firewall Threat Defense を設定する必要があります。

（注） レイヤ 2 スパンド EtherChannels はロードバランシングではサポートされません。

個々のインターフェイス

クラスターフェイスを個々のインターフェイスとして設定できます。

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のローカル IP アドレスを持ちます。インターフェイスの IP アドレスは、DHCP を介して自動的に設定されます。静的 IP 設定はサポートされていません。

制御ノードとデータノードの役割

クラスタ内のメンバーの 1 つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、プライオリティ設定によって決まります。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバーはデータノードです。 最初にクラスタを作成するときに、制御ノードにするノードを指定します。これは、クラスタに追加された最初のノードであるため、制御ノードになります。

クラスタ内のすべてのノードは、同一の設定を共有します。最初に制御ノードとして指定したノードは、データノードがクラスタに参加するときにその設定を上書きします。そのため、クラスタを形成する前に制御ノードで初期設定を実行するだけで済みます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

クラスタ制御リンク

ノードごとに 1 つのインターフェイスをクラスタ制御リンク専用の VXLAN（VTEP）インターフェイスにする必要があります。VXLAN の詳細については、「VXLAN インターフェイスの設定 （707 ページ）」を参照してください。

VXLAN トンネル エンドポイント

VXLANトンネルエンドポイント（VTEP）デバイスは、VXLANのカプセル化およびカプセル化解除を実行します。各VTEPには2つのインターフェイスタイプ（VXLAN Network Identifier（VNI）インターフェイスと呼ばれる1つ以上の仮想インターフェイスと、 VTEP間にVNIをトンネリングするVTEP送信元インターフェイスと呼ばれる通常のインターフェイス）がありますVTEP送信元インターフェイスは、VTEP間通信のトランスポートIPネットワークに接続されます。

VTEP 送信元インターフェイス

VTEP送信元インターフェイスは、VNIインターフェイスに関連付けられる予定の標準のFirewall Threat Defense Virtualインターフェイスです。1つのVTEPソースインターフェイスをクラスタ制御リンクとして機能するように設定できます。ソースインターフェイスは、クラスタ制御リンクの使用専用に予約されています。各VTEPソースインターフェイスには、同じサブネット上のIPアドレスがあります。このサブネットは、他のすべてのトラフィックからは隔離し、クラスタ制御リンクインターフェイスだけが含まれるようにしてください。

VNI インターフェイス

VNIインターフェイスはVLANインターフェイスに似ています。VNIインターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。設定できるVNIインターフェイスは1つだけです。各VNIインターフェイスは、同じサブネット上のIPアドレスを持ちます。

ピア VTEP

単一のVTEPピアを許可するデータインターフェイス用の通常のVXLANとは異なり、Firewall Threat Defense Virtualクラスタリングでは複数のピアを設定できます。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

管理ネットワーク

管理インターフェイスを使用して各ノードを管理する必要があります。クラスタリングでは、データインターフェイスからの管理はサポートされていません。

Threat Defense Virtual クラスタリングのライセンス

各 Firewall Threat Defense Virtual クラスタノードには、同じパフォーマンス階層ライセンスが必要です。すべてのメンバーに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のメンバーに一致するようにすべてのノードで制限されます。スループットレベルは、一致するように制御ノードから各データノードに複製されます。

個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。

制御ノードを Firewall Management Center に追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタのライセンスは、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[ライセンス（License）]** 領域で変更できます。

（注） Firewall Management Center にライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、Firewall Management Center にライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのデータユニットがクラスタをいったん離れてから再参加することになります。

Threat Defense Virtual クラスタリングの要件および前提条件

モデルの要件

- FTDv5、FTDv10、FTDv20、FTDv30、FTDv50、FTDv100

（注） FTDv5 および FTDv10 は、Amazon Web Services（AWS）ゲートウェイロードバランサ（GWLB）をサポートしていません。

- 以下のパブリッククラウドサービス：
  - Amazon Web Services（AWS）
  - Microsoft Azure
  - Google Cloud Platform（GCP）
- 最大 16 ノード

Cisco Secure Firewall Threat Defense Virtual スタートアップガイド の Firewall Threat Defense Virtual の一般要件も参照してください。

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

ハードウェアおよびソフトウェアの要件

クラスタ内のすべてのユニット：

- 同じパフォーマンス層内にある必要があります。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のノードに一致するようにすべてのノードで制限されます。
- Firewall Management Center へのアクセスは管理インターフェイスから行うこと。データインターフェイスの管理はサポートされていません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレス アップグレードがサポートされます。
- クラスタ内のすべてのユニットは、同じ可用性ゾーンに展開する必要があります。
- すべてのユニットのクラスタ制御リンクインターフェイスは、同じサブネット内にある必要があります。

MTU

クラスタ制御リンクに接続されているポートに適切な MTU 値（高い値）が設定されていること。MTU の不一致がある場合、クラスタの形成に失敗します。

クラスタ制御リンクの MTU は、データインターフェイスよりも 154 バイト大きく設定されているはずです。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッド（100 バイト）と VXLAN のオーバーヘッド（54 バイト）にも対応する必要があります。

GWLB を使用する AWS の場合、データインターフェイスは Geneve カプセル化を使用します。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。送信元インターフェイス MTU をネットワーク MTU + 306 バイトに設定する必要があります。したがって、標準の 1500 MTU ネットワークパスの場合、送信元インターフェイスの MTU は 1806 であり、クラスタ制御リンクの MTU は +154 の 1960 である必要があります。

GWLB を使用する Azure の場合、データインターフェイスは VXLAN カプセル化を使用します。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。クラスタ制御リンクの MTU は、送信元インターフェイスの MTU の + 80 バイトになるように設定する必要があります。

次の表は、クラスタ制御リンク MTU のデフォルト値とデータインターフェイス MTU を示しています。

（注） クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。

表 *33 :* デフォルト *MTU*

パブリック クラウド	クラスタ制御リンク MTU	データインターフェイス MTU
GWLB を使用した AWS	1960	1806
AWS	1654	1500
GWLB を使用した Azure	1554	1454
Azure	1554	1400
GCP	1554	1400

Threat Defense Virtual クラスタリングのガイドライン

ハイ アベイラビリティ

クラスタリングでは、高可用性はサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannelインターフェイスの追加または削除、Firewall Threat Defense 上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC または VNet を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイス モニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。
- ノードを既存のクラスタに追加したときや、ノードをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- ノードでクラスタリングを無効にせずにノードの電源を切らないでください。
- 復号されたTLS/SSL接続の場合、復号状態は同期されず、接続オーナーに障害が発生すると、復号された接続がリセットされます。新規ノードへの接続を新たに確立する必要があります。復号されていない接続（復号しないルールに一致）は影響を受けず、正しく複製されます。
- ダイナミックスケーリングはサポートされていません。
- は、AWS にクラスタを展開する場合にステートフル ターゲット フェールオーバーはサポートされません。
- 各メンテナンスウィンドウの完了後にグローバル展開を実行します。
- 自動スケールグループ（AWS）/インスタンスグループ（GCP）/スケールセット（Azure）から一度に複数のデバイスを削除しないでください。また、自動スケールグループ（AWS）/インスタンスグループ（GCP）/スケールセット（Azure）からデバイスを削除する前に、デバイスで **cluster disable** コマンドを実行することを推奨します。
- クラスタ内のデータノードと制御ノードを無効にする場合は、制御ノードを無効にする前にデータノードを無効にすることを推奨します。クラスタ内に他のデータノードがあるときに制御ノードが無効になっている場合は、いずれかのデータノードを制御ノードに昇格させる必要があります。ロールの変更はクラスタを妨害する可能性があることに注意してください。
- このガイドに記載されているカスタマイズした Day 0 構成スクリプトでは、要件に応じて IP アドレスを変更し、カスタムインターフェイス名を指定して、CCL-Link インターフェイスのシーケンスを変更することができます。
- クラウドプラットフォームに Threat Defense 仮想クラスタを展開した後の断続的な ping の失敗など、CCL が不安定になる問題が発生した場合は、CCL の不安定性の原因に対処することをお勧めします。また、CCLが不安定になる問題をある程度軽減するための一時的

な回避策として、保留時間を増やすこともできます。保留時間の変更方法の詳細については、「クラスタの正常性モニタリング設定の編集」を参照してください。

- Management Center Virtual のセキュリティ ファイアウォール ルールまたはセキュリティグループを設定する場合は、Firewall Threat Defense Virtual のプライベート IP アドレスとパブリック IP アドレスの両方を送信元 IP アドレス範囲に含める必要があります。また、Firewall Threat Defense Virtual のセキュリティ ファイアウォール ルールまたはセキュリティグループで、Firewall Management Center Virtual のプライベート IP アドレスとパブリック IP アドレスを指定してください。これは、クラスタリングの展開中にノードを適切に登録するために重要です。

クラスタリングのデフォルト

- cLACP システム ID は自動生成され、システムの優先順位はデフォルトでは 1 になっています。
- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が 5 分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

AWS でクラスタを展開する

AWS にクラスタを展開する場合、手動で展開するか、スタックを展開する CloudFormation テンプレートを使用できます。AWS ゲートウェイロードバランサ、または Cisco Cloud Services Router などの非ネイティブのロード バランサでクラスタを使用できます。

AWS ゲートウェイロードバランサおよび Geneve シングルアームプロキシ

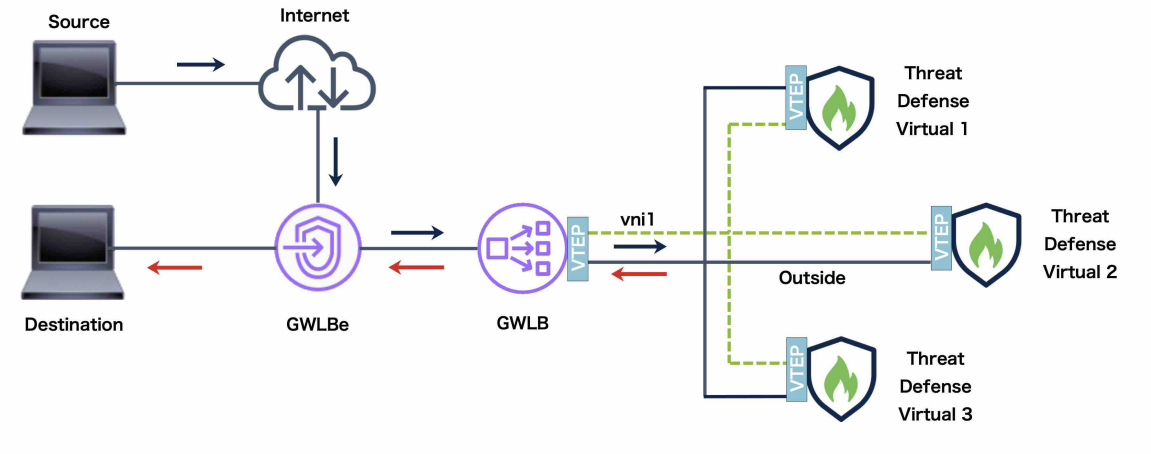
（注） この使用例は、現在サポートされている Geneve インターフェイスの唯一の使用例です。

AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。Threat Defense Virtual は、分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。次の図は、ゲートウェイロードバランサのエンドポイントからゲートウェイロードバランサに転

送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の Threat Defense Virtual の間でトラフィックのバランスを取り、トラフィックをドロップするか、ゲートウェイロードバランサに送り返す（U ターントラフィック）前に検査します。ゲートウェイロードバランサは、トラフィックをゲートウェイロードバランサのエンドポイントと宛先に送り返します。

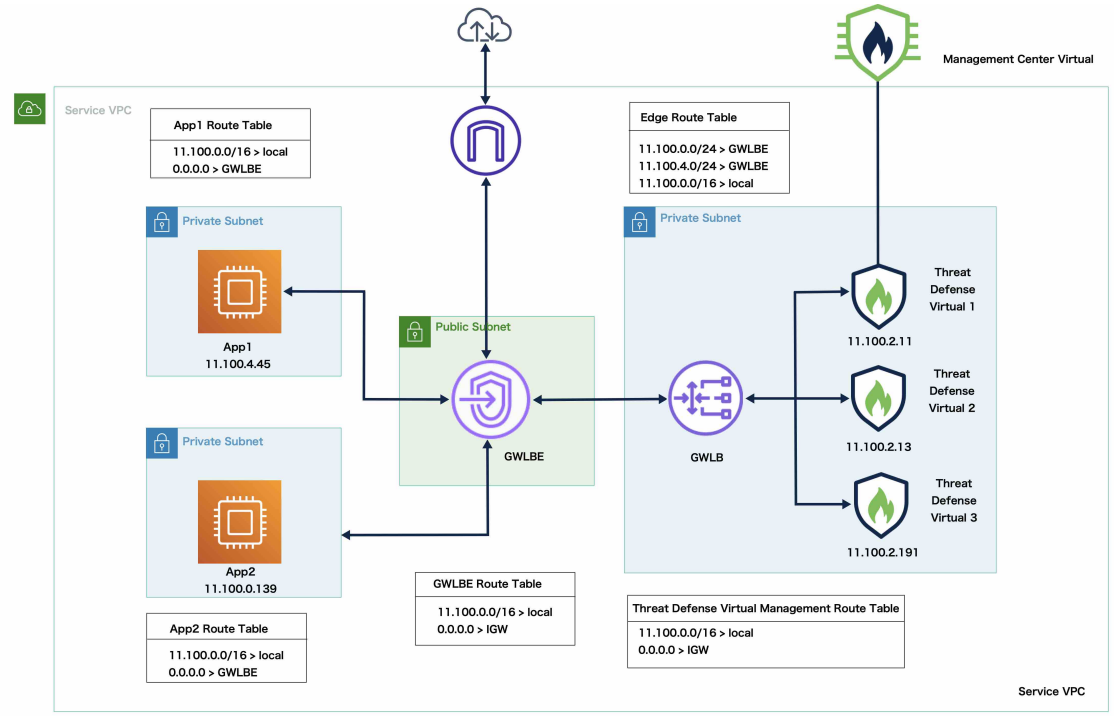
（注） Transport Layer Security（TLS）サーバーアイデンティティ検出は、AWS での Geneve シングルアームセットアップではサポートされていません。

図 *160 : Geneve* シングルアームプロキシ



トポロジの例

次に示すトポロジは、着信と発信の両方のトラフィックフローを示しています。GWLB に接続されているクラスタには、3 つの Threat Defense Virtual インスタンスがあります。Management Center Virtual インスタンスは、クラスタの管理に使用されます。



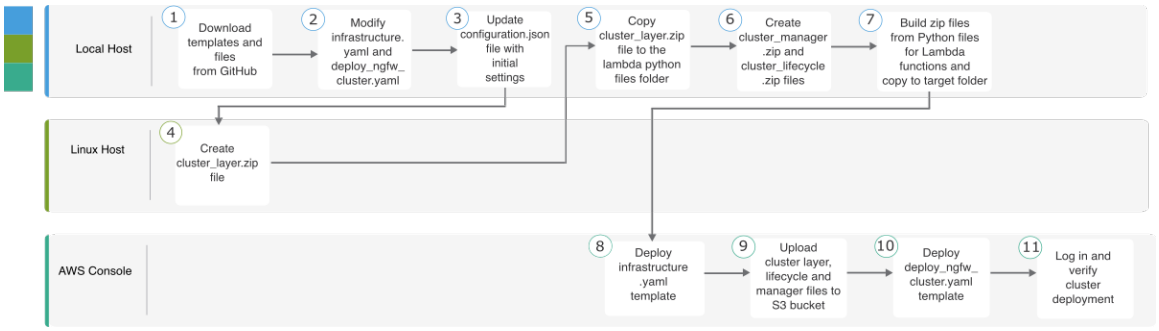
インターネットからの着信トラフィックは、GWLBエンドポイントに送られ、そこからGWLBにトラフィックが送信されます。その後、トラフィックは Threat Defense Virtual クラスタに転送されます。トラフィックは、クラスタ内の Threat Defense Virtual インスタンスによって検査された後、アプリケーション VM App1/App2 に転送されます。

App1/App2からの発信トラフィックは、GWLBエンドポイントに送信され、そこからインターネットに送信されます。

AWS で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス

テンプレートベースの展開

次のフローチャートは、AWS での Threat Defense Virtual クラスタのテンプレートベース展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	GitHub からリポジトリを複製します。
2	ローカルホスト	infrastructure.yaml および deploy_ngfw_cluster.yaml テンプレートを変更します。
3	ローカルホスト	Configuration.json ファイルを FMC オブジェクト名で更新します。
4	Linux ホスト	cluster_layer.zip ファイルを作成します。
5	ローカルホスト	cluster_layer.zip ファイルを Lambda Python ファイルフォルダにコピーします。
6	ローカルホスト	*cluster_manager.zip*、*custom_metrics_publisher.zip*、および *cluster_lifecycle.zip* ファイルを作成します。
7	ローカルホスト	Lambda 関数の Python ファイルから zip ファイルを作成し、ターゲットフォルダにコピーします。
8	AWS コンソール	Infrastructure.yaml テンプレートを展開します。
9	AWS コンソール	*cluster_layer.zip*、*cluster_lifecycle.zip*、*custom_metrics_publisher.zip*、および *cluster_manager.zip* を S3 バケットにアップロードします。
10	AWS コンソール	deploy_ngfw_cluster.yaml テンプレートを展開します。
11	AWS コンソール	ログインして、クラスタの展開を確認します。

手動展開

次のフローチャートは、AWS での Threat Defense Virtual クラスタの手動展開のワークフローを示しています。

	ワークスペース	手順
1	ローカルホスト	Day 0 構成スクリプトを作成します。
2	AWS コンソール	Threat Defense Virtual インスタンスを展開します。
3	AWS コンソール	インスタンスにインターフェイスを接続します。
4	AWS コンソール	ノードがクラスタに参加しているかどうかを確認します。
5	AWS コンソール	ターゲットグループと GWLB を作成します。ターゲットグループを GWLB に割り当てます。
6	AWS コンソール	データインターフェイス IP を使用してターゲットグループにインスタンスを登録します。
7	Management Center	制御ノードを登録します。

テンプレート

以下のテンプレートは GitHub で入手できます。パラメータ値は、テンプレートで指定されたパラメータ名、デフォルト値、使用可能な値、および説明により自明です。

- infrastructure.yaml：インフラストラクチャ展開用のテンプレート。
- deploy_ngfw_cluster.yaml：クラスタ展開用のテンプレート。

（注） クラスタノードを展開する前に、サポートされている AWS インスタンスタイプのリストを確認してください。このリストは、deploy_ngfw_cluster.yaml テンプレートのパラメータ InstanceType に使用可能な値の下にあります。

CloudFormation テンプレートを使用した AWS へのスタックの展開

CloudFormation テンプレートを使用して AWS にスタックを展開します。

始める前に

- Python 3 をインストールした Amazon Linux 仮想マシンが必要です。
- クラスタが Firewall Management Center に自動登録されるようにするには、REST API を使用できる管理者権限を持つ *2* つのユーザーを Firewall Management Center で作成する必要があります。Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。
- `Configuration.json` で指定したポリシー名と一致するアクセスポリシーを Firewall Management Center に追加します。

手順

ステップ 1 テンプレートを準備します。

a) GitHub リポジトリをローカルフォルダに複製します。https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/aws を参照してください。

b) 必要なパラメーターを使用して、**infrastructure.yaml** および **deploy_ngfw_cluster.yaml** を変更します。

c) **cluster/aws/lambda-python-files/Configuration.json** を初期設定に変更します。

次に例を示します。

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv50",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "AWS-ACL"
}
```

- fmcIpforDeviceReg 設定は DONTRESOLVE のままにします。
- fmcAccessPolicyName は、Firewall Management Center のアクセスポリシーと一致している必要があります。

（注）
FTDv5 および FTDv10 階層はサポートされていません。

d) **cluster_layer.zip** という名前のファイルを作成して、重要な Python ライブラリを Lambda 関数に提供します。

cluster_layer.zip ファイルを作成するには、Python 3.9 がインストールされた Amazon Linux を使用することをお勧めします。

（注）
Amazon Linux 環境が必要な場合は、Amazon Linux 2023 AMI を使用して EC2 インスタンスを作成するか、Amazon Linux の最新バージョンを実行する AWS Cloudshell を使用できます。

cluster-layer.zip ファイルを作成するには、最初に Python ライブラリパッケージの詳細で構成される **requirements.txt** ファイルを作成してから、シェルスクリプトを実行する必要があります。

1. Python パッケージの詳細を指定して、**requirements.txt** ファイルを作成します。

   以下は、**requirements.txt** ファイルで指定するサンプルパッケージの詳細です。

```
$ cat requirements.txt
pycryptodome
paramiko
requests
scp
jsonschema
cffi
zipp
importlib-metadata
```

2. 次のシェルスクリプトを実行して、**cluster_layer.zip** ファイルを作成します。

```
$ pip3 install --platform manylinux2014_x86_64
--target=./python/lib/python3.9/site-packages
--implementation cp --python-version 3.9 --only-binary=:all:
--upgrade -r requirements.txt
$ zip -r cluster_layer.zip ./python
```

（注）
インストール中に urllib3 や暗号化などの依存関係の競合エラーが発生した場合は、競合するパッケージを推奨バージョンと一緒に **requirements.txt** ファイルに含めることをお勧めします。その後、インストールを再度実行して競合を解決できます。

e) 結果の **cluster_layer.zip** ファイルを Lambda Python ファイルフォルダ（`cluster/aws/lambda-python-files`）にコピーします。

f) **cluster_layer.zip**、**custom_metrics_publisher.zip**、**cluster_manger.zip**、および **lifecycle_ftdv.zip** ファイルを作成します。

make.py ファイルは、複製されたリポジトリ（`cluster/aws/make.py`）内にあります。これにより、python ファイルが Zip ファイルに圧縮され、ターゲットフォルダにコピーされます。

python3 make.py build

（注）
Management Center Virtual の登録にプライベート IP アドレスを使用している場合は、`cisco-ftdv/cluster/aws/lambda-python-files/constant.py` ファイルで USE_PUBLIC_IP_FOR_FMC_CONN を False に設定していることを確認します。

ステップ 2 **Infrastructure.yaml** を展開し、クラスタ展開の出力値をメモします。インフラストラクチャスタックを展開する前に、使用する AWS リージョンと可用性ゾーンを特定することが重要です。

各 AWS リージョンには異なる可用性ゾーンと VPC インフラストラクチャのセットがあるため、展開に適したリージョンと可用性ゾーンを選択することが不可欠です。

a) AWS コンソールで、[CloudFormation] に移動し、[新しいリソース（標準）を使用（With new resources(standard)）] を選択して、[スタックの作成（Create stack）] をクリックします。
b) [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose file）] をクリックして、ターゲットフォルダから **infrastructure.yaml** を選択します。
c) [次へ（Next）] をクリックして、必要な情報を入力します。
d) クラスタの一意の**クラスタ名**と**クラスタ番号**を入力します。
e) [可用性ゾーン（Availability Zone）] リストから可用性ゾーンを選択します。このフィールドには、ClusterFormation テンプレートを使用してインフラストラクチャ スタックを展開するために選択した AWS リージョンに基づく可用性ゾーンのみが表示されます。
f) [次へ（Next）]、[スタックの作成（Create stack）] の順にクリックします。
g) 展開が完了したら、[出力（Outputs）] に移動し、S3 の **BucketName** を書き留めます。

図 *161 : Infrastructure.yaml* の出力

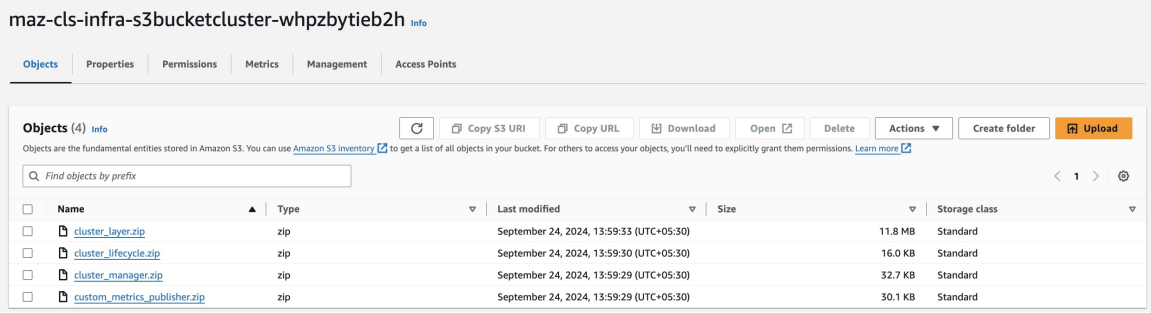
Outputs (13)

Search outputs

Key	Value	Description	Export name
BucketName	maz-cls-infra-s3bucketcluster-whpzbytieb2h	Name of the Amazon S3 bucket	-
BucketUrl	http://maz-cls-infra-s3bucketcluster-whpzbytieb2h.s3-website-us-east-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetIds	subnet-0bc04e2cc9e53e5c0,subnet-0d7d046a0fca25615,subnet-03ef42bf527551569	List of CCL subnet IDs (comma seperated)	-
EIPforNATgw	3.218.44.132	EIP reserved for NAT GW	-
FmcInstanceSGID	sg-076880aa64df2db5c	Security Group ID for FMC if user would like to launch in this VPC itself	-
InInterfaceSGId	sg-06ed933d6624fe51b	Security Group ID for Inside Interfaces	-
InsideSubnetIds	subnet-03d12cab8ee0eafff,subnet-0be9158b0970aebab,subnet-0b53c96fceb7c1f4d	List of Inside subnet IDs (comma seperated)	-
InstanceSGId	sg-0680b74be473186aa	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-057da2a9954e0d204	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-03439803d989e6bdf,subnet-087488a9d6ffc95cd	List of lambda subnet IDs (comma seperated)	-
ListOfAZs	us-east-1a,us-east-1b,us-east-1c	Availability zones for NGFWv instances	-
MgmtSubnetIds	subnet-06f0bbbd3f207a504,subnet-0c339dc43688cddc9,subnet-0a67629632a655de7	List of Mangement subnet IDs (comma seperated)	-
VpcName	vpc-09c2b0ad995e2fb24	Name of the VPC created	-

ステップ 3 **cluster_layer.zip**、**cluster_manager.zip**、**custom_metrics_publisher.zip**、および **cluster_lifecycle.zip** を **infrastructure.yaml** で作成した S3 バケットにアップロードします。

図 *162 : S3* バケット



（注）
Lambda NAT ゲートウェイのエラスチック IP アドレスが Management Center Virtual に関連付けられたセキュリティグループに追加されていることを確認してください。

ステップ 4 **deploy_ngfw_cluster.yaml** を展開します。

a) [CloudFormation] に移動し、[新しいリソース（標準）を使用（With new resources(standard)）] を選択して、[スタックの作成（Create stack）] をクリックします。

b) [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose file）] をクリックして、ターゲットフォルダから **deploy_ngfw_cluster.yaml** を選択します。

c) [次へ（Next）] をクリックして、必要な情報を入力します。

d) 次のクラスタとインフラストラクチャの設定情報を入力します。

パラメータ	使用できる値/タイプ	説明
クラスタの設定		
ClusterGrpNamePrefix	文字列	これはクラスタ名のプレフィックスです。クラスタ番号がサフィックスとして追加されます。
ClusterNumber	文字列	これはクラスタ番号であり、クラスタ名（msa-ftdv-infra）のサフィックスとして追加されます。たとえば、この値が「1」の場合、グループ名は msa-ftdv-infra-1 になります。 1 桁以上 3 桁以下である必要があります。デフォルト：1。
ClusterSize	番号	これは、クラスタ内の Firewall Threat Defense Virtual ノードの総数です。 最小値：1

パラメータ	使用できる値/タイプ	説明
		最大値：16
インフラストラクチャの詳細		
NoOfAZs	文字列	これは、Firewall Threat Defense Virtual が展開される可用性ゾーンの合計数です（可用性ゾーンの数は 1 ～ 3 でリージョンによって異なります）。 サブネットは、これらの可用性ゾーンに作成されます。 このリストで使用可能な可用性ゾーンは、クラスタの展開用に選択されたリージョンに基づいています。 （注） 管理、内部、およびクラスタ制御リンク（CCL）のサブネットは、このパラメータに基づいて 3 つの可用性ゾーンにわたって作成されます。
AZ	文字列	可用性ゾーンリストは、展開するリージョンに基づきます。 [可用性ゾーン（Availability Zone）] リストで、有効な可用性ゾーン（1 つの可用性ゾーン、2 つの可用性ゾーン、または 3 つの可用性ゾーン）を選択します。 カウントは、可用性ゾーン数のパラメータの値と一致する必要があります。
NotifyEmailID	文字列	クラスタイベントの電子メールの送信先となる電子メールアドレス。この電子メール通告を受信するには、サブスクリプション電子メール要求を承認する必要があります。 例：admin@company.com
VpcId	文字列	クラスタグループの VPC ID。 タイプ：AWS::EC2::VPC::Id
S3BktName	文字列	アップロードされた Lambda zip ファイルを含む S3 バケット。正しいバケット名を指定する必要があります。
MgmtSubnetIds	リスト	可用性ゾーンごとに「1 つ」の サブネットのみを入力します。 同じ可用性ゾーンから複数のサブネットを選択する場合、間違ったサブネットを選択すると、Firewall Threat

パラメータ	使用できる値/タイプ	説明
		Defense Virtual インスタンスの展開中に問題が発生する可能性があります。 タイプ：List<AWS::EC2::Subnet::Id>
InsideSubnetIds	リスト	可用性ゾーンごとに少なくとも「1 つ」の サブネットを入力します。 同じ可用性ゾーンから複数のサブネットを選択する場合、間違ったサブネットを選択すると、Firewall Threat Defense Virtual インスタンスの展開中に問題が発生する可能性があります。 タイプ：List<AWS::EC2::Subnet::Id>
LambdaSubnets	リスト	Lambda 関数用に少なくとも「2 つ」のサブネットを入力します。Lambda 関数が、パブリック DNS である AWS サービスと通信できるようにするには、入力する「2つ」のサブネットにNAT ゲートウェイが必要です。 タイプ：List<AWS::EC2::Subnet::Id>
CCLSubnetIds	文字列	可用性ゾーンごとに少なくとも「1 つ」の サブネットを入力します。 同じ可用性ゾーンから複数のサブネットを選択する場合、間違ったサブネットを選択すると、Firewall Threat Defense Virtual インスタンスの展開中に問題が発生する可能性があります。 タイプ：List<AWS::EC2::Subnet::Id>
CCLSubnetRanges	文字列	さまざまな可用性ゾーンの CCL サブネットの IP アドレス範囲を入力します。 最初の 4 つの予約済み IP アドレスを除外します。クラスタ制御リンク（CCL）の IP アドレスプール。 IP アドレスは、CCL IP アドレスプールから Firewall Threat Defense Virtual インスタンスの CCL インターフェイスに割り当てられます。
MgmtInterfaceSG	リスト	Firewall Threat Defense Virtual インスタンスのセキュリティグループ ID を選択します。 タイプ：List<AWS::EC2::SecurityGroup::Id>

パラメータ	使用できる値/タイプ	説明
InsideInterfaceSG	リスト	Firewall Threat Defense Virtual インスタンスの内部インターフェイスのセキュリティグループ ID を選択します。 タイプ：List<AWS::EC2::SecurityGroup::Id>
LambdaSG	リスト	Lambda 関数のセキュリティグループを選択します。 発信接続が [ANYWHERE] に設定されていることを確認します。 タイプ：List<AWS::EC2::SecurityGroup::Id>
CCLInterfaceSG	リスト	Firewall Threat Defense Virtual インスタンスの CCL インターフェイスのセキュリティグループ ID を選択します。
GWLB の設定		
DeployGWLBE	文字列	[はい（Yes）] をクリックして GWLB エンドポイントを展開します。 デフォルトでは、この値は [いいえ（No）] に設定されています。
VpcIdLBE	文字列	ゲートウェイロードバランサのエンドポイントを展開する VPC を入力します。 （注） GWLBエンドポイントを展開しない場合は、このフィールドに値を入力しないでください。
GWLBESubnetId	文字列	サブネット ID を 1 つだけ入力します。 （注） GWLBエンドポイントを展開しない場合は、このフィールドに値を入力しないでください。 サブネットが正しい VPC および指定した可用性ゾーンに属していることを確認します。
TargetFailover	文字列	ターゲットに障害が発生した場合または登録解除された場合のターゲット フェールオーバー サポートを有効にします（このパラメータの値はデフォルトで [再調整（rebalance）] に設定されています）。

パラメータ	使用できる値/タイプ	説明
		• [再調整なし（no_rebalance）]：既存のフローを障害が発生したターゲットに送信し、新しいフローを正常なターゲットに送信し、後方互換性を確保します。 • [再調整（rebalance）]：新しいフローが正常なターゲットに送られるようにしながら、既存のフローを再配布します。 [再調整（rebalance）] は、Firewall Threat Defense Virtual バージョン 7.4.1 以降でサポートされています。
TgHealthPort	文字列	GWLB の正常性チェックポートを入力します。 （注） デフォルトでは、このポートはトラフィックに使用されません。 指定した値が有効な TCP ポートであることを確認します。デフォルト：8080
Cisco NGFWv インスタンスの設定		
InstanceType	文字列	Cisco Firewall Threat Defense Virtual EC2 インスタンスタイプ。 選択したインスタンスタイプが AWS リージョンでサポートされていることを確認します。 デフォルトでは、**c5.xlarge** が選択されています。
LicenseType	文字列	Cisco Firewall Threat Defense Virtual EC2 インスタンス ライセンス タイプを選択します。**AMI-ID** パラメータに入力する AMI ID が同じライセンスタイプであることを確認します。 デフォルトでは、[BYOL] が選択されています。
AssignPublicIP	文字列	AWS IP アドレスプールから Firewall Threat Defense Virtual のパブリック IP アドレスを割り当てるには、値を [はい（true）] に設定します。
AmiID	文字列	リージョン、バージョン、およびライセンスタイプ（BYOL または PAYG）に従って正しい AMI ID を選択します。

パラメータ	使用できる値/タイプ	説明
		Firewall Threat Defense Virtual 7.2 以降ではクラスタリングがサポートされ、Firewall Threat Defense Virtual バージョン 7.6 以降では自動スケーリングと複数の可用性ゾーンの機能拡張がサポートされています。 タイプ：AWS::EC2::Image::Id
ngfwPassword	文字列	Firewall Threat Defense Virtual インスタンスのパスワード。 すべての Firewall Threat Defense Virtual インスタンスには、起動テンプレート（クラスタグループ）の [ユーザーデータ（Userdata）] フィールドにあるデフォルトのパスワードが設定されています。 Firewall Threat Defense Virtual にアクセスできるようになると、パスワードがアクティブになります。 文字数は 8 文字以上にする必要があります。パスワードには、プレーンテキストのパスワードまたはKMS暗号化パスワードを使用できます。
KmsArn	文字列	既存の KMS の ARN（保存時に暗号化するための AWS KMS キー）を入力します。 このフィールドに値を指定する場合、Firewall Threat Defense Virtual インスタンスの**管理者**パスワードは暗号化されたパスワードである必要があります。 暗号化パスワードの生成例："*aws kms encrypt --key-id <KMS ARN> --plaintext <password>* " パスワードの暗号化は、指定されたARNのみを使用して実行する必要があります。
FMC 自動化の設定		
fmcDeviceGrpName	文字列	Management Center でクラスタグループの一意の名前を入力します。
fmcPublishMetrics	文字列	Management Center をポーリングし、特定のデバイスグループメトリックを AWS CloudWatch にパブリッシュする Lambda 関数を作成するには、**`true`** を選択します。 使用可能な値： • true

パラメータ	使用できる値/タイプ	説明
		• false デフォルトでは、この値は **true** に設定されています。
fmcMetricsUsername	文字列	Management Center からメモリメトリックをポーリングするための一意の内部ユーザー名を入力します。 ユーザーには、**ネットワーク管理者**および**メンテナンスユーザー**以上の権限が必要です。
fmcMetricsPassword	文字列	パスワードを入力します。 KMS マスターキー ARN パラメータを指定した場合は、必ず、暗号化されたパスワードを入力してください。 間違ったパスワードを入力するとメトリック収集が失敗する可能性があるため、必ず、正しいパスワードを入力してください。
fmcServer	文字列	IP アドレスには、外部 IP アドレス、または VPC の Firewall Threat Defense Virtual 管理サブネットで到達可能な IP アドレスを指定できます。 最小長：7 最大長：15
fmcOperationsUsername	文字列	CloudWatch 用の Firewall Management Center Virtual に使用する一意の内部ユーザー名を入力します。 ユーザーには**管理者**権限が必要です。
fmcOperationsPassword	文字列	パスワードを入力します。 KMS マスターキー ARN パラメータを指定した場合は、必ず、暗号化されたパスワードを入力してください。
スケーリングの設定		
CpuThresholds	カンマ区切りリスト	（任意）ゼロ以外の下限しきい値と上限しきい値を指定すると、スケールポリシーが作成されます。(0,0) を選択すると、CPU スケーリングアラームまたはポリシーは作成されません。評価ポイントとデータポイントは、デフォルト値または推奨値にします。 デフォルトでは、このテンプレートでは**自動スケール**が有効になっています。自動スケールは展開後に無効にできます。

パラメータ	使用できる値/タイプ	説明
MemoryThresholds	カンマ区切りリスト	ゼロ以外の下限しきい値と上限しきい値を指定すると、スケールポリシーが作成されます。(0,0) を選択すると、メモリスケーリングアラームまたはポリシーは作成されません。評価ポイントとデータポイントは、デフォルト値または推奨値にします。

e) [次へ（Next）]、[スタックの作成（Create stack）] の順にクリックします。

Lambda 関数が残りのプロセスを管理し、Firewall Threat Defense Virtual が自動的に Firewall Management Center に登録されます。

図 *163 :* 展開されたリソース

ステータスが **CREATE_IN_PROGRESS** から **CREATE COMPLETE** に変わり、展開が成功したことが示されます。

ステップ 5 いずれかのノードにログインし、**show cluster info** コマンドを使用して、クラスタの展開を確認します。

図 *164 :* クラスタ ノード

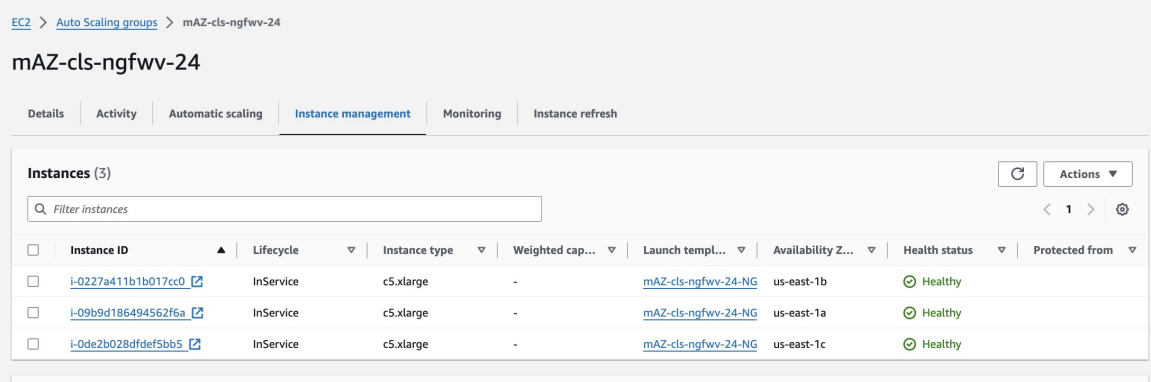
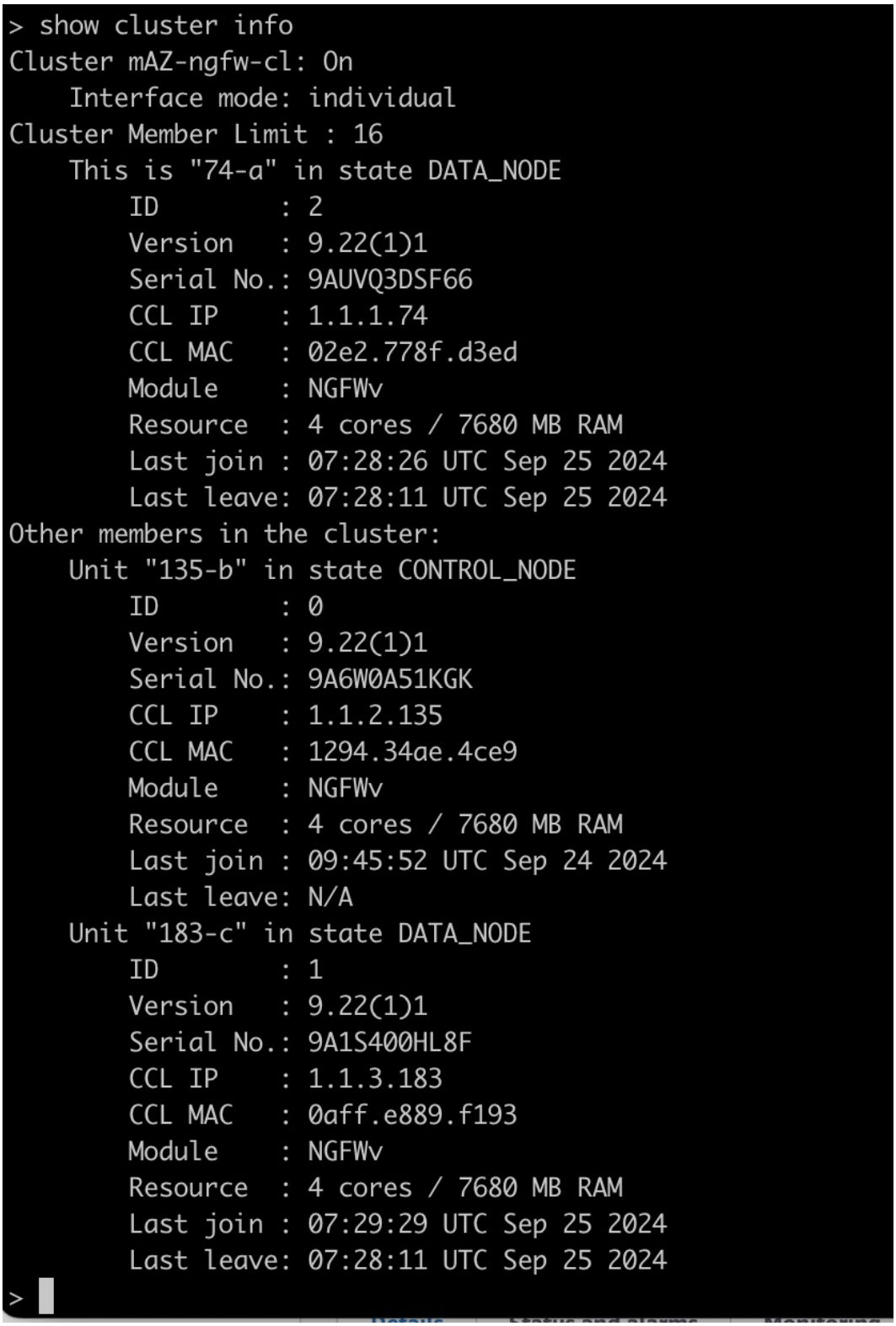


図 *165 : show cluster info*



AWS でのクラスタの手動展開

クラスタを手動で展開するには、Day 0 構成を準備し、各ノードを展開してから制御ノードを Firewall Management Center に追加します。

AWS 向け Day 0 構成の作成

固定構成またはカスタマイズ構成のいずれかを使用できます。固定構成の使用をお勧めします。

AWS 向け固定構成を使用した Day 0 構成の作成

固定構成により、クラスタのブートストラップ構成が自動生成されます。

単一の可用性ゾーン：AWS 向け固定構成を使用した Day 0 構成

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}
```

次に例を示します。

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "ciscoftdv",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
             "CclSubnetRange": "10.5.90.4 10.5.90.30",
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "7777"
 }
}
```

CclSubnetRange 変数には、x.x.x.4 から始まる IP アドレスの範囲を指定します。クラスタリングに使用可能な IP アドレスが 16 個以上あることを確認します。開始（`ip_address_start`）および終了（`ip_address_end`）IP アドレスの例を以下に示します。

表 *34*：開始 *IP* アドレスと終了 *IP* アドレスの例

CIDR	開始 IP アドレス	終了 IP アドレス
10.1.1.0/27	10.1.1.4	10.1.1.30

CIDR	開始 IP アドレス	終了 IP アドレス
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254
10.1.1.0/24	10.1.1.4	10.1.1.254

クラスタノードの展開

クラスタが形成されるようにクラスタノードを展開します。

手順

ステップ 1 必要な数のインターフェイス（ゲートウェイロードバランサ（GWLB）を使用している場合は 4 つのインターフェイス、非ネイティブロードバランサを使用している場合は 5 つのインターフェイス）でクラスタの Day 0 構成を使用することにより、Threat Defense Virtual インスタンスを展開します。これを行うには、[インスタンスの詳細設定（Configure Instance Details）] > [高度な詳細（Advanced Details）] セクションで、クラスタの Day 0 構成に貼り付けます。

（注）
次の順序でインスタンスにインターフェイスを接続していることを確認します。

- AWS ゲートウェイロードバランサの 4 つのインターフェイス：管理、診断、内部、クラスタ制御リンク。
- 非ネイティブロードバランサの 5 つのインターフェイス：管理、診断、内部、外部、クラスタ制御リンク。

AWS での Threat Defense Virtual の展開の詳細については、「Deploy the Threat Defense Virtual on AWS」を参照してください。

ステップ 2 ステップ 1 を繰り返して、必要な数の追加ノードを展開します。

ステップ 3 Threat Defense Virtual コンソールで **show cluster info** コマンドを使用して、すべてのノードがクラスタに正常に参加したかどうかを確認します。

ステップ 4 AWS ゲートウェイロードバランサを設定します。

a) ターゲットグループと GWLB を作成します。

b) ターゲットグループを GWLB に割り当てます。

（注）
正しいセキュリティグループ、リスナー設定、およびヘルスチェック設定を使用するように GWLB を設定していることを確認します。

c) IP アドレスを使用して、データインターフェイス（内部インターフェイス）をターゲットグループに登録します。

詳細については、「Create a Gateway Load Balancer」を参照してください。

ステップ 5 Management Center に制御ノードを追加します。「Management Center へのクラスタの追加（手動展開） （504 ページ）」を参照してください。

Azure でクラスタを展開する

Azure Gateway Load Balancer（GWLB）、または非ネイティブのロードバランサでクラスタを使用できます。Azure でクラスタを展開するには、Azure Resource Manager（ARM）テンプレートを使用して仮想マシンスケールセットを展開します。

GWLB ベースのクラスタ展開のサンプルトポロジ

図 *166 : GWLB* を使用する着信トラフィックの導入例とトポロジ

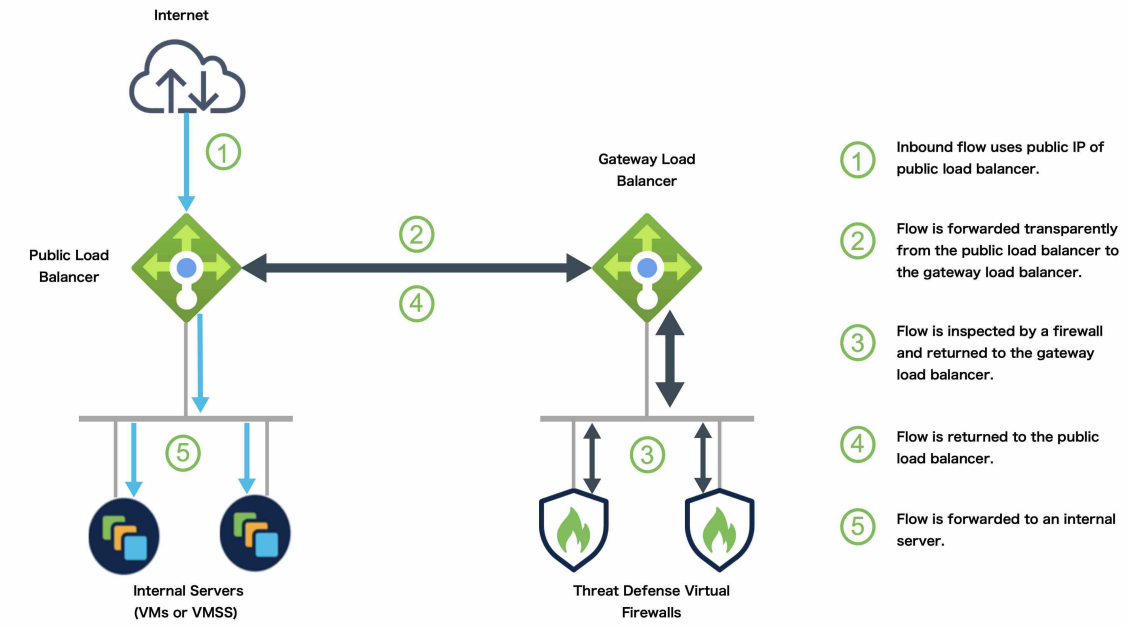
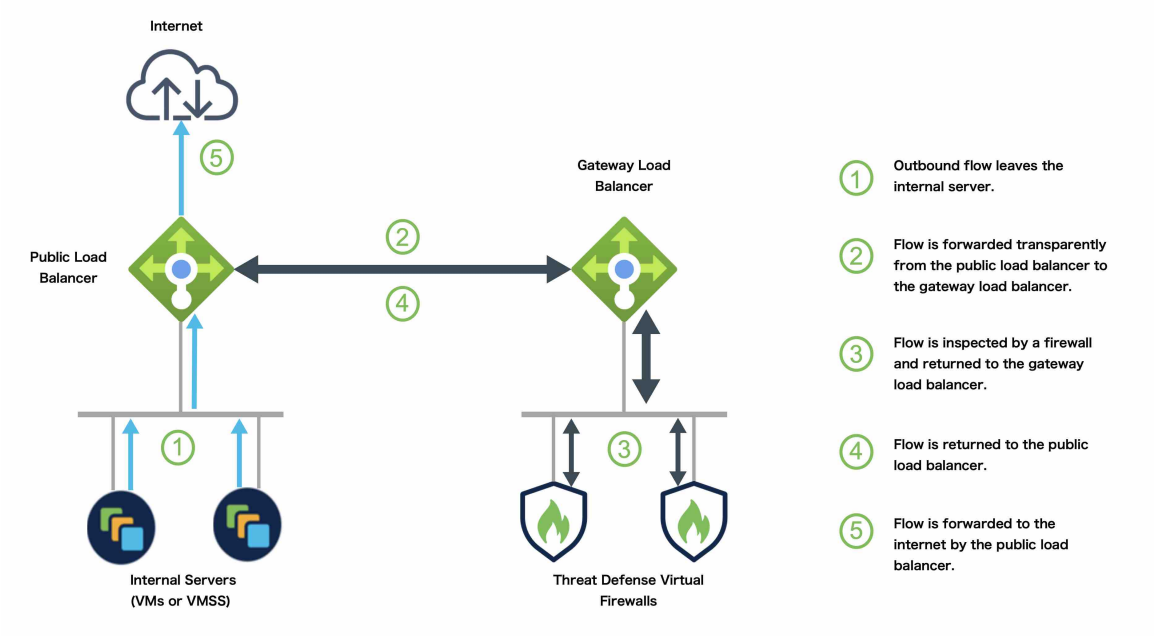


図 *167 : GWLB* を使用する発信トラフィックの導入例とトポロジ

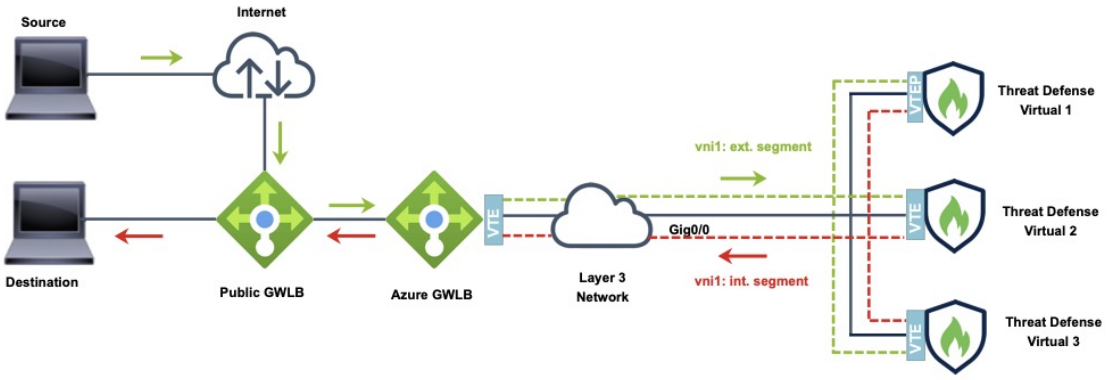


Azure ゲートウェイロードバランサおよびペアプロキシ

Azure サービスチェーンでは、Threat Defense Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。Threat Defense Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

次の図は、外部 VXLAN セグメント上のパブリックゲートウェイロードバランサから Azure ゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の Threat Defense Virtual の間でトラフィックのバランスを取り、トラフィックをドロップするか、内部 VXLAN セグメント上のゲートウェイロードバランサに送り返す前に検査します。Azure ゲートウェイロードバランサは、トラフィックをパブリックゲートウェイロードバランサと宛先に送り返します。

図 *168 :* ペアリングされたプロキシを使用した *Azure Gateway* ロードバランサ

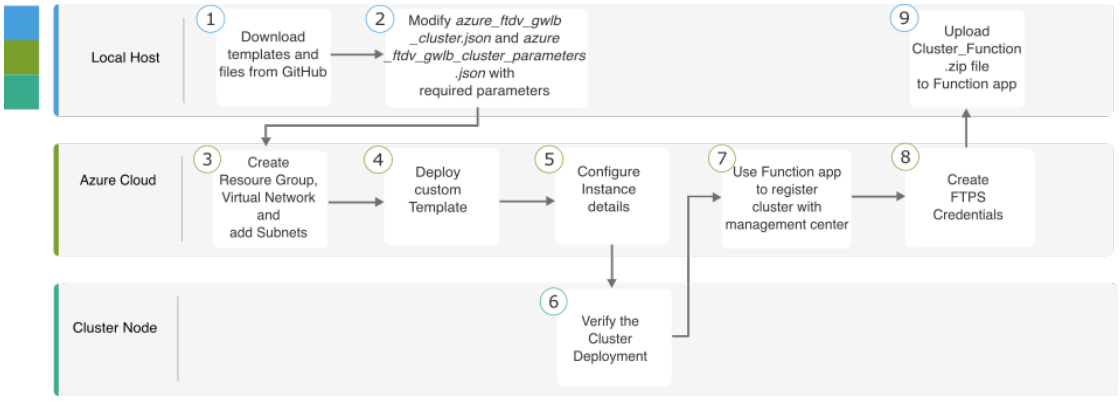


Traffic flow between GWLBe to GWLB (Geneve Single-Arm Proxy) in Azure

GWLB を使用して Azure で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス

テンプレートベースの展開

次のフローチャートは、GWLB を使用した Azure での Threat Defense Virtual クラスタのテンプレートベース展開のワークフローを示しています。

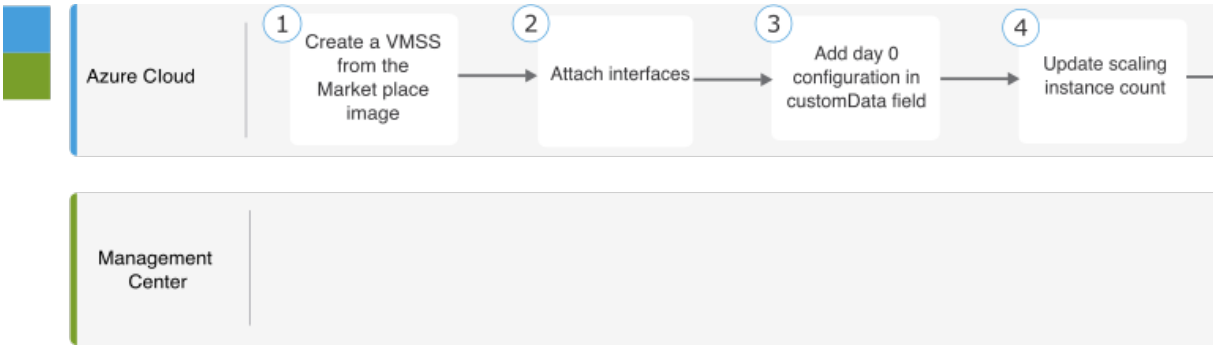


	ワークスペース	手順
1	ローカルホスト	GitHub からテンプレートとファイルをダウンロードします。
2	ローカルホスト	azure_ftdv_gwlb_cluster.json と azure_ftdv_gwlb_cluster_parameters.json を必要なパラメータで変更します。

	ワークスペース	手順
3	Azure Cloud	リソースグループ、仮想ネットワーク、およびサブネットを作成します。
4	Azure Cloud	カスタムテンプレートを展開します。
5	Azure Cloud	インスタンスの詳細を設定します。
6	クラスタノード	クラスタの展開を確認します。
7	Azure Cloud	Function アプリを使用して Management Center にクラスタを登録します。
8	Azure Cloud	FTPS のログイン情報を作成します。
9	ローカルホスト	Cluster_Function.zip ファイルを Function アプリにアップロードします。

手動展開

次のフローチャートは、GWLB を使用した Azure での Threat Defense Virtual クラスタの手動展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	Marketplace イメージから VMSS を作成します。
2	ローカルホスト	インターフェイスを接続します。
3	ローカルホスト	[customData] フィールドに Day 0 構成を追加します。
4	ローカルホスト	スケーリングインスタンス数を更新します。
5	ローカルホスト	GWLB を設定します。

	ワークスペース	手順
6	Management Center	制御ノードを追加します。

テンプレート

以下のテンプレートは GitHub で入手できます。パラメータ値は、テンプレートで指定されたパラメータ名、および値であり、自明です。

- azure_ftdv_gwlb_cluster_parameters.json：GWLB を使用する Firewall Threat Defense Virtual クラスタのパラメータを入力するためのテンプレート。
- azure_ftdv_gwlb_cluster.json：GWLB を使用する Firewall Threat Defense Virtual クラスタを展開するためのテンプレート。

前提条件

- クラスタが Management Center に自動登録できるようにするには、Management Center でネットワーク管理者およびメンテナンスのユーザー権限を持つユーザーを作成します。これらの権限を持つユーザーは、REST API を使用できます。『Cisco Secure Firewall Management Center Administration Guide』を参照してください。
- テンプレートの展開時に指定するポリシー名と一致するアクセスポリシーを Management Center に追加します。
- Management Center Virtual が適切にライセンスされていることを確認します。
- クラスタが Management Center Virtual に追加されたら、次の手順を実行します。

1. Management Center のプラットフォーム設定でヘルスチェックのポート番号を設定します。この設定の詳細については、「Platform Settings」を参照してください。
2. データトラフィックのスタティックルートを作成します。スタティックルートの作成の詳細については、「Add a Static Route」を参照してください。

   スタティックルートの設定例：

```
Network: any-ipv4
Interface: vxlan_tunnel
Leaked from Virtual Router: Global
Gateway: vxlan_tunnel_gw
Tunneled: false
Metric: 2
```

（注） *vxlan_tunnel_gw* は、データサブネットのゲートウェイ IP アドレスです。

Azure Resource Manager テンプレートを使用した Azure と GWLB でのクラスタの展開

カスタマイズされた Azure Resource Manager（ARM）テンプレートを使用して、Azure GWLB の仮想マシンスケールセットを展開します。

手順

ステップ 1 テンプレートを準備します。

a) GitHub リポジトリをローカルフォルダに複製します。https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure を参照してください。

b) azure_ftdv_gwlb_cluster.json と azure_ftdv_gwlb_cluster_parameters.json を必要なパラメータで変更します。

ステップ 2 Azure ポータルにログイン：https://portal.azure.com。

ステップ 3 リソース グループを作成します。

a) [基本（Basics）] タブで、ドロップダウンリストから [サブスクリプション（Subscription）] および [リソースグループ（Resource group）] を選択します。

b) 必須の [リージョン（Region）] を選択します。

ステップ 4 管理、診断、外部、クラスタ制御リンク（CCL）の 4 つのサブネットを持つ仮想ネットワークを作成します。

a) 仮想ネットワークを作成します。

1. [基本（Basics）] タブで、ドロップダウンリストから [サブスクリプション（Subscription）] および [リソースグループ（Resource group）] を選択します。
2. 必須の [リージョン（Region）] を選択します。[次へ：IPアドレス（Next: IP addresses）] をクリックします。

[IPアドレス（IP Addresses）] タブで、[サブネットの追加（Add subnet）] をクリックし、管理、診断、データ、およびクラスタ制御リンクのサブネットを追加します。

b) サブネットを追加します。

ステップ 5 カスタムテンプレートを展開します。

a) **[作成（Create）] > [テンプレートの展開（Template deployment）]（カスタムテンプレートを使用して展開）**をクリックします。

b) [エディタで独自のテンプレートを構築する（Build your own template in the editor）] をクリックします。

c) [ファイルのロード（Load File）] をクリックし、**azure_ftdv_gwlb_cluster.json**

d) [保存（Save）] をクリックします。

ステップ 6 インスタンスの詳細を設定します。

a) 必要な値を入力し、[確認して作成（Review + create）] をクリックします。

b) 検証に合格したら、[作成（Create）] をクリックします。

ステップ 7 インスタンスの実行後、いずれかのノードにログインし、**show cluster info** コマンドを入力して、クラスタの展開を確認します。

図 *169 : show cluster info*

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID        : 0
        Version   : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP    : 10.1.1.12
        CCL MAC   : 000d.3a55.5470
        Module    : NGFWv
        Resource  : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

ステップ 8 Azure ポータルで、Function アプリをクリックしてクラスタを Firewall Management Center に登録します。

（注）
Function アプリを使用しない場合は、**[追加（Add）]** > **[デバイス（Device）]**（ **[追加（Add）]** > **[クラスタ（Cluster）]** ではない）を使用して、制御ノードを Firewall Management Center に直接登録することもできます。その他のクラスタノードは自動的に登録されます。

ステップ 9 **[展開センター（Deployment Center）]** > **[FTPSのログイン情報（FTPS credentials）]** > **[ユーザースコープ（User scope）]** > **[ユーザー名とパスワードの設定（Configure Username and Password）]**をクリックして FTPS のログイン情報を作成し、[保存（Save）] をクリックします。

ステップ 10 ローカルの端末で次の **curl** コマンドを実行し、Cluster_Function.zip ファイルを Function アプリにアップロードします。

curl -X POST -u ユーザー名 **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

（注）
curl コマンドは、実行が完了するまでに数分（2 分未満～ 3 分）かかる場合があります。

関数が Function アプリにアップロードされます。関数が開始され、ストレージアカウントのアウトキューにログが表示されます。Management Center へのデバイス登録が開始されます。

図 *170* : 機能

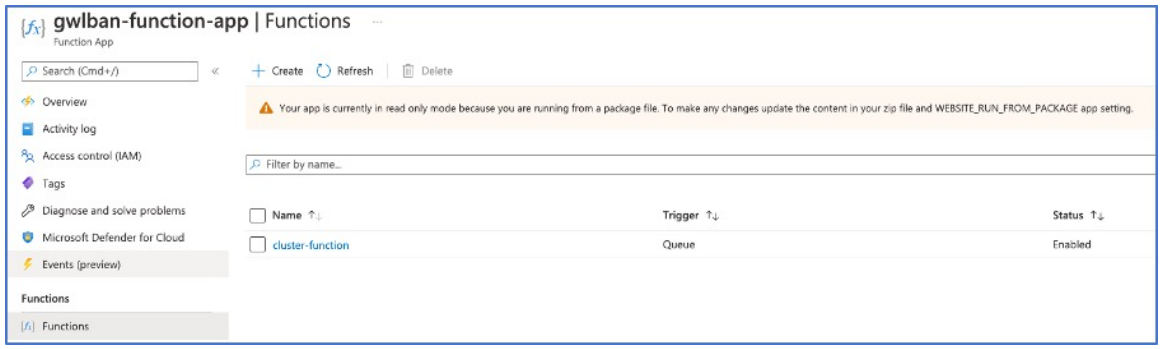


図 *171* : キュー

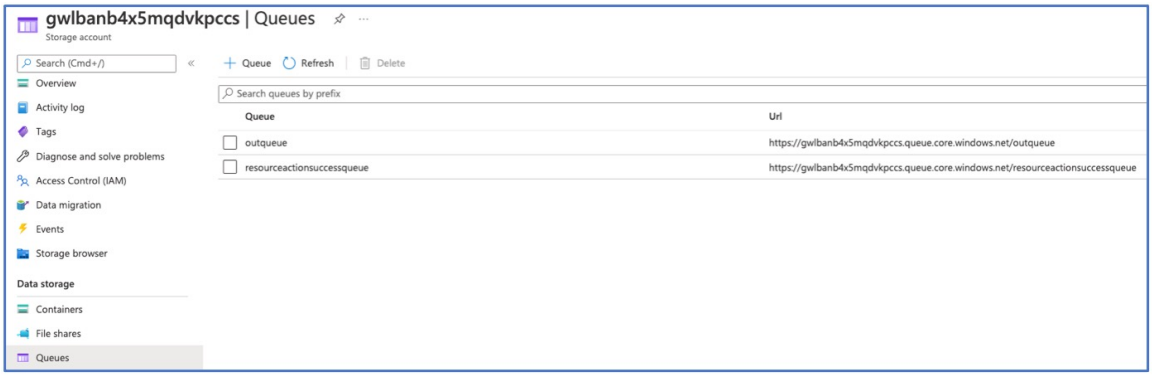
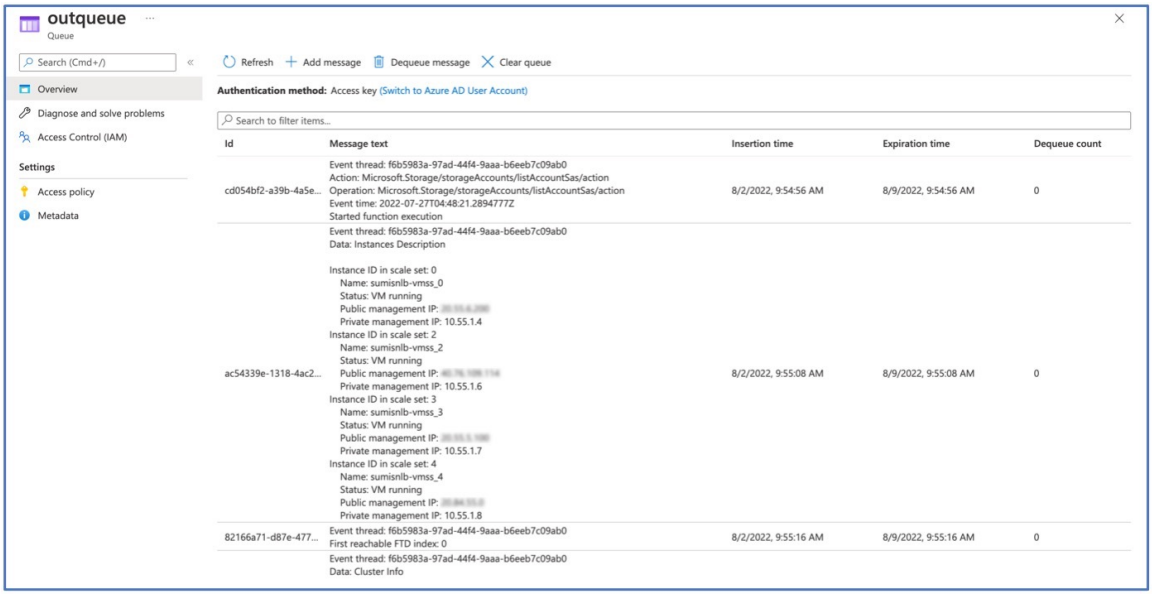
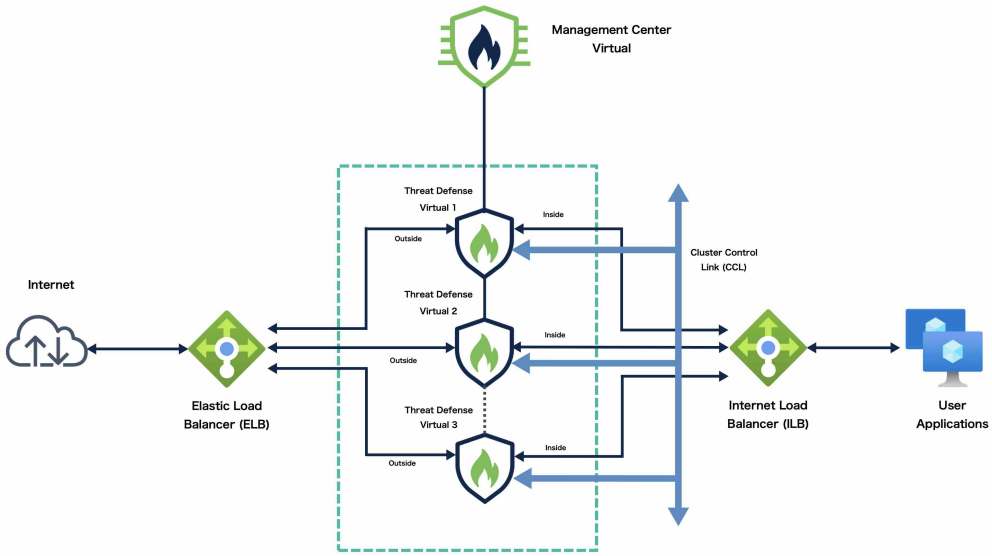


図 *172* : アウトキュー



NLB ベースのクラスタ展開のサンプルトポロジ



このトポロジは、着信と発信の両方のトラフィックフローを示しています。Threat Defense Virtual クラスタは、内部ロードバランサと外部ロードバランサの間に挟まれています。Management Center Virtual インスタンスは、クラスタの管理に使用されます。

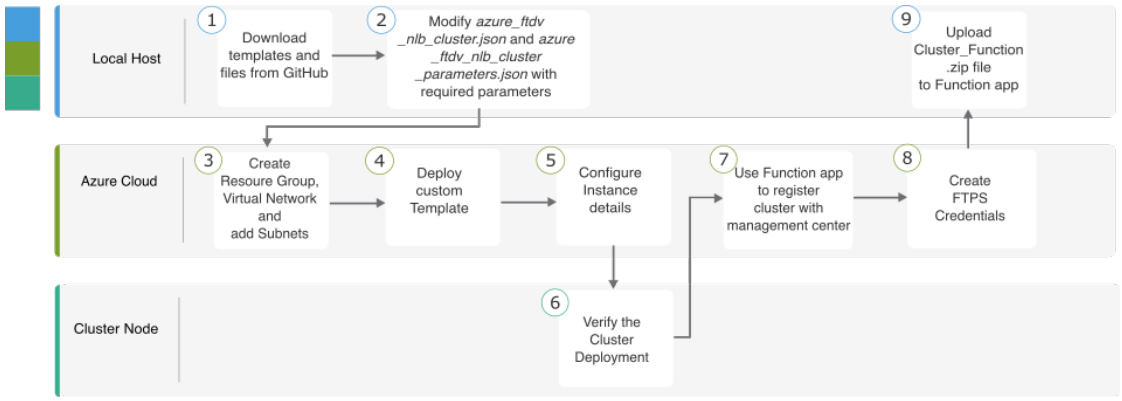
インターネットからの着信トラフィックは、外部ロードバランサに送られ、そこから Threat Defense Virtual クラスタにトラフィックが送信されます。トラフィックは、クラスタ内の Threat Defense Virtual インスタンスによって検査された後、アプリケーション VM に転送されます。

アプリケーション VM からの発信トラフィックは、内部ロードバランサに送信されます。その後、トラフィックは Threat Defense Virtual クラスタに転送され、インターネットに送信されます。

NLB を使用して Azure で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス

テンプレートベースの展開

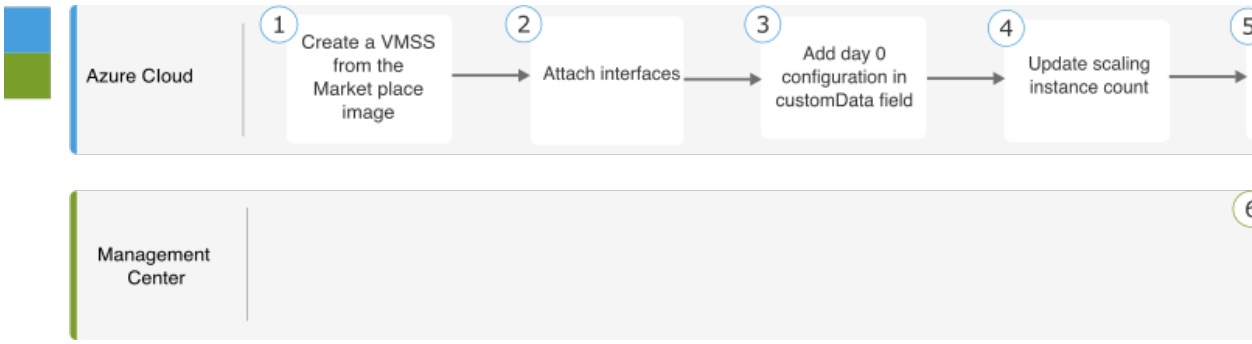
次のフローチャートは、NLB を使用した Azure での Threat Defense Virtual クラスタのテンプレートベース展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	GitHub からテンプレートとファイルをダウンロードします。
2	ローカルホスト	azure_ftdv_nlb_cluster.json と azure_ftdv_nlb_cluster_parameters.json を必要なパラメータで変更します。
3	Azure Cloud	リソースグループ、仮想ネットワーク、およびサブネットを作成します。
4	Azure Cloud	カスタムテンプレートを展開します。
5	Azure Cloud	インスタンスの詳細を設定します。
6	クラスタノード	クラスタの展開を確認します。
7	Azure Cloud	Function アプリを使用して Management Center にクラスタを登録します。
8	Azure Cloud	FTPS のログイン情報を作成します。
9	ローカルホスト	Cluster_Function.zip ファイルを Function アプリにアップロードします。

手動展開

次のフローチャートは、NLB を使用した Azure での Threat Defense Virtual クラスタの手動展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	Marketplace イメージから VMSS を作成します。
2	ローカルホスト	インターフェイスを接続します。
3	ローカルホスト	[customData] フィールドに Day 0 構成を追加します。
4	ローカルホスト	スケーリングインスタンス数を更新します。
5	ローカルホスト	NLB を設定します。
6	Management Center	制御ノードを追加します。

テンプレート

以下のテンプレートは GitHub で入手できます。パラメータ値は、テンプレートで指定されたパラメータ名、および値であり、自明です。

- azure_ftdv_nlb_cluster_parameters.json：NLB を使用して Threat Defense Virtual クラスタのパラメータを入力するためのテンプレート。
- azure_ftdv_nlb_cluster.json：NLB を使用して Threat Defense Virtual クラスタを展開するためのテンプレート。

前提条件

- クラスタが Management Center に自動登録できるようにするには、Management Center でネットワーク管理者およびメンテナンスのユーザー権限を持つユーザーを作成します。これらの権限を持つユーザーは、REST API を使用できます。『Cisco Secure Firewall Management Center Administration Guide』を参照してください。
- テンプレートの展開時に指定するポリシー名と一致するアクセスポリシーを Management Center に追加します。

- Management Center Virtual が適切にライセンスされていることを確認します。
- クラスタが Management Center Virtual に追加されたら、次の手順を実行します。

1. Management Center のプラットフォーム設定でヘルスチェックのポート番号を設定します。この設定の詳細については、「Platform Settings」を参照してください。
2. 外部および内部インターフェイスからのトラフィックのスタティックルートを作成します。スタティックルートの作成の詳細については、「Add a Static Route」を参照してください。

   外部インターフェイスのスタティックルートの設定例：

```
Network: any-ipv4
Interface: outside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-outside
Tunneled: false
Metric: 10
```

（注） *ftdv-cluster-outside* は、外部サブネットのゲートウェイ IP アドレスです。

   内部インターフェイスのスタティックルートの設定例：

```
Network: any-ipv4
Interface: inside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-inside-gw
Tunneled: false
Metric: 11
```

（注） *ftdv-cluster-inside-gw* は、内部サブネットのゲートウェイ IP アドレスです。

3. データトラフィックの NAT ルールを設定します。NAT ルールの設定の詳細については、「Network Address Translation」を参照してください。

Azure Resource Manager テンプレートを使用した Azure と NLB でのクラスタの展開

カスタマイズされた Azure Resource Manager（ARM）テンプレートを使用して、Azure NLB のクラスタを展開します。

手順

ステップ 1 テンプレートを準備します。

a) GitHub リポジトリをローカルフォルダに複製します。https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure を参照してください。

b) azure_ftdv_nlb_cluster.json と azure_ftdv_nlb_cluster_parameters.json を必要なパラメータで変更します。

ステップ 2 Azure ポータルにログイン：https://portal.azure.com。

ステップ 3 リソース グループを作成します。

a) [基本（Basics）] タブで、ドロップダウンリストから [サブスクリプション（Subscription）] および [リソースグループ（Resource group）] を選択します。

b) 必須の [リージョン（Region）] を選択します。

ステップ 4 管理、診断、内部、外部、クラスタ制御リンクの 5 つのサブネットを持つ仮想ネットワークを作成します。

a) 仮想ネットワークを作成します。

1. [基本（Basics）] タブで、ドロップダウンリストから [サブスクリプション（Subscription）] および [リソースグループ（Resource group）] を選択します。
2. b）必須の [リージョン（Region）] を選択します。[次へ：IPアドレス（Next: IP addresses）] をクリックします。

b) サブネットを追加します。

[IPアドレス（IP Addresses）] タブで、[サブネットの追加（Add subnet）] をクリックし、管理、診断、内部、外部、およびクラスタ制御リンクのサブネットを追加します。

ステップ 5 カスタムテンプレートを展開します。

a) **[作成（Create）]** > **[テンプレートの展開（Template deployment）]（カスタムテンプレートを使用して展開）**をクリックします。

b) [エディタで独自のテンプレートを構築する（Build your own template in the editor）] をクリックします。

c) [ファイルのロード（Load File）] をクリックし、**azure_ftdv_nlb_cluster.json** 。

d) [保存（Save）] をクリックします。

ステップ 6 インスタンスの詳細を設定します。

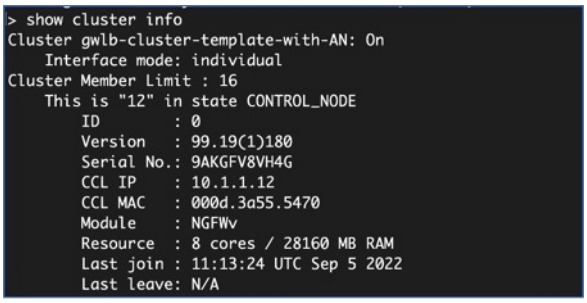
a) 必要な値を入力し、[確認して作成（Review + create）] をクリックします。

（注）
クラスタ制御リンクの開始アドレスと終了アドレスは、必要な数だけ指定してください（最大 16 個）。範囲を大きくすると、パフォーマンスに影響する可能性があります。

b) 検証に合格したら、[作成（Create）] をクリックします。

ステップ 7 インスタンスの実行後、いずれかのノードにログインし、**show cluster info** コマンドを使用して、クラスタの展開を確認します。

図 *173 : show cluster info*



ステップ 8 Azure ポータルで、Function アプリをクリックしてクラスタを Firewall Management Center に登録します。

（注）
Function アプリを使用しない場合は、[追加（Add）] > [デバイス（Device）]（[追加（Add）] > [クラスタ（Cluster）] ではない）を使用して、制御ノードを Management Center に直接登録することもできます。その他のクラスタノードは自動的に登録されます。

ステップ 9 **[展開センター（Deployment Center）] > [FTPSのログイン情報（FTPS credentials）] > [ユーザースコープ（User scope）] > [ユーザー名とパスワードの設定（Configure Username and Password）]**をクリックして FTPS のログイン情報を作成し、[保存（Save）] をクリックします。

ステップ 10 ローカルの端末で次の **curl** コマンドを実行し、Cluster_Function.zip ファイルを Function アプリにアップロードします。

curl -X POST -u ユーザー名 **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

（注）
curl コマンドは、実行が完了するまでに数分（2 分未満～ 3 分）かかる場合があります。

関数が Function アプリにアップロードされます。関数が開始され、ストレージアカウントのアウトキューにログが表示されます。Management Center へのデバイス登録が開始されます。

Azure でのクラスタの手動展開

クラスタを手動で展開するには、Day0 構成を準備し、各ノードを展開してから制御ノードを Firewall Management Center に追加します。

Azure 向け Day 0 構成の作成

固定構成またはカスタマイズ構成のいずれかを使用できます。

Azure 向け固定構成を使用した Day 0 構成の作成

固定構成により、クラスタのブートストラップ構成が自動生成されます。

```
{
 "AdminPassword": "password",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Diagnostic": "OFF",    //For deployment of version 7.4.1 and later without Diagnostics
 template, set this parameter to OFF.
. "FmcIp": "<FMC_IP>",
 "FmcRegKey": "<REGISTRATION_KEY>",
 "FmcNatId": "<NAT_ID>",
 "Cluster": {
  "CclSubnetRange": "ip_address_start ip_address_end",
  "ClusterGroupName": "cluster_name",
  "HealthProbePort": "port_number",
  "GatewayLoadBalancerIP": "ip_address",
  "EncapsulationType": "vxlan",
  "InternalPort": "internal_port_number",
  "ExternalPort": "external_port_number",
  "InternalSegId": "internal_segment_id",
  "ExternalSegId": "external_segment_id"
 }
}
```

例

次に、Day 0 構成の例を示します。

```
{
 "AdminPassword": "password",
 "FirewallMode": "routed",
 "ManageLocally": "No",
 "Diagnostic": "OFF",    //For deployment of version 7.4.1 and later without Diagnostics
 template, set this parameter to OFF.
 "FmcIp":"<FMC_IP>",
 "FmcRegKey":"<REGISTRATION_KEY>",
 "FmcNatId":"<NAT_ID>",
 "Cluster": {
  "CclSubnetRange": "10.45.3.4 10.45.3.30",     //mandatory user input
  "ClusterGroupName": "ngfwv-cluster",          //mandatory user input
  "HealthProbePort": "7777",                    //mandatory user input
  "GatewayLoadBalancerIP": "10.45.2.4",          //mandatory user input
  "EncapsulationType": "vxlan",
  "InternalPort": "2000",
  "ExternalPort": "2001",
  "InternalSegId": "800",
  "ExternalSegId": "801"
 }
}
```

（注） 上記の設定をコピーして貼り付ける場合は、設定から **//mandatory user input** を必ず削除してください。

Azureヘルスチェックの設定では、ここで設定した**HealthProbePort**を必ず指定してください。

CclSubnetRange 変数には、x.x.x.4 から始まる IP アドレスの範囲を指定します。クラスタリングに使用可能な IP アドレスが 16 個以上あることを確認します。開始 IP アドレスと終了 IP アドレスの例を次に示します。

表 *35 :* 開始 *IP* アドレスと終了 *IP* アドレスの例

CIDR	開始 IP アドレス	終了 IP アドレス
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254

Azure 向けカスタマイズ構成を使用した Day 0 構成の作成

コマンドを使用して、クラスタのブートストラップ設定をすべて入力できます。

```
{
 "AdminPassword": "password",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Diagnostic": "OFF",    //For deployment of version 7.4.1 and later without Diagnostics
 template, set this parameter to OFF.
 "FmcIp": "<FMC_IP>",
 "FmcRegKey": "<REGISTRATION_KEY>",
 "FmcNatId": "<NAT_ID>",
 "Cluster": {
  "CclSubnetRange": "ip_address_start ip_address_end",
  "ClusterGroupName": "cluster_name",
  "HealthProbePort": "port_number",
  "GatewayLoadBalancerIP": "ip_address",
  "EncapsulationType": "vxlan",
  "InternalPort": "internal_port_number",
  "ExternalPort": "external_port_number",
  "InternalSegId": "internal_segment_id",
  "ExternalSegId": "external_segment_id"
 }
}
```

例

以下に、**バージョン 7.4 以降**の Day 0 構成の例を示します。

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "clusterftdv",
 "FirewallMode": "routed",
 "ManageLocally": "No",
```

```
"Diagnostic": "OFF",    //For deployment of version 7.4.1 and later without Diagnostics
template, set this parameter to OFF.
"FmcIp": "<FMC_IP>",
"FmcRegKey": "<REGISTRATION_KEY>",
"FmcNatId": "<NAT_ID>",
"run_config": [
 "cluster interface-mode individual force",
 "policy-map global_policy",
 "class inspection_default",
 "no inspect h323 h225",
 "no inspect h323 ras",
 "no inspect rtsp",
 "no inspect skinny",
 "interface Management0/0",
 "management-only",
 "nameif management",
 "security-level 0",
 "ip address dhcp",
 "interface GigabitEthernet0/0",
 "no shutdown",
 "nameif vxlan_tunnel",
 "security-level 0",
 "ip address dhcp",
 "interface GigabitEthernet0/1",
 "no shutdown",
 "nve-only cluster",
 "nameif ccl_link",
 "security-level 0",
 "ip address dhcp",
 "interface vni1",
 "description Clustering Interface",
 "segment-id 1",
 "vtep-nve 1",
 "interface vni2",
 "proxy paired",
 "nameif GWLB-backend-pool",
 "internal-segment-id 800",
 "external-segment-id 801",
 "internal-port 2000",
 "external-port 2001",
 "security-level 0",
 "vtep-nve 2",
 "object network ccl#link",
 "range 10.45.3.4 10.45.3.30",                          //mandatory user input
 "object-group network cluster#group",
 "network-object object ccl#link",
 "nve 1 ",
 "encapsulation vxlan",
 "source-interface ccl_link",
 "peer-group cluster#group",
 "nve 2 ",
 "encapsulation vxlan",
 "source-interface vxlan_tunnel",
 "peer ip <GatewayLoadbalancerIP>",
 "cluster group ftdv-cluster",                          //mandatory user input
 "local-unit 1",
 "cluster-interface vni1 ip 1.1.1.1 255.255.255.0",
 "priority 1",
 "enable",
 "mtu vxlan_tunnel 1454",
 "mtu ccl_link 1454"
]
}
```

以下に、**バージョン 7.3 以前**の Day 0 構成の例を示します。

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "clusterftdv",
 "FirewallMode": "routed",
 "ManageLocally": "No",
 "FmcIp": "<FMC_IP>",
 "FmcRegKey": "<REGISTRATION_KEY>",
 "FmcNatId": "<NAT_ID>",
 "run_config": [
  "cluster interface-mode individual force",
  "policy-map global_policy",
  "class inspection_default",
  "no inspect h323 h225",
  "no inspect h323 ras",
  "no inspect rtsp",
  "no inspect skinny",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "security-level 0",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif vxlan_tunnel",
  "security-level 0",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nve-only cluster",
  "nameif ccl_link",
  "security-level 0",
  "ip address dhcp",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "interface vni2",
  "proxy paired",
  "nameif GWLB-backend-pool",
  "internal-segment-id 800",
  "external-segment-id 801",
  "internal-port 2000",
  "external-port 2001",
  "security-level 0",
  "vtep-nve 2",
  "object network ccl#link",
  "range 10.45.3.4 10.45.3.30",                          //mandatory user input
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 1 ",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "nve 2 ",
  "encapsulation vxlan",
  "source-interface vxlan_tunnel",
  "peer ip <GatewayLoadbalancerIP>",
  "cluster group ftdv-cluster",                          //mandatory user input
  "local-unit 1",
  "cluster-interface vni1 ip 1.1.1.1 255.255.255.0",
  "priority 1",
```

```
  "enable",
  "mtu vxlan_tunnel 1454",
  "mtu ccl_link 1554"
 ]
}
```

（注） 上記の設定をコピーして貼り付ける場合は、設定から **//mandatory user input** を必ず削除してください。

クラスタノードの手動展開：GWLB ベースの展開

クラスタが形成されるようにクラスタノードを展開します。

手順

ステップ 1 **az vmss create** CLI を使用して、インスタンス数が 0 の Marketplace イメージから仮想マシンスケールセットを作成します。

az vmss create --resource-group <*ResourceGroupName*> **--name** <*VMSSName*> **--vm-sku** <*InstanceSize*> **--image** <*FTDvImage*> **--instance-count 0 --admin-username** <*AdminUserName*> **--admin-password** <*AdminPassword*> **--plan-name** <*ftdv-azure-byol/ftdv-azure-payg*> **--plan-publisher cisco --plan-product cisco-ftdv --plan-promotion-code** <*ftdv-azure-byol/ftdv-azure-payg*> **--vnet-name** <*VirtualNetworkName*> **--subnet** <*MgmtSubnetName*>

ステップ 2 3 つのインターフェイス（診断、データ、およびクラスタ制御リンク）を接続します。

ステップ 3 作成した仮想マシンスケールセットに移動し、次の手順を実行します。

a) [オペレーティングシステム（Operating system）] セクションで、[customData] フィールドに Day 0 構成を追加します。

b) [保存（Save）] をクリックします。

c) [スケーリング（Scaling）] セクションで、インスタンス数を必要なクラスタノードで更新します。インスタンス数は、最小 1、最大 16 の範囲に設定できます。

ステップ 4 Azure ゲートウェイロードバランサを設定します。詳細については、「Azure ゲートウェイロードバランサを使用した Auto Scale の導入例」を参照してください。

ステップ 5 Firewall Management Center に制御ノードを追加します。「Management Center へのクラスタの追加（手動展開） （504 ページ）」を参照してください。

クラスタノードの手動展開：NLB ベースの展開

クラスタが形成されるようにクラスタノードを展開します。

手順

ステップ 1 **az vmss create** CLI を使用して、インスタンス数が 0 の Marketplace イメージから仮想マシンスケールセットを作成します。

az vmss create --resource-group <*ResourceGroupName*> **--name** <*VMSSName*> **--vm-sku** <*InstanceSize*> **--image** <*FTDvImage*> **--instance-count 0 --admin-username** <*AdminUserName*> **--admin-password** <*AdminPassword*> **--plan-name** <*ftdv-azure-byol/ftdv-azure-payg*> **--plan-publisher cisco --plan-product cisco-ftdv --plan-promotion-code** <*ftdv-azure-byol/ftdv-azure-payg*> **--vnet-name** <*VirtualNetworkName*> **--subnet** <*MgmtSubnetName*>

ステップ 2 4 つのインターフェイス（診断、内部、外部、およびクラスタ制御リンク）を接続します。

ステップ 3 作成した仮想マシンスケールセットに移動し、次の手順を実行します。

a) [オペレーティングシステム（Operating system）] セクションで、[customData] フィールドに Day 0 構成を追加します。

b) [保存（Save）] をクリックします。

c) [スケーリング（Scaling）] セクションで、インスタンス数を必要なクラスタノードで更新します。インスタンス数は、最小 1、最大 16 の範囲に設定できます。

ステップ 4 Management Center に制御ノードを追加します。「Management Center へのクラスタの追加（手動展開）（504 ページ）」を参照してください。

Azure でのトラブルシューティング クラスタ展開

- 問題：トラフィックフローがない

  トラブルシューティング：

  - GWLB で展開された Threat Defense Virtual インスタンスの正常性プローブステータスが正常かどうかを確認します。
  - Threat Defense Virtual インスタンスの正常性プローブステータスが異常である場合：
    - Management Center Virtual でスタティックルートが設定されているかどうかを確認します。
    - デフォルトゲートウェイがデータサブネットのゲートウェイ IP であるかどうかを確認します。
    - Threat Defense Virtual インスタンスが正常性プローブトラフィックを受信しているかどうかを確認します。
    - Management Center Virtual で設定されたアクセスリストが正常性プローブトラフィックを許可しているかどうかを確認します。

- 問題：クラスタが形成されていない

トラブルシューティング：

- nve-only クラスタインターフェイスの IP アドレスを確認します。他のノードの nve-only のクラスタインターフェイスにピン可能であることを確認します。
- nve-only のクラスタインターフェイスの IP アドレスが、オブジェクトグループの一部であることを確認します。
- NVE インターフェイスがオブジェクトグループで設定されていることを確認します。
- クラスタグループのクラスタインターフェイスに適切な VNI インターフェイスがあることを確認します。この VNI インターフェイスには、対応するオブジェクトグループを持つ NVE があります。
- ノードが相互にピン可能であることを確認します。各ノードに独自のクラスタインターフェイス IP があるため、これらは相互にピン可能である必要があります。
- テンプレート展開中に指定された CCL サブネットの開始アドレスと終了アドレスが正しいかどうかを確認します。開始アドレスは、サブネット内で使用可能な最初の IP アドレスで始まる必要があります。たとえばサブネットが 192.168.1.0/24 の場合、開始アドレスは 192.168.1.4 である必要があります（最初の 3 つの IP アドレスは Azure によって予約されています）。
- Management Center Virtual に有効なライセンスがあるかどうかを確認します。

- 問題：同じリソースグループに再度リソースを展開しているときにロールに関連するエラーが発生する。

  トラブルシューティング：端末で次のコマンドを使用して、以下のロールを削除します。

  エラー メッセージ：

```
"error": {
"code": "RoleAssignmentUpdateNotPermitted",
"message": "Tenant ID, application ID, principal ID, and scope are not allowed to
be
updated.”}
```

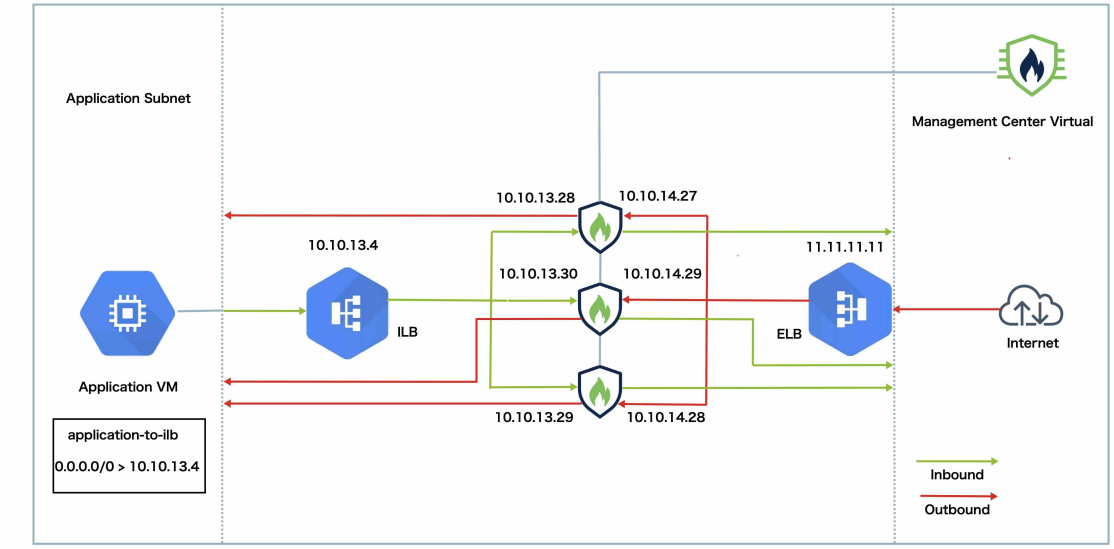
  - **az role assignment delete --resource-group** <リソースグループ名> **--role "Storage Queue Data Contributor"**
  - **az role assignment delete --resource-group** <リソースグループ名> **--role "Contributor"**

GCP でのクラスタの展開

クラスタを GCP で展開するには、手動で展開するか、インスタンステンプレートを使用してインスタンスグループを展開します。GCP ロードバランサ、または Cisco Cloud Services Router などの非ネイティブのロードバランサでクラスタを使用できます。

（注） 発信トラフィックはインターフェイス NAT が必要であり、64K 接続に制限されています。

トポロジの例



このトポロジは、着信と発信の両方のトラフィックフローを示しています。Threat Defense Virtual クラスタは、内部ロードバランサと外部ロードバランサの間に挟まれています。Management Center Virtual インスタンスは、クラスタの管理に使用されます。

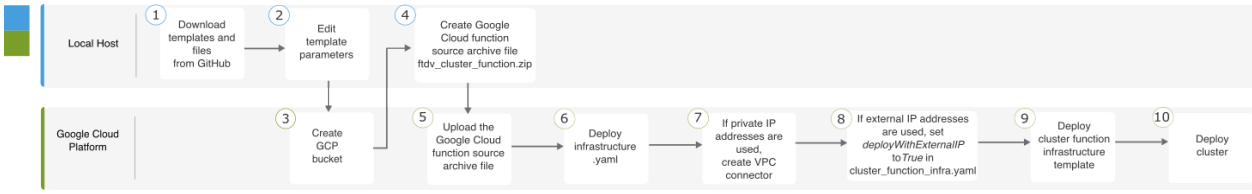
インターネットからの着信トラフィックは、外部ロードバランサに送られ、そこから Threat Defense Virtual クラスタにトラフィックが送信されます。トラフィックは、クラスタ内の Threat Defense Virtual インスタンスによって検査された後、アプリケーション VM に転送されます。

アプリケーション VM からの発信トラフィックは、内部ロードバランサに送信されます。その後、トラフィックは Threat Defense Virtual クラスタに転送され、インターネットに送信されます。

GCP で Threat Defense Virtual クラスタを展開するためのエンドツーエンドのプロセス

テンプレートベースの展開

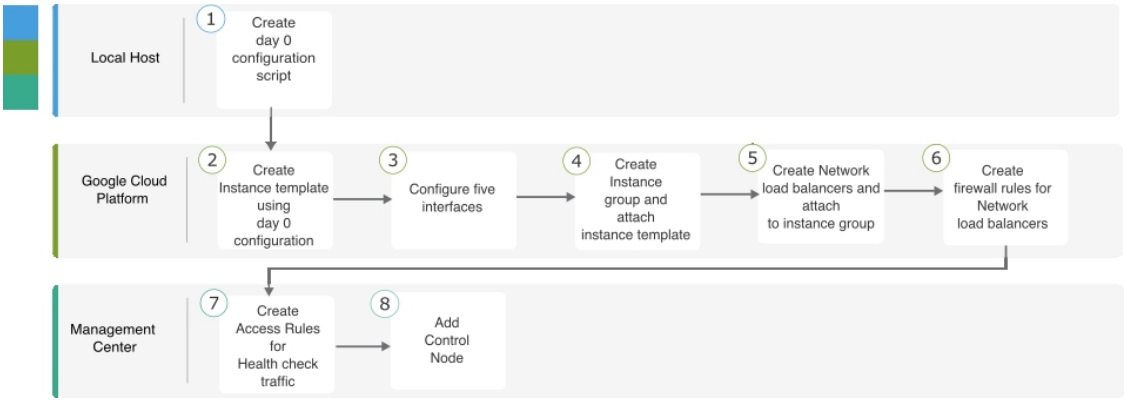
次のフローチャートは、GCP での Threat Defense Virtual クラスタのテンプレートベース展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	GitHub からテンプレートとファイルをダウンロードします。
2	ローカルホスト	テンプレートパラメータを編集します。
3	Google Cloud Platform	GCP バケットを作成します。
4	ローカルホスト	Google Cloud 関数ソースアーカイブファイル ftdv_cluster_function.zip を作成します。
5	Google Cloud Platform	Google 関数ソースアーカイブファイルをアップロードします。
6	Google Cloud Platform	infrastructure.yaml を展開します。
7	Google Cloud Platform	プライベート IP アドレスが使用されている場合は、VPC コネクタを作成します。
8	Google Cloud Platform	外部 IP アドレスが使用されている場合は、cluster_function_infra.yaml で deployWithExternalIP を True に設定します。
9	Google Cloud Platform	クラスタ機能インフラストラクチャ テンプレートを展開します。
10	Google Cloud Platform	クラスタを展開します。

手動展開

次のフローチャートは、GCP での Threat Defense Virtual クラスタの手動展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	Day 0 構成スクリプトを作成します。
2	Google Cloud Platform	Day 0 構成を使用してインスタンステンプレートを作成します。
3	Google Cloud Platform	インターフェイスを設定します。
4	Google Cloud Platform	インスタンスグループを作成し、インスタンステンプレートを割り当てます。
5	Google Cloud Platform	NLB を作成し、インスタンスグループにアタッチします。
6	Google Cloud Platform	NLB のファイアウォールルールを作成します。
7	Management Center	ヘルスチェックトラフィックのアクセスルールを作成します。
8	Management Center	制御ノードを追加します。

テンプレート

以下のテンプレートは GitHub で入手できます。パラメータ値は、テンプレートで指定されたパラメータ名、および値であり、自明です。

- East-West トラフィック用のクラスタ展開テンプレート：deploy_ngfw_cluster_yaml
- North-South トラフィック用のクラスタ展開テンプレート：deploy_ngfw_cluster.yaml

インスタンステンプレートを使用したGCPでのインスタンスグループの展開

インスタンステンプレートを使用して、GCP にインスタンスグループを展開します。

始める前に

- 展開には Google Cloud Shell を使用します。または、任意の macOS/Linux/Windows マシンで Google SDK を使用できます。
- クラスタが Management Center に自動登録されるようにするには、REST API を使用できる管理者権限を持つユーザーを Management Center で作成する必要があります。Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。
- cluster_function_infra.yaml で指定したポリシー名と一致するアクセスポリシーを Management Center に追加します。

手順

ステップ 1 テンプレートを GitHub からローカルフォルダにダウンロードします。

ステップ 2 必要な resourceNamePrefix パラメータ（ngfwvcls など）と他の必要なユーザー入力を使用して、**infrastructure.yaml**、**cluster_function_infra.yaml**、および **deploy_ngfw_cluster.yaml** を編集します。

deploy_ngfw_cluster.yaml ファイルは、GitHub で **east-west** フォルダと **north-south** フォルダの両方にあることに注意してください。トラフィックフローの要件に従って、適切なテンプレートをダウンロードします。

ステップ 3 Google Cloud Shell を使用してバケットを作成し、Google Cloud 関数ソースアーカイブファイル ftdv_cluster_function.zip をアップロードします。

gsutil mb --pap enforced gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

ここでの *resourceNamePrefix* 変数が **cluster_function_infra.yaml** で指定した resourceNamePrefix 変数と一致していることを確認します。

ステップ 4 クラスタ インフラストラクチャのアーカイブファイルを作成します。

例：

```
zip -j ftdv_cluster_function.zip ./cluster-function/*
```

ステップ 5 前に作成した Google ソースアーカイブをアップロードします。

gsutil cp ftdv_cluster_function.zip gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

ステップ 6 クラスタのインフラストラクチャを展開します。

gcloud deployment-manager deployments create *cluster_name* **--config infrastructure.yaml**

ステップ 7 プライベート IP アドレスを使用している場合は、次の手順を実行します。

a) Threat Defense Virtual 管理 VPC を使用して、Management Center Virtual を起動してセットアップします。

b) VPC コネクタを作成して、Google Cloud 関数を Threat Defense Virtual 管理 VPC に接続します。

gcloud compute networks vpc-access connectors create *vpc-connector-name* **--region us-central1 --subnet** *resourceNamePrefix*-**ftdv-mgmt-subnet28**

ステップ 8 Management Center が Threat Defense Virtual からリモートに配置され、Threat Defense Virtual に外部 IP アドレスが必要な場合は、必ず **cluster_function_infra.yaml** で **deployWithExternalIP** を **True** に設定してください。

ステップ 9 クラスタ機能インフラストラクチャを展開します。

gcloud deployment-manager deployments create *cluster_name* **--config cluster_function_infra.yaml**

ステップ 10 クラスタを展開します。

1. North-South トポロジ展開の場合：

   gcloud deployment-manager deployments create *cluster_name* **--config north-south/deploy_ngfw_cluster.yaml**

2. East-West トポロジ展開の場合：

   gcloud deployment-manager deployments create *cluster_name* **--config east-west/deploy_ngfw_cluster.yaml**

GCP でのクラスタの手動展開

クラスタを手動で展開するには、Day0 構成を準備し、各ノードを展開してから制御ノードを Firewall Management Center に追加します。

GCP 向け Day 0 構成の作成

固定構成またはカスタマイズ構成のいずれかを使用できます。

GCP 向け固定構成を使用した Day 0 構成の作成

固定構成により、クラスタのブートストラップ構成が自動生成されます。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
                "Diagnostic": "OFF",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name"
```

```
    }
}
```

次に例を示します。

```
{
    "AdminPassword": "DeanW1nche$ter",
    "Hostname": "ciscoftdv",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "10.10.55.2 10.10.55.253",      //mandatory user input
        "ClusterGroupName": "ftdv-cluster"                //mandatory user input
    }
}
```

（注） 上記の設定をコピーして貼り付ける場合は、設定から **//mandatory user input** を必ず削除してください。

CclSubnetRange 変数では、サブネット内の最初の 2 つの IP アドレスと最後の 2 つの IP アドレスを使用できないことに注意してください。詳細については、「Reserved IP addresses in IPv4 subnets」を参照してください。クラスタリングに使用可能な IP アドレスが 16 個以上あることを確認します。開始 IP アドレスと終了 IP アドレスの例を次に示します。

表 *36 :* 開始 *IP* アドレスと終了 *IP* アドレスの例

CIDR	開始 IP アドレス	終了 IP アドレス
10.1.1.0/27	10.1.1.2	10.1.1.29
10.1.1.32/27	10.1.1.34	10.1.1.61
10.1.1.64/27	10.1.1.66	10.1.1.93
10.1.1.96/27	10.1.1.98	10.1.1.125
10.1.1.128/27	10.1.1.130	10.1.1.157
10.1.1.160/27	10.1.1.162	10.1.1.189
10.1.1.192/27	10.1.1.194	10.1.1.221
10.1.1.224/27	10.1.1.226	10.1.1.253
10.1.1.0/24	10.1.1.2	10.1.1.253

GCP 向けカスタマイズ構成を使用した Day 0 構成の作成

コマンドを使用して、クラスタのブートストラップ設定をすべて入力できます。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
```

```
"run_config": [comma_separated_threat_defense_configuration]
}
```

次の例では、管理、内部、および外部インターフェイスと、クラスタ制御リンク用の VXLAN インターフェイスを使用して構成を作成します。太字の値はノードごとに一意である必要があることに注意してください。

```
{
 "AdminPassword": "W1nch3sterBr0s",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif outside",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nameif inside",
  "ip address dhcp",
  "interface GigabitEthernet0/2",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "object network ccl#link",
  "range 10.1.90.2 10.1.90.17",
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "mtu outside 1400",
  "mtu inside 1400"
 ]
}
```

（注） クラスタ制御リンク ネットワーク オブジェクトには、アドレスを必要な数だけ指定します（最大 16個）。範囲を大きくすると、パフォーマンスに影響する可能性があります。

クラスタノードの手動展開

クラスタが形成されるようにクラスタノードを展開します。GCP でのクラスタリングの場合、4 vCPU マシンタイプは使用できません。4 vCPU マシンタイプがサポートするインターフェイスは 4 つのみですが、インターフェイスは 5 つ必要です。c2-standard-8 など、5 つのインターフェイスがサポートされるマシンタイプを使用します。

手順

ステップ 1 5 つのインターフェイス（外部、内部、管理、診断、クラスタ制御リンク）を備えた Day 0 構成を使用して、インスタンステンプレートを作成します（[メタデータ（Metadata）] > [スタートアップスクリプト（Startup Script）] セクション）。

Cisco Secure Firewall Threat Defense Virtual スタートアップガイド を参照してください。

ステップ 2 インスタンスグループを作成し、インスタンステンプレートを割り当てます。

ステップ 3 GCP ネットワークロードバランサ（内部および外部）を作成し、インスタンスグループを割り当てます。

ステップ 4 GCP ネットワークロードバランサの場合、Management Center のセキュリティポリシーでヘルスチェックを許可します。GCP ネットワークロードバランサのヘルスチェックの許可 （502 ページ） を参照してください。

ステップ 5 Management Center に制御ノードを追加します。「Management Center へのクラスタの追加（手動展開） （504 ページ）」を参照してください。

GCP ネットワークロードバランサのヘルスチェックの許可

Google Cloud は、バックエンドがトラフィックに応答するかどうかを判断するヘルスチェック機能を提供します。

ネットワークロードバランサのファイアウォール ルールを作成するには、「https://cloud.google.com/load-balancing/docs/health-checks」を参照してください。次に、Firewall Management Center でヘルスチェックトラフィックを許可するアクセスルールを作成します。必要なネットワーク範囲については、「https://cloud.google.com/load-balancing/docs/health-check-concepts」を参照してください。アクセス コントロール ルール （1775 ページ）を参照してください。

また、動的な手動 NAT ルールを設定して、ヘルスチェックトラフィックを 169.254.169.254 の Google メタデータサーバーにリダイレクトする必要もあります。ダイナミック手動 NAT の設定 （934 ページ）を参照してください。

正常性プローブの構成に使用されるすべてのインターフェイスに対する GCP 正常性チェックのルートを設定できます。これは、GCP 正常性チェック用のルートがまだ利用可能になっていないインターフェイスで、より高いメトリックを持つルートを作成することで実現できます。

North-South NAT ルールの設定例

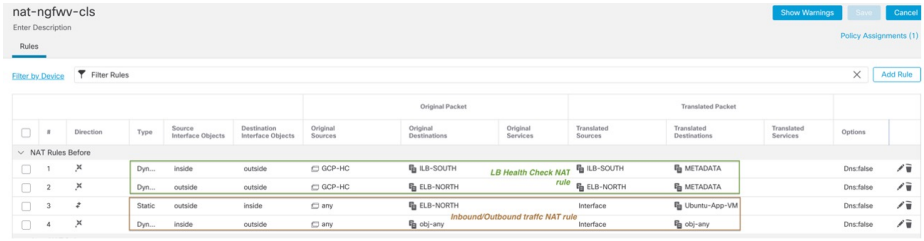
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH
METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



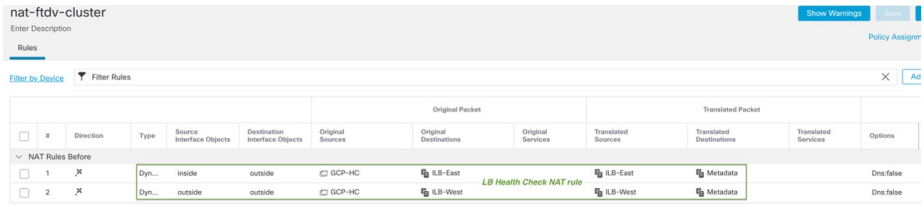
East-West NAT ルールの設定例

```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
host <ILB_East_IP>
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



ノースサウスおよびイーストウェスト トラフィック ルーティングの設定例

```
route outside 0.0.0.0 0.0.0.0 <Outside_Gateway> 1
route inside 35.191.0.0 255.255.0.0 <Inside_Gateway> 1
route inside 130.211.0.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.152.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.204.0 255.255.252.0 <Inside_Gateway> 1
```

デフォルト ルートが使用できない場合、ヘルス チェック用のトラフィックのルーティングにポリシーベース ルーティングを使用できます。

Management Center へのクラスタの追加（手動展開）

クラスタを手動で展開した場合は、この手順を使用してクラスタを Firewall Management Center に追加します。テンプレートを使用した場合、クラスタは自動的に Firewall Management Center に登録されます。

クラスタ ユニットのいずれかを新しいデバイスとして Firewall Management Center に追加します。Firewall Management Center は、他のすべてのクラスタ メンバーを自動検出します。

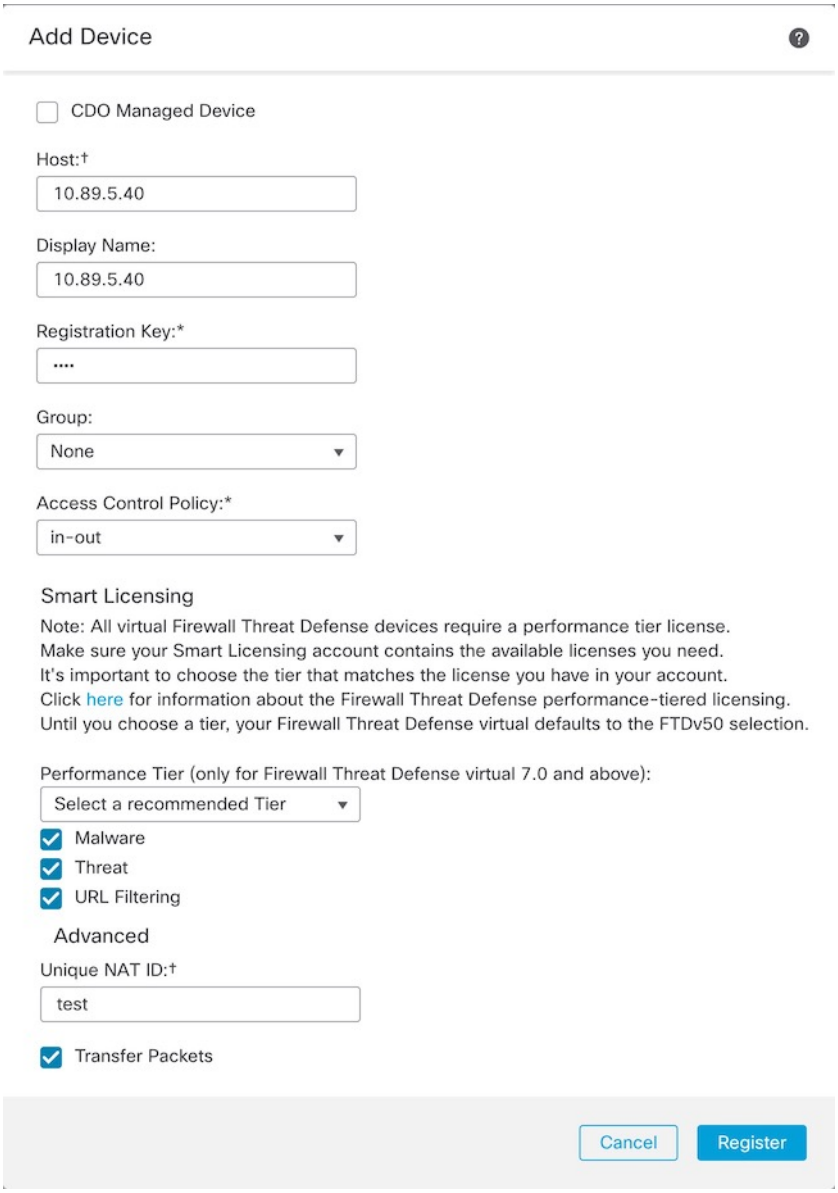
始める前に

- すべてのクラスタユニットは、Firewall Management Center に追加する前に、正常な形式のクラスタ内に存在している必要があります。また、どのユニットが制御ユニットかを確認することも必要です。Firewall Threat Defense **show cluster info** コマンドを使用します。

手順

ステップ 1 Firewall Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択してから、**[追加（Add）]** > **[デバイスの追加（Add Device）]** を選択し、制御ユニットの管理 IP アドレスを使用して制御ユニットを追加します。

図 *174* : デバイスの追加



a) [ホスト（Host）] フィールドに、制御ユニットの IP アドレスまたはホスト名を入力します。

最適なパフォーマンスを得るため、制御ユニットの追加を推奨しますが、クラスタの任意のユニットを追加できます。

デバイスのセットアップ時に NAT ID を使用した場合は、このフィールドを入力する必要がない可能性があります。詳細については、「NAT 環境 （8 ページ）」を参照してください。

b) [表示名（Display Name）] フィールドに、Firewall Management Center での制御ユニットの表示名を入力します。

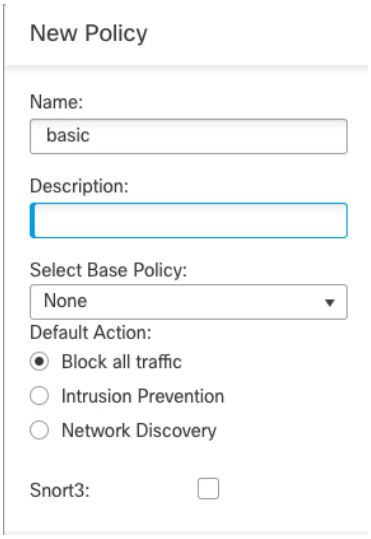
この表示名はクラスタ用ではありません。追加する制御ユニット専用です。後で、他のクラスタメンバーの名前やクラスタ表示名を変更できます。

c) [登録キー（Registration Key）] フィールドに、デバイスの設定時に使用したものと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。

d) （任意） デバイスをデバイス**グループ**に追加します。

e) 登録後すぐに、デバイスに展開する最初の [アクセスコントロールポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。

新しいポリシーを作成する場合は、基本ポリシーのみを作成します。必要に応じて、後でポリシーをカスタマイズできます。



f) デバイスに適用するライセンスを選択します。

g) デバイスの設定時に、NAT ID を使用した場合、[詳細（Advanced）] セクションを展開し、[一意の NAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

h) [パケットの転送（Transfer Packets）] チェックボックスをオンにし、デバイスで Firewall Management Center にパケットを転送することを許可します。

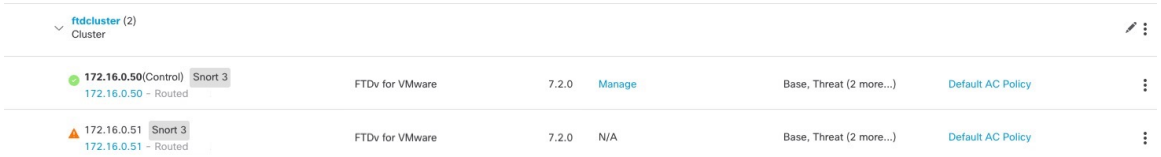
このオプションは、デフォルトで有効です。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Firewall Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Firewall Management Center に送信され、パケットデータは送信されません。

i) [登録（Register）] をクリックします。

Firewall Management Center は、制御ユニットを識別して登録した後に、すべてのデータユニットを登録します。制御ユニットが正常に登録されていない場合、クラスタは追加されません。クラスタが稼働状態になかった場合や、接続問題などが原因で、登録エラーが発生する場合があります。こうした状況では、クラスタユニットを再度追加することをお勧めします。

[デバイス（Devices）] > **[デバイス管理（Device Management）]** ページにクラスタ名が表示されます。クラスタを展開して、クラスタユニットを表示します。

図 *175* : クラスタの管理

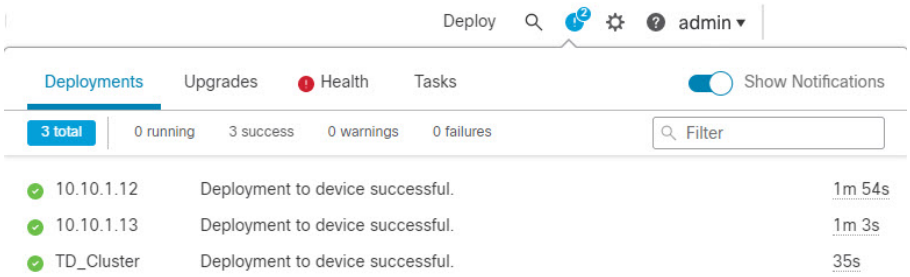


現在登録されているユニットには、ロード アイコンが表示されます。

図 *176* : ノードの登録

（注）
GCP は、クラスタノードの検出中にパブリック IP アドレスを持つノードを優先します。Firewall Threat Defense Virtual クラスタがプライベート IP アドレスを使用して Management Center Virtual に登録されるようにするには、最初に Firewall Threat Defense Virtual クラスタノードでパブリック IP アドレスを無効にする必要があります。これにより、GCP ノードの検出が Management Center Virtual への登録ノードのプライベート IP アドレスを使用して続行されます。

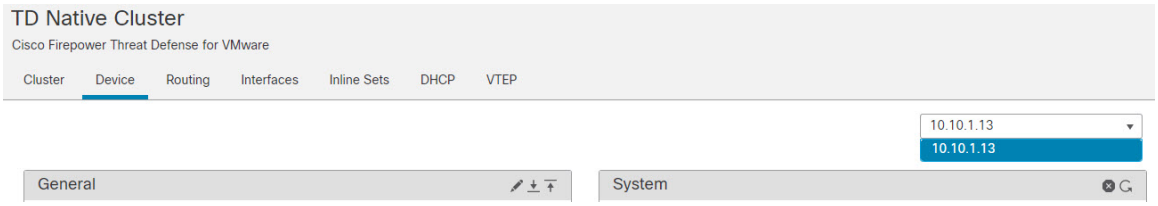
クラスタユニットの登録をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。Firewall Management Center は、ユニットの登録ごとにクラスタ登録タスクを更新します。いずれかのユニットの登録に失敗した場合には、クラスタノードの照合 （518 ページ） を参照してください。



ステップ 2 クラスタの [編集（Edit）]（✎） をクリックして、デバイス固有の設定を指定します。

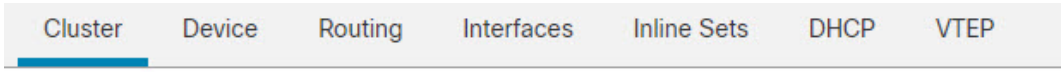
ほとんどの設定は、クラスタ内のノードではなく、クラスタ全体に適用できます。たとえば、ノードごとに表示名を変更できますが、インターフェイスはクラスタ全体についてのみ設定できます。

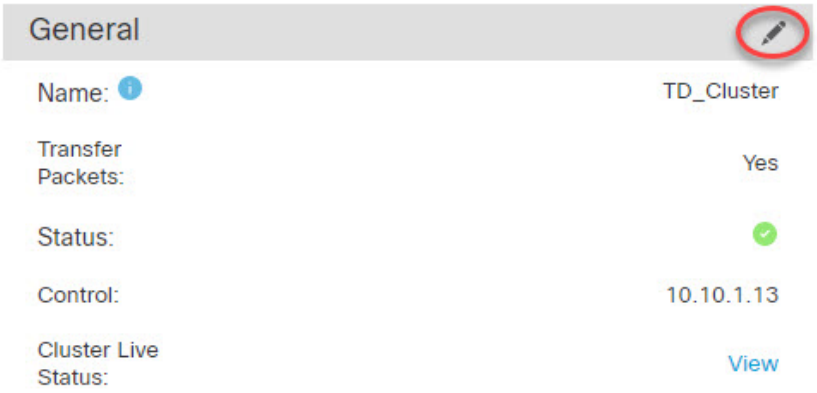
ステップ 3 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** 画面に、[全般（General）]、[ライセンス（License）]、[システム（System）]、および [ヘルス（Health）] の設定が表示されます。



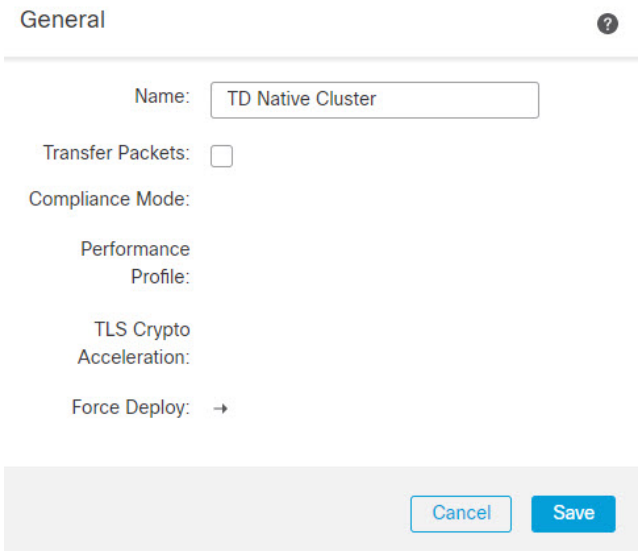
次のクラスタ固有の項目を参照してください。

- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタの表示名を変更します。

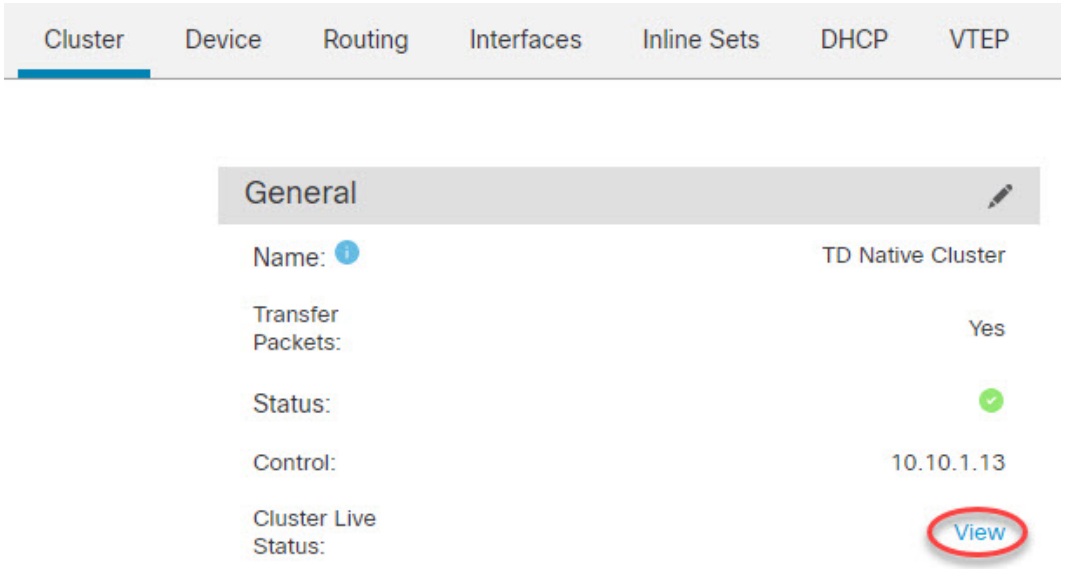




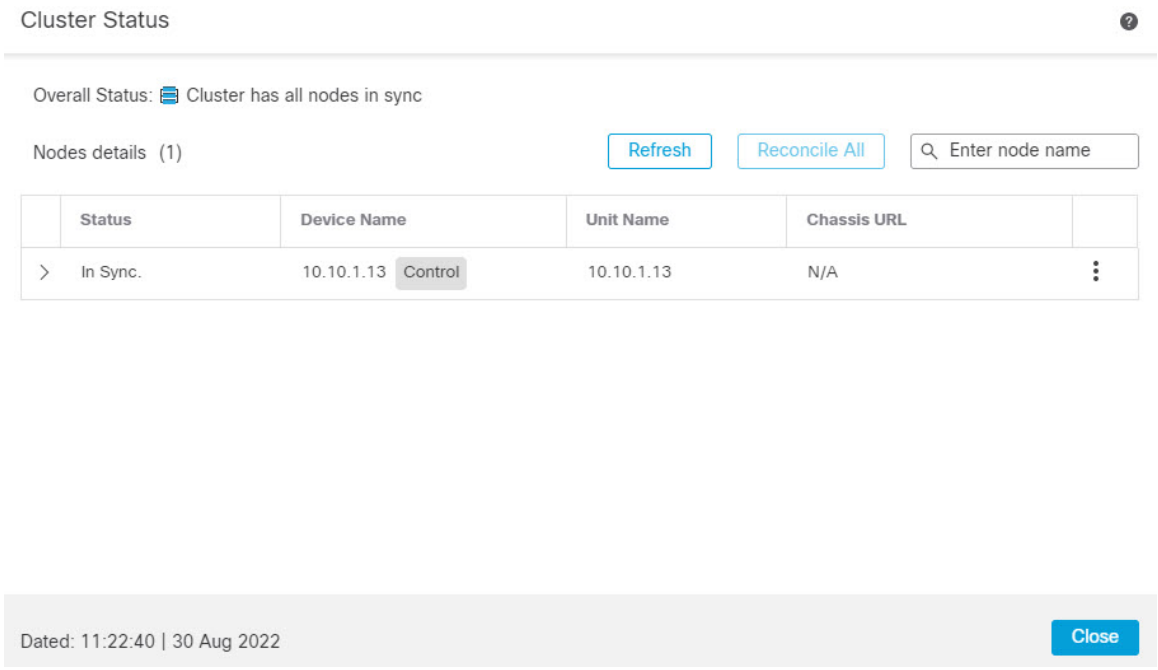
その後に、[名前（Name）] フィールドを設定します。



- [全般（General）] > [クラスタステータスの表示（View cluster status）] : [クラスタステータスの表示（View cluster status）] リンクをクリックして [クラスタステータス（Cluster Status）] ダイアログボックスを開きます。



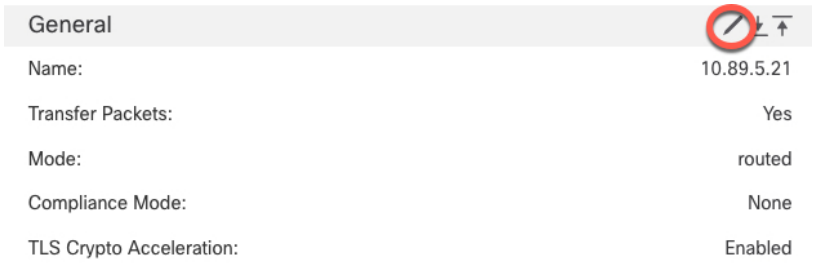
[クラスタステータス（Cluster Status）] ダイアログボックスで、[照合（Reconcile）] をクリックしてデータユニットの登録を再試行することもできます。



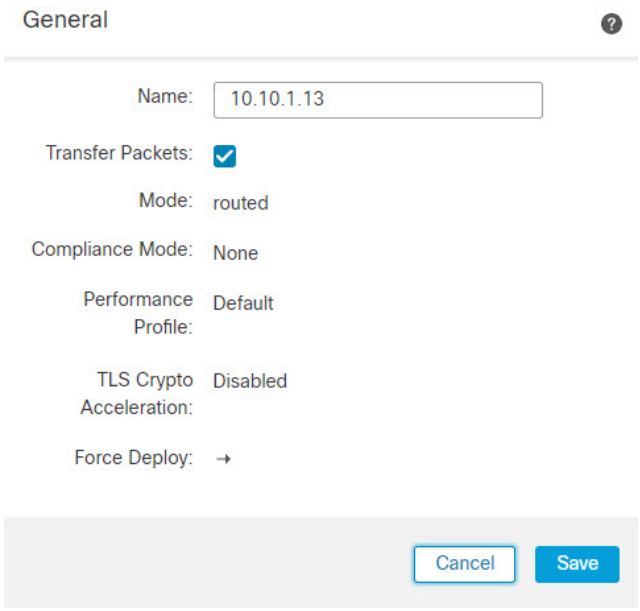
- [ライセンス（License）]：[編集（Edit）]（✎）をクリックして、ライセンス付与資格を設定します。

ステップ 4 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Devices）]** の右上のドロップダウンメニューで、クラスタ内の各メンバーを選択し、次の設定を指定することができます。

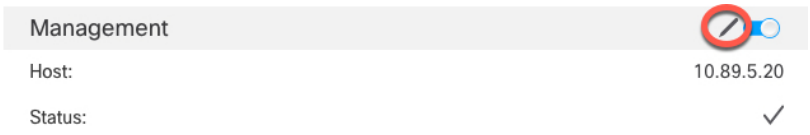
- [全般（General）] > [名前（Name）]：[編集（Edit）]（✎）をクリックして、クラスタメンバーの表示名を変更します。



その後に、[名前（Name）] フィールドを設定します。



- [管理（Management）]>[ホスト（Host）]：デバイス設定で管理 IP アドレスを変更する場合、Firewall Management Center で新しいアドレスを一致させてネットワーク上のデバイスに到達できるようにし、[管理（Management）]領域で[ホスト（Host）]アドレスを編集します。



クラスタのヘルスモニターの設定

[クラスタ（Cluster）]ページの[クラスタヘルスモニターの設定（Cluster Health Monitor Settings）]セクションには、次の表で説明されている設定が表示されます。

図 *177 :* クラスタのヘルスモニターの設定

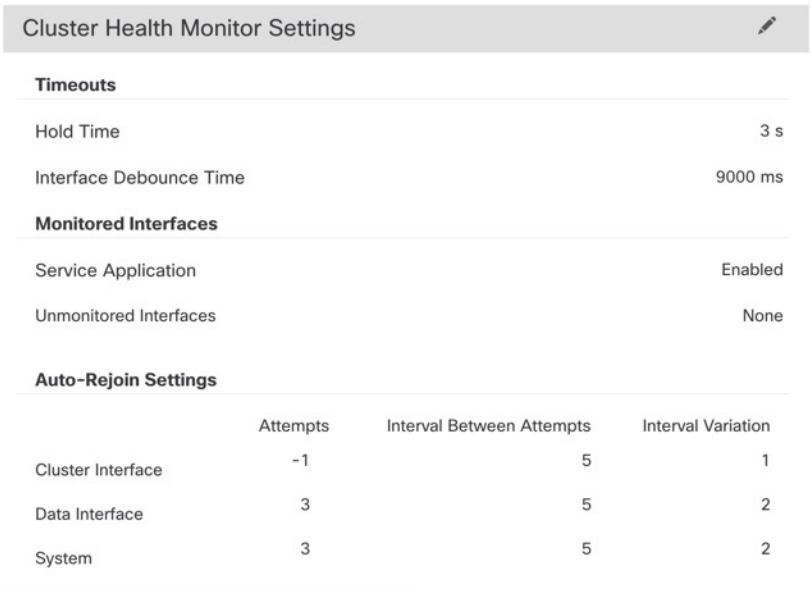


表 *37 : [*クラスタヘルスモニターの設定（***Cluster Health Monitor Settings***）*]* セクションテーブルのフィールド

フィールド	説明
タイムアウト（Timeouts）	
保留時間（Hold Time）	指定できる範囲は 0.3 ～ 45 秒です。デフォルトは 3 秒です。ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間（Interface Debounce Time）	指定できる範囲は 300 ～ 9000 ミリ秒です。デフォルトは 500 ms です。インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると見なされ、クラスタからノードが削除されるまでの時間です。
Monitored Interfaces（モニタリング対象インターフェイス）	インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。

フィールド	説明
サービスアプリケーション（Service Application）	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。
モニタリング対象外のインターフェイス（Unmonitored Interfaces）	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定（Auto-Rejoin Settings）	
クラスタインターフェイス（Cluster Interface）	クラスタ制御リンクに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは -1（無制限）です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 1 倍です。試行ごとに間隔を長くするかどうかを定義します。
データインターフェイス（Data Interfaces）	データインターフェイスに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。
システム（System）	内部エラーが発生した後に自動再結合の設定を表示します。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。

（注） システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

これらの設定は、このセクションから変更できます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI やBVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

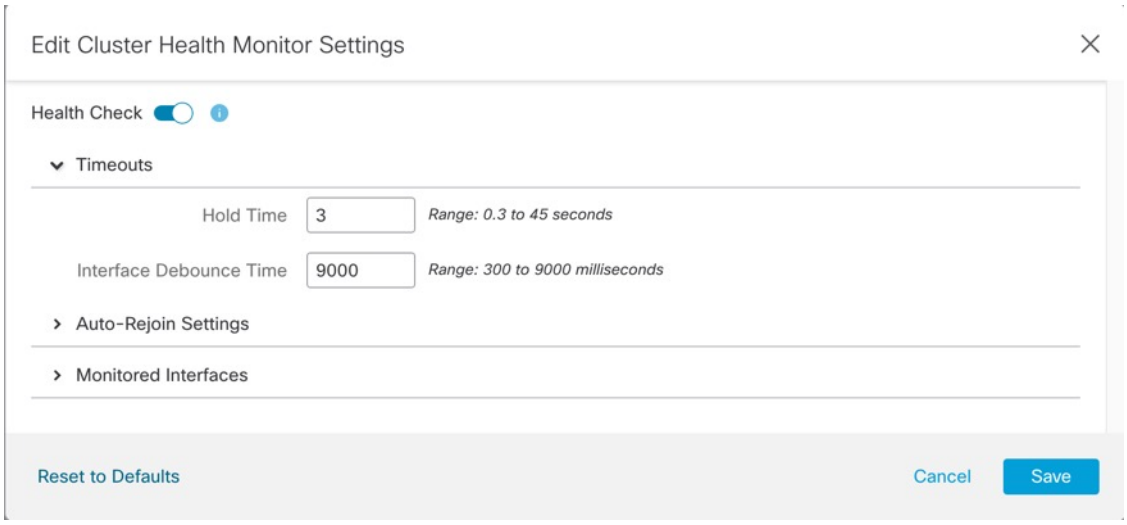
ステップ 2 変更するクラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [クラスタ（Cluster）] をクリックします。

ステップ 4 [クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）] セクションで、[編集（Edit）]（✎） をクリックします。

ステップ 5 [ヘルスチェック（Health Check）] スライダをクリックして、システムのヘルスチェックを無効にします。

図 *178 :* システムヘルスチェックの無効化



何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノー

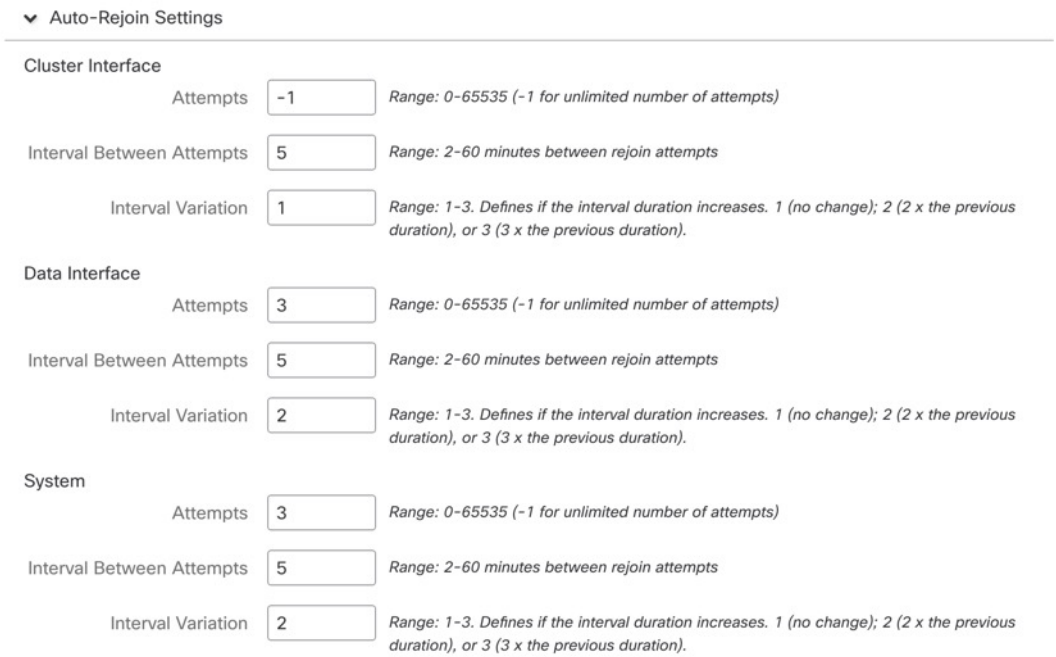
ドに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間（Hold Time）]：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ～ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間（Interface Debounce Time）]：デバウンス時間は 300 ～ 9000 ms の範囲で値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 *179*：自動再結合の設定

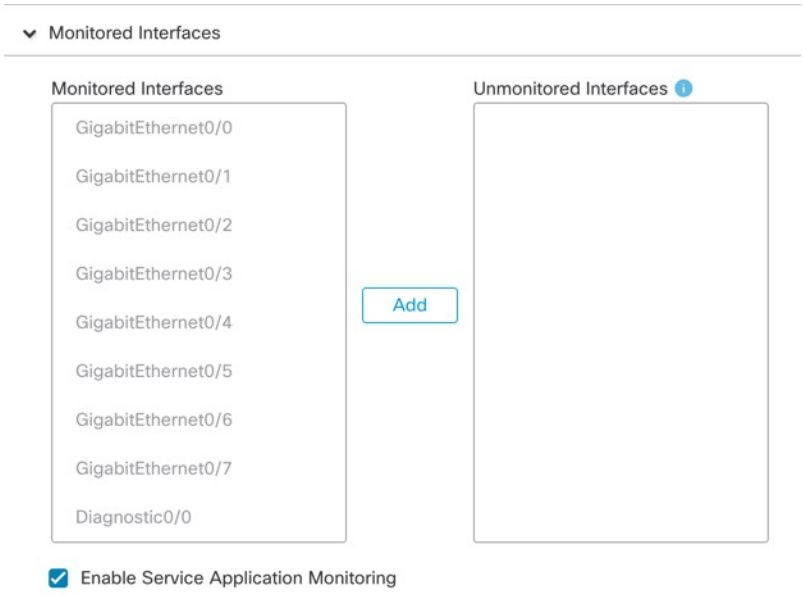


[クラスタインターフェイス（Cluster Interface）]、[データインターフェイス（Data Interface）]、および[システム（System）]に次の値を設定します（内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります）。

- [試行数（Attempts）]：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。[クラスタインターフェイス（Cluster Interface）] のデフォルト値は -1（無制限）です。[データインターフェイス（Data Interface）] と [システム（System）] のデフォルト値は 3 です。
- [試行の間隔（Interval Between Attempts）]：再結合試行の間隔を 2 ～ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [間隔のバリエーション（Interval Variation）]：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、[クラスタインターフェイス（Cluster Interface）] の場合は **1**、[データインターフェイス（Data Interface）] および [システム（System）] の場合は **2** です。

ステップ 8 [モニタリング対象のインターフェイス（Monitored Interfaces）] または [モニタリング対象外のインターフェイス（Unmonitored Interfaces）] ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリングを有効にする（Enable Service Application Monitoring）] をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 *180*：モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異

なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングを無効にできます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

クラスタノードの管理

クラスタリングを無効にする

ノードの削除に備えて、またはメンテナンスのために一時的にノードを非アクティブ化する場合があります。この手順は、ノードを一時的に非アクティブ化するためのものです。ノードは引き続き Firewall Management Center のデバイスリストに表示されます。ノードが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。

（注） クラスタリングを無効にせずにノードの電源を切らないでください。

手順

ステップ 1 無効にするユニットに対して、[デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択して [その他（More）] （⋮） をクリックし、[ノードのクラスタリングを無効にする（Disable Node Clustering）] を選択します。

ステップ 2 ノードのクラスタリングを無効にすることを確認します。

ノードは、[デバイス（Devices）]>[デバイス管理（Device Management）] リストの名前の横に [（無効（Disabled））] と表示されます。

ステップ 3 クラスタリングを再び有効にするには、クラスタへの再参加 （518 ページ）を参照してください。

クラスタへの再参加

（たとえば、インターフェイスで障害が発生したために）ノードがクラスタから削除された場合、または手動でクラスタリングを無効にした場合は、クラスタに手動で再参加する必要があります。クラスタへの再参加を試行する前に、障害が解決されていることを確認します。ノードをクラスタから削除できる理由の詳細については、「クラスタへの再参加（536ページ）」を参照してください。

手順

ステップ 1 再度有効にするユニットに対して、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択して [その他（More）] をクリックし、[ノードのクラスタリングを有効にする（Enable Node Clustering）] を選択します。 >

ステップ 2 ノードのクラスタリングを有効にすることを確認します。

クラスタノードの照合

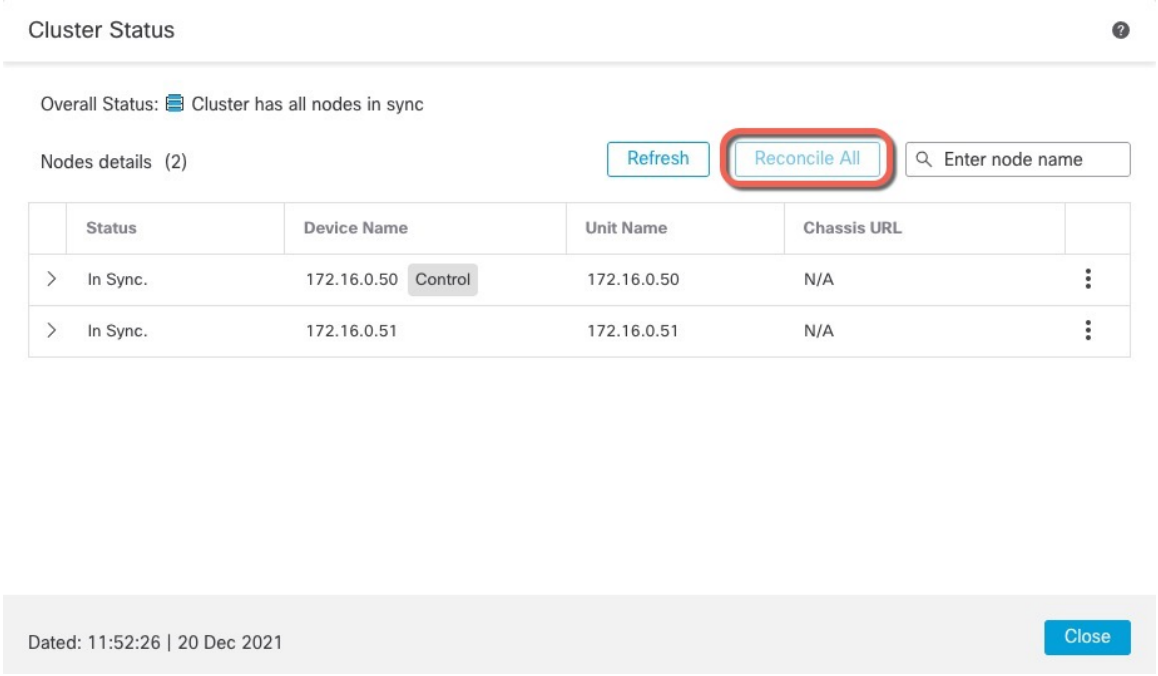
クラスタノードの登録に失敗した場合は、デバイスから Firewall Management Center に対してクラスタメンバーシップを照合できます。たとえば、Firewall Management Center が特定のプロセスで占領されているか、ネットワークに問題がある場合、データノードの登録に失敗することがあります。

手順

ステップ 1 クラスタの **[Devices]** > **[Device Management]** > [その他（More）] を選択し、次に [Cluster Live Status] を選択して [Cluster Status] ダイアログボックスを開きます。

ステップ 2 [すべてを照合（Reconcile All）] をクリックします。

図 *181* : すべてを照合



クラスタ ステータスの詳細については、クラスタのモニタリング （520ページ）を参照してください。

クラスタまたはノードの削除（登録解除）と新しいFirewaManagement Center への登録

Firewall Management Center からクラスタを登録解除できます。これにより、クラスタはそのまま維持されます。クラスタを新しいFirewall Management Centerに追加する場合は、クラスタを登録解除することができます。

クラスタからノードを除外することなく、Firewall Management Center からノードを登録解除することもできます。ノードはFirewall Management Centerに表示されていませんが、まだクラスタの一部であり、引き続きトラフィックを渡して制御ノードになることも可能です。現在動作している制御ノードを登録解除することはできません。Firewall Management Center から到達不可能になったノードは登録解除してもかまいませんが、管理接続をトラブルシューティングする間、クラスタの一部として残しておくことも可能です。

クラスタの登録解除：

- Firewall Management Center とクラスタとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからクラスタが削除されます。

- クラスタのプラットフォーム設定ポリシーで、NTP を使用して Firewall Management Center から時間を受信するように設定されている場合は、クラスタがローカル時間管理に戻されます。
- 設定はそのままになるため、クラスタはトラフィックの処理を続行します。

  NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Firewall Management Center にクラスタを再登録すると、設定が削除されるため、クラスタはその時点でトラフィックの処理を停止します。クラスタ設定はそのまま維持されるため、クラスタ全体を追加できます。登録時にアクセス コントロール ポリシーを選択できますが、トラフィックを再度処理する前に、登録後に他のポリシーを再適用してから設定を展開する必要があります。

始める前に

この手順では、いずれかのノードへの CLI アクセスが必要です。

手順

ステップ 1 [デバイス（Devices）]>[デバイス管理（Device Management）]の順に選択し、クラスタかノードの [その他（More）] (⋮) をクリックして [登録解除] [削除（Delete）] を選択します。 >

ステップ 2 クラスタかノードを削除するよう求められたら、[はい（Yes）] をクリックします。

ステップ 3 クラスタメンバーの 1 つを新しいデバイスとして追加することにより、クラスタを新しい（または同じ）Firewall Management Center に登録できます。

クラスタノードの 1 つをデバイスとして追加するだけで、残りのクラスタノードが検出されます。

a) 1 つのクラスタノードの CLI に接続し、**configure manager add** コマンドを使用して新しい Firewall Management Center を識別します。

b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、[デバイスの追加（Add Device）] をクリックします。

ステップ 4 削除したノードを再度追加する方法については、「クラスタノードの照合 （518 ページ）」を参照してください。

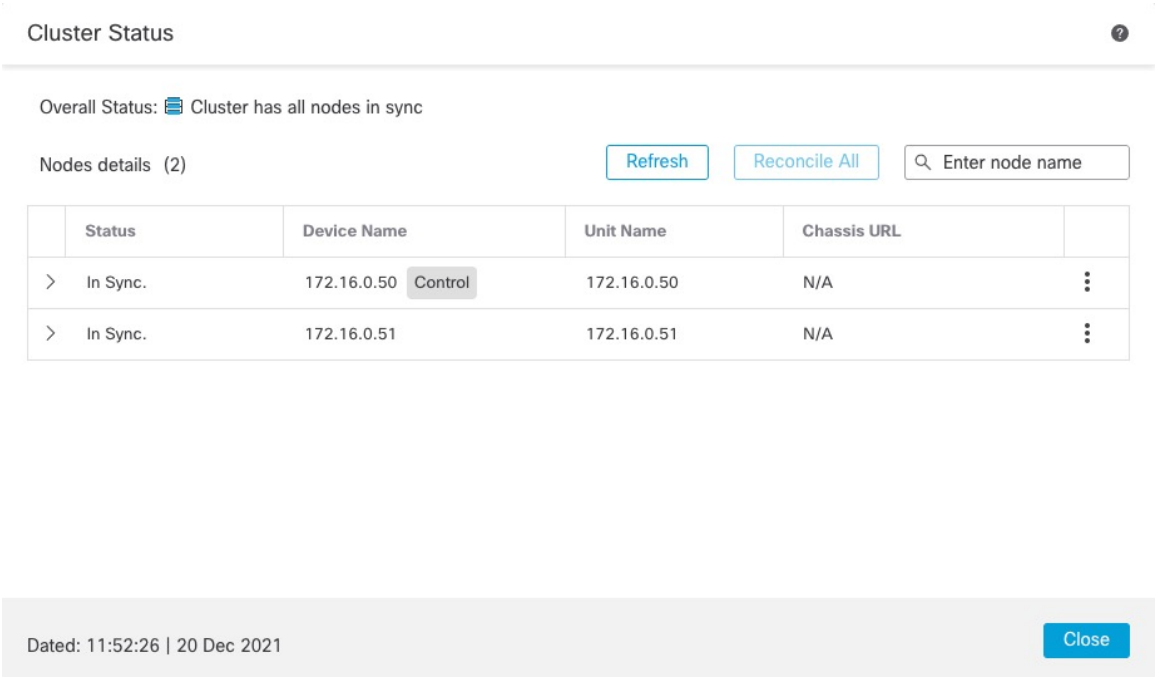
クラスタのモニタリング

クラスタは、Firewall Management Center と Firewall Threat Defense の CLI でモニターできます。

- [クラスタステータス（Cluster Status）] ダイアログボックスには、[デバイス（Devices）] > [デバイス管理（Device Management）] > [その他（More）] (⋮) アイコンから、または [デバイス（Devices）]>[デバイス管理（Device Management）]>[クラスタ（Cluster）] ペー

ジ > [全般（General）] 領域 > [クラスタのライブステータス（Cluster Live Status）] リンクからアクセスできます。 > > >

図 *182 :* クラスタのステータス



制御ノードには、そのロールを示すグラフィックインジケータがあります。

クラスタメンバーステータスには、次の状態が含まれます。

- 同期中（In Sync）：ノードは Firewall Management Center に登録されています。
- 登録の保留中（Pending Registration）：ノードはクラスタの一部ですが、まだ Firewall Management Center に登録されていません。ノードの登録に失敗した場合は、[すべてを照合（Reconcile All）] をクリックして登録を再試行できます。
- クラスタリングが無効（Clustering is disabled）：ノードは Firewall Management Center に登録されていますが、クラスタの非アクティブなメンバーです。クラスタリング設定は、後で再有効化する予定がある場合は変更せずに維持できます。また、ノードをクラスタから削除することも可能です。
- クラスタに参加中...（Joining cluster...）：ノードがシャーシ上でクラスタに参加していますが、参加は完了していません。参加後に Firewall Management Center に登録されます。

ノードごとに [概要（Summary）] と [履歴（History）] を表示できます。

図 *183 : ノードの [概要（Summary）]*

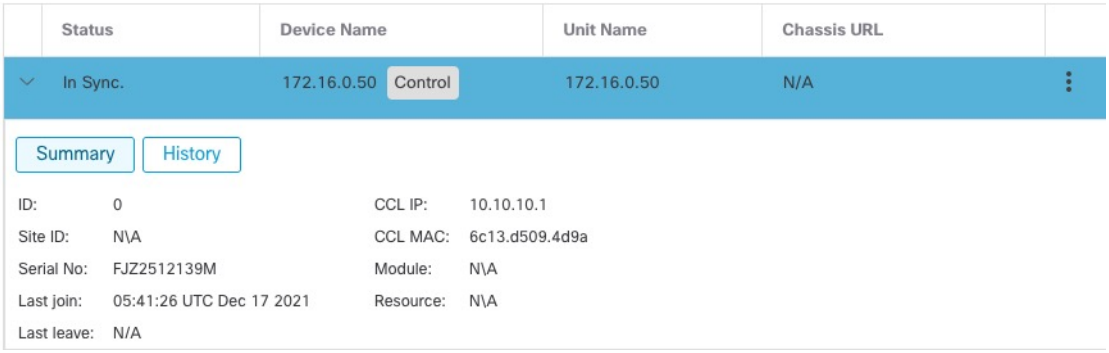
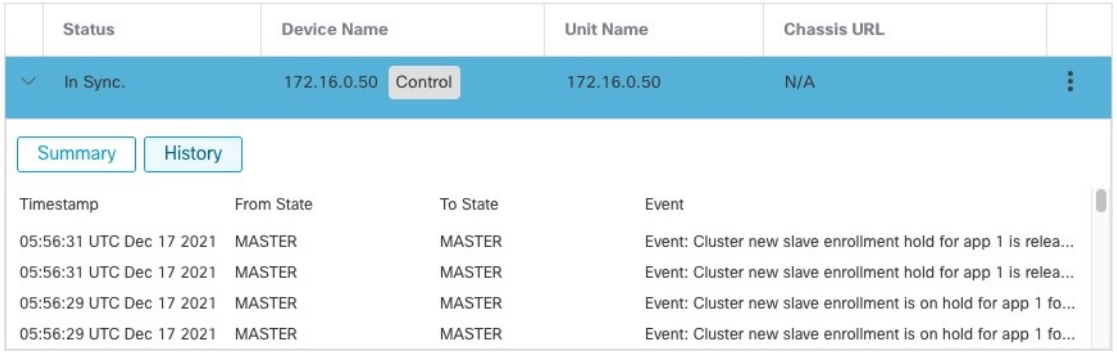


図 *184 : ノードの [履歴（History）]*



- [システム（System）]（⚙）> [Tasks] ページ。

  [タスク（Tasks）]ページには、ノードが登録されるたびにクラスタ登録タスクの最新情報が表示されます。

- [デバイス（Devices）] > [デバイス管理（Device Management）] > cluster_name。 >

  デバイスの一覧表示ページでクラスタを展開すると、IPアドレスの横にそのロールが表示されている制御ノードを含む、すべてのメンバーノードを表示できます。登録中のノードには、ロード中のアイコンが表示されます。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

クラスタ ヘルス モニター ダッシュボード

クラスタのヘルスモニター

Firewall Threat Defense がクラスタの制御ノードである場合、Firewall Management Center はデバイス メトリック データ コレクタからさまざまなメトリックを定期的に収集します。クラスタの ヘルスモニターは、次のコンポーネントで構成されています。

- 概要ダッシュボード：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。
  - トポロジセクションには、クラスタのライブステータス、個々の脅威防御の状態、脅威防御ノードのタイプ（制御ノードまたはデータノード）、およびデバイスの状態が表示されます。デバイスの状態は、[無効（Disabled）]（デバイスがクラスタを離れたとき）、[初期状態で追加（Added out of box）]（パブリッククラウドクラスタで Firewall Management Center に属していない追加ノード）、または [標準（Normal）]（ノードの理想的な状態）のいずれかです。
  - クラスタの統計セクションには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するクラスタの現在のメトリックが表示されます。

（注） CPU とメモリのメトリックは、データプレーンと Snort の使用量の個々の平均を示します。

  - メトリックチャート、つまり、CPU使用率、メモリ使用率、スループット、および接続数は、指定された期間におけるクラスタの統計を図表で示します。
- 負荷分散ダッシュボード：2 つのウィジェットでクラスタノード全体の負荷分散を表示します。
  - 分布ウィジェットには、クラスタノード全体の時間範囲における平均パケットおよび接続分布が表示されます。このデータは、ノードによって負荷がどのように分散されているかを示します。このウィジェットを使用すると、負荷分散の異常を簡単に特定して修正できます。
  - ノード統計ウィジェットには、ノードレベルのメトリックが表形式で表示されます。クラスタノード全体の CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するメトリックデータが表示されます。このテーブルビューでは、データを関連付けて、不一致を簡単に特定できます。
- メンバー パフォーマンス ダッシュボード：クラスタノードの現在のメトリックを表示します。セレクタを使用してノードをフィルタリングし、特定ノードの詳細を表示できます。メトリックデータには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数が含まれます。

- CCLダッシュボード：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- 時間範囲：さまざまなクラスタ メトリック ダッシュボードやウィジェットに表示される情報を制限するための調整可能な時間枠。
- カスタムダッシュボード：クラスタ全体のメトリックとノードレベルのメトリックの両方に関するデータを表示します。ただし、ノードの選択は脅威防御メトリックにのみ適用され、ノードが属するクラスタ全体には適用されません。

クラスタ ヘルスの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

クラスタヘルスモニターは、クラスタとそのノードのヘルスステータスの詳細なビューを提供します。このクラスタヘルスモニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

- Firewall Management Center の 1 つ以上のデバイスからクラスタを作成しているかを確認します。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択します。

[モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、ノード固有のヘルスモニターにアクセスします。

ステップ 2 デバイスリストで [展開（Expand）]（>）と [折りたたみ（Collapse）]（⌄）をクリックして、管理対象のクラスタデバイスのリストを展開または折りたたみます。

ステップ 3 クラスタのヘルス統計を表示するには、クラスタ名をクリックします。デフォルトでは、クラスタモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- [概要（Overview）]：他の事前定義されたダッシュボードからの主要なメトリックを表示します。ノード、CPU、メモリ、入力レート、出力レート、接続統計情報、NAT変換情報などが含まれます。
- [負荷分散（Load Distribution）]：クラスタノード間のトラフィックとパケットの分散。

- [メンバーパフォーマンス（Member Performance）]：CPU 使用率、メモリ使用率、入力スループット、出力スループット、アクティブな接続、および NAT 変換に関するノードレベルの統計情報。
- [CCL]：インターフェイスのステータスおよび集約トラフィックの統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているクラスタメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で1時間前（デフォルト）から、最長では 2 週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を 5 分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの展開アイコンをクリックします。

展開アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されます。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 （ノード固有のヘルスモニターの場合）ページ上部のデバイス名の右側にあるアラート通知で、ノードの正常性アラートを確認します。

正常性アラートにポインタを合わせると、ノードの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 7 （ノード固有のヘルスモニターの場合）デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- [Snort]：Snort プロセスに関連する統計情報。
- [ASP ドロップ（ASP drops）]：さまざまな理由でドロップされたパケットに関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 正常性モニターの右上隅にあるプラス記号[新しいダッシュボードの追加（Add New Dashboard）]（＋）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタムダッシュボードを作成します。

クラスタ全体のダッシュボードの場合は、クラスタのメトリックグループを選択してから、メトリックを選択します。

クラスタメトリック

クラスタのヘルスモニターは、クラスタとそのノードに関連する統計情報と、負荷分散、パフォーマンス、および CCL トラフィックの統計データの集約結果を追跡します。

表 *38*：クラスタメトリック

メトリック	説明	フォーマット（Format）
CPU	クラスタノード上の CPU メトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
メモリ	クラスタノード上のメモリメトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
データスループット	クラスタの着信および発信データトラフィックの統計。	バイト
CCL スループット	クラスタの着信および発信 CCL トラフィックの統計。	バイト
接続	クラスタ内のアクティブな接続数。	番号
NAT 変換数	クラスタの NAT 変換数。	番号
分布	1 秒ごとのクラスタ内の接続分布数。	番号
パケット	クラスタ内の1秒ごとのパケット配信の件数。	番号

クラスタのアップグレード

Firewall Threat Defense Virtual クラスタをアップグレードするには、次の手順を実行します。

始める前に

- パブリッククラウドでクラスタをアップグレードする前に、ターゲットバージョンのイメージをクラウドイメージリポジトリにコピーし、クラスタ展開テンプレートのイメージ ID を更新します（実際には、既存のテンプレートを変更したコピーで置き換えることを推奨します）。これにより、アップグレード後に新しいインスタンス（クラスタスケーリング中に起動されたインスタンスなど）が正しいバージョンを使用するようになります。クラスタにパッチが適用されている場合など、必要なイメージがマーケットプレイスにない場合は、インスタンス固有（Day 0）の設定がなく、正しいバージョンを実行しているスタンドアロンの Firewall Threat Defense Virtual インスタンスのスナップショットからカスタムイメージを作成します。
- AWS 向け Firewall Threat Defense Virtual の場合、自動スケーリングされたクラスタのアップグレードの前に HealthCheck プロセスと ReplaceUnhealthy プロセスを一時停止します。これにより、アップグレード後の再起動中に Auto Scaling グループによってインスタンスが終了されなくなります。一時停止したプロセスは、後で再開できます。手順については、Amazon EC2 Auto Scaling のユーザーガイドの「Suspend and resume Amazon EC2 Auto Scaling processes」を参照してください。

手順

ステップ 1 ターゲット イメージ バージョンをクラウドイメージストレージにアップロードします。

ステップ 2 更新されたターゲット イメージ バージョンでクラスタのクラウド インスタンス テンプレートを更新します。

a) ターゲット イメージ バージョンを使用してインスタンステンプレートのコピーを作成します。

b) 新しく作成したテンプレートをクラスタ インスタンス グループにアタッチします。

ステップ 3 ターゲット イメージ バージョンのアップグレードパッケージを Firewall Management Center にアップロードします。

ステップ 4 アップグレードするクラスタで準備状況チェックを実行します。

ステップ 5 準備状況チェックが成功したら、アップグレードパッケージのインストールを開始します。

ステップ 6 Firewall Management Center は、クラスタノードを一度に 1 つずつアップグレードします。

ステップ 7 クラスタのアップグレードが成功すると、Firewall Management Center に通知が表示されます。

アップグレード後のインスタンスのシリアル番号と UUID に変更はありません。

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

Threat Defense の機能とクラスタリング

Firewall Threat Defense の一部の機能はクラスタリングではサポートされず、一部は制御ユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

サポートされていない機能とクラスタリング

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

（注） クラスタリングでもサポートされていない FlexConfig 機能（WCCP インスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーション ガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- リモート アクセス VPN（SSL VPN および IPsec VPN）
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- 仮想トンネルインターフェイス（VTI）
- 高可用性
- 統合ルーティングおよびブリッジング
- Firewall Management Center UCAPL/CC モード

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

（注） クラスタリングでも一元化されている FlexConfig 機能（RADIUS インスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーションガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- スタティック ルート モニタリング

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

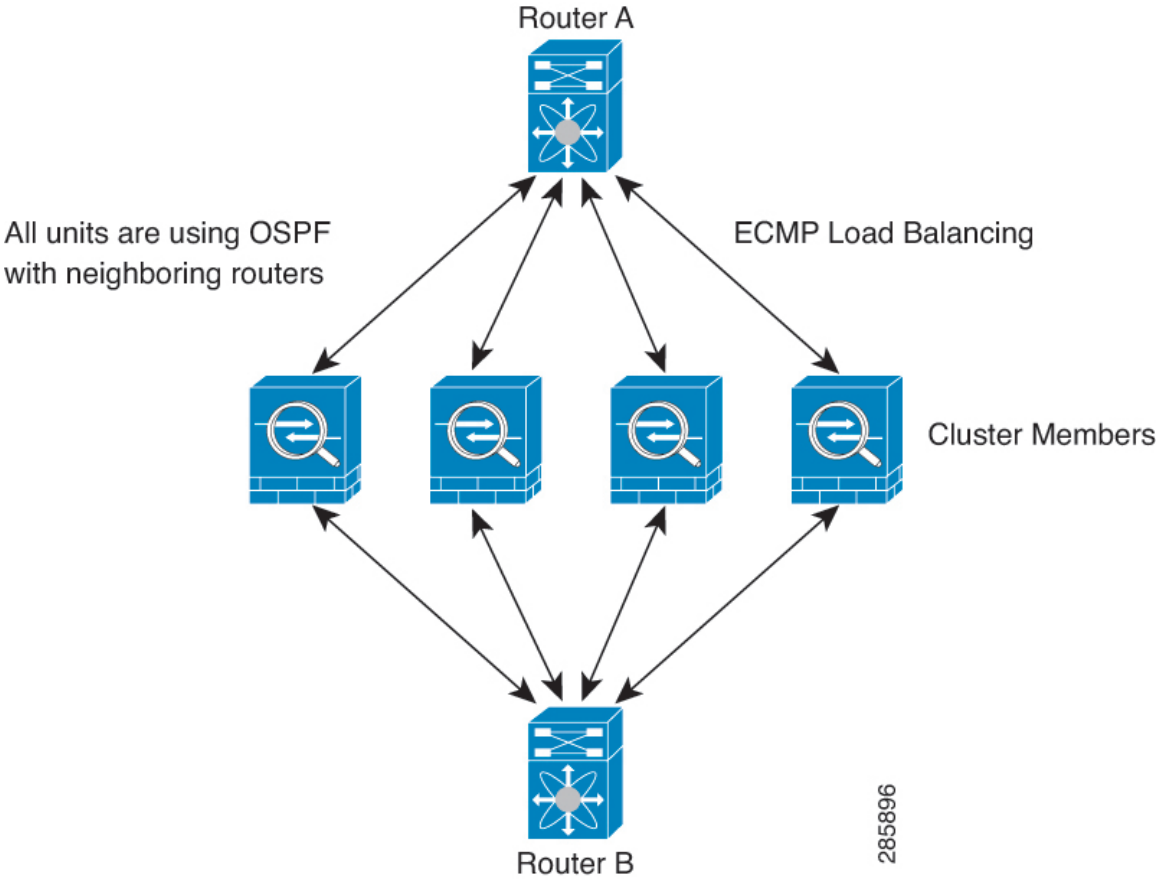
接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

ダイナミック ルーティングおよびクラスタリング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *185 :* 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタプールを設定する必要があります。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

NAT とクラスタリング

NAT の使用については、次の制限事項を参照してください。

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の Firewall Threat Defense に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない Firewall Threat Defense に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。

- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。

  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。

  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。

  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。

  - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。

- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロック

は512ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。

- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

SNMP とクラスタリング

SNMP エージェントは、個々の Firewall Threat Defense を、その [診断（Diagnostic）] 診断インターフェイスのローカルIPアドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザは新しいノードに複製されません。SNMPv3ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

syslog とクラスタリング

- クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ノードのみが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノードが選定されたときに、VPN接続を再確立する必要があります。

PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80%になります。

たとえば、モデルが単独稼働で約 10 Gbps のトラフィックを処理できる場合、8 ユニットのクラスタでは、最大合計スループットは 80 Gbps（8 ユニット x 10 Gbps）の約 80% で 64 Gbps になります。

制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。

（注） 最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままです。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。
5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。

（注） ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

クラスタ内のハイアベイラビリティ

クラスタリングは、ノードとインターフェイスの正常性をモニターし、ノード間で接続状態を複製することにより、ハイアベイラビリティを実現します。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからハートビートパケットまたはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション 2 のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。

インターフェイス モニタリング

各ノードは、使用中のすべての指名されたハードウェア インターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

すべての物理インターフェイスがモニタリングされます。ただし、モニタリングできるのは、名前付きインターフェイスのみです。ヘルスチェックは、インターフェイスごとに、モニターリングをオプションで無効にすることができます。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。ノードは 500 ミリ秒後に削除されます。

障害後のステータス

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、Firewall Threat Defense は自動的にクラスタへの再参加を試みます。

（注） Firewall Threat Defenseが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理/診断インターフェイスのみがトラフィックを送受信できます。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- 最初に参加するときに障害が発生したクラスタ制御リンク：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：FTDは、無限に5分ごとに自動的に再参加を試みます。
- データ インターフェイスの障害：Firewall Threat Defense は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、Firewall Threat Defense アプリケーションはクラスタリングを無効にします。データ インターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ノードは再起動するとクラスタに再参加します。Firewall Threat Defense アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。
- 障害が発生した設定の展開：FMC から新しい設定を展開し、展開が一部のクラスタメンバーでは失敗したものの、他のメンバーでは成功した場合、失敗したノードはクラスタから削除されます。クラスタリングを再度有効にして手動でクラスタに再参加する必要があります。制御ノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。すべてのデータノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *39*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システムアップタイムをトラッキングします。
ARP Table	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	Yes	—
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—

クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。
- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づい

てディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

ICMP/ICMPv6 ハッシュの詳細：

- エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
- 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
- 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定

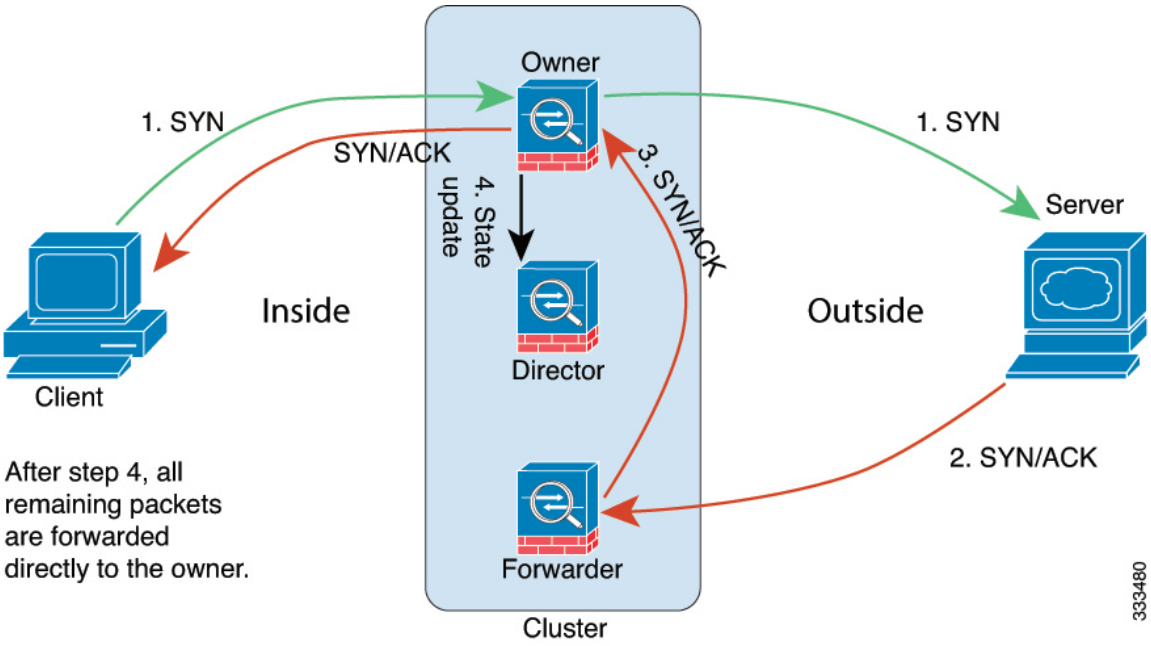
できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。



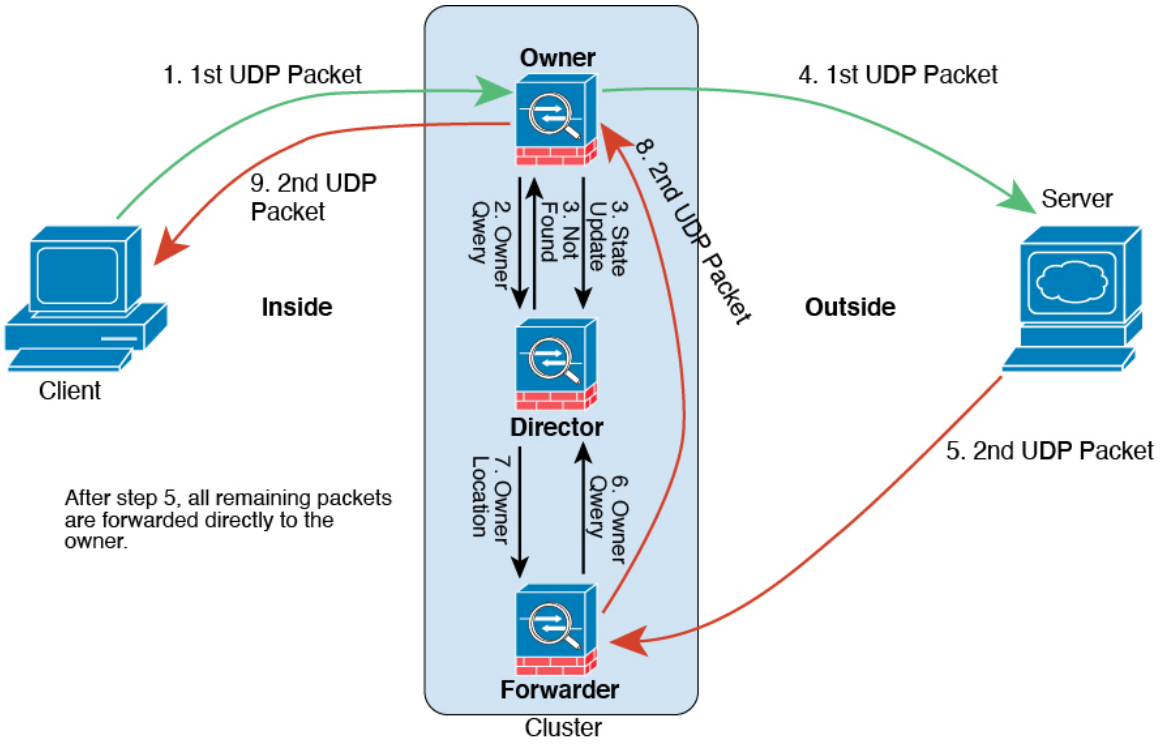
1. SYN パケットがクライアントから発信され、Firewall Threat Defense の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firewall Threat Defense（ロード バランシング方法に基づく）に配信されます。この Firewall Threat Defense はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。

5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様にTCPステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータフロー

次の例は、新しい接続の確立を示します。

1. 図 *186 : ICMP* および *UDP* データフロー



UDP パケットがクライアントから発信され、1 つの Firewall Threat Defense（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。

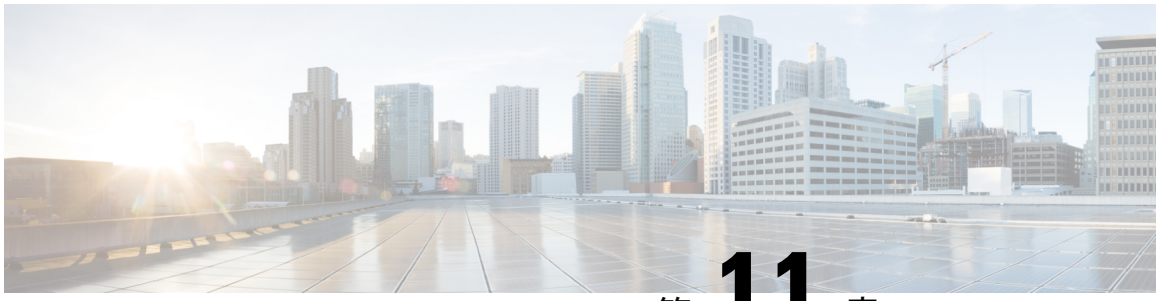
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

パブリッククラウドの Threat Defense Virtual クラスタリングの履歴

表 *40 :*

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタのヘルスモニターの設定。	7.3.0	いずれか	クラスタのヘルスモニター設定を編集できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **クラスタ（Cluster）** > **[クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）]** （注） 以前に FlexConfig を使用してこれらの設定を行った場合は、展開前に必ず FlexConfig の設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。
クラスタ ヘルス モニターダッシュボード。	7.3.0	いずれか	クラスタのヘルス モニター ダッシュボードでクラスタの状態を表示できるようになりました。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Azure の Firewall Threat Defense Virtual のクラスタリング	7.3.0	7.3.0	Azure ゲートウェイロードバランサまたは外部のロードバランサについて、Azure の Firewall Threat Defense Virtual で最大 16 ノードのクラスタリングを構成できるようになりました。 新規/変更された画面： • [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタの追加（Add Cluster）] • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [詳細（More）]**メニュー • **[Devices] > [Device Management] > [Cluster]** サポートされているプラットフォーム：Azure の Firewall Threat Defense Virtual
パブリッククラウドでの Firewall Threat Defense Virtual のクラスタリング（Amazon Web Services および Google Cloud Platform）。	7.2.0	7.2.0	Firewall Threat Defense Virtual はパブリッククラウド（AWS および GCP）で最大 16 ノードの個別インターフェイスのクラスタリングをサポートします。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの追加（Add Device）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [詳細（More）]**メニュー • **[Devices] > [Device Management] > [Cluster]** サポートされているプラットフォーム：AWS および GCP 上の Firewall Threat Defense Virtual



第 11 章

Firepower 4100/9300 のクラスタリング

クラスタリングを利用すると、複数の Firewall Threat Defense ノードをグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「クラスタリングでサポートされない機能 （606 ページ）」を参照してください。

- Firepower 4100/9300 シャーシのクラスタリングについて （543 ページ）
- クラスタリングのライセンス （549 ページ）
- クラスタリングの要件と前提条件 （549 ページ）
- クラスタリング ガイドラインと制限事項 （553 ページ）
- クラスタリングの設定 （557 ページ）
- FXOS：クラスタノードの削除 （588 ページ）
- FMC：クラスタメンバーの管理 （590 ページ）
- Firewall Management Center：クラスタのモニタリング （597 ページ）
- クラスタリングの例 （603 ページ）
- クラスタリングの参考資料 （605 ページ）
- クラスタリングの履歴 （620 ページ）

Firepower 4100/9300 シャーシのクラスタリングについて

Firepower 4100/9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ネイティブインスタンスのクラスタリングの場合：ノード間通信用のクラスタ制御リンク（デフォルトのポートチャネル 48）を作成します。

  マルチインスタンス クラスタリングの場合：1 つ以上のクラスタタイプの EtherChannel でサブインターフェイスを事前設定する必要があります。各インスタンスには、独自のクラスタ制御リンクが必要です。

1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタの場合、このリンクはクラスタ通信に Firepower 9300 バックプレーンを使用します。

複数のシャーシによるクラスタリングでは、シャーシ間通信用にこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。

- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがシャーシスーパバイザから各ユニットに対してプッシュされます。

- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

  1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタの場合、スパンドインターフェイスは、複数のシャーシによるクラスタリングの場合のように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。複数のシャーシによるクラスタリングでは、すべてのデータインターフェイスでスパンド EtherChannel を使用します。

（注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

クラスタリングの詳細については、以下の項を参照してください。

ブートストラップ設定

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションが Firepower 4100/9300 シャーシスーパバイザから各ユニットに対してプッシュされます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

クラスタ内のメンバーの 1 つが**制御**ユニットになります。制御ユニットは自動的に決定されます。他のすべてのメンバーは**データ**ユニットになります。

すべてのコンフィギュレーション作業は制御ユニット上でのみ実行する必要があります。コンフィギュレーションはその後、データユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能を参照してください。

クラスタ制御リンク

ネイティブ インスタンス クラスタリングの場合：クラスタ制御リンクは、ポートチャネル 48 インターフェイスを使用して自動的に作成されます。

マルチインスタンス クラスタリングの場合：1 つ以上のクラスタタイプの EtherChannel でサブインターフェイスを事前設定する必要があります。各インスタンスには、独自のクラスタ制御リンクが必要です。

1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタの場合、このインターフェイスにメンバーインターフェイスはありません。このクラスタタイプの EtherChannel は、クラスタ通信に Firepower 9300 バックプレーンを使用します。複数シャーシでのクラスタリングでは、EtherChannel に 1 つ以上のインターフェイスを追加する必要があります。

2 シャーシによるクラスタの場合、シャーシと別のシャーシとの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

クラスタ制御リンクのサイジング

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

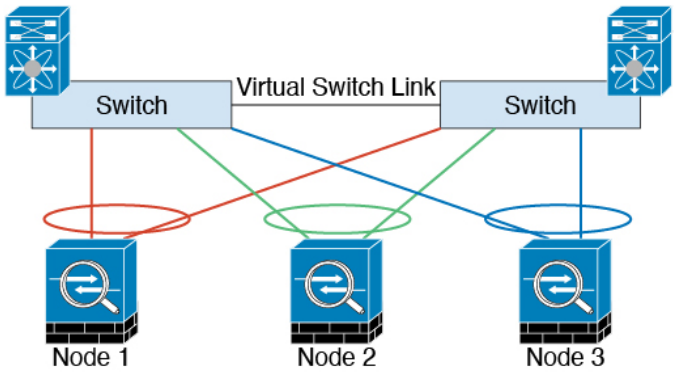
- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンクの冗長性

次の図は、仮想スイッチングシステム（VSS）、仮想ポートチャネル（vPC）、StackWise、または StackWise Virtual 環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが冗長システムの一部である場合は、同じ EtherChannel 内のファイアウォールインターフェイスをそれぞれ、冗長システム内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット ID（127.2.*chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。通常、同じ EtherChannel の異なる VLAN サブインターフェイスを使用するマルチインスタンスクラスタの場合は、VLAN の分離によって異なるクラスタに同じ IP アドレスを使用できます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。この管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Secure Firewall Management Center にデバイスを設定し、登録するために使用されます。独自のローカル認証、IPアドレス、およびスタティック ルーティングを使用します。クラスタの各メンバーは、管理ネットワーク上で、それぞれに異なる IP アドレスを使用します。これらの IP アドレスは、ブートストラップ構成の一部としてユーザーが設定します。

管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。診断論理インターフェイスはオプションであり、ブートストラップ構成の一部としては設定されません。診断インターフェイスは、他のデータインターフェイスと併せて設定できます。診断インターフェイスを設定する場合、メインクラスタ IP アドレスを、そのクラスタの固定アドレス（常に現在の制御ユニットに属するアドレス）として設定します。アドレス範囲も設定して、現在の制御ユニットを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、診断アクセスのアドレスが一本化されます。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御ユニットに移動するので、クラスタへのアクセスをシームレスに続行できます。TFTPやsyslogなどの発信管理トラフィックの場合、制御ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバーに接続します。

クラスタ インターフェイス

1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタでは、物理インターフェイスと EtherChannel（「ポートチャネル」とも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロード バランシングを行うスパンド インターフェイスです。

複数のシャーシによるクラスタリングでは、データ EtherChannel のみをクラスタに割り当てできます。これらのスパンドEtherChannelは、各シャーシの同じメンバーインターフェイスを含みます。上流に位置するスイッチでは、これらのインターフェイスはすべて単一のEtherChannelに含まれ、スイッチは複数のデバイスに接続されていることを察知しません。

通常のファイアウォールインターフェイスまたはIPS専用インターフェイス（インラインセットまたはパッシブインターフェイス）を使用できます。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

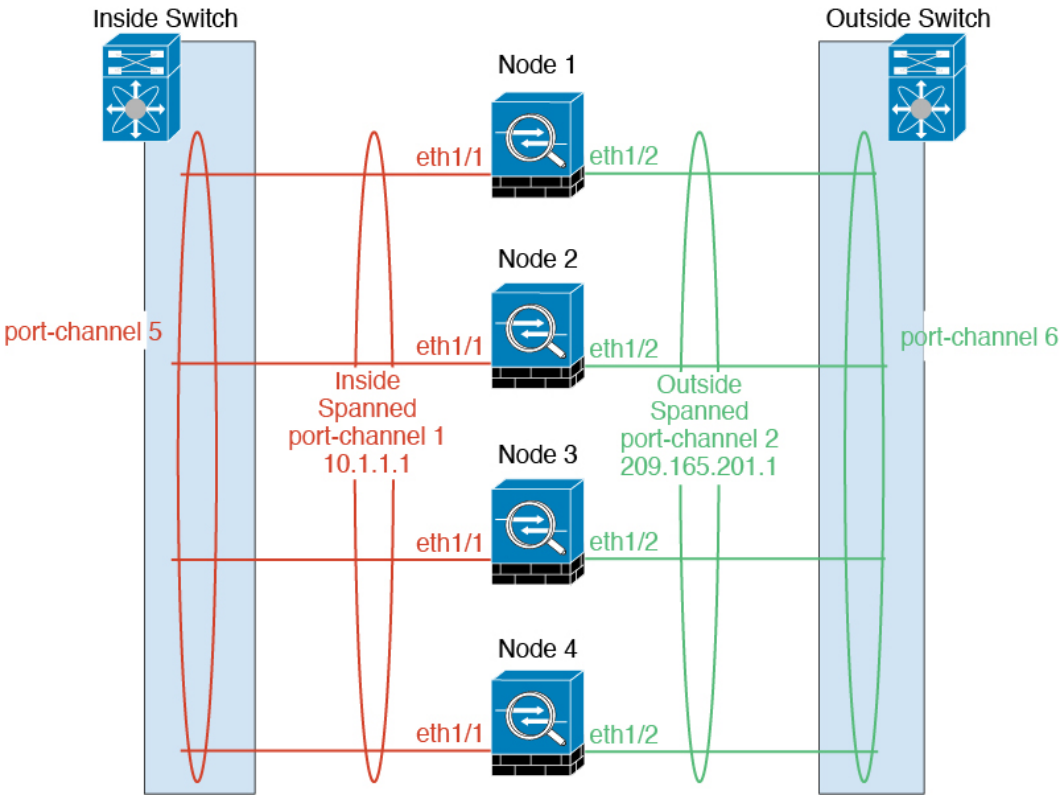
スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。

通常のファイアウォール インターフェイスの場合：スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジグループ メンバーではなく BVI に割り当てられます。

EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。

マルチインスタンスのクラスタの場合、各クラスタには専用データ Etherchannel が必要です。共有インターフェイスまたは VLAN サブインターフェイスを使用することはできません。



冗長スイッチシステムへの接続

インターフェイスに冗長性を持たせるために、EtherChannel を VSS、vPC、StackWise、または StackWise Virtual システムなどの冗長スイッチシステムに接続することをお勧めします。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

クラスタリングのライセンス

個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。

クラスタノードをFirewall Management Centerに追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタのライセンスは、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[ライセンス（License）]** 領域で変更できます。

（注） Firewall Management Centerにライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、Firewall Management Centerにライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのデータユニットがクラスタをいったん離れてから再参加することになります。

クラスタリングの要件と前提条件

クラスタ モデルのサポート

Threat Defense は、次のモデルでのクラスタリングをサポートしています。

- Firepower 9300：クラスタには最大 16 ノードを含めることができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、 8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。複数のシャーシによるクラスタリングと、1 つのシャーシ内のセキュリティモジュールに分離されたクラスタリングがサポートされます。
- Firepower 4100：複数のシャーシでクラスタリングを使用して、最大 16 ノードがサポートされます。

ユーザの役割

- 管理者
- アクセス管理者

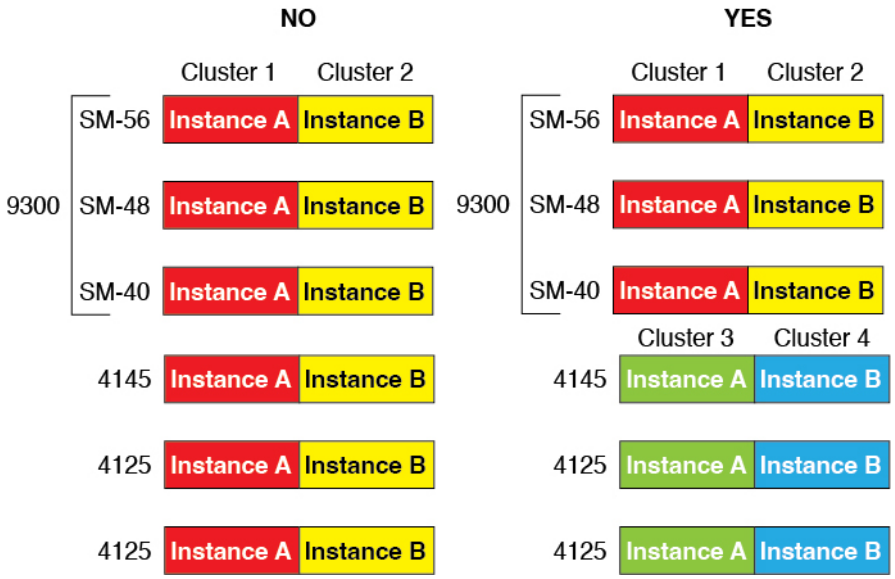
- ネットワーク管理者

クラスタリングハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- ネイティブインスタンスのクラスタリング—Firepower 4100：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。空のスロットを含め、シャーシ内にあるすべてのモジュールはクラスタに属している必要がありますが、各シャーシに設置されているセキュリティ モジュールの数はさまざまでかまいません。

- コンテナインスタンスのクラスタリング—クラスタインスタンスごとに同じセキュリティ モジュールまたはシャーシモデルを使用することをお勧めします。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。または、Firepower 4145 および 4125 でクラスタを作成できます。



- イメージアップグレード時を除き、同じ FXOS およびアプリケーション ソフトウェアを実行する必要があります。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。

- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成を含める必要があります。同じインターフェイス ID の容量が一致し、インターフェイスが同じスパンド EtherChannel に内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワーク モジュールを使用できます。複数のシャーシによるクラスタでは、すべて

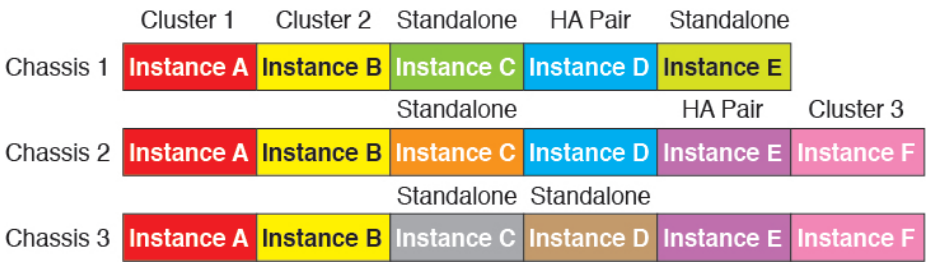
のデータインターフェイスを EtherChannel にする必要があることに注意してください。（インターフェイスモジュールの追加や削除、または EtherChannel の設定などにより）クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（データノードから始めて、制御ノードで終わります）。

- 同じ NTP サーバを使用する必要があります。Firewall Threat Defense では、Firewall Management Center も同じ NTP サーバーを使用する必要があります。時間を手動で設定しないでください。

マルチインスタンス クラスタリングの要件

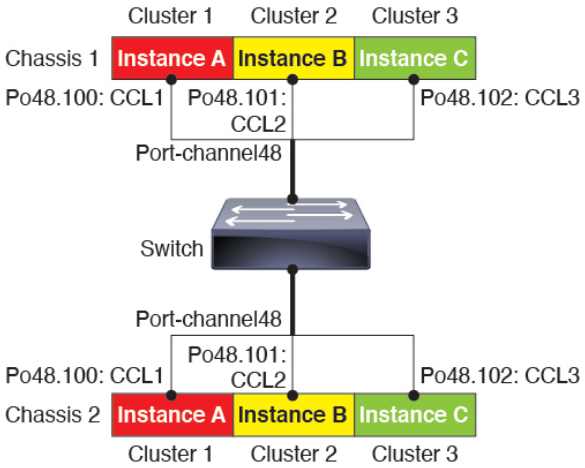
- セキュリティモジュール/エンジン間クラスタリングなし：特定のクラスタでは、セキュリティモジュール/エンジンごとに 1 つのコンテナインスタンスのみを使用できます。同じモジュール上で実行されている場合、同じクラスタに 2 つのコンテナインスタンスを追加することはできません。

- クラスタとスタンドアロンインスタンスの混在：セキュリティモジュール/エンジン上のすべてのコンテナインスタンスがクラスタに属している必要はありません。一部のインスタンスをスタンドアロンノードまたは高可用性ノードとして使用できます。また、同じセキュリティモジュール/エンジン上で別々のインスタンスを使用して複数のクラスタを作成することもできます。

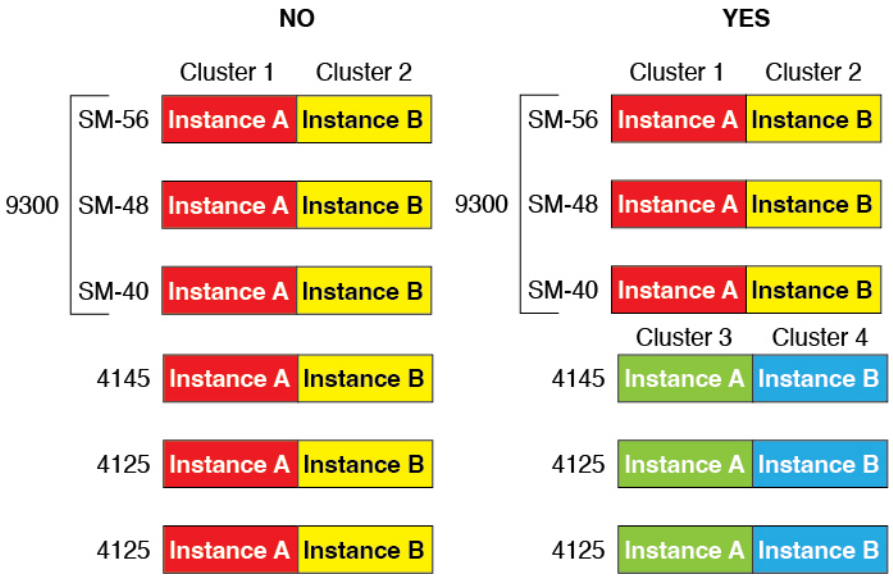


- Firepower 9300 の 3 つすべてのモジュールはクラスタに属している必要があります。Firepower 9300 の場合、クラスタには 3 つすべてのモジュールで 1 つのコンテナインスタンスが必要です。たとえば、モジュール 1 と 2 のインスタンスを使用してクラスタを作成し、モジュール 3 のネイティブインスタンスを使用することはできません。

- リソースプロファイルの一致：クラスタ内の各ノードで同じリソースプロファイル属性を使用することを推奨します。ただし、クラスタノードを別のリソースプロファイルに変更する場合、または異なるモデルを使用する場合は、リソースの不一致が許可されます。
- 専用クラスタ制御リンク：複数のシャーシによるクラスタの場合、各クラスタには専用のクラスタ制御リンクが必要です。たとえば、各クラスタは、同じクラスタタイプの EtherChannel で個別のサブインターフェイスを使用したり、個別の EtherChannel を使用したりできます。



- 共有インターフェイスなし：共有タイプのインターフェイスは、クラスタリングではサポートされません。ただし、同じ管理インターフェイスとイベントインターフェイスを複数のクラスタで使用することはできます。
- サブインターフェイスなし：マルチインスタンスクラスタは、FXOS 定義の VLAN サブインターフェイスを使用できません。クラスタ制御リンクは例外で、クラスタ EtherChannel のサブインターフェイスを使用できます。
- シャーシモデルの混在：クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。または、Firepower 4145 および 4125 でクラスタを作成できます。



- 最大 6 ノード：クラスタ内では最大 6 つのコンテナインスタンスを使用できます。

スイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチの特性については、『Cisco FXOS Compatibility』を参照してください。

クラスタリング ガイドラインと制限事項

クラスタリングのスイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンクインターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンクインターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。さらに、クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。
- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS XR インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗

する可能性があります。クラスタデバイス MTU は、IOS XR *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。

- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **src-dst-mixed-ip-port** を使用することをお勧めします（Cisco Nexus OS および Cisco IOS-XE の **port-channel load-balance** コマンドを参照）。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

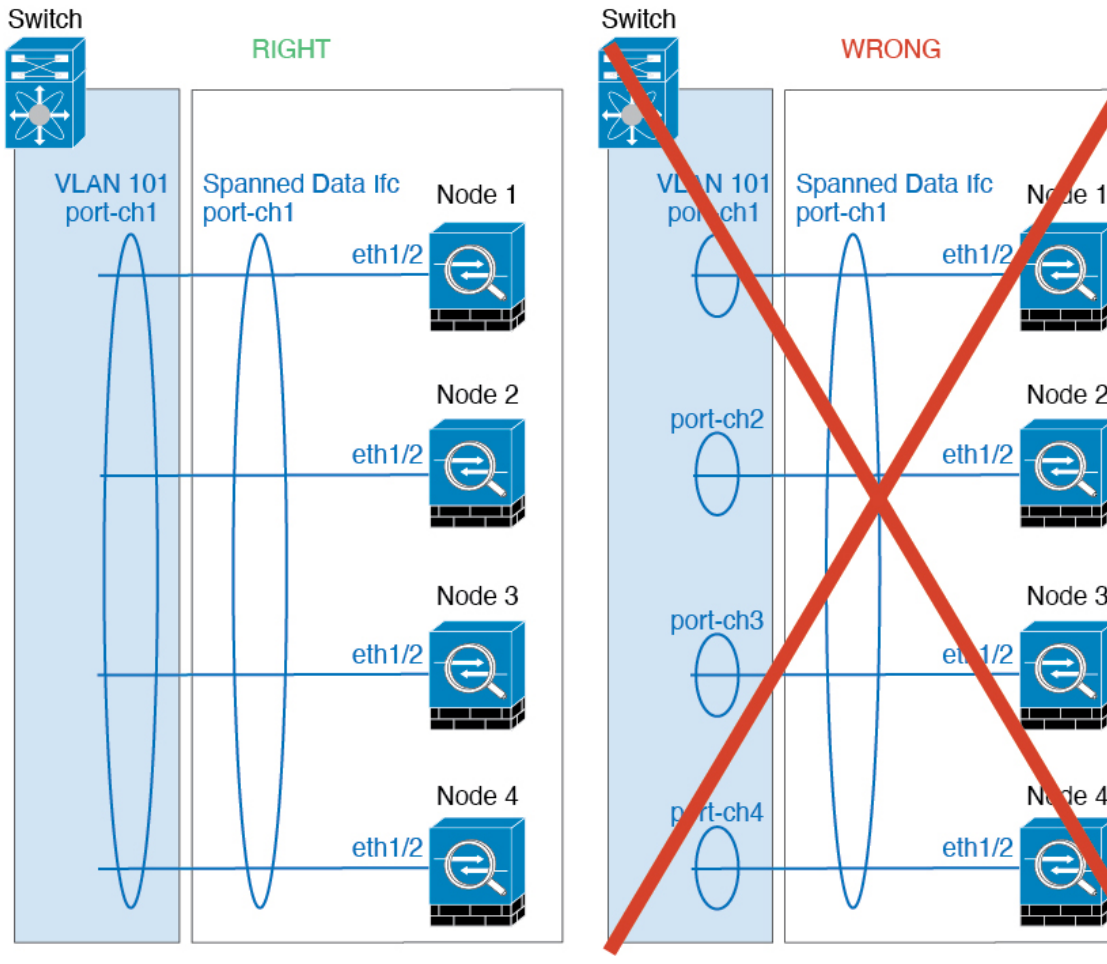
- Firepower 4100/9300 クラスタは LACP グレースフル コンバージェンスをサポートしています。したがって、接続されている Cisco Nexus スイッチで LACP グレースフル コンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速（fast）] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。

クラスタリングの EtherChannel

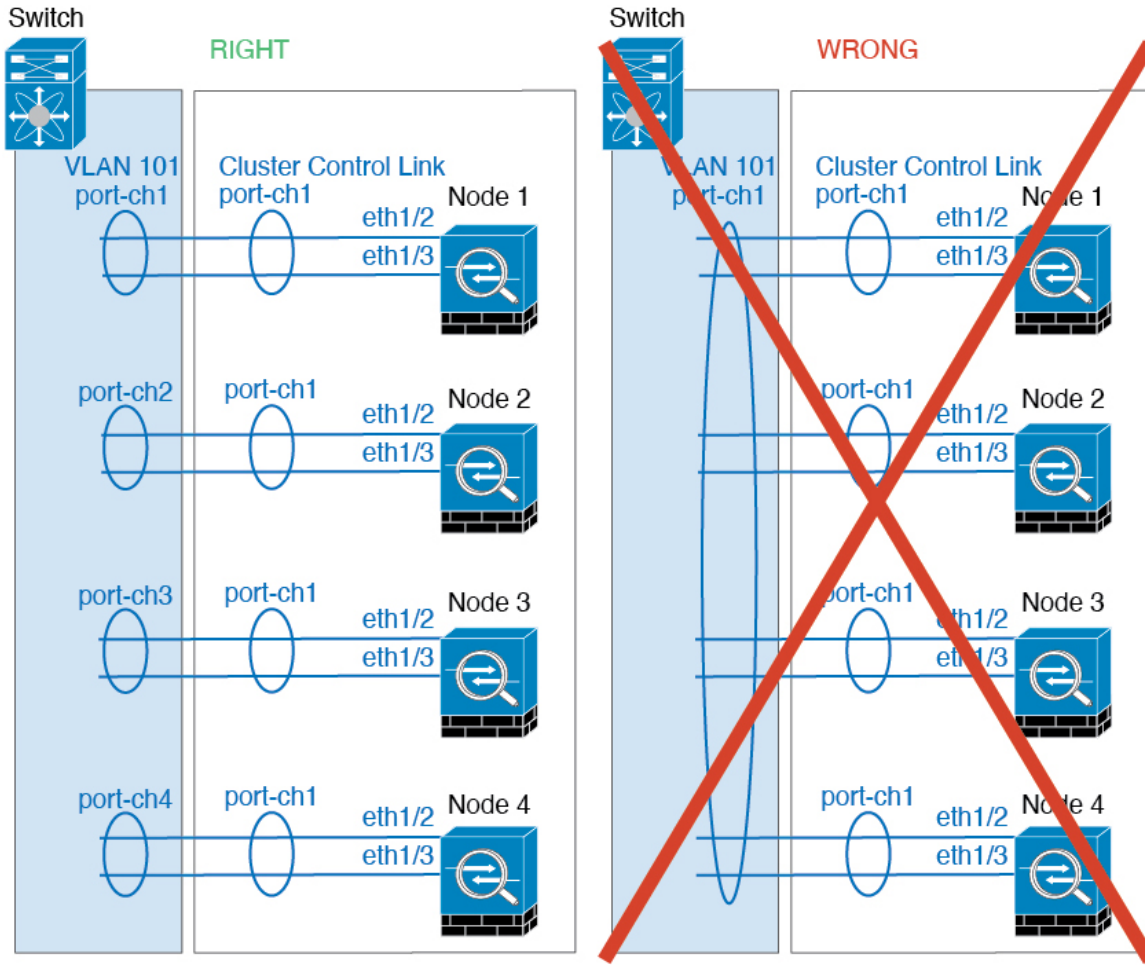
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでし

た。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



  - デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannelインターフェイスの追加または削除、Firepower4100/9300 シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するための追加スイッチの追加など）、ヘルスチェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制

しないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。

- 冗長性を持たせるため、VSS、vPC、StackWise、または StackWise Virtual に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。
- 復号された TLS/SSL 接続の場合、復号状態は同期されず、接続オーナーに障害が発生すると、復号された接続がリセットされます。新しいユニットへの新しい接続を確立する必要があります。復号されていない接続（復号しないルールに一致）は影響を受けず、正しく複製されます。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ自動再参加機能は、5 分間隔で無制限に試行されるように設定されます。
- 失敗したデータインターフェイスのクラスタ自動再参加機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

クラスタリングの設定

クラスタは、Firepower 4100/9300 スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。その後、ユニットを Firewall Management Center に追加し、1 つのクラスタにグループ化できます。

FXOS：Firewall Threat Defense クラスタの追加

ネイティブモードの場合：シャーシ内のセキュリティモジュールに分離された単一の Firepower 9300 シャーシにクラスタを追加できます。または、複数のシャーシを使用できます。

マルチインスタンスモード：シャーシ内のセキュリティモジュールに分離された単一の Firepower 9300 シャーシに 1 つ以上のクラスタを追加できます（各モジュールにインスタンスを含める必要があります）。または、複数のシャーシに 1 つ以上のクラスタを追加できます。

複数のシャーシにわたるクラスタの場合は、各シャーシを個別に設定する必要があります。1つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

Firewall Threat Defense クラスタの作成

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

複数のシャーシにわたるクラスタリングの場合は、各シャーシを個別に設定する必要があります。導入を容易にするために、1 つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3 つのすべてのモジュール、またはコンテナインスタンス、各スロットの 1 つのコンテナインスタンスでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。
- コンテナインスタンスに対して、デフォルトのプロファイルを使用しない場合は、コンテナインスタンスにリソースプロファイルを追加（260 ページ）に従ってリソース プロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティ モジュール/エンジン を再度初期化する必要があります。[Security Modules] または [Security Engine] を選択して、[Reinitialize] アイコン（ ） をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテナインスタンスに置き換える場合は、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレス、およびネットワークマスク
  - ゲートウェイ IP アドレス
  - Firewall Management Center 選択した IP アドレス/NAT ID
  - DNS サーバの IP アドレス
  - Firewall Threat Defense ホスト名とドメイン名

手順

ステップ 1 インターフェイスを設定します。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。EtherChannel（ポート チャネル）の追加（256 ページ）または物理インターフェイスの設定 （254 ページ）を参照してください。

複数のシャーシにわたるクラスタリングの場合は、すべてのデータインターフェイスが、少なくとも 1 つのメンバーインターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタ ユニットからメンバーインターフェイスを 1 つの EtherChannel へと結合します。EtherChannel の詳細については、クラスタリング ガイドラインと制限事項 （553 ページ）を参照してください。

マルチインスタンス クラスタリングでは、クラスタ内で FXOS 定義の VLAN サブインターフェイスまたはデータ共有インターフェイスを使用できません。アプリケーション定義のサブインターフェイスのみがサポートされています。詳細については、FXOS インターフェイスとアプリケーション インターフェイス （217 ページ）を参照してください。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポート チャネル）の追加（256 ページ）または物理インターフェイスの設定（254 ページ）を参照してください。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

複数のシャーシにわたるクラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

マルチインスタンスのクラスタリングでは、同じシャーシ上の複数のクラスタ、またはスタンドアロンインスタンスで同じ管理インターフェイスを共有できます。

c) 複数のシャーシにわたるクラスタリングでは、メンバーインターフェイスをクラスタ制御リンクの EtherChannel（デフォルトではポートチャネル 48）に追加します。EtherChannel（ポート チャネル）の追加 （256 ページ） を参照してください。

1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタのメンバーインターフェイスを追加しないでください。メンバーを追加すると、シャーシはこのクラスタが複数のシャーシを使用すると見なし、たとえば、スパンド EtherChannel の使用のみが許可されます。

[インターフェイス（Interfaces）] タブで、ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバ インターフェイスが含まれていない場合は、[動作状態（Operation State）] を [失敗（failed）] と表示します。1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタの場合、この EtherChannel はメンバーインターフェイスを必要としないため、この動作状態は無視して構いません。

各シャーシに同じメンバインターフェイスを追加します。クラスタ制御リンクは、各シャーシのデバイスローカル EtherChannel です。デバイスごとにスイッチで個別の EtherChannel を使用します。EtherChannel の詳細については、クラスタリング ガイドラインと制限事項（553 ページ）を参照してください。

マルチインスタンス クラスタリングの場合は、追加のクラスタタイプの EtherChannel を作成できます。管理インターフェイスとは異なり、クラスタ制御リンクを複数のデバイスで共有することはできないため、クラスタごとにクラスタインターフェイスが必要になります。ただし、複数の Etherchannel の代わりに VLAN サブインターフェイスを使用することを推奨します。クラスタインターフェイスに VLAN サブインターフェイスを追加するには、次の手順を参照してください。

d) マルチインスタンス クラスタリングの場合、クラスタごとに 1 つのサブインターフェイスを使用できるように、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。コンテナインスタンスの VLAN サブインターフェイスの追加（258 ページ）を参照してください。

クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタに使用することはできません。

e) （任意）イベントインターフェイスを追加します。EtherChannel（ポート チャネル）の追加（256 ページ）または物理インターフェイスの設定（254 ページ）を参照してください。

このインターフェイスは、Firewall Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Firewall Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Firewall Threat Defense コマンドリファレンスの **configure network** コマンドを参照してください。

複数のシャーシにわたるクラスタリングの場合、各シャーシに同じイベンティング インターフェイスを追加します。

ステップ 2 [論理デバイス（Logical Devices）] を選択します。

ステップ 3 **[追加（Add）] > [クラスタ（Cluster）]** をクリックし、次のパラメータを設定します。

図 *187*：ネイティブクラスタ

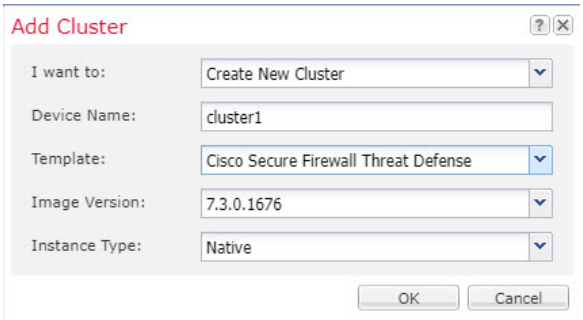
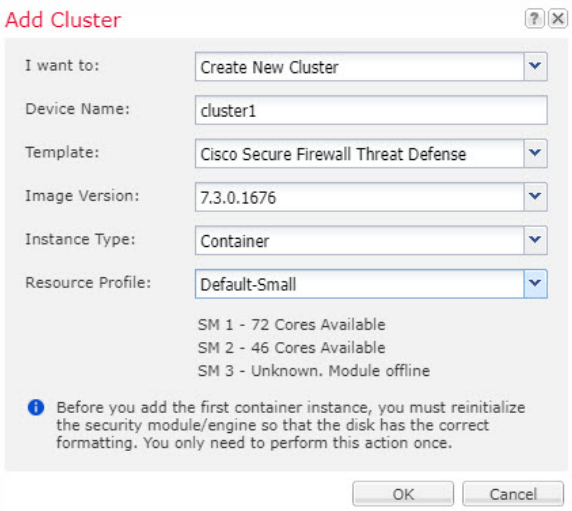


図 *188* : マルチインスタンスクラスタ



a) **[必要な操作（I want to:）]** > **[新しいクラスタの作成（Create New Cluster）]** を選択します。

b) **デバイス名**を入力します。

この名前は、シャーシスーパバイザが管理設定を行ってインターフェイスを割り当てるために内部で使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

c) [テンプレート（Template）] には、[Cisco Firepower 脅威に対する防御（Cisco Firepower Threat Defense）] を選択します。

d) [Image Version] を選択します。

e) [Instance Type] の場合、[Native] または [Container] を選択します。

ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブインスタンスを 1 つだけインストールできます。コンテナインスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

f) （コンテナインスタンスのみ）[リソースタイプ（Resource Type）] で、ドロップダウンリストからいずれかのリソースプロファイルを選択します。

Firepower 9300 の場合、このプロファイルは各セキュリティモジュールの各インスタンスに適用されます。この手順の後半では、セキュリティモジュールごとに異なるプロファイルを設定できます。たとえば、異なるセキュリティモジュールのタイプを使用していて、ローエンドのモデルでより多くの CPU を使用する場合に設定できます。クラスタを作成する前に、正しいプロファイルを選択することを推奨します。新しいプロファイルを作成する必要がある場合は、クラスタの作成をキャンセルし、コンテナインスタンスにリソースプロファイルを追加 （260 ページ） を使用して 1 つ追加します。

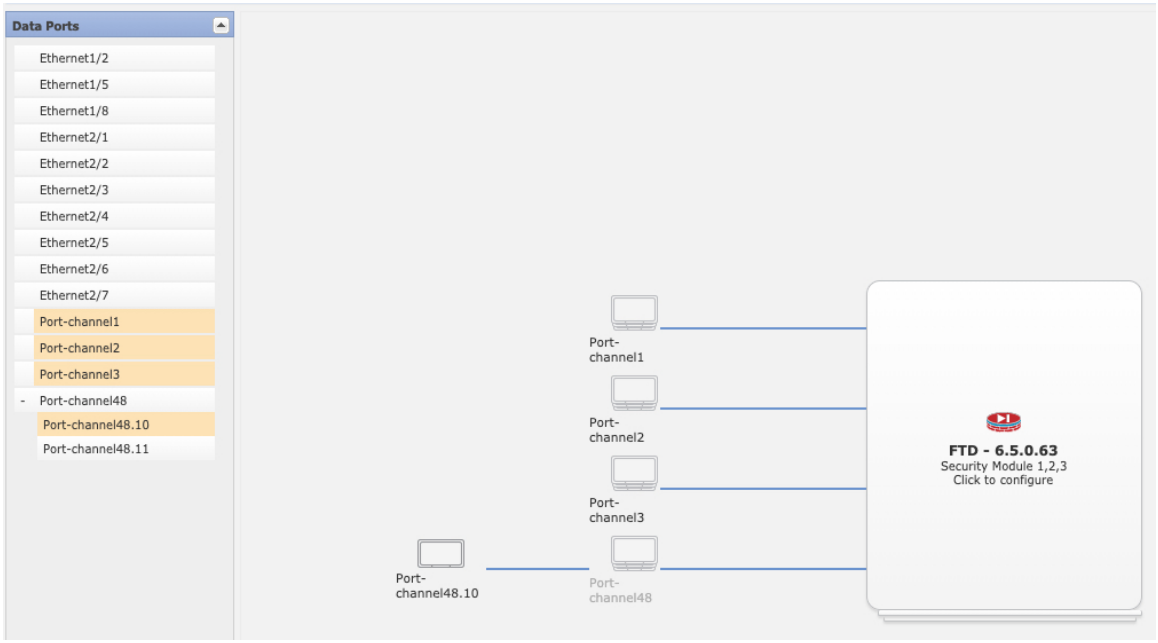
（注）

確立されたクラスタ内のインスタンスに異なるプロファイルを割り当てる場合は、プロファイルが一致する必要がないため、最初に新しいプロファイルをデータノードに適用します。再起動して復旧したら、新しいプロファイルを制御ノードに適用できます。

g) [OK] をクリックします。

[プロビジョニング - デバイス名（Provisioning - device name）] ウィンドウが表示されます。

ステップ 4 このクラスタに割り当てるインターフェイスを選択します。



ネイティブモードのクラスタリングの場合：デフォルトでは、すべての有効なインターフェイスが割り当てられます。マルチクラスタタイプのインターフェイスを定義した場合は、すべての選択を解除し、1 つのみ選択します。

マルチインスタンス クラスタリングの場合：クラスタに割り当てる各データインターフェイスを選択し、クラスタタイプのポートチャネルまたはポートチャネルのサブインターフェイスも選択します。

ステップ 5 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 6 [Cluster Information] ページで、次の手順を実行します。

図 *189* : ネイティブクラスタ

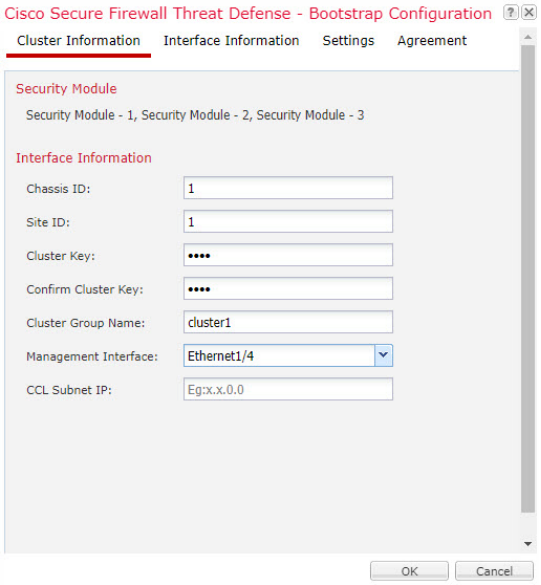
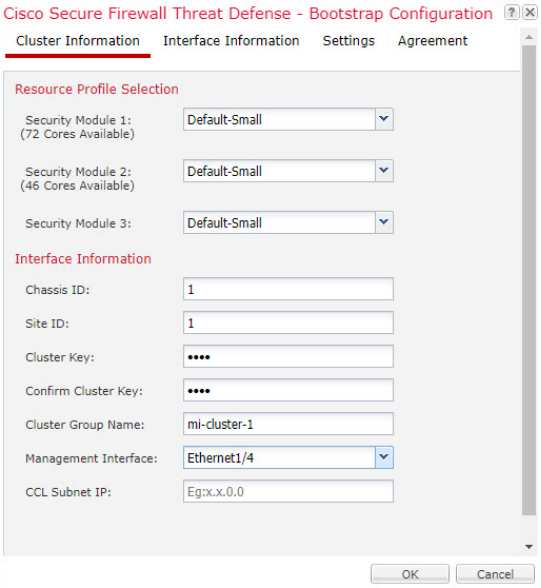


図 *190* : マルチインスタンスクラスタ



a) （Firepower 9300 のコンテナインスタンスのみ）[セキュリティモジュール（SM）とリソースプロファイルの選択（Security Module (SM) and Resource Profile Selection）] エリアで、モジュールごとに異なるリソースプロファイルを設定できます。たとえば、異なるセキュリティモジュールのタイプを使用していて、ローエンドのモデルでより多くの CPU を使用する場合に設定できます。

b) 複数のシャーシにわたるクラスタリングの場合は、[シャーシID（Chassis ID）] フィールドにシャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。

このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバーインターフェイスを追加した場合にのみ表示されます。

c) サイト間クラスタリングの場合、[サイトID（Site ID）] フィールドに、このシャーシのサイト ID を 1 ～ 8 の範囲で入力します。FlexConfig 機能。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加のカスタマイズは、Firewall Management Center FlexConfig 機能を使用した場合にのみ設定できます。

d) [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

e) [クラスタ グループ名（Cluster Group Name）] を設定します。これは、論理デバイス設定のクラスタ グループ名です。

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

重要
2.4.1 以降、クラスタグループ名のスペースは特殊文字と見なされ、論理デバイスの展開時にエラーが発生する可能性があります。この問題を回避するには、クラスタグループ名をスペースのない名前に変更する必要があります。

f) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

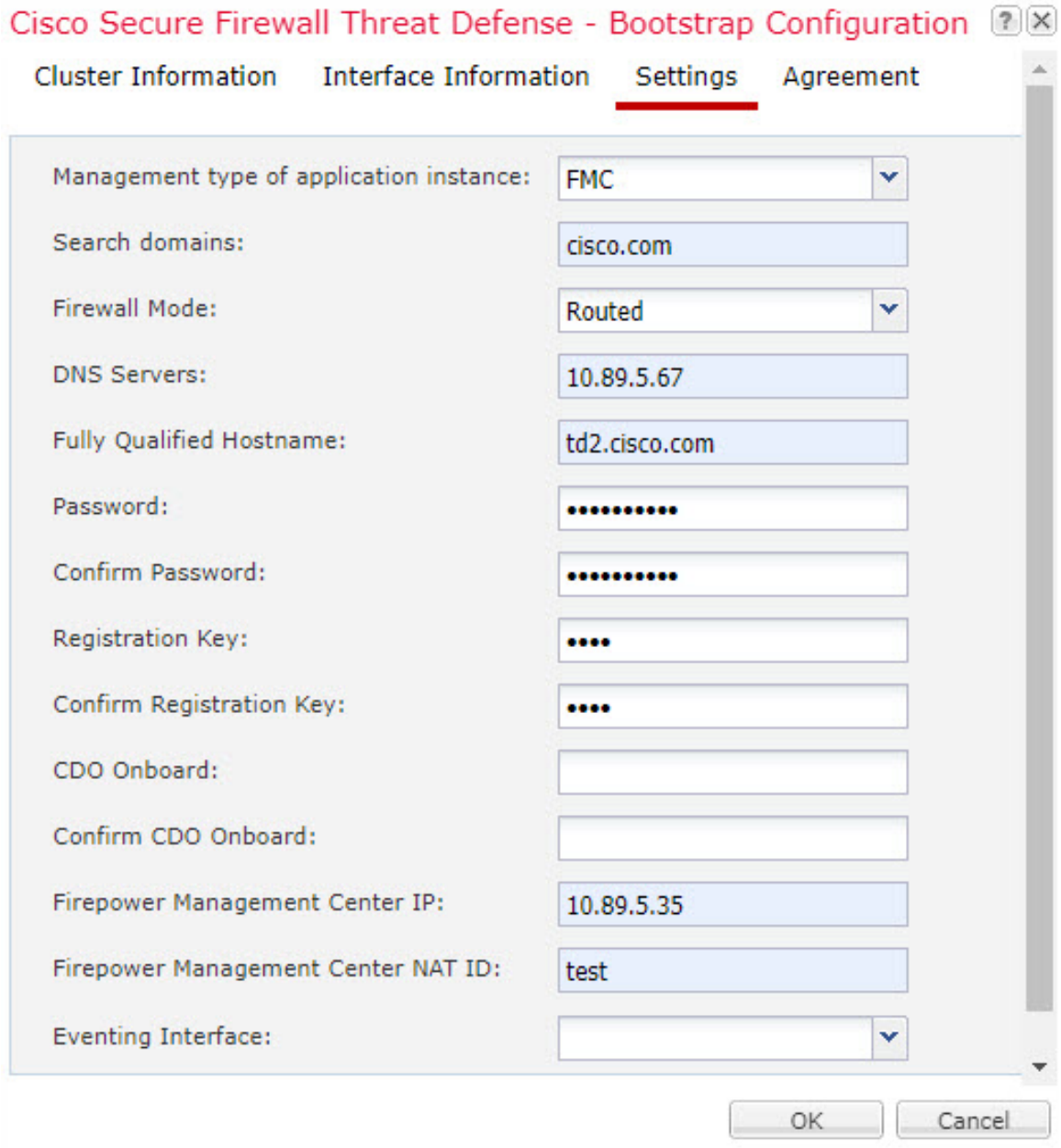
ハードウェア バイパス 対応のインターフェイスをマネジメント インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

g) （任意） **CCL サブネット IP** を ***a.b*.0.0** に設定します。

クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。この場合、クラスタの固有ネットワークに任意の/16 ネットワークアドレスを指定します（ループバック（127.0.0.0/8）、マルチキャスト（224.0.0.0/4）、内部（169.254.0.0/16）のアドレスを除く）。値を 0.0.0.0 に設定すると、デフォルトのネットワークが使用されます。

シャーシは、シャーシ ID とスロット ID（*a.b.chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

ステップ 7 [**設定（Settings**）] ページで、以下を実行します。



a) [登録キー（Registration Key）] フィールドに、登録時に Firewall Management Center とクラスタメンバー間で共有するキーを入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。Firewall Threat Defense を追加するときに、Firewall Management Center に同じキーを入力します。

b) CLI アクセス用の Firewall Threat Defense 管理ユーザの [Password] を入力します。

c) [Firepower Management CenterのIP（Firepower Management Center IP）] フィールドに、管理側の Firewall Management Center の IP アドレスを入力します。Firewall Management Center

の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

d) （任意） **FTD SSH セッションからエキスパート モード**、[**Yes**]、または [**No**] を許可します。エキスパート モードでは、高度なトラブルシューティングに Firewall Threat Defense シェルからアクセスできます。

このオプションで [Yes] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザがエキスパートモードを開始できます。[いいえ（No）] を選択した場合、FXOS CLI からコンテナインスタンスにアクセスするユーザのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、Firewall Threat Defense CLI で **expert** コマンドを使用します。

e) （任意） [Search Domains] フィールドに、管理ネットワークの検索ドメインのカンマ区切りのリストを入力します。

f) （任意） [Firewall Mode] ドロップダウン リストから、[Transparent] または [Routed] を選択します。

ルーテッド モードでは、Firewall Threat Defenseはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

g) （任意） [**DNSサーバ（DNS Servers**）] フィールドに、DNS サーバのカンマ区切りのリストを入力します。

たとえば、Firewall Management Centerのホスト名を指定する場合、Firewall Threat Defense は DNS を使用します。

h) （任意） [Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。このパスフレーズは、新しいデバイスとしてクラスタを追加するときに Firewall Management Center でも入力します。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。Firewall Management Center がデバイスの IP アドレスを指定し、デバイスが Firewall Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。NAT ID として、1～37 文字の任意のテキスト文字列を指定できます。Firewall Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

i) （任意）[Fully Qualified Hostname] フィールドに、Firewall Threat Defense デバイスの完全修飾名を入力します。

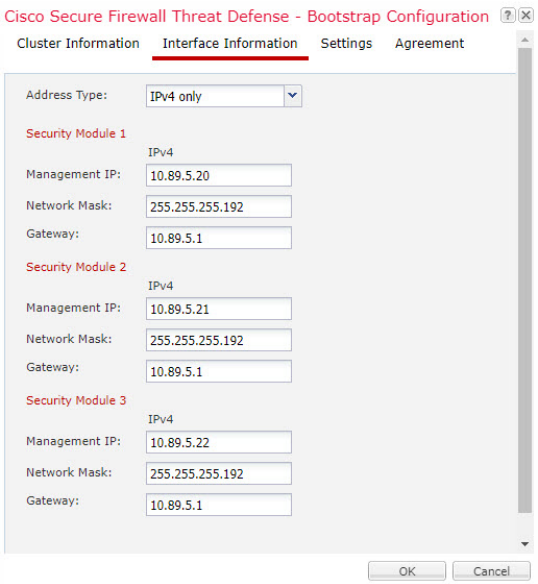
有効な文字は、a ー z の文字、0 ー 9 の数字、ドット（.）、ハイフン（-）です。最大文字数は 253 です。

j) （任意）[イベンティングインターフェイス（Eventing Interface）] ドロップダウンリストから、イベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

イベントに使用する別のインターフェイスを指定するには、*firepower-eventing* インターフェイスとしてインターフェイスを設定する必要があります。ハードウェアバイパス対応のインターフェイスを Eventing インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

ステップ 8 [インターフェイス情報（Interface Information）] ページで、クラスタ内のセキュリティモジュールのそれぞれに管理 IP アドレスを設定します。[アドレス タイプ（Address Type）] ドロップダウン リストからアドレスのタイプを選択し、セキュリティ モジュールごとに次の手順を実行します。

（注）
モジュールがインストールされていない場合でも、シャーシの 3 つすべてのモジュール スロットで IP アドレスを設定する必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。



a) [Management IP] フィールドで、IP アドレスを設定します。

モジュールごとに同じネットワーク上の一意の IP アドレスを指定します。

b) [Network Mask] または [Prefix Length] に入力します。

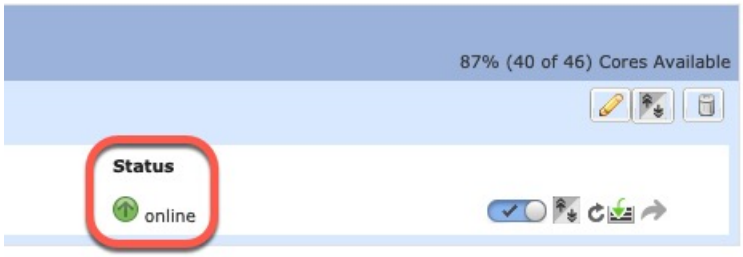
c) [ネットワーク ゲートウェイ（Network Gateway）] にネットワーク ゲートウェイ アドレスを入力します。

ステップ 9 [利用規約（Agreement）] タブで、エンドユーザ ライセンス（EULA）を読んで、同意します。

ステップ 10 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 11 **[保存（Save）]** をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されている場合は、残りのクラスタシャーシを追加できます。また、1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタの場合は、アプリケーションのクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 12 複数のシャーシにわたるクラスタリングの場合は、クラスタに次のシャーシを追加します。

a) Firewall Chassis Manager の最初のシャーシで、右上の [設定の表示（Show Configuration）] アイコンをクリックして、表示されるクラスタ設定をコピーします。

b) 次のシャーシの Firewall Chassis Manager に接続し、この手順に従って論理デバイスを追加します。

c) [必要な操作（I want to:）] > [既存のクラスタへの参加（Join an Existing Cluster）] を選択します。

d) **[OK]** をクリックします。

e) [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

f) 画面中央のデバイスアイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加の

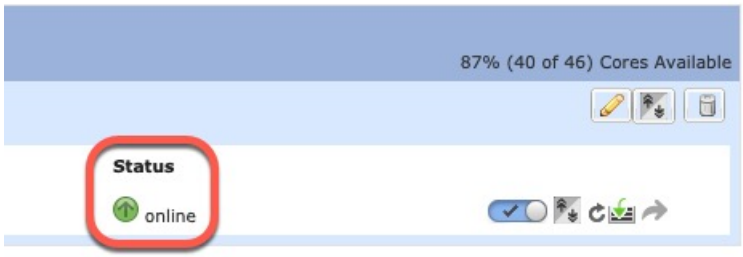
カスタマイズは、Firewall Management Center FlexConfig 機能を使用した場合にのみ設定できます。

- **Cluster Key**：（事前に入力されていない）同じクラスタ キーを入力します。
- [管理IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

g) **[保存（Save）]** をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。各クラスタメンバの [論理デバイス（Logical Devices）] ページで、新しい論理デバイスのステータスを確認します。各クラスタメンバの論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 13 管理 IP アドレスを使用して、Firewall Management Center に制御ユニットを追加します。

すべてのクラスタ ユニットは、Firewall Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。

Firewall Management Center がデータユニットを自動的に検出します。

クラスタノードの追加

既存のクラスタ内の Firewall Threat Defense クラスタノードを追加または交換します。FXOS に新しいクラスタノードを追加すると、Firewall Management Center によりノードが自動的に追加されます。

（注） このプロシージャにおけるFXOSの手順は、新しいシャーシの追加のみに適用されます。クラスタリングがすでに有効になっている Firepower 9300 に新しいモジュールを追加する場合、モジュールは自動的に追加されます。

始める前に

- 置き換える場合は、Firewall Management Center から古いクラスタノードを削除する必要があります。新しいノードに置き換えると、Firewall Management Center 上の新しいデバイスとみなされます。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。

手順

ステップ 1 以前に Firewall Management Center を使用して Firewall Threat Defense イメージをアップグレードした場合は、クラスタ内の各シャーシで次の手順を実行します。

Firewall Management Center からアップグレードしたときに、FXOS 設定のスタートアップバージョンが更新されておらず、スタンドアロンパッケージがシャーシにインストールされていませんでした。新しいノードが正しいイメージバージョンを使用してクラスタに参加できるように、これらの項目は両方とも手動で設定する必要があります。

（注）
パッチリリースのみを適用した場合は、この手順をスキップできます。シスコではパッチ用のスタンドアロンパッケージを提供していません。

a) **[システム（System）]** > **[更新（Updates）]**ページを使用して、実行中の Firewall Threat Defense イメージをシャーシにインストールします。
b) [論理デバイス（Logical Devices）] をクリックし、[バージョンの設定（Set Version）] アイコン（ ） をクリックします。複数のモジュールを備えた Firepower 9300 の場合、各モジュールのバージョンを設定します。

[スタートアップバージョン（Startup Version）] には、展開した元のパッケージが表示されます。[現在のバージョン（Current Version）] には、アップグレード後のバージョンが表示されます。

c) [新しいバージョン（New Version）] ドロップダウンメニューで、アップロードしたバージョンを選択します。このバージョンは、表示されている [現在のバージョン（Current Version）] と一致する必要があり、スタートアップバージョンが新しいバージョンと一致するように設定されます。
d) 新しいシャーシに、新しいイメージパッケージがインストールされていることを確認します。

ステップ 2 既存のクラスタシャーシ Firewall Chassis Manager で、[論理デバイス（Logical Devices）] をクリックします。

ステップ 3 右上の [設定の表示（Show Configuration）] アイコンをクリックし、表示されるクラスタ設定をコピーします。

ステップ 4 新しいシャーシの Firewall Chassis Manager に接続して、**[追加（Add）]**>**[クラスタ（Cluster）]** をクリックします。

ステップ 5 [デバイス名（Device Name）] に論理デバイスの名前を入力します。

ステップ 6 **[OK]** をクリックします。

ステップ 7 [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

ステップ 8 画面中央のデバイス アイコンをクリックします。クラスタ情報の一部は事前に入力済みですが、次の設定は入力する必要があります。

図 *191* : クラスタ情報

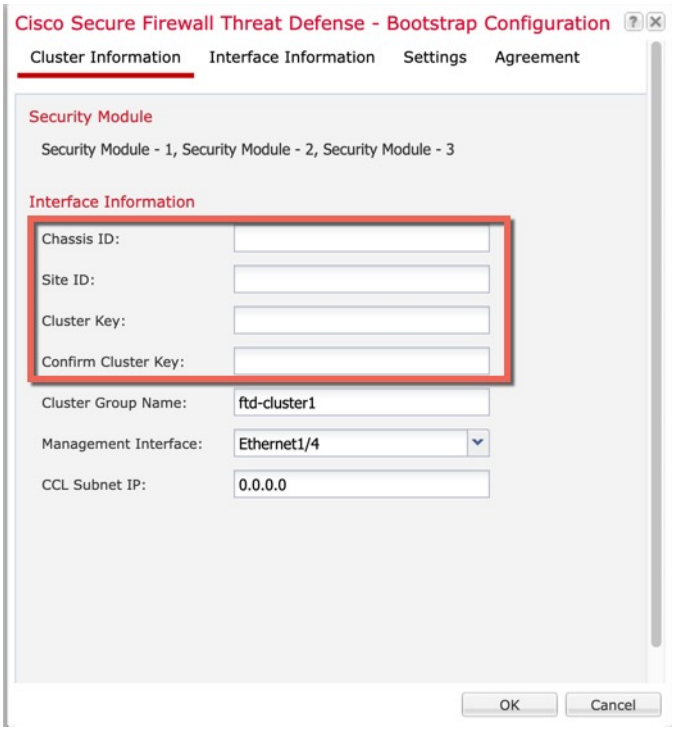


図 *192* : インターフェイス情報

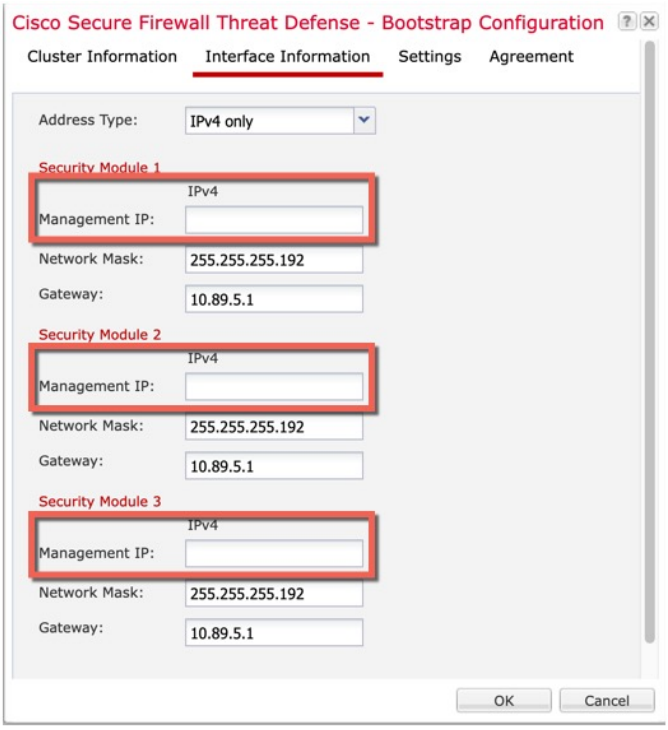
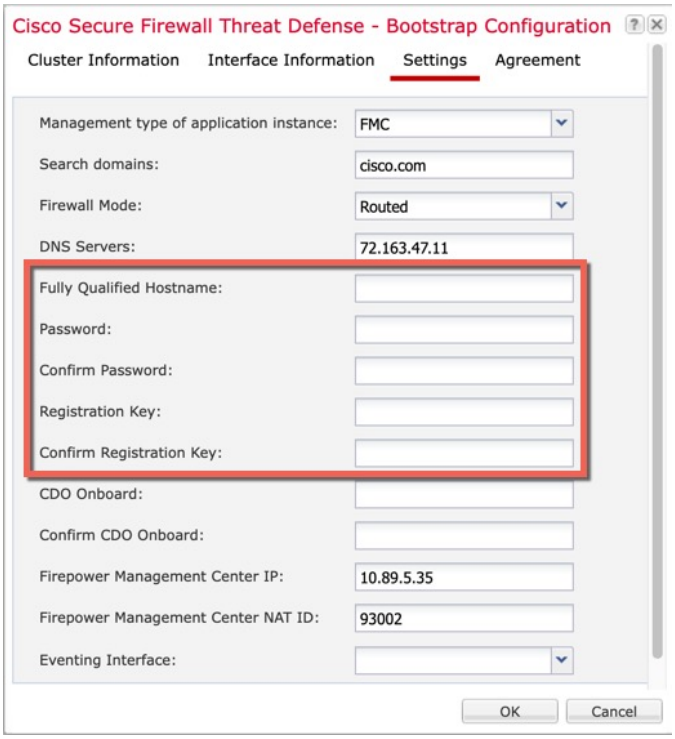


図 *193* : 設定

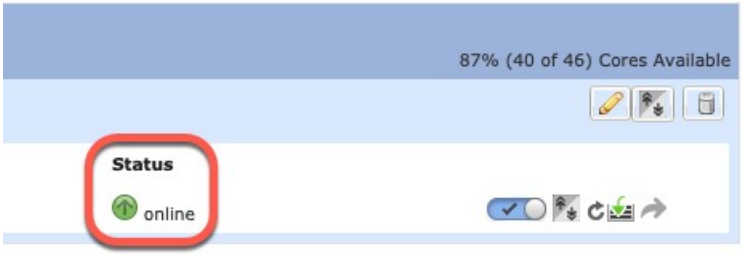


- [シャーシID（Chassis ID）]：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。この機能は、Firewall Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- [クラスタキー（Cluster Key）]：同じクラスタキーを入力します。
- [管理IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタメンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。
- [完全就職ホスト名（Fully Qualified Hostname）]：同じホスト名を入力します。
- [パスワード（Password）]：同じパスワードを入力します。
- [登録キー（Registration Key）]： 同じ 登録キーを入力します。

[OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。各クラスタメンバの [論理デバイス（Logical Devices）] ページで、新しい論理デバイスのステータスを確認します。各クラスタメンバの論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



Firewall Management Center：クラスタの追加

クラスタ ユニットのいずれかを新しいデバイスとして Secure Firewall Management Center に追加します。Firewall Management Center は、他のすべてのクラスタ メンバーを自動検出します。

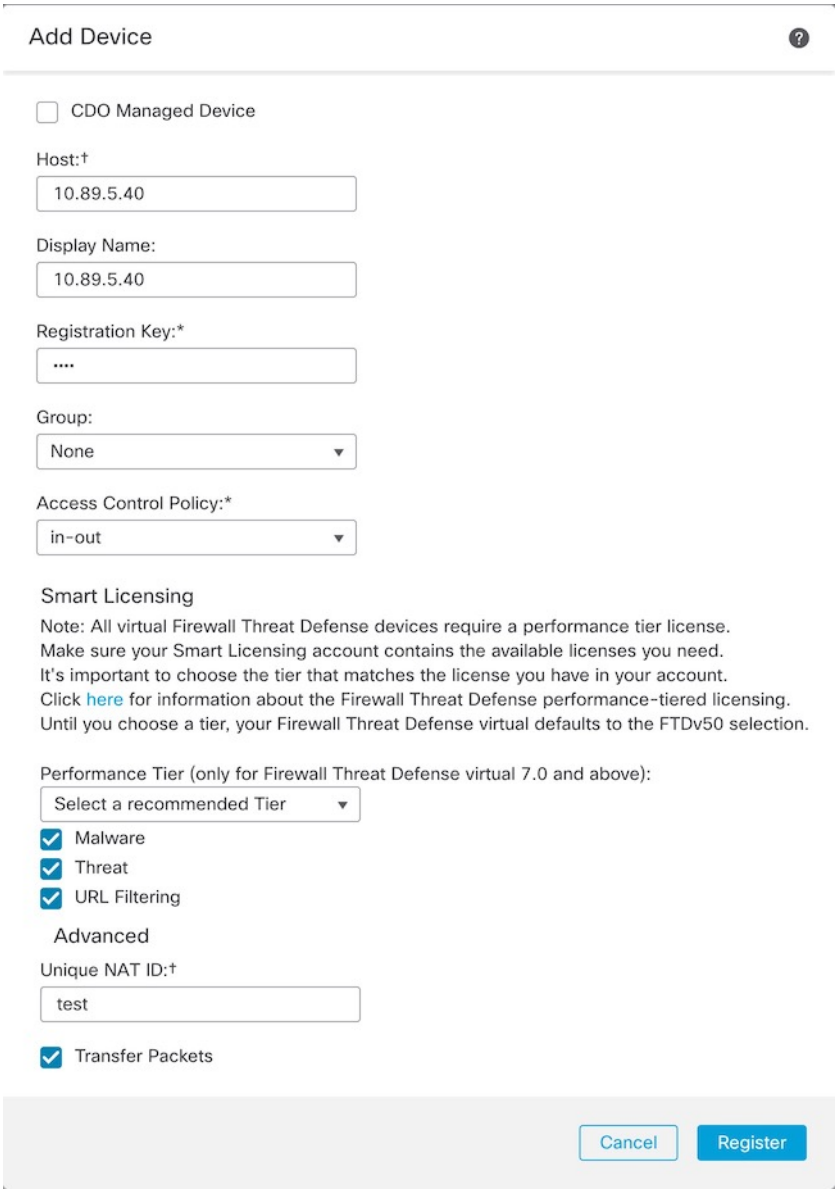
始める前に

- すべてのクラスタユニットは、Firewall Management Center に追加する前に、FXOS 上にある正常な形式のクラスタ内に存在している必要があります。また、どのユニットが制御ユニットかを確認することも必要です。Firewall Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、Firewall Threat Defense の **show cluster info** コマンドを使用します。

手順

ステップ 1 Firewall Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択してから、**[追加（Add）]** > **[デバイスの追加（Add Device）]** を選択し、クラスタを展開したときに割り当てた制御ユニットの管理 IP アドレスを使用して制御ユニットを追加します。

図 *194* : デバイスの追加



a) [ホスト（Host）] フィールドに、制御ユニットの IP アドレスまたはホスト名を入力します。

最適なパフォーマンスを得るため、制御ユニットの追加を推奨しますが、クラスタの任意のユニットを追加できます。

デバイスのセットアップ時に NAT ID を使用した場合は、このフィールドを入力する必要がない可能性があります。詳細については、「NAT 環境 （8 ページ）」を参照してください。

b) [表示名（Display Name）] フィールドに、Firewall Management Center での制御ユニットの表示名を入力します。

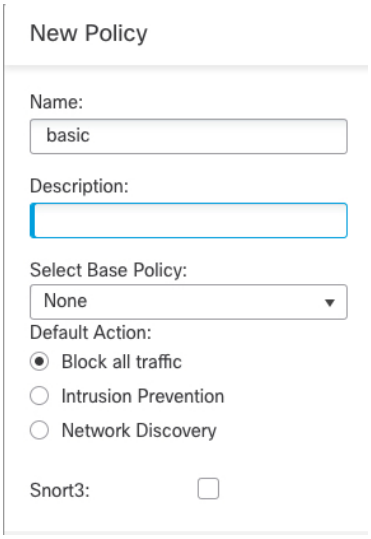
この表示名はクラスタ用ではありません。追加する制御ユニット専用です。後で、他のクラスタメンバーの名前やクラスタ表示名を変更できます。

c) [登録キー（Registration Key）] フィールドに、FXOS にクラスタを展開したときに使用したものと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。

d) （任意） デバイスをデバイス**グループ**に追加します。

e) 登録後すぐに、デバイスに展開する最初の [アクセスコントロールポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。

新しいポリシーを作成する場合は、基本ポリシーのみを作成します。必要に応じて、後でポリシーをカスタマイズできます。



f) デバイスに適用するライセンスを選択します。

g) デバイスの設定時に、NAT ID を使用した場合、[詳細（Advanced）] セクションを展開し、[一意の NAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

h) [パケットの転送（Transfer Packets）] チェックボックスをオンにし、デバイスで Firewall Management Center にパケットを転送することを許可します。

このオプションは、デフォルトで有効です。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Firewall Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Firewall Management Center に送信され、パケットデータは送信されません。

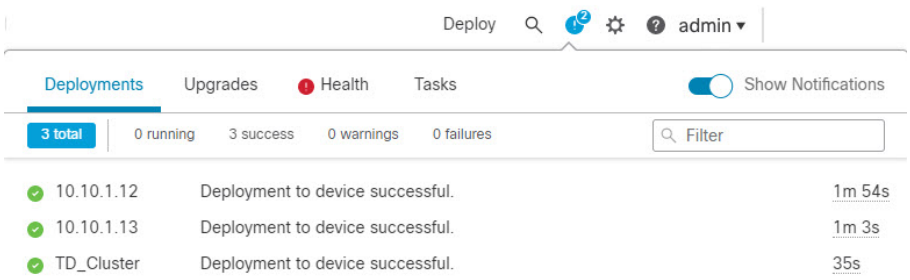
i) [登録（Register）] をクリックします。

Firewall Management Center は、制御ユニットを識別して登録した後に、すべてのデータユニットを登録します。制御ユニットが正常に登録されていない場合、クラスタは追加されません。クラスタがシャーシで稼働状態になかったか、その他の接続問題が原因で、登録エラーが発生する場合があります。こうした状況では、クラスタユニットを再度追加することをお勧めします。

[デバイス（Devices）] > **[デバイス管理（Device Management）]** ページにクラスタ名が表示されます。クラスタを展開して、クラスタユニットを表示します。

現在登録されているユニットには、ロード アイコンが表示されます。

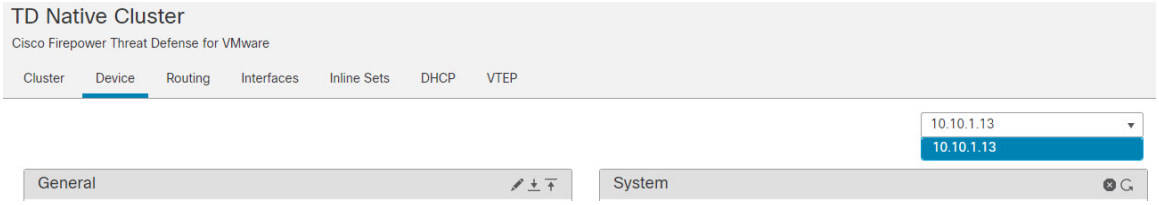
クラスタユニットの登録をモニターするには、[通知（Notifications）]アイコンをクリックし、[タスク（Tasks）]を選択します。Firewall Management Center は、ユニットの登録ごとにクラスタ登録タスクを更新します。いずれかのユニットの登録に失敗した場合には、クラスタ メンバーの照合 （597 ページ） を参照してください。



ステップ 2 クラスタの [編集（Edit）]（✎） をクリックして、デバイス固有の設定を指定します。

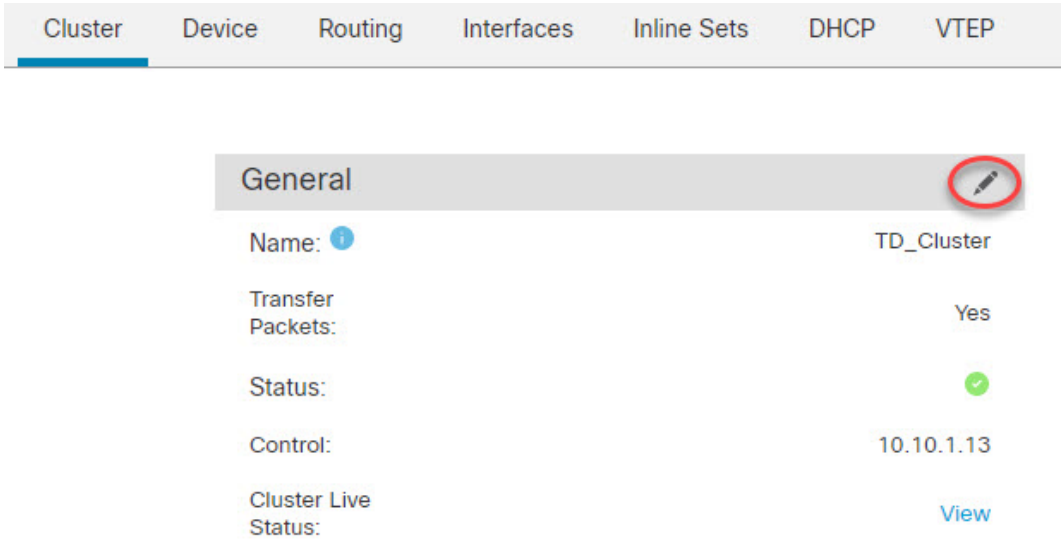
ほとんどの設定は、クラスタ内のメンバーユニットではなくクラスタ全体に適用できます。たとえば、ユニットごとに表示名を変更できますが、インターフェイスはクラスタ全体についてのみ設定できます。

ステップ 3 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** 画面に、[全般（General）]、[ライセンス（License）]、[システム（System）]、および [ヘルス（Health）] の設定が表示されます。

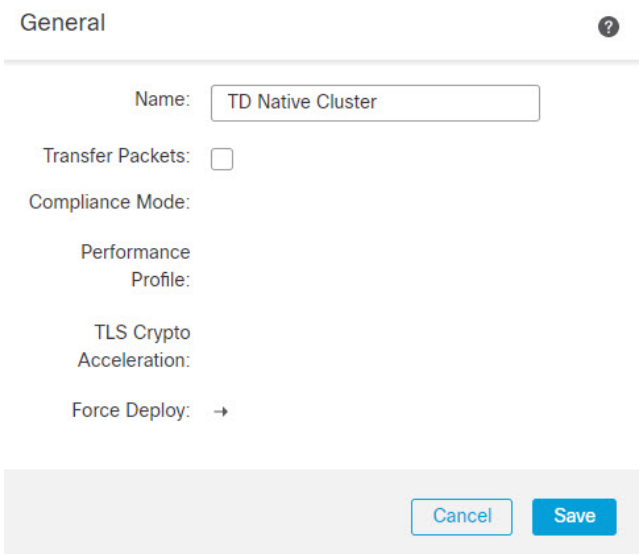


次のクラスタ固有の項目を参照してください。

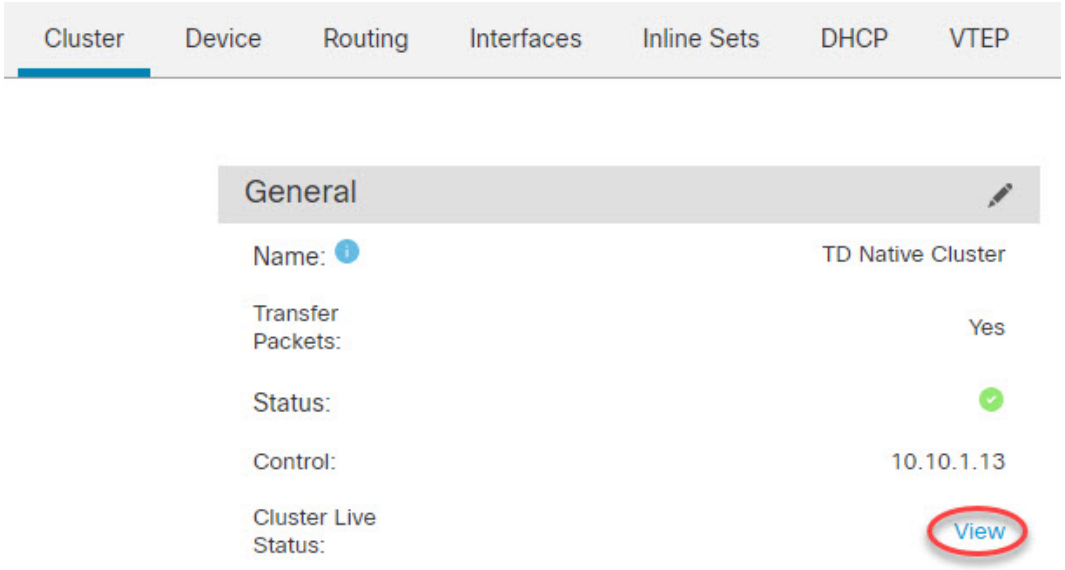
- [全般（General）]>[名前（Name）]：[編集（Edit）]（✎）をクリックして、クラスタの表示名を変更します。



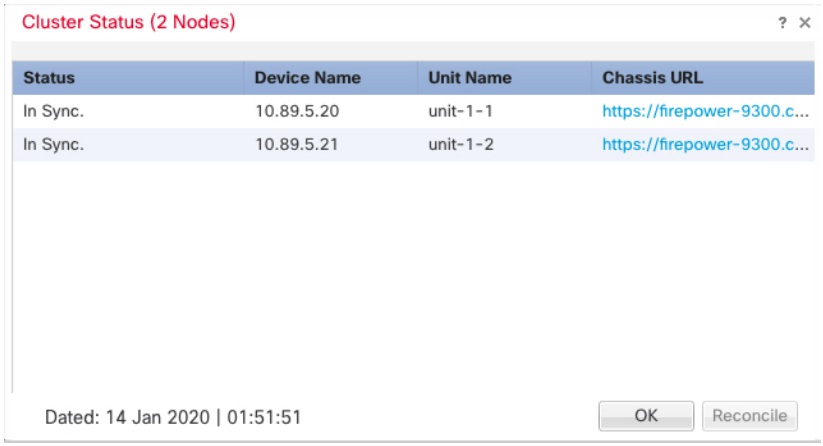
その後に、[名前（Name）]フィールドを設定します。



- [全般（General）]>[クラスタステータスの表示（View cluster status）]：[クラスタステータスの表示（View cluster status）]リンクをクリックして[クラスタステータス（Cluster Status）]ダイアログボックスを開きます。



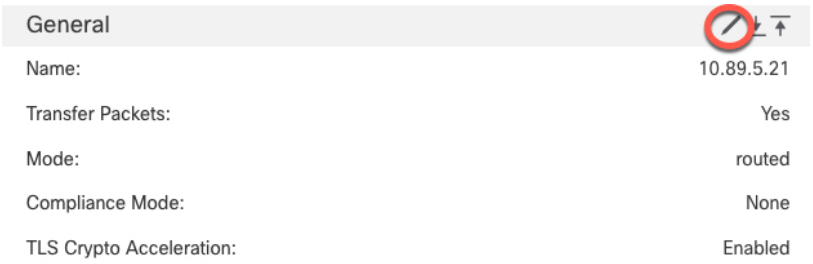
[クラスタステータス（Cluster Status）] ダイアログボックスで、[照合（Reconcile）] をクリックしてデータユニットの登録を再試行することもできます。



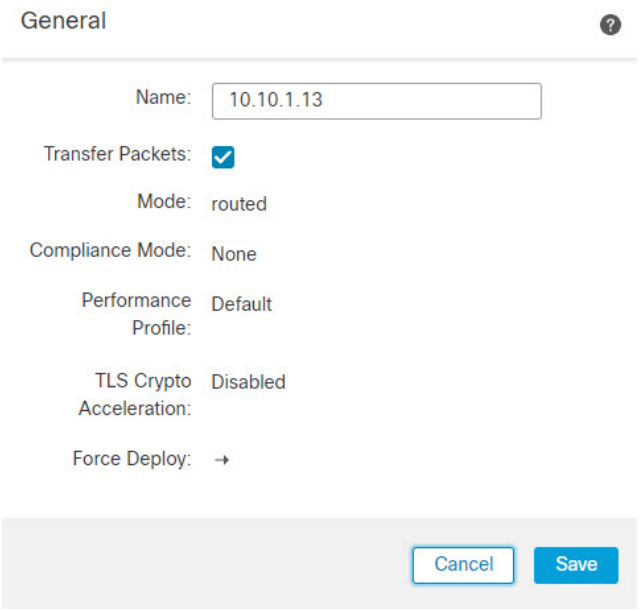
- [ライセンス（License）]：[編集（Edit）]（✎）をクリックして、ライセンス付与資格を設定します。

ステップ 4 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Devices）]** の右上のドロップダウンメニューで、クラスタ内の各メンバーを選択し、次の設定を指定することができます。

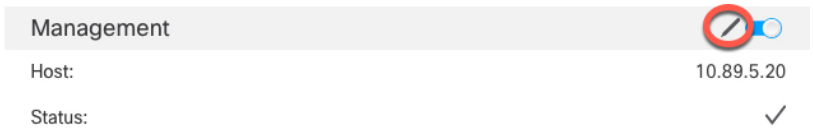
- [全般（General）] > [名前（Name）]：[編集（Edit）]（✎）をクリックして、クラスタメンバーの表示名を変更します。



その後に、[名前（Name）] フィールドを設定します。



- [管理（Management）] > [ホスト（Host）]：デバイス設定で管理 IP アドレスを変更する場合、Firewall Management Center で新しいアドレスを一致させてネットワーク上のデバイスに到達できるようにし、[管理（Management）] 領域で [ホスト（Host）] アドレスを編集します。



Firewall Management Center：クラスタ、データ、および診断インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。複数のシャーシにわたるクラスタリングの

場合、データインターフェイスは常にスパンド EtherChannel インターフェイスです。1 つの Firepower 9300 シャーシ内のセキュリティモジュール内に隔離されたクラスタのクラスタ制御リンクインターフェイスの場合、MTUをデフォルトから増やす必要があります。個別インターフェイスとして実行できる唯一のインターフェイスである診断インターフェイスを設定することもできます。

（注） 複数のシャーシによるクラスタリングにスパンドEtherChannelを使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、クラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 2 [インターフェイス（Interfaces）] をクリックします。

ステップ 3 クラスタ制御リンクを設定します。

複数シャーシによるクラスタリングの場合、クラスタ制御リンクMTUに、データインターフェイスの最大 MTU より少なくとも 100 バイト高い値を指定します。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。MTU の最大値を 9184 バイトに設定し、最小値を 1400 バイトに設定することをお勧めします。たとえば、最大 MTU は 9184 バイトであるため、データインターフェイスの最大 MTU は 9084 になり、クラスタ制御リンクは 9184 に設定できます。

ネイティブクラスタの場合：クラスタ制御リンクインターフェイスは、デフォルトで Port-Channel48 です。どのインターフェイスがクラスタ制御リンクであるかがわからない場合は、クラスタに割り当てられたクラスタ タイプ インターフェイスのシャーシの FXOS 設定を確認します。

a) クラスタ制御リンクインターフェイスの [編集（Edit）]（✎） をクリックします。
b) [全般（General）] ページの [MTU] フィールドに、1400 ～ 9184 の値を入力します。ただし、2561 ～ 8362 の範囲の値は入力しないでください。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。最大の 9184 を使用することをお勧めします。
c) [OK] をクリックします。

ステップ 4 データインターフェイスを設定します。

a) （任意） 通常のファイアウォール インターフェイスの場合は、データインターフェイスに VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。サブインターフェイスの追加（694 ページ）を参照してください。

b) データインターフェイスの [編集（Edit）]（） をクリックします。

c) 名前とその他のパラメータを設定します。通常のファイアウォールインターフェイスについては、ルーテッドモードのインターフェイスの設定（717ページ）を参照してください。また、トランスペアレントモードについては、ブリッジ グループ インターフェイスの設定（724ページ）を参照してください。IPS専用インターフェイスについては、インラインセットとパッシブインターフェイス（763 ページ）を参照してください。.

（注）
クラスタ制御リンクインターフェイスのMTUがデータインターフェイスのMTUより100バイト以上大きくない場合、データインターフェイスのMTUを減らす必要があるというエラーが表示されます。ステップ 3（581 ページ）を参照して、クラスタ制御リンクのMTUを増やしてください。その後、データインターフェイスの設定を続行できます。

d) 複数シャーシによるクラスタリングの場合は、EtherChannelの手動グローバルMACアドレス（一意）を設定します。[詳細設定（Advanced）] をクリックし、[アクティブなMACアドレス（Active MAC Address）] フィールドに、MACアドレスをH.H.H形式で設定します。Hは16ビットの16進数です。

たとえば、MACアドレスが00-0C-F1-42-4C-DEの場合、000C.F142.4CDEと入力します。MACアドレスはマルチキャストビットセットを持つことはできません。つまり、左から2番目の16進数字を奇数にすることはできません。

[スタンバイMACアドレス（Standby MAC Address）] は設定しないでください。無視されます。

潜在的なネットワークの接続問題を回避するために、スパンドEtherChannelには、現在ネットワークで使用されていない、一意のMACアドレスを設定する必要があります。MACアドレスが手動設定されている場合、そのMACアドレスは現在の制御ユニットに留まります。MACアドレスを設定していない場合に、制御ユニットが変更された場合、新しい制御ユニットはインターフェイスに新しいMACアドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

e) [OK] をクリックします。他のデータ インターフェイスについても前述の手順を繰り返します。

ステップ 5 （任意） 診断インターフェイスを設定します。

診断インターフェイスは、個別インターフェイスモードで実行できる唯一のインターフェイスです。syslogメッセージやSNMPなどに、このインターフェイスを使用できます。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレスプール（Address Pools）]** を選択して、IPv4またはIPv6アドレスプールを追加します。アドレス プール（1323 ページ）を参照してください。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。仮想IPアドレスはこのプールには含まれませんが、同一ネットワーク上に存在している必要があります。各ユニットに割り当てられる正確なローカルアドレスを事前に決定することはできません。

b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** で、診断インターフェイスの [編集（Edit）]（✎） をクリックします。
c) [IPv4] で [IPアドレス（IP Address）] とマスクを入力します。この IP アドレスは、そのクラスタの固定アドレスで、常に現在の制御ユニットに属します。
d) 作成したアドレス プールを [IPv4 アドレス プール（IPv4 Address Pool）] ドロップダウンリストから選択します。
e) [IPv6] > [基本（Basic）] で、[IPv6アドレスプール（IPv6 Address Pool）] ドロップダウンリストから、作成したアドレスプールを選択します。
f) 通常どおり、他のインターフェイス設定を行います。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

Firewall Management Center：クラスタのヘルスモニターの設定

[クラスタ（Cluster）]ページの[クラスタヘルスモニターの設定（Cluster Health Monitor Settings）]セクションには、次の表で説明されている設定が表示されます。

図 *195 :* クラスタのヘルスモニターの設定

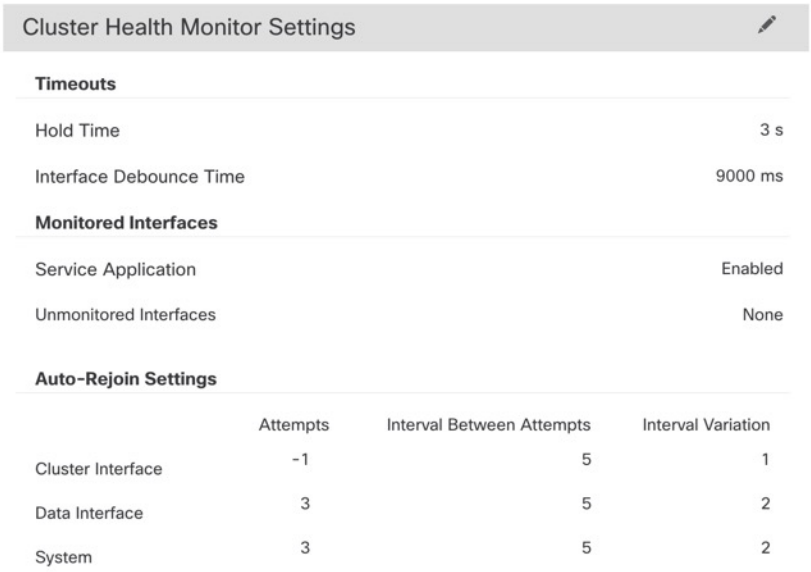


表 *41 : [*クラスタヘルスモニターの設定（*Cluster Health Monitor Settings***）*]* セクションテーブルのフィールド**

フィールド	説明
タイムアウト（Timeouts）	

フィールド	説明
保留時間（Hold Time）	指定できる範囲は0.3 ～ 45秒です。デフォルトは3秒です。ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間（Interface Debounce Time）	指定できる範囲は 300 ～ 9000 ミリ秒です。デフォルトは 500 ms です。インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると見なされ、クラスタからノードが削除されるまでの時間です。
Monitored Interfaces（モニタリング対象インターフェイス）	インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。
サービスアプリケーション（Service Application）	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。
モニタリング対象外のインターフェイス（Unmonitored Interfaces）	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定（Auto-Rejoin Settings）	
クラスタインターフェイス（Cluster Interface）	クラスタ制御リンクに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは -1（無制限）です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 1 倍です。試行ごとに間隔を長くするかどうかを定義します。
データインターフェイス（Data Interfaces）	データインターフェイスに障害が発生した後に自動再結合の設定を表示します。

フィールド	説明
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。
システム（System）	内部エラーが発生した後に自動再結合の設定を表示します。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。

（注） システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

これらの設定は、このセクションから変更できます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI やBVIなどの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

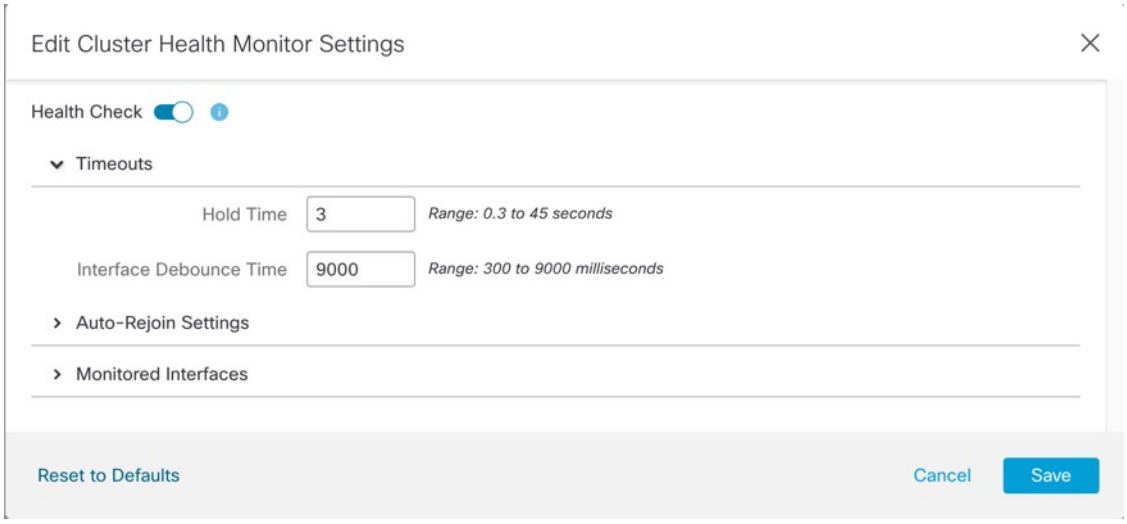
ステップ 2 変更するクラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [クラスタ（Cluster）] をクリックします。

ステップ 4 [クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）] セクションで、[編集（Edit）]（✎） をクリックします。

ステップ 5 [ヘルスチェック（Health Check）] スライダをクリックして、システムのヘルスチェックを無効にします。

図 *196 :* システムヘルスチェックの無効化



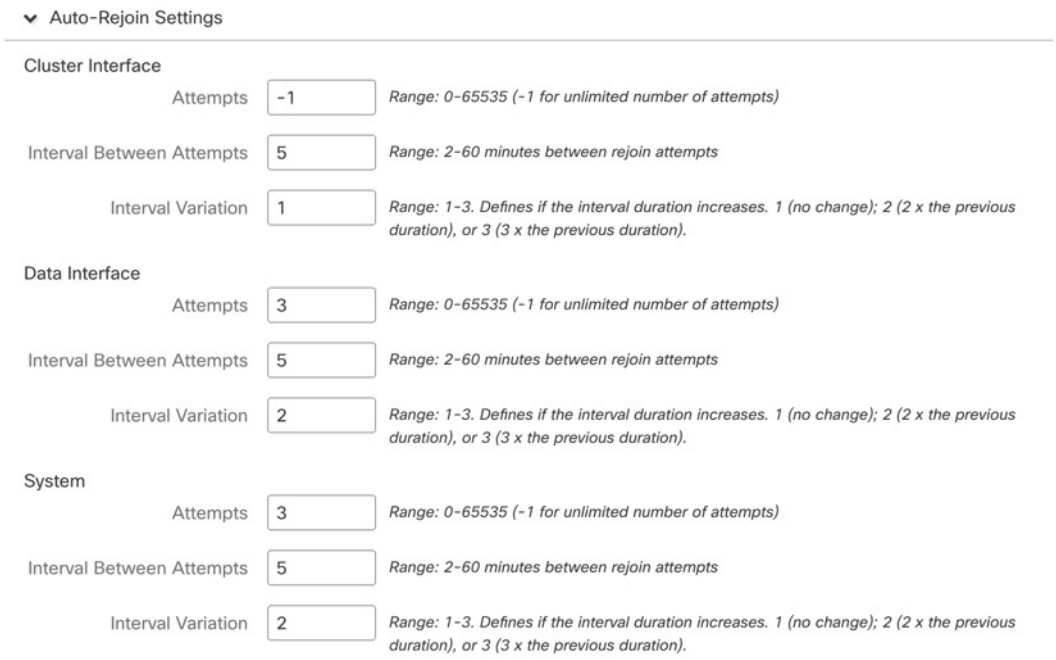
何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間（Hold Time）]：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ～ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間（Interface Debounce Time）]：デバウンス時間は 300 ～ 9000 ms の範囲で値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 *197 :* 自動再結合の設定

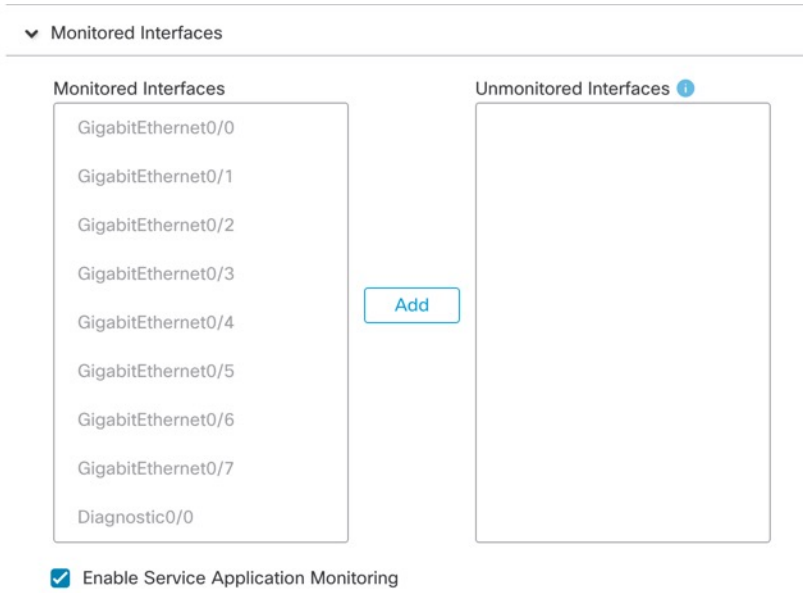


[クラスタインターフェイス（Cluster Interface）]、[データインターフェイス（Data Interface）]、および[システム（System）]に次の値を設定します（内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります）。

- [試行数（Attempts）]：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。[クラスタインターフェイス（Cluster Interface）] のデフォルト値は -1（無制限）です。[データインターフェイス（Data Interface）] と [システム（System）] のデフォルト値は 3 です。
- [試行の間隔（Interval Between Attempts）]：再結合試行の間隔を 2 ～ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [間隔のバリエーション（Interval Variation）]：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、[クラスタインターフェイス（Cluster Interface）] の場合は **1**、[データインターフェイス（Data Interface）] および [システム（System）] の場合は **2** です。

ステップ 8 [モニタリング対象のインターフェイス（Monitored Interfaces）] または [モニタリング対象外のインターフェイス（Unmonitored Interfaces）] ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリングを有効にする（Enable Service Application Monitoring）] をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 *198 :* モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングを無効にできます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

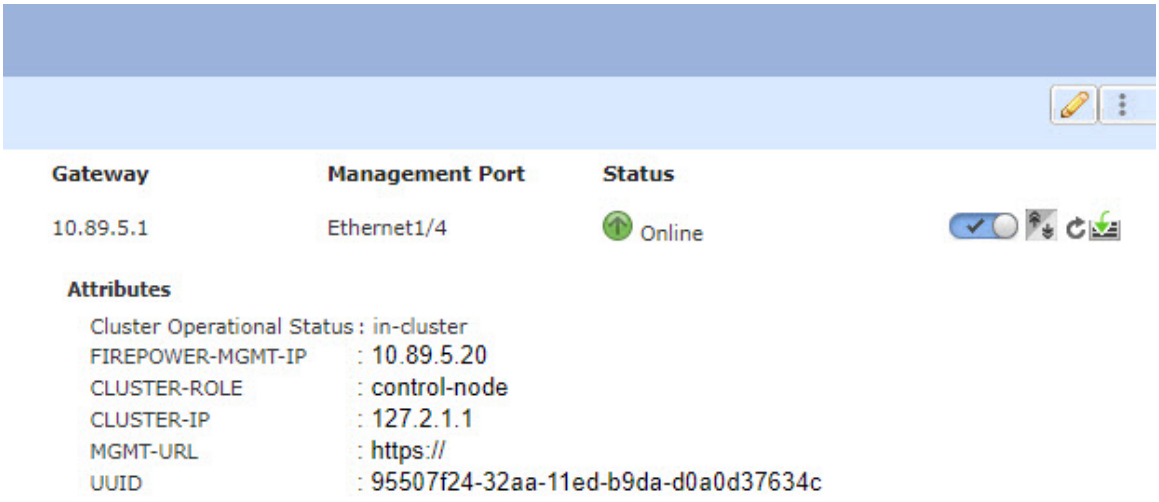
FXOS：クラスタノードの削除

ここでは、ノードをクラスタから一時的に、または永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタノードはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内に存在するか確認するには、Firewall Chassis Manager [論理デバイス（Logical Devices）] ページで、**show cluster info** コマンドを使用してアプリケーション内のクラスタステータスを確認します。



Firewall Management Center を使用した Firewall Threat Defense では、Firewall Management Center デバイスリストにデバイスを残し、クラスタリングを再度有効にした後ですべての機能を再開できるようにする必要があります。

- アプリケーションでのクラスタリングの無効化：アプリケーションCLIを使用してクラスタリングを無効にすることができます。**cluster remove unit** *name* コマンドを入力して、ログインしているノード以外のすべてのユニットを削除します。ブートストラップコンフィギュレーションは変更されず、制御ノードから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのノードを再度追加できます。制御ノードを削除するためにデータノードでこのコマンドを入力した場合は、新しい制御ノードが選定されます。

  デバイスが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合、管理インターフェイスは無効になります。

  クラスタリングを再度有効にするには、Firewall Threat Defense で **cluster enable** を入力します。

- アプリケーションインスタンスの無効化：Firewall Chassis Manager の [論理デバイス（Logical Devices）] ページで **Slider enabled**（ ） をクリックします。**Slider disabled**（ ）を使用して後で再度有効にすることができます。
- セキュリティ モジュール/エンジン のシャットダウン：Firewall Chassis Manager の [セキュリティモジュール/エンジン（Security Module/Engine）] ページで、[電源オフ（Power Off）] アイコンをクリックします。
- シャーシのシャットダウン：Firewall Chassis Managerの [概要（Overview）] ページで、[シャットダウン（Shut Down）] アイコンをクリックします。

完全な削除

次の方法を使用して、クラスタノードを完全に削除できます。

Firewall Management Center を使用した Firewall Threat Defense の場合、シャーシでクラスタリングを無効にした後でノードを Firewall Management Center デバイスリストから削除してください。

- 論理デバイスの削除：Firewall Chassis Manager の [論理デバイス（Logical Devices）] ページで、をクリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加したりすることもできます。
- サービスからのシャーシまたはセキュリティモジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいノードとして追加できます。

FMC：クラスタメンバーの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

新規クラスタ メンバーの追加

FXOS に新しいクラスタ メンバーを追加すると、Secure Firewall Management Center によりメンバーが自動的に追加されます。

始める前に

- インターフェイスの設定が他のシャーシと交換用ユニットで同じ設定になっていることを確認します。

手順

ステップ 1 FXOS のクラスタに新しいユニットを追加します。『FXOS コンフィギュレーション ガイド』を参照してください。

新しいユニットがクラスタに追加されるまで待機します。Firepower Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、または Firepower Threat Defense の **show cluster info** コマンドを使用してクラスタ ステータスを表示します。

ステップ 2 新しいクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニターするには、次のように表示します。

- [クラスタステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** [その他（More）] アイコンまたは **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** タブ > [全般（General）] 領域 > [クラスタステータスの表示（View Cluster Status）]> [クラスタのライブステータス（Cluster Live Status）] リンクから使用可能）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、Firewall Management Center はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ステータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for Registration）」の状態に留まります。この場合、[照合（Reconcile）] をクリックして再登録を強制します。
- [システムステータス（System status）] > [タスク（Tasks）]：Firewall Management Center にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

クラスタ メンバーの置換

既存クラスタ内のクラスタ メンバーを置き換えることができます。Firewall Management Center は交換ユニットを自動検出します。ただし、Firewall Management Center 内の古いクラスタ メンバーは手動で削除する必要があります。また、この手順は再初期化したユニットにも適用されます。その場合は、ハードウェアが同じでも新しいメンバーとして表示されます。

始める前に

- インターフェイス設定が他のシャーシに関する交換ユニットと同じであることを確認します。

手順

ステップ 1 新しいシャーシの場合、可能であれば、FXOS内の古いシャーシの設定をバックアップして復元します。

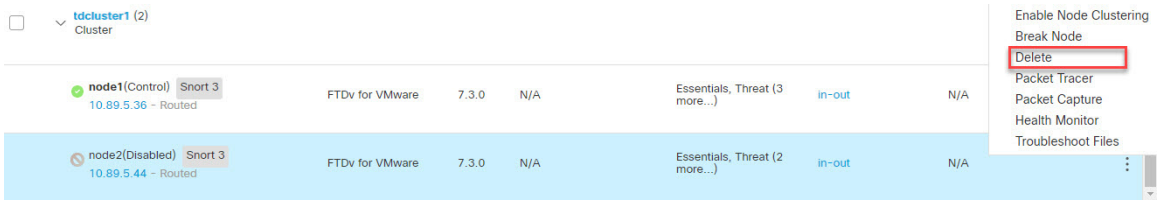
Firepower 9300 のモジュールを交換する場合は、次の手順を実行する必要はありません。

古いシャーシのバックアップ FXOS 設定がない場合は、最初に新規クラスタ メンバーの追加（590 ページ）の手順を実行します。

以下のすべての手順については、FXOS コンフィギュレーション ガイド[英語]を参照してください。

a) 設定のエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォームの構成時の設定を含んでいる XML ファイルをエクスポートします。
b) 交換用シャーシに設定ファイルをインポートします。
c) ライセンス契約に同意します。
d) 必要に応じて、論理デバイスのアプリケーションインスタンスバージョンをアップグレードして、残りのクラスタと一致させます。

ステップ 2 古いユニットの Firewall Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [その他（More）] (⋮) > **[削除（Delete）]** を選択し。



ステップ 3 ユニットを削除することを確認します。

ユニットがクラスタから削除され、Firewall Management Center デバイス リストからも削除されます。

ステップ 4 新しいクラスタ メンバーまたは再初期化したクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニターするには、次のように表示します。

- [クラスタステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** [その他（More）] (⋮) アイコンまたは **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** ページ > [全般（General）] 領域 > [クラスタステータスの表示（View Cluster Status）]> [クラスタのライブステータス（Cluster Live Status）] リンク）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、Firewall Management Center はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ステータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for

Registration）」の状態に留まります。この場合、[照合（Reconcile）][すべて（All）]をクリックして再登録を強制します。

- [システム（System）]（⚙）>[タスク（Tasks）]：Firewall Management Center にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）]>[デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

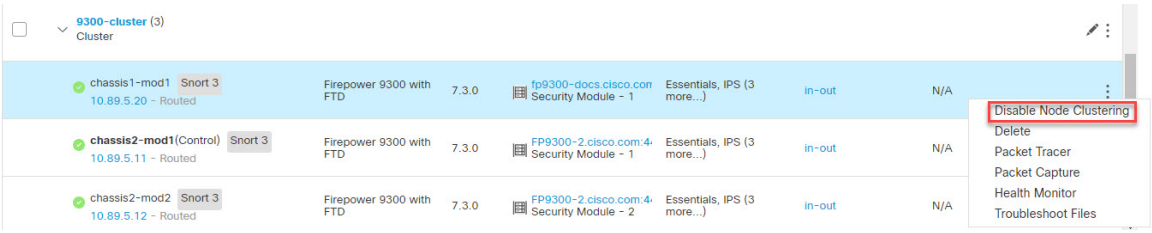
メンバーの非アクティブ化

ユニットの削除に備えて、またはメンテナンスのために一時的にメンバーを非アクティブ化する場合があります。この手順は、メンバーを一時的に非アクティブ化するためのものです。ユニットは引き続き Firewall Management Center デバイスリストに表示されます。

（注） ユニットが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールを使用する必要があります。

手順

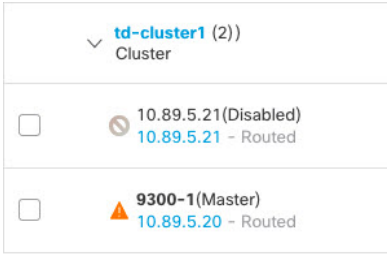
ステップ 1 非アクティブ化するユニットに対し、**[デバイス（Devices）]>[デバイス管理（Device Management）]**[その他（More）]（⋮）>[クラスタリングを無効にする（Disable Clustering）]を選択します。



[クラスタステータス（Cluster Status）]ダイアログボックスから、ユニットを非アクティブ化することもできます（**[デバイス（Devices）]>[デバイス管理（Device Management）]**[その他（More）]（⋮）>[クラスタのライブステータス（Cluster Live Status）]）。

ステップ 2 ユニットのクラスタリングを無効にすることを確認します。

ユニットは、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**リストの名前の横に [（無効（Disabled））] と表示されます。



ステップ 3 クラスタリングを再び有効にするには、クラスタへの再参加 （594 ページ）を参照してください。

クラスタへの再参加

障害が発生したインターフェイスなど、ユニットがクラスタから削除された場合または手動でクラスタリングを無効にした場合、クラスタに手動で再参加させる必要があります。クラスタへの再参加を試行する前に、障害が解決されていることを確認します。クラスタからユニットが削除される理由の詳細については、クラスタへの再参加 （615 ページ）を参照してください。

手順

ステップ 1 再アクティブ化するユニットに対し、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** [その他（More）] (⋮) > [クラスタリングを有効にする（Enable Clustering）] を選択します。

[クラスタステータス（Cluster Status）] ダイアログボックスから、ユニットを再アクティブ化することもできます（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [その他（More）] (⋮) > [クラスタのライブステータス（Cluster Live Status）]）。

ステップ 2 ユニットでクラスタリングを有効にすることを確認します。

データノードの削除（登録解除）

クラスタノードを完全に削除する必要がある場合（たとえば、Firepower 9300 でモジュールを削除する場合、またはシャーシを削除する場合）は、Firewall Management Center からメンバーを登録解除する必要があります。

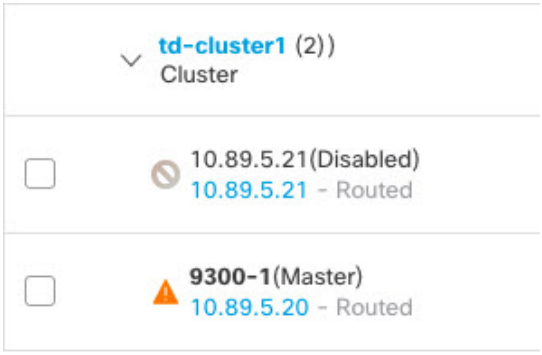
ノードが正常なクラスタの一部である場合、またはノードを一時的に無効にするだけの場合は、ノードを登録解除しないでください。FXOS のクラスタから完全に削除するには、FXOS：クラスタノードの削除（588 ページ）を参照してください。Firewall Management Center から登録解除しても、まだクラスタの一部である場合、トラフィックを引き続き通過させ、制御ノード（Firewall Management Center が管理できない制御ノード）になる可能性もあります。

始める前に

ユニットを手動で非アクティブ化するには、メンバーの非アクティブ化（593 ページ）を参照してください。ノードを登録解除する前に、手動で、またはヘルス障害により、ノードが非アクティブになっている必要があります。

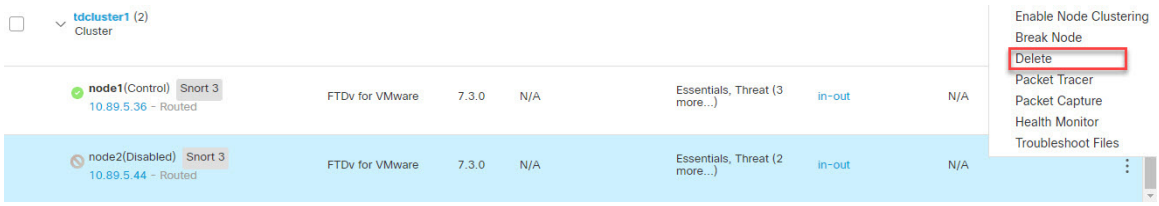
手順

ステップ 1 ノードが Firewall Management Center から登録解除できる状態であることを確認します。[デバイス（Devices）]>[デバイス管理（Device Management）] で、ユニットに[（無効（Disabled））] と表示されていることを確認します。



また、各ノードのステータスは、[その他（More）] から [クラスタステータス（Cluster Status）] ダイアログボックスで確認できます。ステータスが古い場合は、[クラスタステータス（Cluster Status）] ダイアログボックスの [照合（Reconcile）] をクリックして強制的に更新します。

ステップ 2 削除するデータユニットの Firewall Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [その他（More）] > **[削除（Delete）]** を選択します。



ステップ 3 ノードを削除することを確認します。

ノードがクラスタから削除され、Firewall Management Center デバイス リストからも削除されます。

制御ユニットの変更

⚠

注意 制御ユニットを変更する最良の方法は、制御ユニットでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ユニットにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。中央集中型機能については、制御ユニット変更を強制するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

制御ユニットを変更するには、次の手順を実行します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [その他（More）] ⋮ > [クラスタのライブステータス（Cluster Live Status）] を選択して [クラスタステータス（Cluster Status）] ダイアログボックスを開きます。

[クラスタステータス（Cluster Status）] ダイアログボックスは、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]**ページ > [全般（General）] 領域 > [クラスタのライブステータス（Cluster Live Status）] リンクからも開くことができます。

ステップ 2 制御ユニットにしたいユニットについて、[その他（More）] ⋮ >[ロールを制御に変更（Change Role to Control）] を選択します。

ステップ 3 ロールの変更を確認するように求められます。チェックボックスをオンにして [OK] をクリックします。

クラスタ メンバーの照合

クラスタ メンバーの登録に失敗した場合、シャーシから Secure Firewall Management Center に対してクラスタ メンバーシップを照合することができます。たとえば、Firewall Management Center が特定のプロセスで占領されているか、またはネットワークに問題がある場合、データ ユニットの登録に失敗することがあります。

手順

ステップ 1 クラスタの **[Devices]** > **[Device Management]** > [その他（More）] (⋮) を選択し、次に [Cluster Live Status] を選択して [Cluster Status] ダイアログボックスを開きます。

[Cluster Status] ダイアログボックスは、**[Devices]** > **[Device Management]** > **[Cluster]** ページ > [General] 領域 > [Cluster Live Status] リンクからも開くことができます。

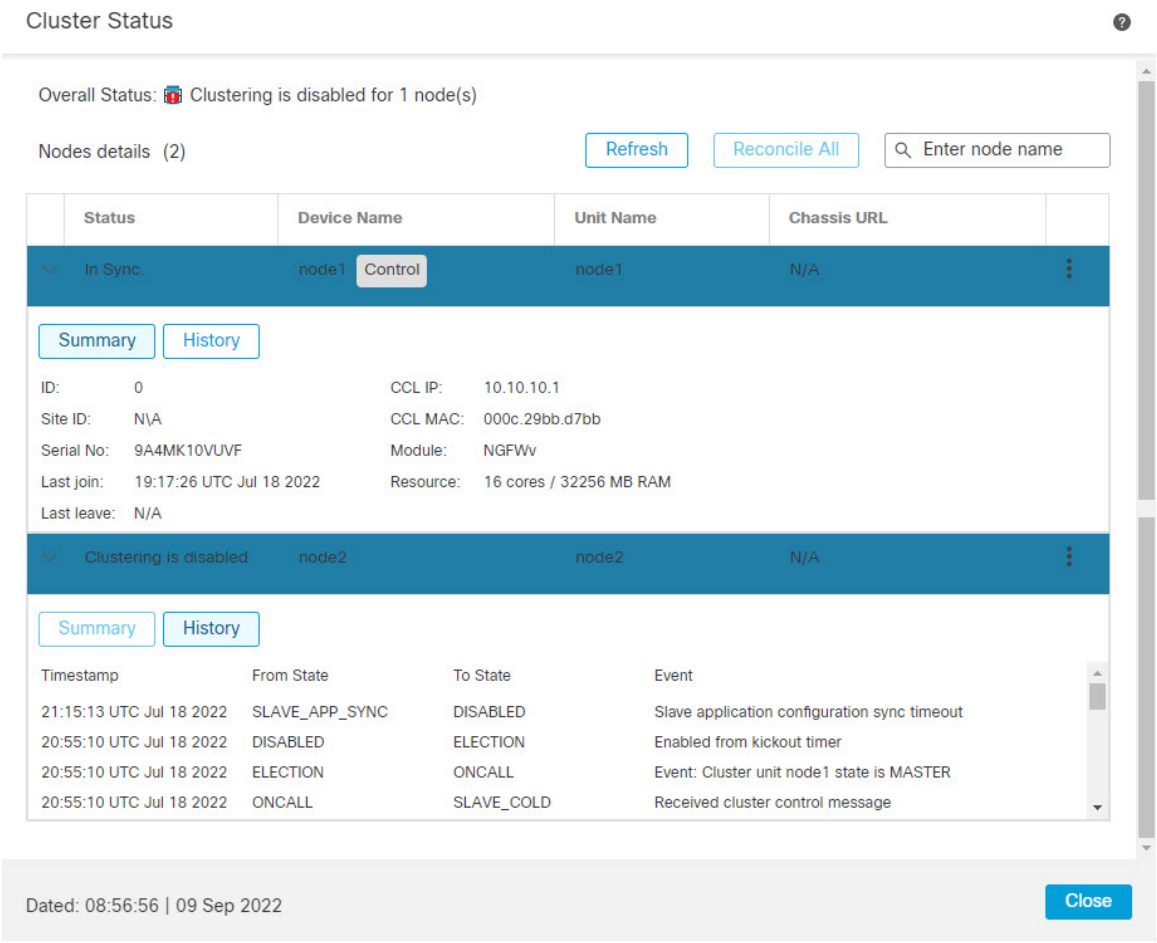
ステップ 2 [**Reconcile All**] をクリックします。

クラスタ ステータスの詳細については、Firewall Management Center：クラスタのモニタリング（597 ページ）を参照してください。

Firewall Management Center：クラスタのモニタリング

クラスタのモニタリングは、Secure Firewall Management Center および Firewall Threat Defense CLI で実行できます。

- [Cluster Status] ダイアログボックスには、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [その他（More）] (⋮) アイコンから、または **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** ページ > [全般（General）] 領域 > [クラスタステータスの表示（View cluster status）] > [クラスタのライブステータス（Cluster Live Status）] リンクからアクセスできます。



コントロールユニットには、そのロールを示すグラフィックインジケータがあります。

クラスタメンバーステータスには、次の状態が含まれます。

- 同期中（In Sync）：装置は Firewall Management Center に登録されています。
- Pending Registration：装置はクラスタの一部ですが、まだ Firewall Management Center に登録されていません。装置が登録に失敗した場合、[**Reconcile All**] をクリックして登録を再試行することができます。
- Clustering is disabled：装置は Firewall Management Center に登録されていますが、クラスタの非アクティブなメンバーです。クラスタリング設定は、後で再有効化する予定がある場合は変更せずに維持できます。または、装置をクラスタから削除することも可能です。
- クラスタに参加中（Joining cluster）：装置がシャーシ上でクラスタに参加していますが、参加は完了していません。参加後に Firewall Management Center に登録されます。

装置ごとに、[Summary] または [History] で、それぞれ概要と履歴を表示できます。

[その他（More）] (⋮) メニューから、装置ごとに次のステータス変更を実行できます。

- クラスタリングを無効にする
- クラスタリングを有効にする
- ロールを Control に変更する

- [システム（System）]（⚙）> [Tasks] ページ。

  [Tasks] ページには、各装置が登録されるごとに、クラスタ登録タスクの最新の状況が表示されます。

- **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > *cluster_name*。

  デバイスの一覧表示ページでクラスタを展開すると、制御装置（IPアドレスの横にその役割が示されている）を含め、すべてのメンバ装置を表示できます。登録中の装置には、ロード中のアイコンが表示されます。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

クラスタ ヘルス モニター ダッシュボード

クラスタのヘルスモニター

Firewall Threat Defense がクラスタの制御ノードである場合、Firewall Management Center はデバイス メトリック データ コレクタからさまざまなメトリックを定期的に収集します。クラスタの ヘルスモニターは、次のコンポーネントで構成されています。

- 概要ダッシュボード：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。
  - トポロジセクションには、クラスタのライブステータス、個々の脅威防御の状態、脅威防御ノードのタイプ（制御ノードまたはデータノード）、およびデバイスの状態が表示されます。デバイスの状態は、[無効（Disabled）]（デバイスがクラスタを離れたとき）、[初期状態で追加（Added out of box）]（パブリッククラウドクラスタでFirewall Management Center に属していない追加ノード）、または [標準（Normal）]（ノードの理想的な状態）のいずれかです。
  - クラスタの統計セクションには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するクラスタの現在のメトリックが表示されます。

（注） CPU とメモリのメトリックは、データプレーンと Snort の使用量の個々の平均を示します。

- メトリックチャート、つまり、CPU使用率、メモリ使用率、スループット、および接続数は、指定された期間におけるクラスタの統計を図表で示します。

- 負荷分散ダッシュボード：2 つのウィジェットでクラスタノード全体の負荷分散を表示します。
  - 分布ウィジェットには、クラスタノード全体の時間範囲における平均パケットおよび接続分布が表示されます。このデータは、ノードによって負荷がどのように分散されているかを示します。このウィジェットを使用すると、負荷分散の異常を簡単に特定して修正できます。
  - ノード統計ウィジェットには、ノードレベルのメトリックが表形式で表示されます。クラスタノード全体の CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するメトリックデータが表示されます。このテーブルビューでは、データを関連付けて、不一致を簡単に特定できます。
- メンバー パフォーマンス ダッシュボード：クラスタノードの現在のメトリックを表示します。セレクタを使用してノードをフィルタリングし、特定ノードの詳細を表示できます。メトリックデータには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数が含まれます。
- CCL ダッシュボード：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。
- トラブルシューティングとリンク： 頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- 時間範囲：さまざまなクラスタ メトリック ダッシュボードやウィジェットに表示される情報を制限するための調整可能な時間枠。
- カスタムダッシュボード：クラスタ全体のメトリックとノードレベルのメトリックの両方に関するデータを表示します。ただし、ノードの選択は脅威防御メトリックにのみ適用され、ノードが属するクラスタ全体には適用されません。

クラスタ ヘルスの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザーである必要があります。

クラスタヘルスモニターは、クラスタとそのノードのヘルスステータスの詳細なビューを提供します。このクラスタヘルスモニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

- Firewall Management Center の 1 つ以上のデバイスからクラスタを作成しているかを確認します。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択します。

[モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、ノード固有のヘルスモニターにアクセスします。

ステップ 2 デバイスリストで [展開（Expand）]（>） と [折りたたみ（Collapse）]（⌄） をクリックして、管理対象のクラスタデバイスのリストを展開または折りたたみます。

ステップ 3 クラスタのヘルス統計を表示するには、クラスタ名をクリックします。デフォルトでは、クラスタモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- [概要（Overview）]：他の事前定義されたダッシュボードからの主要なメトリックを表示します。ノード、CPU、メモリ、入力レート、出力レート、接続統計情報、NAT 変換情報などが含まれます。
- [負荷分散（Load Distribution）]：クラスタノード間のトラフィックとパケットの分散。
- [メンバーパフォーマンス（Member Performance）]：CPU 使用率、メモリ使用率、入力スループット、出力スループット、アクティブな接続、および NAT 変換に関するノードレベルの統計情報。
- [CCL]：インターフェイスのステータスおよび集約トラフィックの統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているクラスタメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で 1 時間前（デフォルト）から、最長では 2 週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を 5 分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの展開アイコンをクリックします。

展開アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されます。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 （ノード固有のヘルスモニターの場合）ページ上部のデバイス名の右側にあるアラート通知で、ノードの正常性アラートを確認します。

正常性アラートにポインタを合わせると、ノードの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 7 （ノード固有のヘルスモニターの場合）デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- [Snort]：Snort プロセスに関連する統計情報。
- [ASP ドロップ（ASP drops）]：さまざまな理由でドロップされたパケットに関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 正常性モニターの右上隅にあるプラス記号[新しいダッシュボードの追加（Add New Dashboard）]（＋）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタムダッシュボードを作成します。

クラスタ全体のダッシュボードの場合は、クラスタのメトリックグループを選択してから、メトリックを選択します。

クラスタメトリック

クラスタのヘルスモニターは、クラスタとそのノードに関連する統計情報と、負荷分散、パフォーマンス、および CCL トラフィックの統計データの集約結果を追跡します。

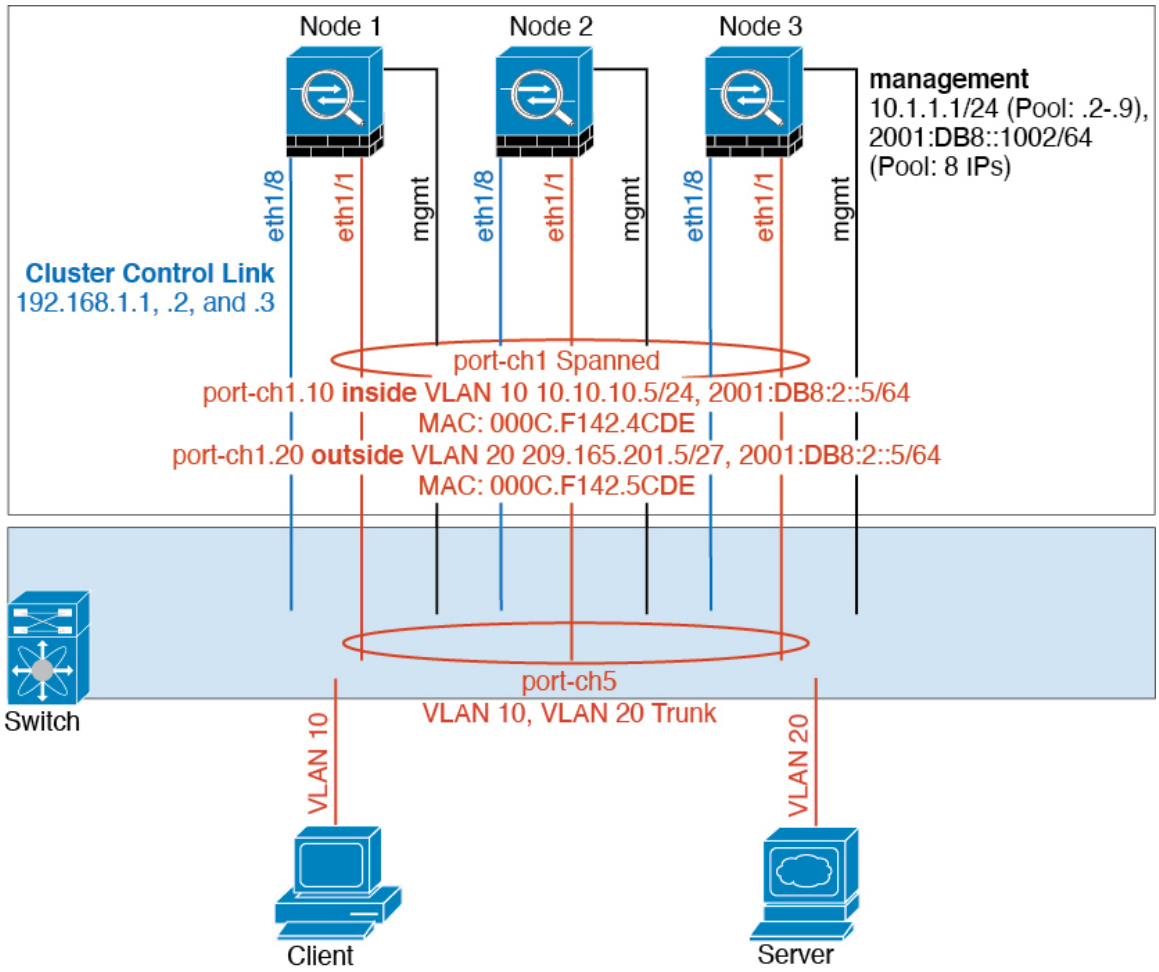
表 *42 :* クラスタメトリック

メトリック	説明	フォーマット（Format）
CPU	クラスタノード上の CPU メトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
メモリ	クラスタノード上のメモリメトリックの平均（データプレーンと snort についてそれぞれ表示）。	パーセンテージ
データスループット	クラスタの着信および発信データトラフィックの統計。	バイト
CCL スループット	クラスタの着信および発信 CCL トラフィックの統計。	バイト
接続	クラスタ内のアクティブな接続数。	番号
NAT 変換数	クラスタの NAT 変換数。	番号
分布	1 秒ごとのクラスタ内の接続分布数。	番号
パケット	クラスタ内の1秒ごとのパケット配信の件数。	番号

クラスタリングの例

これらの例には、一般的な導入が含まれます。

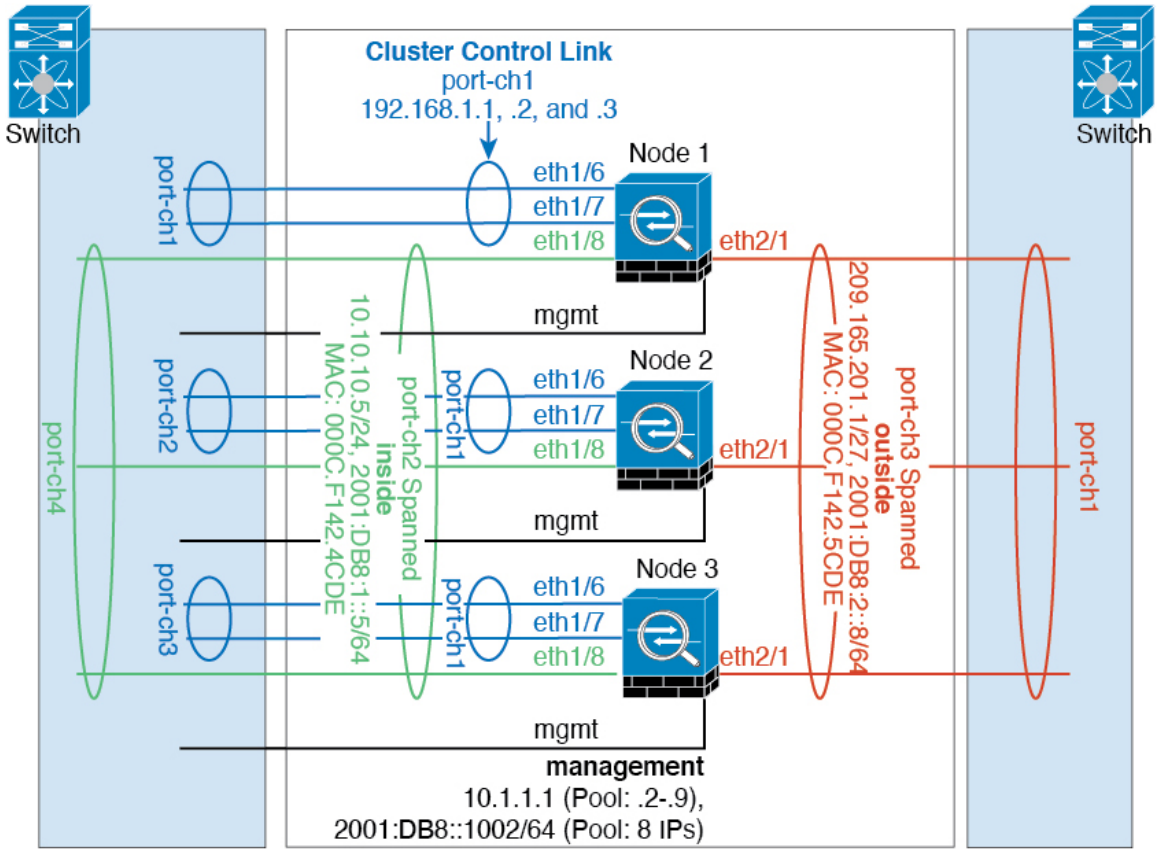
スティック上のファイアウォール



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータ リンクがグループ化されて 1 つの EtherChannel となります。が使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

Firewall Threat Defense の機能とクラスタリング

Firewall Threat Defenseの一部の機能はクラスタリングではサポートされず、一部は制御ユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

（注） クラスタリングでもサポートされていないFlexConfig機能（WCCPインスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーション ガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- リモート アクセス VPN（SSL VPN および IPsec VPN）
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- 仮想トンネルインターフェイス（VTI）
- 高可用性
- 統合ルーティングおよびブリッジング
- Firewall Management Center UCAPL/CC モード
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

（注） クラスタリングでも一元化されているFlexConfig機能（RADIUSインスペクションなど）を表示するには、ASA の一般的な操作のコンフィギュレーションガイドを参照してください。FlexConfig では、Firewall Management Center GUI にはない多くの ASA 機能を設定できます。FlexConfig ポリシー （2687 ページ）を参照してください。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- スタティック ルート モニタリング
- サイト間 VPN
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ダイナミック ルーティング

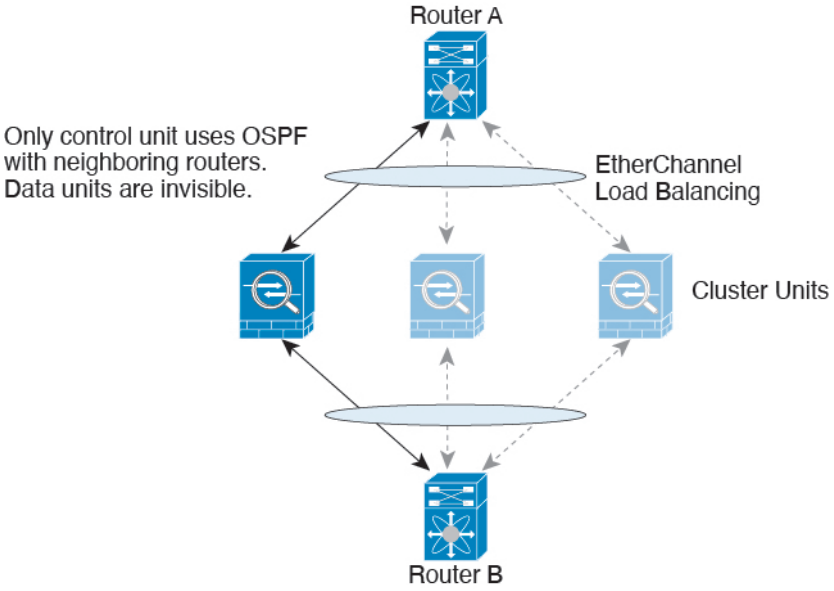
接続設定

接続制限は、クラスタ全体に適用されます。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

ダイナミック ルーティングおよびクラスタリング

ルーティングプロセスは制御ユニット上だけで実行されます。ルートは制御ユニットを介して学習され、セカンダリに複製されます。ルーティングパケットがデータユニットに到着した場合は、制御ユニットにリダイレクトされます。

図 *199* : ダイナミック ルーティング



データユニットが制御ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、制御ユニットからデータユニットに同期されません。制御ユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

マルチキャスト ルーティングとクラスタリング

ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを処理します。接続が確立された後は、各データユニットがマルチキャスト データ パケットを転送できます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の Firewall Threat Defense に送信されることがあります。ロードバランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない Firewall Threat Defense に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
  - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。
- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。

- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

SNMP とクラスタリング

SNMP エージェントは、個々の Firewall Threat Defense を、その [診断（Diagnostic）] 診断インターフェイスのローカルIPアドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザは新しいノードに複製されません。SNMPv3ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

syslog とクラスタリング

- クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。

TLS/SSL 接続とクラスタリング

TLS/SSL接続の復号状態は同期されず、接続オーナーに障害が発生すると、復号された接続がリセットされます。新しいユニットへの新しい接続を確立する必要があります。復号されていない接続（復号しないルールに一致）は影響を受けず、正しく複製されます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ユニットのみが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN機能を使用できるのは制御ユニットだけであり、クラスタの高可用性機能は活用されません。制御ユニットで障害が発生した場合は、すべての既存のVPN接続が失われ、VPNユーザーにとってはサービスの中断となります。新しい制御ユニットが選定されたときに、VPN接続を再確立する必要があります。

VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的に制御ユニットに転送されます。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80% になります。

たとえば、TCP スループットについては、3 つの SM-40 モジュールを備えた Firepower 9300 が処理できる実際のファイアウォール トラフィックは、単独動作時は約 135 Gbps となります。2 シャーシの場合、最大スループットの合計は 270 Gbps（2 シャーシ X 135 Gbps）の約 80 %、つまり 216 Gbps です。

制御ユニットの選定

クラスタのメンバーは、クラスタ制御リンクを介して通信して制御ユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットが制御ユニットになります。

（注） 最高のプライオリティを持つユニットが複数ある場合は、クラスタユニット名、次にシリアル番号を使用して制御ユニットが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的に制御ユニットになることはありません。既存の制御ユニットは常に制御ユニットのままです。ただし、制御ユニットが応答を停止すると、その時点で新しい制御ユニットが選定されます。
5. 「スプリットブレイン」シナリオで一時的に複数の制御ユニットが存在する場合、優先順位が最も高いユニットが制御ユニットの役割を保持し、他のユニットはデータユニットの役割に戻ります。

（注） 特定のユニットを手動で強制的に制御ユニットにすることができます。中央集中型機能については、制御ユニット変更を強制するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

シャーシ アプリケーションのモニターリング

シャーシ アプリケーションのヘルス モニターリングは常に有効になっています。Firepower 4100/9300 シャーシ スーパバイザは、Firewall Threat Defense アプリケーションを定期的に確認します（毎秒）。Firewall Threat Defense デバイス が作動中で、Firepower 4100/9300 シャーシ スーパバイザと 3 秒間通信できなければ、Firewall Threat Defense デバイス は syslog メッセージを生成して、クラスタを離れます。

Firepower 4100/9300 シャーシ スーパバイザが 45 秒後にアプリケーションと通信できなければ、Firewall Threat Defense デバイス をリロードします。Firewall Threat Defense デバイス がスーパバイザと通信できなければ、自身をクラスタから削除します。

装置のヘルス モニターリング

各ユニットは、クラスタ制御リンクを介してブロードキャストキープアライブハートビートパケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからキープアライブハートビートパケット、またはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション 2 のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。詳細については、制御ユニットの選定 （612 ページ）を参照してください。

インターフェイス モニタリング

各ノードは、使用中のすべてのハードウェアインターフェイスのリンクステータスを監視し、ステータスの変更を制御ノードに報告します。複数のシャーシにわたるクラスタリングの場合、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用しま

す。各シャーシはリンク ステータスとcLACPプロトコル メッセージをモニターしてEtherChannelでポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合にはFirewall Threat Defense アプリケーションに通知します。ヘルスモニターリングを有効にすると、デフォルトではすべての物理インターフェイスがモニターされます（EtherChannelインターフェイスのメイン EtherChannel を含む）。アップ状態の名前付きインターフェイスのみモニターできます。たとえば、名前付きEtherChannelがクラスタから削除されるまでは、EtherChannelのすべてのメンバー ポートは失敗しなければなりません。ヘルス チェックは、インターフェイスごとに、モニターリングをオプションで無効にすることができます。

特定のノードで監視対象のインターフェースに障害が発生し、その他のノードでそのインターフェイスがアクティブになっている場合、そのノードはクラスタから削除されます。Firewall Threat Defense デバイス によってノードがクラスタから削除されるまでの時間は、そのノードが確立済みのメンバーであるかクラスタに参加しようとしているかによって異なります。Firewall Threat Defenseデバイスは、ノードがクラスタに参加する最初の90秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、Firewall Threat Defenseデバイスはクラスタから削除されません。確立済みのメンバーの場合は、500ミリ秒後にノードが削除されます。

複数のシャーシにわたるクラスタリングの場合、クラスタからEtherChannelを追加または削除すると、各シャーシに変更を加えられるように、インターフェイス ヘルス モニタリングは95秒間中断されます。

デコレータ アプリケーションのモニタリング

インターフェイスにRadware DefenseProアプリケーションなどのデコレータ アプリケーションをインストールした場合、ユニットがクラスタ内にとどまるにはFirewall Threat Defenseデバイス、デコレータ アプリケーションの両方が動作している必要があります。両方のアプリケーションが動作状態になるまで、ユニットはクラスタに参加しません。いったんクラスタに参加すると、ユニットはデコレータ アプリケーションが正しく動作しているか3秒ごとにモニターします。デコレータ アプリケーションがダウンすると、ユニットはクラスタから削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、Firewall Threat Defense は自動的にクラスタへの再参加を試みます。

（注） Firewall Threat Defenseが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理/診断インターフェイスのみがトラフィックを送受信できます。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- 最初に参加するときに障害が発生したクラスタ制御リンク：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：FTDは、無限に5分ごとに自動的に再参加を試みます。
- データ インターフェイスの障害：Firewall Threat Defense は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、Firewall Threat Defense アプリケーションはクラスタリングを無効にします。データ インターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ノードは再起動するとクラスタに再参加します。Firewall Threat Defense アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。
- 障害が発生した設定の展開：FMC から新しい設定を展開し、展開が一部のクラスタメンバーでは失敗したものの、他のメンバーでは成功した場合、失敗したノードはクラスタから削除されます。クラスタリングを再度有効にして手動でクラスタに再参加する必要があります。制御ノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。すべてのデータノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。
- シャーシアプリケーション通信の障害：Firewall Threat Defense アプリケーションはシャーシアプリケーションの状態が回復したことを検出すると、自動的にクラスタへの再参加を試みます。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *43 :* クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システムアップタイムをトラッキングします。
ARP Table	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	Yes	—
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—

クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- バックアップオーナー：オーナーから受信したTCP/UDP ステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。
- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づい

てディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

ICMP/ICMPv6 ハッシュの詳細：

- エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
- 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
- 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定

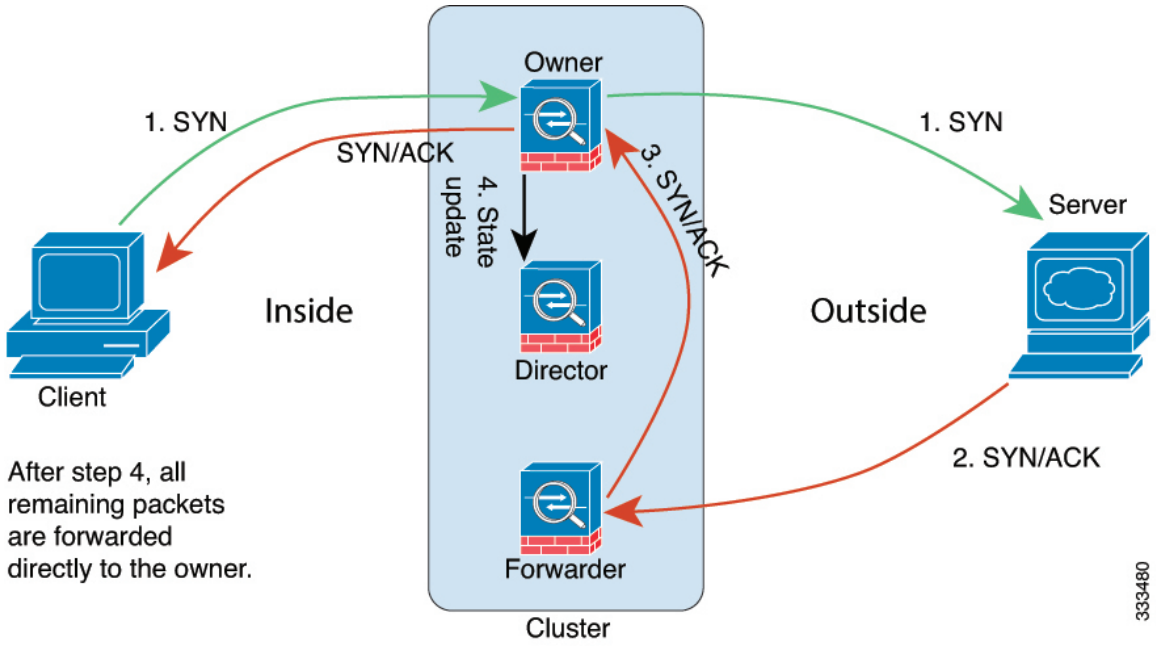
できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。



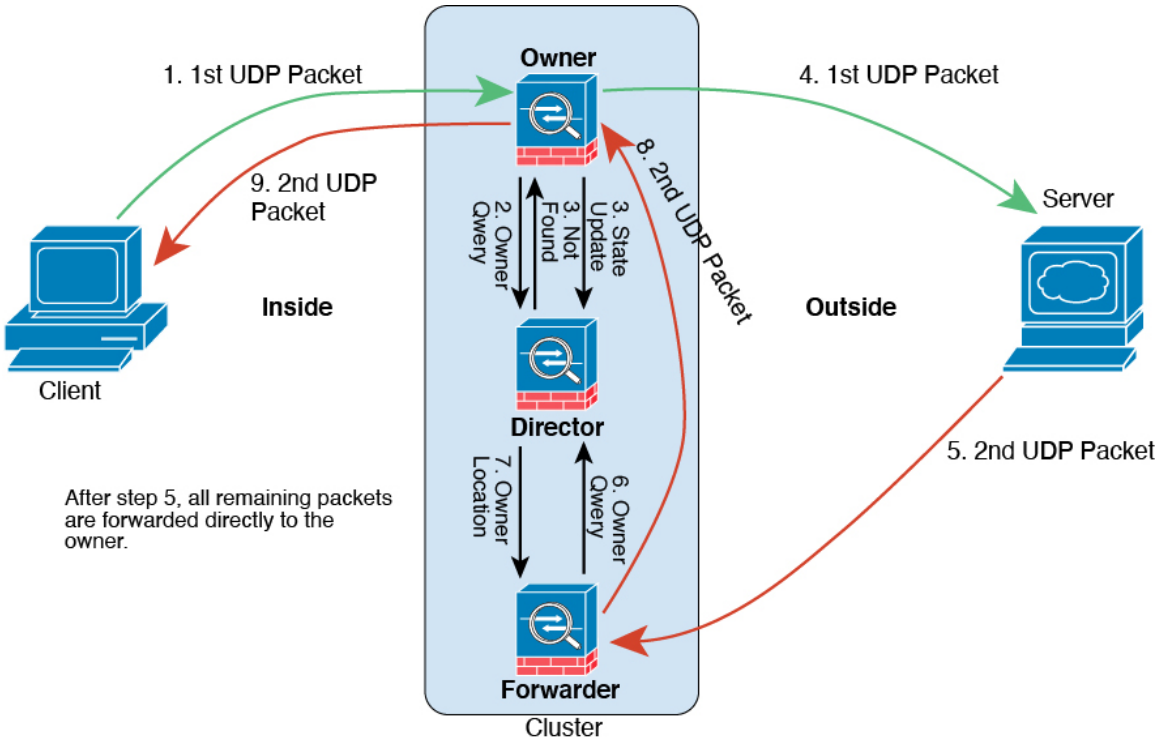
1. SYN パケットがクライアントから発信され、Firewall Threat Defense の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firewall Threat Defense（ロード バランシング方法に基づく）に配信されます。この Firewall Threat Defense はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。

5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様にTCPステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

1. 図 *200 : ICMP* および *UDP* データ フロー



UDP パケットがクライアントから発信され、1 つの Firewall Threat Defense（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。

4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

クラスタリングの履歴

表 *44 :*

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタのヘルスモニターの設定。	7.3.0	いずれか	クラスタのヘルスモニター設定を編集できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **クラスタ（Cluster）** > **[クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）]** （注） 以前に FlexConfig を使用してこれらの設定を行った場合は、展開前に必ず FlexConfig の設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。
クラスタ ヘルス モニターダッシュボード。	7.3.0	いずれか	クラスタのヘルス モニター ダッシュボードでクラスタの状態を表示できるようになりました。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]**
16 ノードクラスタのサポート。	7.2.0	7.2.0	Firepower 4100/9300 で 16 ノードクラスタを構成できるようになりました。これまでは最大で 6 ユニットでした。 新規/変更された画面：なし。 サポートされるプラットフォーム：Firepower 4100/9300

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ファイアウォールの変更に対するクラスタの展開がより迅速に完了します。	7.1.0	7.1.0	ファイアウォールの変更に対するクラスタの展開がより迅速に完了するようになりました。 新規/変更された画面：なし。
クラスタリング用の PAT ポートブロック割り当ての改善。	7.0.0	7.0.0	PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するには、FlexConfig を使用して **cluster-member-limit** コマンドを実行して、予定しているクラスタ内の最大ノード数を設定します。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。 新規/変更されたコマンド：**cluster-member-limit**（FlexConfig）、**show nat pool cluster** [**summary**]、**show nat pool ip detail**
Snort の変更に対するクラスタの展開がより迅速に完了し、イベントが発生するとより迅速に失敗する。	6.7.0	6.7.0	Snort の変更に対するクラスタの展開がより迅速に完了するようになりました。また、Firewall Management Center 展開が失敗する原因となるイベントがクラスタにある場合、エラーがより迅速に発生するようになりました。 新規/変更された画面：なし。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタ管理の改善。	6.7.0	6.7.0	Firewall Management Center では、以前は CLI を使用することでしか実現できなかった、次のようなクラスタ管理機能が改善されました。 • クラスタユニットの有効化および無効化 • [デバイス管理（Device Management）] ページからクラスタのステータスを表示（ユニットごとの履歴とサマリーを含む） • ロールの制御ユニットへの変更 新規/変更された画面： • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[詳細（More）]**メニュー • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[全般（General）]**エリア > [クラスタのライブステータス（Cluster Live Status）] リンク > [クラスタステータス（Cluster Status）] サポートされるプラットフォーム：Firepower 4100/9300

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
マルチインスタンス クラスタリング。	6.6.0	6.6.0	コンテナインスタンスを使用してクラスタを作成できるようになりました。Firepower 9300 では、クラスタ内の各モジュールに 1 つのコンテナインスタンスを含める必要があります。セキュリティエンジン/モジュールごとに複数のコンテナインスタンスをクラスタに追加することはできません。クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。 新規/変更された FXOS コマンド： **set port-type cluster** 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [クラスタの追加（Add Cluster）]** • **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）]** ドロップダウン メニュー **[サブインターフェイス（Subinterface）] [タイプ（Type）]** フィールド サポートされるプラットフォーム：Firepower 4100/9300 上の Firewall Threat Defense
データユニットとの設定の並列同期。	6.6.0	6.6.0	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更された画面：なし。
クラスタへの参加の失敗や削除のメッセージを **show cluster history** に追加。	6.6.0	6.6.0	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 **show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history** 新規/変更された画面：なし。

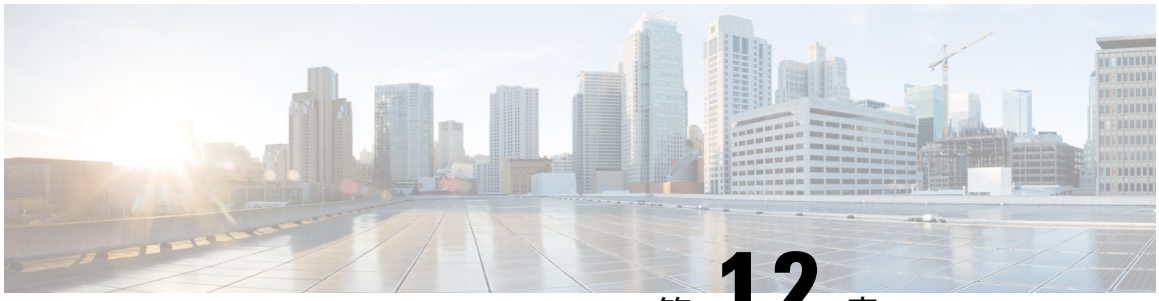
機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	6.5.0	6.5.0	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新しい/変更されたコマンド：**show conn**（出力のみ） サポートされるプラットフォーム：Firepower 4100/9300 上の Firewall Threat Defense
クラスタの追加が容易に。	6.3.0	6.3.0	Firewall Management Center にクラスタの任意のユニットを追加できるようになりました。他のクラスタユニットは自動的に検出されます。以前は、各クラスタユニットを個別のデバイスとして追加し、グループ化してクラスタにする必要がありました。クラスタユニットの追加も自動で実行されるようになりました。ユニットは手動で削除する必要があることに注意してください。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）]**ドロップダウン メニュー **[デバイス（Devices）] > [デバイスの追加（Add Device）]**ダイアログボックス **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブ **[全般（General）]** エリア **[クラスタの登録ステータス（Cluster Registration Status）] [現在のクラスタの概要（Current Cluster Summary）]** リンク **[クラスタ ステータス（Cluster Status）]** ダイアログ ボックス サポートされるプラットフォーム：Firepower 4100/9300 上の Firewall Threat Defense
中央集中型機能としてのクラスタリングによるサイト間 VPN のサポート。	6.2.3.3	6.2.3.3	クラスタリングを使用してサイト間 VPN を設定できるようになりました。サイト間 VPN は、中央集中型機能です。制御ユニットのみが VPN 接続をサポートします。 サポートされるプラットフォーム：Firepower 4100/9300 上の Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
内部障害発生後に自動的にクラスタに再参加します。	6.2.3	6.2.3	以前は、多くの内部エラー状態によって、クラスタユニットがクラスタから削除され、ユーザーが問題を解決した後で、手動でクラスタに再参加する必要がありました。現在は、ユニットが自動的に、5 分、10 分、20 分の間隔でクラスタに再参加しようとします。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。 新しい/変更されたコマンド：**show cluster info auto-join** 変更された画面はありません。 サポートされるプラットフォーム：Firepower 4100/9300 上の Firewall Threat Defense
6 モジュールの複数シャーシのクラスタリング、Firepower 4100 をサポート。	6.2.0	6.2.0	FXOS 2.1.1 では、Firepower 9300 および 4100 の複数のシャーシでクラスタリングを有効にできるようになりました。Firepower 9300 の場合、最大 6 つのモジュールを含めることができます。たとえば、6 つのシャーシで 1 つのモジュールを使用したり、3 つのシャーシで 2 つのモジュールを使用したり、最大 6 つのモジュールを組み合わせたりできます。Firepower 4100 の場合、最大 6 つのシャーシを含めることができます。 （注） サイト間クラスタリングもサポートされていません。しかし、サイト固有の MAC および IP アドレス、ディレクタのローカリゼーション、サイトの冗長性、クラスタフローモビリティなどの冗長性と安定性を向上させるためのカスタマイズは、FlexConfig 機能を使用した場合にのみ設定できます。 変更された画面はありません。 サポートされるプラットフォーム：Firepower 4100/9300 上の Firewall Threat Defense
1 つの Firepower 9300 シャーシを使用した複数モジュールでのクラスタリング。	6.0.1	6.0.1	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [クラスタの追加（Add Cluster）]** **[Devices] > [Device Management] > [Cluster]** サポートされるプラットフォーム：Firepower 9300 上の Firewall Threat Defense

第 III 部

インターフェイスとデバイスの設定

- インターフェースの概要 （629 ページ）
- 通常のファイアウォール インターフェイス （673 ページ）
- インラインセットとパッシブインターフェイス （763 ページ）
- DHCP および DDNS （781 ページ）
- Firepower 1000/2100 の SNMP （803 ページ）
- QoS （809 ページ）
- プラットフォーム設定 （823 ページ）
- ネットワーク アドレス変換 （901 ページ）
- Cisco ISA 3000 のアラーム （1053 ページ）



第 12 章

インターフェースの概要

Firewall Threat Defense デバイスには、種々のモードで設定できるデータインターフェイス、および管理/診断インターフェイスが組み込まれています。

- 管理/診断インターフェイス （629 ページ）
- インターフェイス モードとタイプ （630 ページ）
- セキュリティ ゾーンとインターフェイス グループ （631 ページ）
- Auto-MDI/MDIX 機能 （633 ページ）
- 冗長インターフェイス（廃止） （633 ページ）
- インターフェイスのデフォルト設定 （633 ページ）
- セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成 （634 ページ）
- 物理インターフェイスの有効化およびイーサネット設定の構成 （635 ページ）
- EtherChannel インターフェイスの設定 （638 ページ）
- Firewall Management Center とのインターフェイスの変更の同期 （648 ページ）
- Cisco Secure Firewall 3100 のネットワークモジュールの管理 （652 ページ）
- インターフェイスの履歴 （669 ページ）

管理/診断インターフェイス

物理管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有されています。

管理インターフェイス

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Firewall Management Centerにデバイスを設定し、登録するために使用されます。また、固有の IP アドレスとスタティック ルーティングを使用します。管理インターフェイスを設定するには、CLI で **configure network** コマンドを使用します。管理インターフェイスを Firewall Management Center に追加した後にその IP アドレスを CLI で変更した場合、Secure Firewall Management Center での IP アドレスを **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）] > [管理（Management）]** エリアで一致させることができます。

または、管理インターフェイスの代わりにデータインターフェイスを使用して Firewall Threat Defense を管理できます。

診断インターフェイス（レガシー）

診断論理インターフェイスは残りのデータインターフェイスとともに、**[Devices]** > **[Device Management]** > **[Interfaces]** 画面で構成できます。診断インターフェイスの使用はオプションです（シナリオについては、ルーテッド モードおよびトランスペアレント モードの展開を参照）。診断インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。これはSSHをサポートしません。データインターフェイスまたは管理インターフェイスのみに SSH を使用できます。診断インターフェイスは、SNMP や syslog のモニタリングに役立ちます。

（注） 診断インターフェイスと管理インターフェイスは1つの物理ポートを共有しますが、同じネットワーク上の各インターフェイスには異なる IP アドレスを割り当てる必要があります。

インターフェイス モードとタイプ

通常のファイアウォール モードと IPS 専用モードの 2 つのモードで Firewall Threat Defense インターフェイスを展開できます。同じデバイスにファイアウォールインターフェイスとIPS専用インターフェイスの両方を含めることができます。

通常のファイアウォール モード

ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、IP 最適化、TCP の正規化などのファイアウォール機能の対象となります。オプションで、セキュリティポリシーに従ってこのトラフィックに IPS 機能を設定することもできます。

設定できるファイアウォール インターフェイスのタイプは、ルーテッド モードとトランスペアレントモードのどちらのファイアウォールモードがそのデバイスに設定されているかによって異なります。詳細については、トランスペアレントファイアウォールモードまたはルーテッド ファイアウォール モード （199 ページ）を参照してください。

- ルーテッド モード インターフェイス（ルーテッド ファイアウォール モードのみ）：ルーティングを行う各インターフェイスは異なるサブネット上にあります。
- ブリッジグループ インターフェイス（ルーテッドおよびトランスペアレント ファイアウォールモード）：複数のインターフェイスをネットワーク上でグループ化することができ、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通過させることができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。ルーテッド モードでは、Firepower Threat Defense デバイスは BVI と通常のルーテッド イ

ンターフェイス間をルーティングします。トランスペアレントモードでは、各ブリッジグループは分離されていて、相互通信できません。

IPS 専用モード

パッシブまたはインラインのいずれかのIPS展開でデバイスを設定できます。パッシブ展開では、ネットワークトラフィックのフローからアウトオブバンドでシステムを展開します。インライン展開では、2つのインターフェイスを一緒にバインドすることで、ネットワークセグメント上でシステムを透過的に設定します。

セキュリティ ゾーンとインターフェイス グループ

各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てることができます。その上で、ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、1つ以上のデバイスの「内部」インターフェイスを「内部」ゾーンに割り当て、「外部」インターフェイスを「外部」ゾーンに割り当てることができます。次に、同じゾーンを使用するすべてのデバイスについて、トラフィックが内部ゾーンから外部ゾーンに移動できるようにアクセス コントロール ポリシーを設定できます。

各オブジェクトに属するインターフェイスを表示するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択し、[インターフェイス（Interface）] の順に選択します。このページでは、管理対象デバイスで設定されているセキュリティゾーンとインターフェイスグループの一覧が表示されます。各インターフェイスオブジェクトを展開して、各インターフェイス オブジェクトのインターフェイスのタイプを表示できます。

（注） **あらゆる**ゾーンに適用されるポリシー（グローバルポリシー）は、ゾーン内のインターフェイスだけでなく、ゾーンに割り当てられていないインターフェイスにも適用されます。

（注） 診断/管理インターフェイスは、ゾーンまたはインターフェイスグループには属しません。

セキュリティゾーンとインターフェイスグループ

インターフェイス オブジェクトには次の 2 つのタイプがあります。

- セキュリティゾーン：インターフェイスは、1つのセキュリティゾーンにのみ属することができます。
- インターフェイスグループ：インターフェイスは複数のインターフェイスグループ（および1つのセキュリティ ゾーン）に属することができます。

  NAT ポリシー、プレフィルタポリシー、およびQoSポリシーでインターフェイスグループを使用できるほか、Syslogサーバーや DNS サーバーなどのインターフェイス名を直接指定できる機能も使用できます。

ポリシーによっては、セキュリティゾーンだけをサポートする場合も、ゾーンとグループの両方をサポートする場合もあります。セキュリティゾーンはすべての機能でサポートされているため、インターフェイスグループが提供する機能を必要としないない限り、デフォルトでセキュリティゾーンを使用する必要があります。

既存のセキュリティ ゾーンをインターフェイス グループに、またはその逆に変更することはできません。代わりに、新しいインターフェイス オブジェクトを作成する必要があります。

（注） トンネルゾーンはインターフェイス オブジェクトではありませんが、特定の設定ではセキュリティ ゾーンの代わりにトンネルゾーンを使用できます。トンネル ゾーンおよびプレフィルタリング （1907 ページ）を参照してください。

インターフェイス オブジェクト タイプ

次のインターフェイス オブジェクト タイプを参照してください。

- パッシブ：IPS 専用パッシブまたは ERSPAN インターフェイスの場合。
- インライン：IPS 専用インライン セット インターフェイスの場合。
- スイッチド：通常のファイアウォール ブリッジ グループ インターフェイスの場合。
- ルーテッド：通常のファイアウォール ルーテッド インターフェイスの場合。
- ASA：（セキュリティゾーンのみ）レガシー ASA FirePOWER デバイスインターフェイスの場合。

インターフェイス オブジェクト内のすべてのインターフェイスは、同じタイプである必要があります。インターフェイス オブジェクトを作成した後、それに含まれるインターフェイスのタイプを変更することはできません。

インターフェイス名

インターフェイス（またはゾーン名）自体では、セキュリティポリシーに関してデフォルトの動作が提供されません。将来の構成での間違いを防ぐために、わかりやすい名前を使用することをお勧めします。適切な名前とは、論理セグメントまたはトラフィック仕様を表すものです。次に例を示します。

- 内部インターフェイスの名前：InsideV110、InsideV160、InsideV195
- DMZ インターフェイスの名前：DMZV11、DMZV12、DMZV-TEST
- 外部インターフェイスの名前：Outside-ASN78、Outside-ASN91

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロスケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

冗長インターフェイス（廃止）

冗長インターフェイスは、ASA 5500-X プラットフォームでのみサポートされます。他のプラットフォームに対して設定することは推奨しません。

インターフェイスのデフォルト設定

この項では、インターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスの状態は、タイプによって異なります。

- 物理インターフェイス：ディセーブル。初期セットアップで有効になる管理インターフェイスは例外です。物理インターフェイスには、スイッチ ポートが含まれます。
- VLAN サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（ISA 3000）：有効。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（Firepower および Cisco Secure Firewall モデル）：無効。

（注） Firepower 4100/9300 の場合、管理上、シャーシおよび Firewall Management Center の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと Firewall Management Center の間の不一致が生じることがあります。

デフォルトの速度および二重通信

デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。

デフォルトでは、光ファイバ（SFP）インターフェイスの速度とデュプレックスは最大速度に設定され、自動ネゴシエーションが有効です。

Cisco Secure Firewall 3100 の場合、速度は、インストールされている SFP の速度を検出するように設定されています。

セキュリティゾーンおよびインターフェイスグループオブジェクトの作成

デバイスインターフェイスを割り当てることができるセキュリティゾーンとインターフェイスグループを追加します。

ヒント 空のインターフェイスオブジェクトを作成し、後からインターフェイスを追加できます。インターフェイスを追加するには、インターフェイスに名前が付いている必要があります。インターフェイスを設定しているときに、セキュリティゾーンを作成することもできます（インターフェイスグループは作成できません）。

始める前に

各種インターフェイス オブジェクトの使用要件および制限を理解します。セキュリティ ゾーンとインターフェイス グループ （631 ページ） を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクトタイプのリストから、[インターフェイス（Interface）] を選択します。

ステップ 3 [追加（Add）] > [セキュリティゾーン（Security Zone）] または [追加（Add）] > [インターフェイスグループ（Interface Group）] をクリックします。

ステップ 4 名前を入力します。

ネットワークまたはポート オブジェクトと同じ名前を使用しないでください。これらのオブジェクト名はデバイスに展開されますが、名前が重複すると展開が失敗します。

ステップ 5 [インターフェイス タイプ（Interface Type）] を選択します。

ステップ 6 （任意）**[デバイス（Device）] > [インターフェイス（Interfaces）]** ドロップダウンリストから、追加するインターフェイスを含むデバイスを選択します。

この画面でインターフェイスを割り当てる必要はありません。代わりに、インターフェイスを設定するときに、インターフェイスをゾーンまたはグループに割り当てることができます。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

物理インターフェイスの有効化およびイーサネット設定の構成

ここでは、次の方法について説明します。

- 物理インターフェイスを有効にします。デフォルトでは、物理インターフェイスは無効になっています（Diagnostic インターフェイスを除く）。
- 特定の速度と二重通信を設定します。デフォルトでは、速度とデュプレックスは [自動（Auto）] に設定されます。

この手順は、インターフェイス設定のごく一部にすぎません。この時点では、他のパラメータを設定しないようにします。たとえば、EtherChannel インターフェイスの一部として使用するインターフェイスには名前を付けることはできません。

（注） Firepower 4100/9300 の場合、FXOS の基本インターフェイスの設定を行います。詳細については、物理インターフェイスの設定 （254 ページ）を参照してください。

（注） Firepower 1010 のスイッチポートについては、Firepower 1010 のスイッチポートの設定 （674 ページ）を参照してください。

始める前に

Firewall Management Center に追加した後、デバイスの物理インターフェイスを変更した場合、[インターフェイス（Interfaces）]の左上にある[デバイスからのインターフェイスの同期（Sync Interfaces from device）] をクリックしてそのインターフェイスリストを更新する必要があります。ホットスワップをサポートする Cisco Secure Firewall 3100 については、デバイスのインターフェイスを変更する前に「Cisco Secure Firewall 3100 のネットワークモジュールの管理 （652 ページ）」を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 4 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 （任意） **[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]**をクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。SFP インターフェイスは [全二重（Full）] のみをサポートします。
- [速度（Speed）] : 速度を選択します（モデルによって異なります）。（Cisco Secure Firewall 3100 のみ）[SFPを検出（Detect SFP）] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。

  （注）
  高可用性（HA）またはクラウド制御リンクインターフェイスの速度は変更できません。

- [自動ネゴシエーション（Auto-negotiation）] : 速度、リンクステータス、およびフロー制御をネゴシエートするようにインターフェイスを設定します。
- [前方誤り訂正モード（Forward Error Correction Mode）] : （Cisco Secure Firewall 3100 のみ）25 Gbps 以上のインターフェイスの場合は、前方誤り訂正（FEC）を有効にします。EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。**自動**を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *45 :* 自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト **FEC**（イーサネット **1/9** ～ **1/16**）	ネットワークモジュールのデフォルト **FEC**
25G-SR	第 74 条 FC-FEC	第 108 条 RS-FEC
25G-LR	第 74 条 FC-FEC	第 108 条 RS-FEC
10/25G-CSR	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-AOC*x*M	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション

ステップ 6 （任意）（Firepower 1100/2100、Cisco Secure Firewall 3100）**[ハードウェア設定（Hardware Configuration）]** > **[ネットワーク接続（Network Connectivity）]** の順にクリックして Link Layer Discovery Protocol（LLDP）を有効にします。

- [LLDP受信の有効化（Enable LLDP Receive）]：ファイアウォールがピアから LLDP パケットを受信できるようにします。
- [LLDP送信の有効化（Enable LLDP Transmit）]：ファイアウォールがピアに LLDP パケットを送信できるようにします。

ステップ 7 （任意）（Cisco Secure Firewall 3100）**[ハードウェア設定（Hardware Configuration）]** > **[ネットワーク接続（Network Connectivity）]** をクリックし、[フロー制御送信（Flow Control Send）] をオンにして、フロー制御の一時停止（XOFF）フレームを有効にします。

フロー制御により、接続しているイーサネットポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。脅威防御ポートで輻輳が生じ（内部スイッチでキューイングリソースが枯渇）、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

（注）
Firewall Threat Defense は、リモートピアがトラフィックをレート制御できるように、ポーズフレームの送信をサポートしています。

ただし、ポーズフレームの受信はサポートされていません。

内部スイッチには、それぞれ 250 バイトの 8000 バッファのグローバルプールがあり、スイッチはバッファを各ポートに動的に割り当てます。バッファ使用量がグローバル ハイ ウォーターマーク（2 MB（8000 バッファ））を超えると、フロー制御が有効になっているすべてのインターフェイスからポーズフレームが送信されます。また、バッファがポートのハイ ウォーター

マーク（.3125 MB（1250 バッファ））を超えると、特定のインターフェイスからポーズフレームが送信されます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XON フレームを送信できます（グローバルでは 1.25MB（5000 バッファ）、ポートごとに 25 MB（1000 バッファ））リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。

802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

ステップ 8 [モード（Mode）] ドロップダウン リストで、次のいずれかを選択します。

- [なし（None）]: この設定を通常のファイアウォール インターフェイスおよびインラインセットに選択します。その後の設定に基づいて、モードが [ルーテッド（Routed）]、[スイッチド（Switched）]、または [インライン（Inline）] に自動的に変更されます。
- [パッシブ（Passive）]：この設定を IPS 専用インターフェイスに選択します。
- [Erspan]：この設定を Erspan パッシブ IPS 専用インターフェイスに選択します。

ステップ 9 [優先度（Priority）] フィールドに、0 ～ 65535 の範囲の数値を入力します。

この値は、ポリシーベースのルーティング構成で使用されます。優先度は、複数の出力インターフェイス間でトラフィックを分散する方法を決定するために使用されます。

ステップ 10 [OK] をクリックします。

ステップ 11 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ステップ 12 インターフェイスの構成を続行します。

- 通常のファイアウォール インターフェイス （673 ページ）
- インラインセットとパッシブインターフェイス （763 ページ）

EtherChannel インターフェイスの設定

ここでは、EtherChannel インターフェイスの設定方法について説明します。

（注） Firepower 4100/9300 の場合は、FXOS の EtherChannel を設定します。詳細については、EtherChannel（ポート チャネル）の追加 （256 ページ）を参照してください。

EtherChannel インターフェイスについて

ここでは、EtherChannel インターフェイスについて説明します。

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャネル インターフェイスと呼びます）。ポートチャネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャネル グループのインターフェイス

各チャネルグループには、最大 8 個のアクティブインターフェイスを持たせることができます。ただし、ISA 3000 は、16 個のアクティブインターフェイスをサポートしています。8 個のアクティブインターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

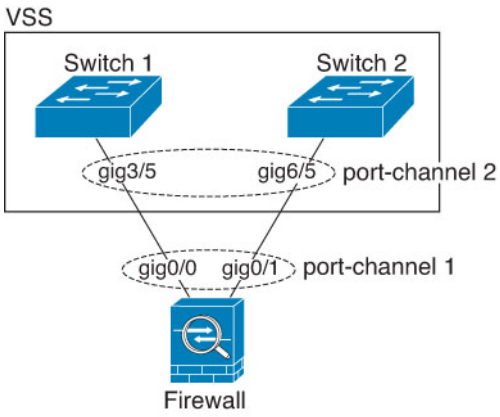
EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

Firewall Threat Defense EtherChannelの接続先のデバイスも802.3ad EtherChannelをサポートしている必要があります。たとえば、Catalyst 6500スイッチまたはCisco Nexus 7000に接続できます。

スイッチが仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）の一部である場合、同じ EtherChannel 内の Firewall Threat Defense インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。個別のスイッチは単一のスイッチのように動作するため、スイッチインターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。

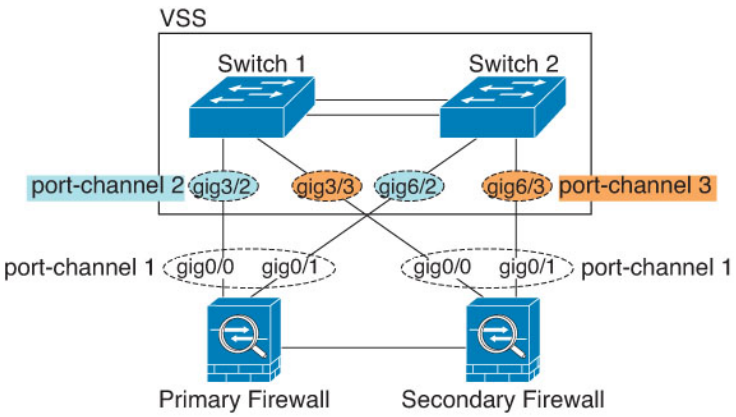
図 *201 : VSS/vPC*への接続



（注） Firewall Threat Defenseデバイスがトランスペアレントファイアウォールモードになっており、2 組の VSS/vPC スイッチ間に Firewall Threat Defense デバイスを配置する場合は、EtherChannel 内で Firewall Threat Defense デバイスに接続されたすべてのスイッチポートで単方向リンク検出（UDLD）を無効にしてください。UDLDを有効にすると、スイッチポートは他のVSS/vPCペアの両方のスイッチから送信されたUDLDパケットを受信する場合があります。受信側スイッチは、"UDLDネイバーの不一致" という理由で受信側インターフェイスをダウン状態にします。

Firewall Threat Defense デバイスをアクティブ/スタンバイフェールオーバー展開で使用する場合、Firewall Threat Defense デバイスごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 Firewall Threat Defense デバイスで、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチインターフェイスを両方の Firewall Threat Defense デバイスに接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の Firewall Threat Defense システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ Firewall Threat Defense デバイスに送信しないようにするためです。

図 *202 :* アクティブ/スタンバイ フェールオーバーと *VSS/vPC*



Link Aggregation Control Protocol

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。ハードウェアモデルではサポートされていません。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

Firewall Threat Defense デバイスは、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設定可能です）。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が0となるすべてのパケットは、EtherChannel内の最初のインターフェイスへ送信され、以降は結果が1となるものは2番目のインターフェイスへ、結果が2となるものは3番目のインターフェイスへ、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対して透過的になります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

Firepower および Secure Firewall ハードウェア

ポートチャネル インターフェイスは、内部インターフェイスの内部データ 0/1 の MAC アドレスを使用します。または、ポート チャネル インターフェイスの MAC アドレスを手動で設定することもできます。シャーシ上のすべての EtherChannel インターフェイスは同じ MAC アドレスを使用するため、たとえば、SNMP ポーリングを使用する場合、複数のインターフェイスが同じ MAC アドレスを持つことに注意してください。

（注） メンバーインターフェイスは、再起動後に内部データ 0/1 MAC アドレスのみを使用します。再起動する前に、メンバーインターフェイスは独自の MAC アドレスを使用するた再起動後に新しいメンバーインターフェイスを追加する場合、MAC アドレスを更新するためにもう一度再起動する必要があります。

EtherChannel インターフェイスのガイドライン

ブリッジグループ

ルーテッドモードでは、Firewall Management Center 定義の EtherChannel はブリッジグループメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。

高可用性

- EtherChannel インターフェイスを 高可用性 リンクとして使用する場合、高可用性 ペアの両方のユニットでその事前設定を行う必要があります。プライマリユニットで設定し、セカンダリユニットに複製されることは想定できません。これは、複製には 高可用性 リンク自体が必要であるためです。
- EtherChannel インターフェイスをステートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリユニットから複製されます。Firepower 4100/9300 シャーシ では、EtherChannel を含むすべてのインターフェイスを、両方のユニットで事前に設定する必要があります。
- 高可用性 の EtherChannel インターフェイスをモニターできます。アクティブなメンバーインターフェイスがスタンバイインターフェイスにフェールオーバーした場合、デバイスレベルの高可用性をモニタしているときには、EtherChannel インターフェイスで障害が発生しているようには見えません。すべての物理インターフェイスで障害が発生した場合にのみ、EtherChannel インターフェイスで障害が発生しているように見えます（EtherChannel インターフェイスでは、障害の発生が許容されるメンバインターフェイスの数を設定できます）。
- EtherChannel インターフェイスを高可用性 リンクまたはステートリンクに対して使用する場合、異常なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。高可用性リンクとして使用中のEtherChannelの設定は変更できま

せん。設定を変更するには、高可用性 を一時的に無効にする必要があります。これにより、その期間中は 高可用性 が発生することはありません。

サポート モデル

- Firepower 4100/9300 または Firewall Threat Defense Virtual の場合、Firewall Management Center で EtherChannel を追加することはできません。Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。
- EtherChannel で Firepower 1010 のスイッチポートまたは VLAN インターフェイスを使用することはできません。

EtherChannelの一般的なガイドライン

- モデルで利用可能なインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャネルグループには、最大 8 個のアクティブインターフェイスを持たせることができます。ただし、ISA 3000 は、16 個のアクティブインターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。ただし、Cisco Secure Firewall 3100 の場合は、速度が [SFPを検出（Detect SFP）] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。
- Firewall Threat Defense の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- Firewall Threat Defense デバイスは、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して隣接スイッチのネイティブ VLAN タギングを有効にすると、Firewall Threat Defense デバイスはタグ付きの LACPDU をドロップします。隣接スイッチのネイティブVLANタギングは、必ず無効にしてください。
- LACP レートはモデルによって異なります。レート（通常または高速）を設定すると、デバイスは接続中のスイッチにそのレートを要求します。デバイスの方も接続中のスイッチによって要求されたレートで送信します。両側で同じレートを設定することを推奨します。
  - Firepower 4100/9300：LACP レートは、FXOS ではデフォルトで高速に設定されていますが、通常（低速とも呼ばれる）に設定することもできます。

- Cisco Secure Firewall 3100LACP レートは、デフォルトで通常（低速）に設定されていますが、デバイスで高速に設定することもできます。
- 他のすべてのモデル：LACP レートが通常（低速とも呼ばれる）に設定されており、変更できません。つまり、デバイスは接続中のスイッチに常に低速レートを要求します。スイッチのレートを低速に設定して、両側が同じレートでLACPメッセージを送信するように設定することを推奨します。

- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行する Firewall Threat Defense では、スイッチスタックへのEtherChannelの接続がサポートされていませんでした。デフォルトのスイッチ設定では、Firewall Threat Defense EtherChannel がクロススタックに接続されている場合、プライマリスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば8分、0（無制限）などを設定します。または、15.1(1)S2など、より安定したスイッチソフトウェアバージョンにアップグレードできます。
- すべてのFirewall Threat Defenseコンフィギュレーションは、メンバー物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。

EtherChannel の設定

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

ガイドライン

- モデルのインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャネルグループには、最大8個のアクティブインターフェイスを持たせることができます。ただし、ISA 3000は、16個のアクティブインターフェイスをサポートしています。8 個のアクティブインターフェイスだけをサポートするスイッチの場合、1 つのチャネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは8個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイリンクとして動作できます。
- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。メディアタイプはRJ-45またはSFPのいずれかです。異なるタイプ（銅と光ファイバ）のSFPを混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GBと10GBのインターフェイスなど）を混在させることはできません。ただし、Cisco Secure Firewall 3100 の場合は、速度が [SFPを検出（Detect SFP）] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。

（注） Firepower 4100/9300 の場合は、FXOS の EtherChannel を設定します。詳細については、EtherChannel（ポート チャネル）の追加 （256 ページ）を参照してください。

始める前に

- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に名前を削除する必要があります。

（注） コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

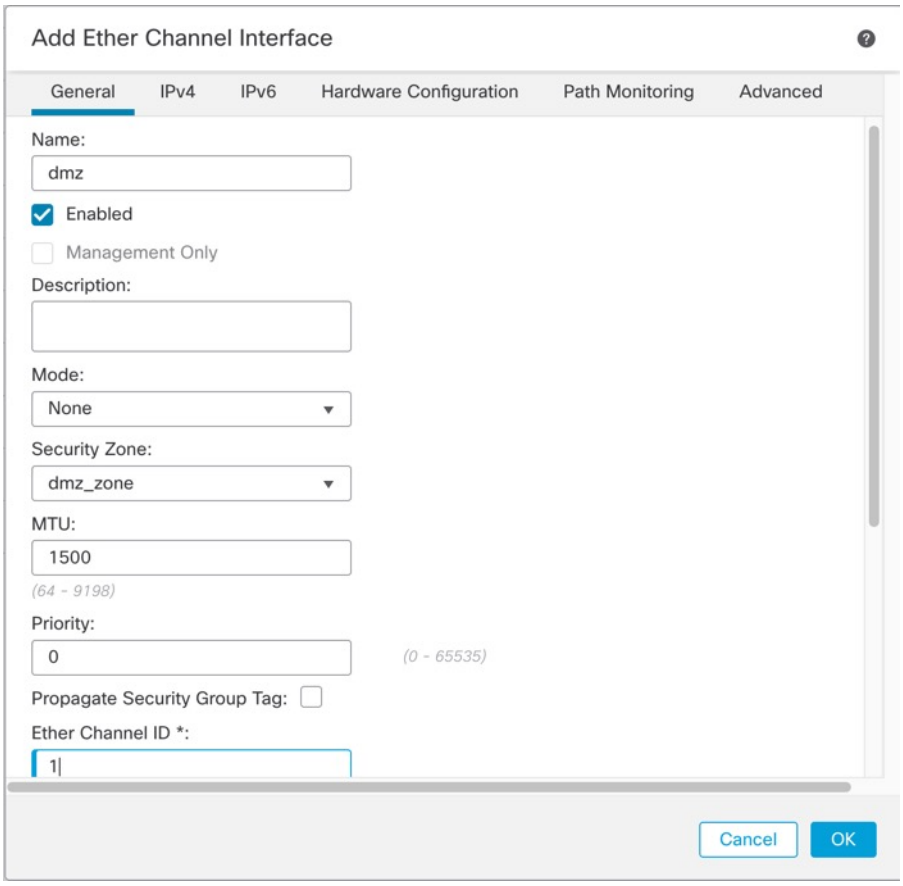
ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（ ） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 物理インターフェイスの有効化およびイーサネット設定の構成（635 ページ）に従って、メンバー インターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）]** > **[Ether Channel インターフェイス（Ether Channel Interface）]** をクリックします。

ステップ 4 [一般（General）] タブで、[イーサネットチャネルID（Ether Channel ID）] を 1 ～ 48（Firepower 1010 の場合は 1 ～ 10）の数値に設定します。

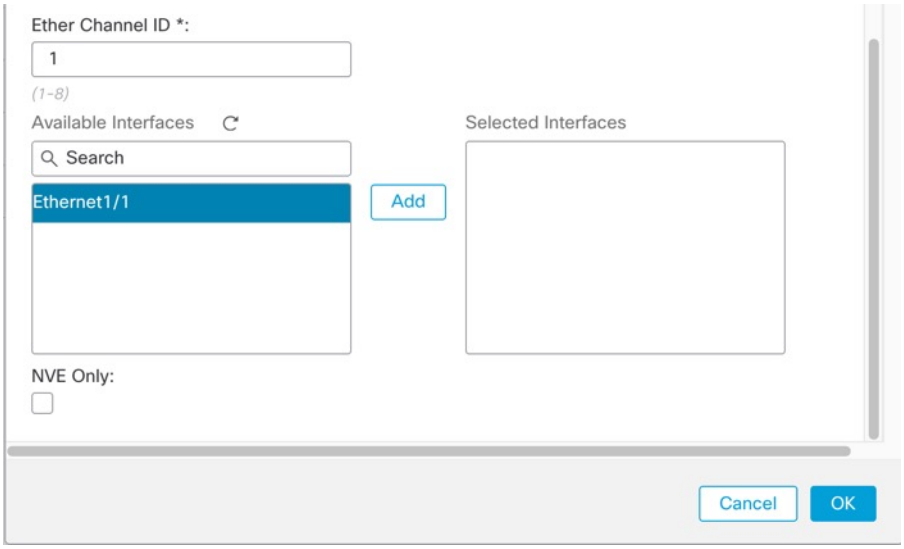
図 *203 : EtherChannel* インターフェイスの追加



ステップ 5 [使用可能なインターフェイス（Available Interfaces）] 領域でインターフェイスをクリックし、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interface）] 領域にそのインターフェイスを移動します。メンバーを作成するすべてのインターフェイスに対して繰り返します。

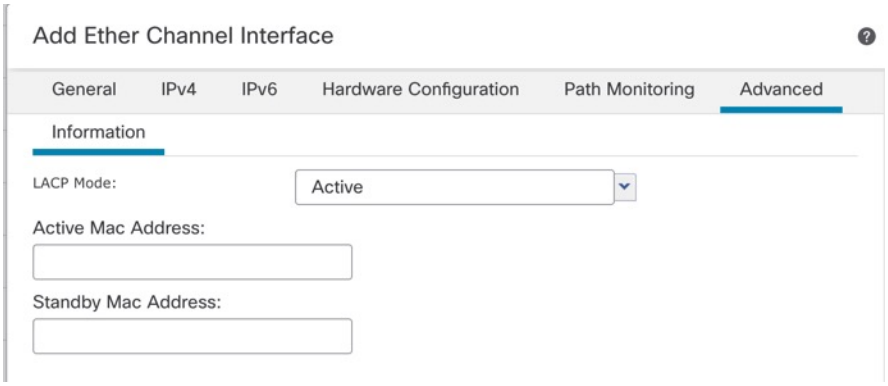
すべてのインターフェイスのタイプと速度が同じになるようにします。

図 *204 : Available Interfaces*



ステップ 6 （任意）[詳細（Advanced）] タブをクリックして EtherChannel をカスタマイズします。[情報（Information）] サブタブで次のパラメータを設定します。

図 *205 :* 作成する*Advanced*



- （ISA 3000 のみ）[ロードバランシング（Load Balance）] : パケットをグループ チャネル インターフェイス間でロードバランスするために使用する基準を選択します。デフォルトでは、Firewall Threat Defense デバイスはパケットの送信元および宛先 IP アドレスに従って、インターフェイスでのパケットのロードをバランスします。パケットが分類される基準になるプロパティを変更する場合は、別の基準のセットを選択します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロードバランシングの詳細については、ロードバランシング（641 ページ）を参照してください。
- [LACP モード（LACP Mode）] : [アクティブ（Active）]、[パッシブ（Passive）]、または [オン（On）] を選択します。[アクティブ（Active）] モード（デフォルト）を使用することを推奨します。パッシブモードは、ISA 3000 でのみ使用できます。

- （Cisco Secure Firewall 3100 のみ）[LACP レート（LACP Rate）]：[デフォルト（Default）]、[標準（Normal）]、または [高速（Fast）] を選択します。デフォルトは [標準（Normal）]（低速とも呼ばれる）です。チャネルグループの物理インターフェイスの LACP データユニット受信レートを設定します。両側で同じレートを設定することを推奨します。
- （ISA 3000 のみ）[アクティブな物理インターフェイス：範囲（Active Physical Interface: Range）]：左側のドロップダウンリストから、EtherChannel をアクティブにするために必要なアクティブインターフェイスの最小数を 1 ～ 16 の範囲で選択します。デフォルトは 1 です。右側のドロップダウン リストから、EtherChannel で許可されるアクティブ インターフェイスの最大数を 1 ～ 16 の範囲で選択します。デフォルトは 16 です。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。
- [アクティブな MAC アドレス（Active Mac Address）]：必要に応じて手動 MAC アドレスを設定します。mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

ステップ 7 [ハードウェア構成（Hardware Configuration）] タブをクリックし、すべてのメンバーインターフェイスのデュプレックスと速度を設定します。

ステップ 8 [OK] をクリックします。

ステップ 9 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ステップ 10 （任意） 通常のファイアウォール インターフェイスの場合は、VLAN サブインターフェイスを追加します。サブインターフェイスの追加 （694 ページ）を参照してください。

ステップ 11 通常のファイアウォールインターフェイスの場合、ルーテッドまたはトランスペアレントモードインターフェイスのパラメータを設定します（ルーテッド モードのインターフェイスの設定 （717 ページ） またはブリッジ グループ インターフェイスの設定 （724 ページ））。IPS 専用インターフェイスについては、「インラインセットとパッシブインターフェイス （763 ページ）」を参照してください。

Firewall Management Center とのインターフェイスの変更の同期

デバイスでのインターフェイスの変更は、Firewall Management Centerや、同期外れの原因となることがあります。Firewall Management Center は次の方法のいずれかでインターフェイスの変更を検出できます。

- デバイスから送信されたイベント
- Firewall Management Center からの展開の同期

展開を試行したときにFirewall Management Centerがインターフェイスを検出すると、その展開は失敗します。最初にインターフェイスの変更を承認する必要があります。

- 手動同期

Firewall Management Center の外部で実行されるインターフェイスの変更には、同期が必要な 2 つのタイプがあります。

- 物理インターフェイスの追加または削除：新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、Firewall Threat Defense の設定に対する影響は最小限で済みます。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバなど、Firewall Threat Defense の設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつ Firewall Management Center での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

  Firewall Management Center が変更を検出すると、[インターフェイス（Interface）] ページの各インターフェイスの左側にステータス（[削除済み（removed）]、[変更済み（changed）]、または [追加済み（added）]）が表示されます。

- Firewall Management Center アクセスインターフェイスの変更：**configure network management-data-interface** コマンドを使用して Management Center を管理するためのデータインターフェイスを設定する場合は、Management Center で一致する設定変更を手動で行ってから変更を確認する必要があります。これらのインターフェイスの変更を自動で行うことはできません。

この手順では、必要に応じてインターフェイスの変更を手動で同期する方法と検出された変更を確認する方法について説明します。デバイスの変更が一時的なものである場合は、その変更をFirewall Management Centerに保存する必要はありません。デバイスが安定するまで待機してから再同期します。

始める前に

- ユーザの役割：
  - 管理者
  - アクセス管理者
  - ネットワーク管理者

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 必要に応じて、**[インターフェイス（Interfaces）]** の左上にある **[デバイスの同期（Sync Device）]** をクリックします。

ステップ 3 変更が検出されたら、次の手順を参照してください。

物理インターフェイスの追加または削除

a) インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス（Interfaces）] に表示されます。[クリックして詳細を表示（Click to know more）] リンクをクリックしてインターフェイスの変更内容を表示します。

b) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

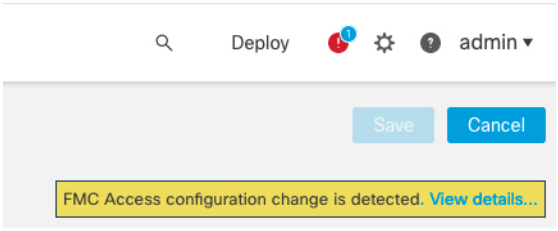
エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

c) **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。

FMC アクセスインターフェイスの変更

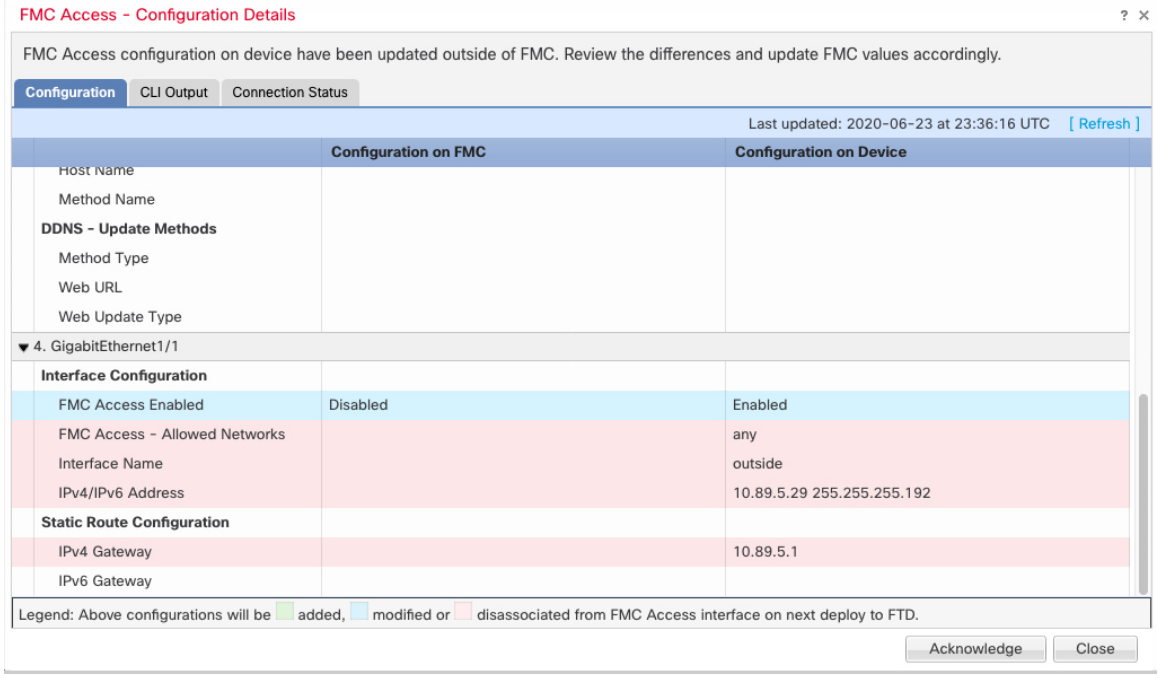
a) Firewall Management Center のアクセス設定が変更されたことを示す黄色のバナーが [デバイス（Device）] ページの右上に表示されます。[詳細を表示（View details）] リンクをクリックしてインターフェイスの変更内容を表示します。



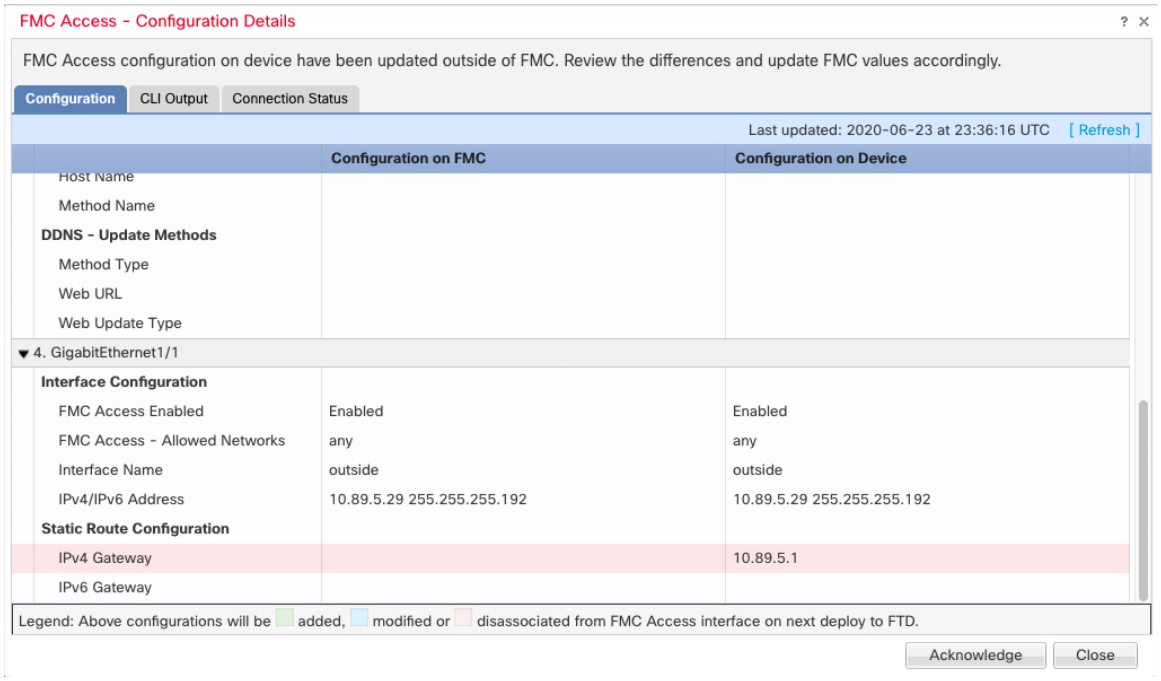
[FMCアクセス-設定の詳細（FMC Access - Configuration Details）] ダイアログボックスが開きます。

b) 強調表示されているすべての設定、特にピンクで強調表示されている設定に注意してください。Firewall Management Center で値を手動で設定し、Firewall Threat Defense で値を一致させる必要があります。

たとえば、以下のピンク色のハイライトは、Firewall Threat Defense に存在するものの、Firewall Management Center にはまだ存在しない設定を示しています。



Firewall Management Center でインターフェイスを設定した後のこのページの例を以下に示します。インターフェイス設定が一致し、ピンクのハイライトが消えています。



c) [確認（Acknowledge）] をクリックします。

Firewall Management Center の設定が完了して展開の準備ができるまで、[確認（Acknowledge）] をクリックしないことをお勧めします。[確認（Acknowledge）] をクリックすると、展開時にブロックが削除されます。Firewall Management Center 設定は、次回展

開時に Firewall Threat Defense の残りの競合する設定を上書きします。再展開の前に Firewall Management Center の設定を手動で修正する必要があります。

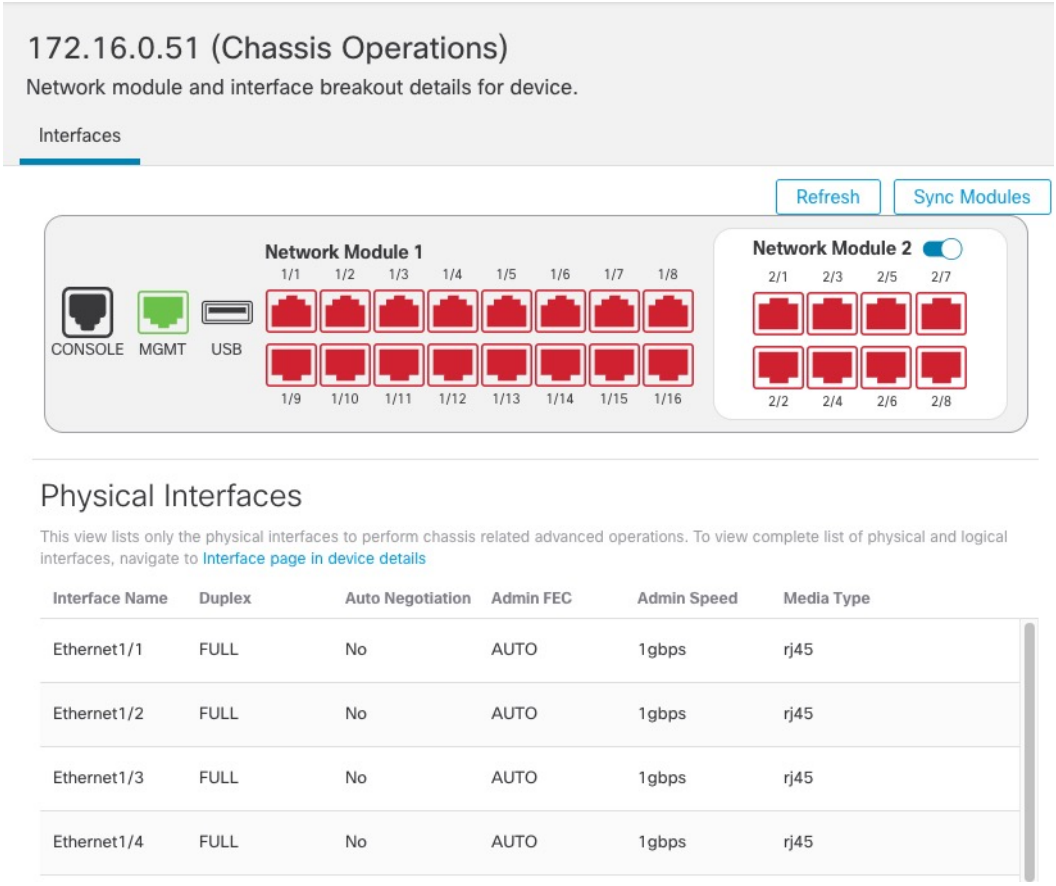
d) これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。

Cisco Secure Firewall 3100 のネットワークモジュールの管理

最初にデバイスの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。

デバイスの物理インターフェイスの詳細を表示してネットワークモジュールを管理するには、[シャーシの操作（Chassis Operations）] ページを開きます。[デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。

図 *206 :* シャーシの操作



[更新（Refresh）]をクリックして、インターフェイスのステータスを更新します。検出する必要があるデバイスでハードウェアの変更を行った場合は、[モジュールを同期（Sync Modules）]をクリックします。

初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、次の手順を参照してください。

ブレークアウトポートの設定

40GB 以上のインターフェイスごとに 10GB のブレークアウトポートを設定できます。この手順では、ポートの分割と再参加の方法について説明します。ブレークアウトポートは、EtherChannel への追加を含め、他の物理イーサネットポートと同じように使用できます。

変更はすぐに反映され、デバイスに展開する必要はありません。中断または再参加した後は、以前のインターフェイス状態にロールバックできません。

始める前に

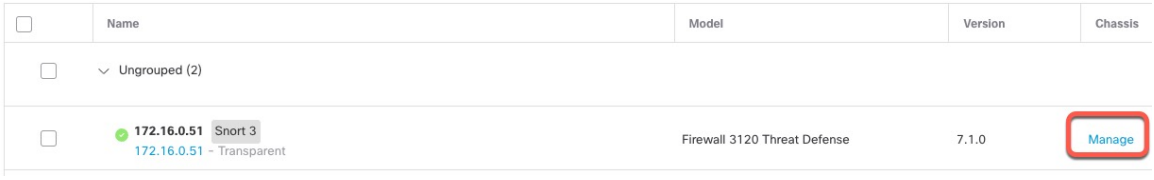
- サポートされているブレークアウトケーブルを使用する必要があります。詳細については、ハードウェア設置ガイドを参照してください。

- 中断または再参加する前に、インターフェイスを次の目的で使用することはできません。
  - フェールオーバー リンク
  - クラスタ制御リンク
  - サブインターフェイスを設定する
  - EtherChannel メンバー
  - BVI メンバー
  - マネージャ アクセス インターフェイス
- セキュリティポリシーで直接使用されているインターフェイスの中断または再参加は、構成に影響を与える可能性がありますが、アクションはブロックされません。

手順

ステップ 1 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 *207* : シャーシの管理



デバイスの [シャーシの操作（Chassis Operations）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

ステップ 2 40GB 以上のインターフェイスから 10GB ポートを分割します。

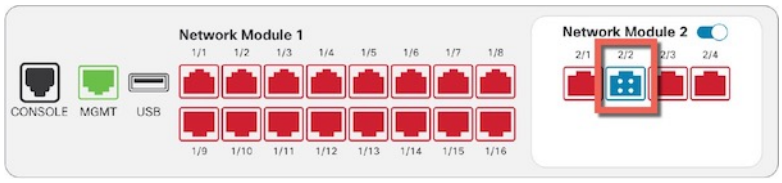
a) インターフェイスの右側の [ブレイク（Break）] （ ） をクリックします。

確認ダイアログボックスで [Yes] をクリックします。インターフェイスが使用中の場合は、エラーメッセージが表示されます。分割を再試行する前に、ユースケースを解決する必要があります。

たとえば、Ethernet2/1 40GB インターフェイスを分割する場合、分割後の子インターフェイスは、Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3、および Ethernet2/1/4 として識別されます。

インターフェイスのグラフィックでは、分割されたポートの表示は次のようになります。

図 *208* : ブレークアウト ポート



b) 画面上部のメッセージ内のリンクをクリックして[インターフェイス（Interfaces）]ページに移動し、インターフェイスの変更を保存します。

図 *209* : *[インターフェイス（Interface）]* ページへの移動

c) [インターフェイス（Interfaces）]ページの上部で、[クリックして詳細を表示（Click to know more）]をクリックします。[インターフェイスの変更（Interface Changes）]ダイアログボックスが開きます。

図 *210* : インターフェイスの変更の表示

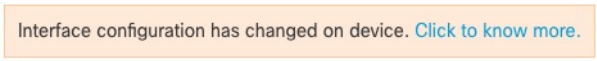
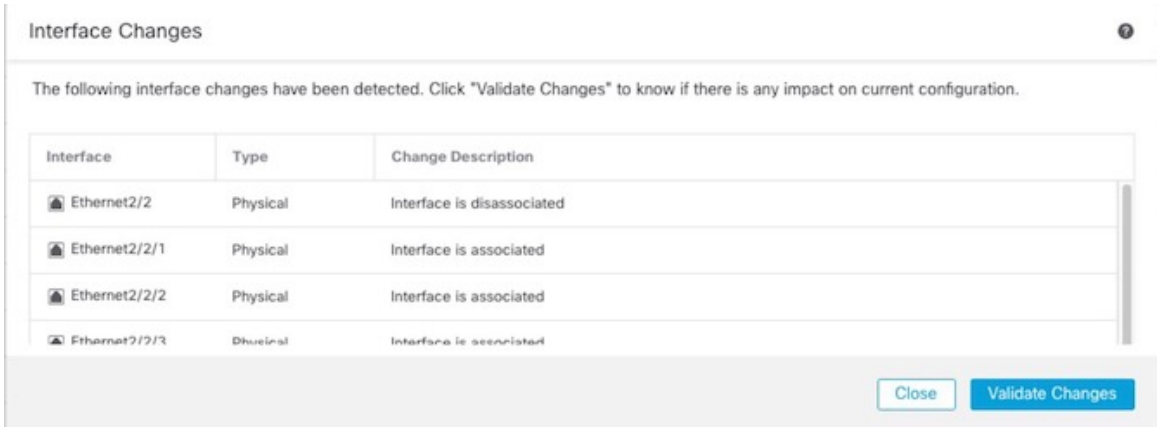


図 *211* : インターフェイスの変更



d) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

セキュリティポリシーで使用されている親インターフェイスを置き換えると、設定に影響を与える場合があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

e) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。
f) [保存（Save）]をクリックしてインターフェイスの変更をファイアウォールに保存します。
g) 構成を変更する必要があった場合は、**[展開（Deploy）]** > **[展開（Deployment）]** に移動してポリシーを展開します。

ブレークアウトポートの変更を保存するためだけに展開する必要はありません。

ステップ 3 ブレークアウトポートを再結合します。

インターフェイスのすべての子ポートを再結合する必要があります。

a) インターフェイスの右側の [参加（Join）]（） をクリックします。

確認ダイアログボックスで [Yes] をクリックします。子ポートが使用中の場合は、エラーメッセージが表示されます。再参加を再試行する前に、ユースケースを解決する必要があります。

b) 画面上部のメッセージ内のリンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

図 *212* : [インターフェイス（*Interface*）] ページへの移動

c) [インターフェイス（Interfaces）] ページの上部で、[クリックして詳細を表示（Click to know more）] をクリックします。[インターフェイスの変更（Interface Changes）] ダイアログボックスが開きます。

図 *213* : インターフェイスの変更の表示

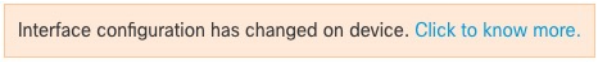
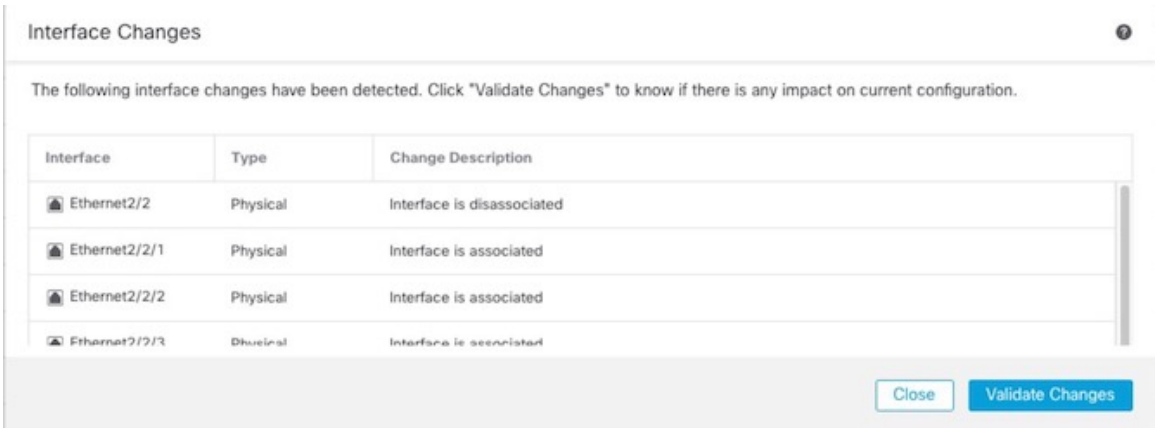


図 *214* : インターフェイスの変更



d) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

セキュリティポリシーで使用されている子インターフェイスを置き換えると、構成に影響を与える可能性があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

e) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。
f) [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。
g) 構成を変更する必要があった場合は、**[展開（Deploy）]** > **[展開（Deployment）]** に移動してポリシーを展開します。

ブレークアウトポートの変更を保存するためだけに展開する必要はありません。

ネットワークモジュールの追加

初回起動後にファイアウォールにネットワークモジュールを追加するには、次の手順を実行します。新しいモジュールを追加するには、再起動が必要です。

手順

ステップ 1 ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。

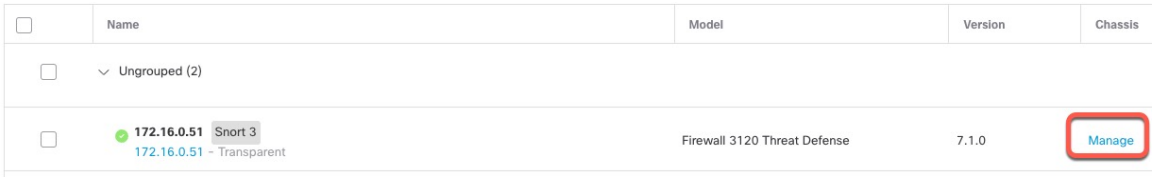
クラスタリングまたは高可用性の場合は、すべてのノードにネットワークモジュールをインストールします。

ステップ 2 ファイアウォールを再起動します。デバイスのシャットダウンまたは再起動 （41 ページ）を参照してください。

クラスタリングまたは高可用性の場合は、最初にデータノード/スタンバイユニットを再起動し、それらが復旧するのを待ちます。その後、制御ノード（制御ノードの変更 （360 ページ）を参照）またはアクティブユニット（Firewall Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替え （311 ページ）を参照）を変更し、以前の制御ノードまたはアクティブユニットを再起動できます。

ステップ 3 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 *215* : シャーシの管理

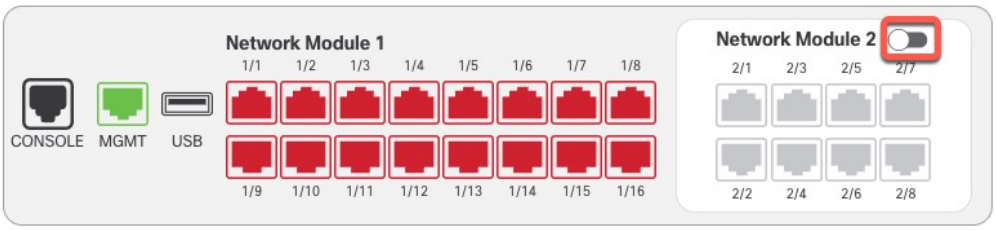


デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

ステップ 4 [モジュールの同期（Sync Modules）] をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。

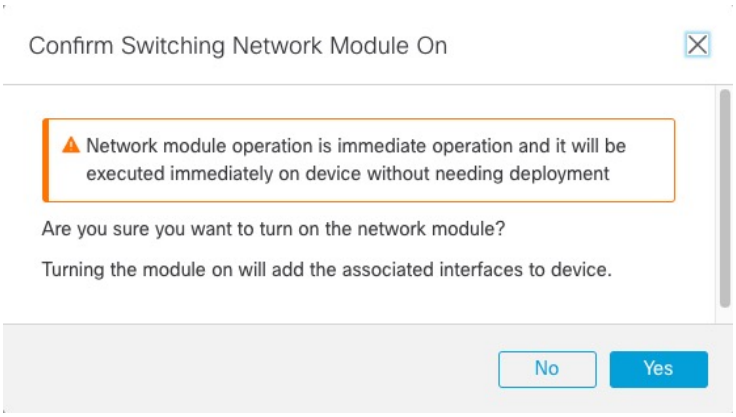
ステップ 5 インターフェイスのグラフィックで、スライダ （ ） をクリックしてネットワークモジュールを有効にします。

図 *216* : ネットワークモジュールの有効化



ステップ 6 ネットワークモジュールの有効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *217* : 有効化の確認



ステップ 7 画面の上部にメッセージが表示されます。リンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

図 *218* : *[*インターフェイス（*Interface*）*]*ページへの移動

ステップ 8 （任意）[インターフェイス（Interfaces）]ページの上部に、インターフェイスの設定が変更されたことを示すメッセージが表示されます。[クリックして詳細を表示（Click to know more）]をクリックすると、[インターフェイスの変更（Interface Changes）] ダイアログボックスが開き、変更が表示されます。

図 *219* : インターフェイスの変更の表示

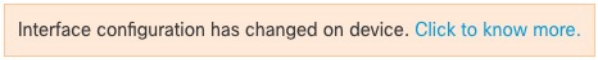
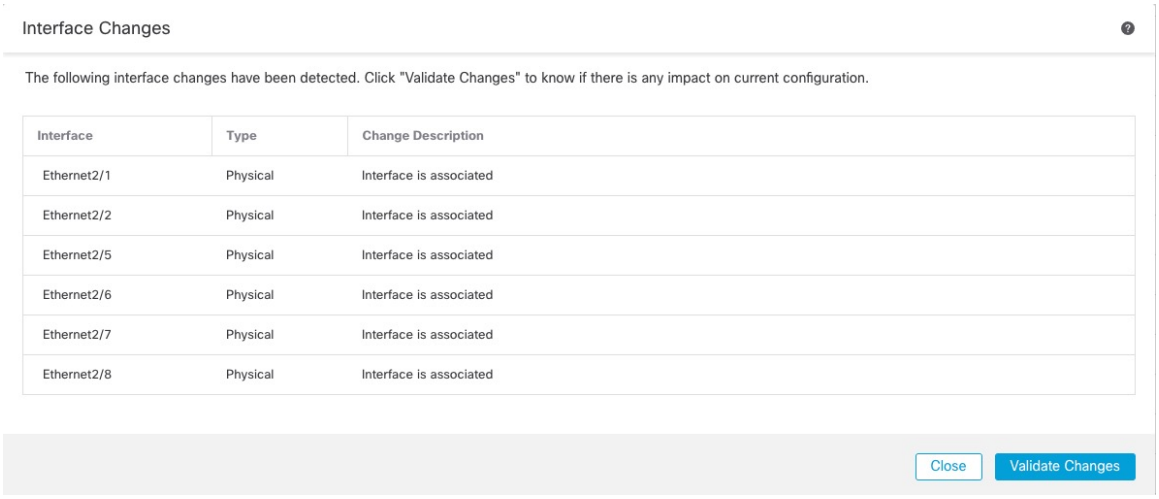


図 *220* : インターフェイスの変更



[閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります（新しいモジュールを追加しているので、設定への影響はないため、[変更の検証（Validate Changes）]をクリックする必要はありません）。

ステップ 9 [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。

ネットワークモジュールの交換方法

再起動することなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。この手順では、古いモジュールをシャットダウンし、新しいモジュールをインストールして有効にする方法について説明します。

クラスタリングまたは高可用性の場合、制御ノード/アクティブユニットでのみシャーシの操作を実行できます。クラスタ制御リンク/フェールオーバーリンクがモジュール上にある場合は、ネットワークモジュールを無効化できません。

始める前に

手順

ステップ 1 クラスタリングまたは高可用性の場合は、次の手順を実行します。

- **クラスタリング**：ホットスワップを実行するユニットがデータノードであることを確認します（制御ノードの変更（360ページ）を参照）。次に、そのノードを分断して、クラスタリングから外します。ノードの除外（357ページ）を参照してください。

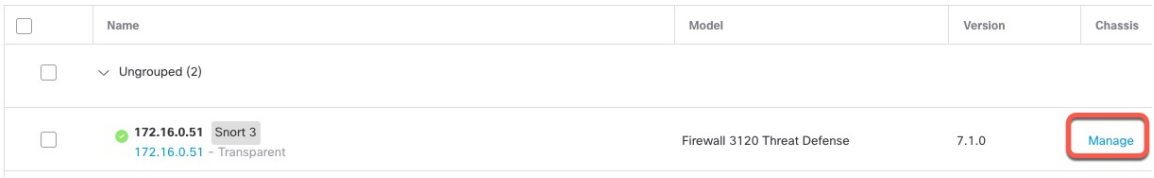
  ホットスワップを実行後、ノードをクラスタに追加し直します。または、制御ノードですべての操作を実行できます。ネットワークモジュールの変更はすべてのデータノードに同期されます。ただし、ホットスワップ中は、すべてのノードでインターフェイスが使用できなくなります。

- **高可用性**：ネットワークモジュールを無効にするときにフェールオーバーを回避するには、次の手順を実行します。

  - フェールオーバーリンクがネットワークモジュール上にある場合は、高可用性を分断する必要があります。高可用性ペアの解除（315ページ）を参照してください。アクティブなフェールオーバーリンクがあるネットワークモジュールを無効化することはできません。
  - ネットワークモジュールのインターフェイスのインターフェイスモニタリングを無効にします。スタンバイIPアドレスとインターフェイスモニタリングの設定（308ページ）を参照してください。

ステップ 2 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。＞クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 *221*：シャーシの管理



デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

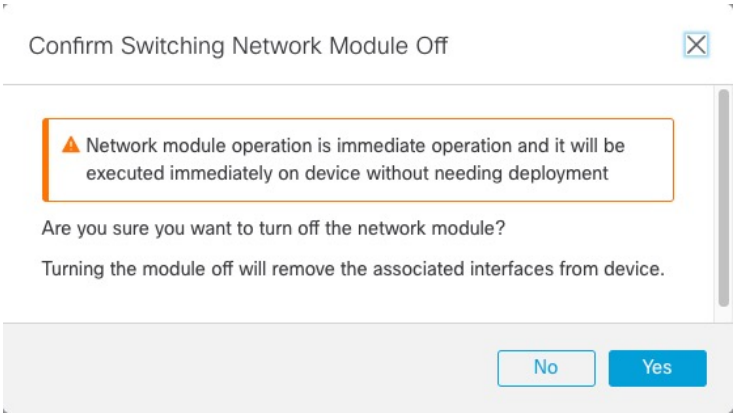
ステップ 3 インターフェイスのグラフィックで、スライダ（ ）をクリックしてネットワークモジュールを無効にします。

図 *222* : ネットワークモジュールの無効化

[インターフェイス（Interfaces）] ページでは変更を保存しないでください。ネットワークモジュールを交換するため、既存の構成を中断する必要はありません。

ステップ 4 ネットワークモジュールの無効化を確認するプロンプトが表示されます。[Yes] をクリックします。

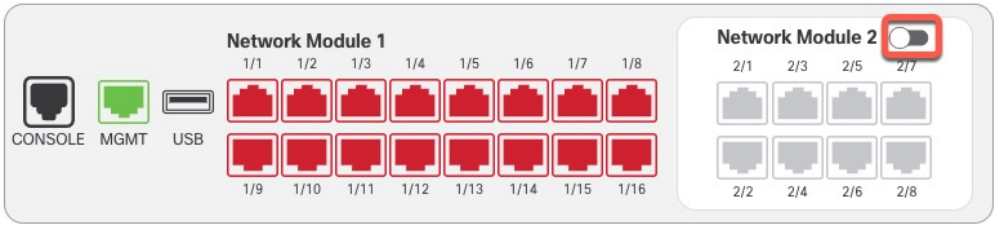
図 *223* : 無効化の確認



ステップ 5 ハードウェア設置ガイドに従って、デバイスの古いネットワークモジュールを取り外し、新しいネットワークモジュールと交換します。

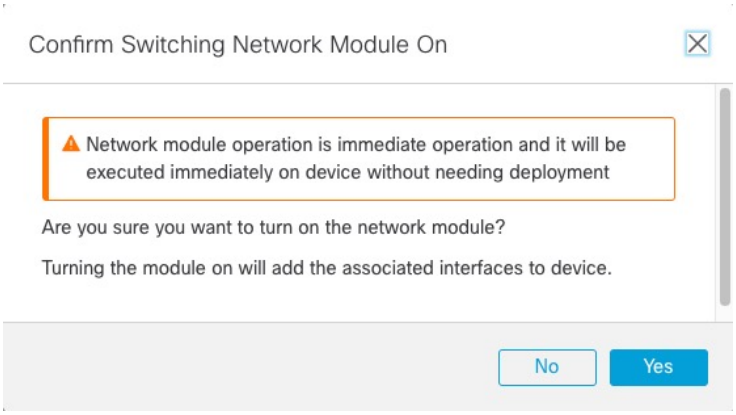
ステップ 6 Firewall Management Center で、スライダ （ ） をクリックして新しいモジュールを有効にします。

図 *224* : ネットワークモジュールの有効化



ステップ 7 ネットワークモジュールの有効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *225 :* 有効化の確認



ステップ 8 クラスタリングまたは高可用性の場合は、次の手順を実行します。

- **クラスタリング**：ノードをクラスタに追加して戻します。新しいクラスタノードの追加（355 ページ）を参照してください。
- **高可用性**：
  - 高可用性を解除した場合は、高可用性を再構築します。ハイ アベイラビリティ ペアの追加 （305 ページ）を参照してください。
  - ネットワークモジュールのインターフェイスのインターフェイスモニタリングを再度有効にします。「スタンバイ IP アドレスとインターフェイス モニタリングの設定（308 ページ）」を参照してください。

ネットワークモジュールを別のタイプに交換する

ネットワークモジュールを別のタイプに交換する場合は、再起動が必要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。

クラスタリングまたは高可用性の場合、制御ノード/アクティブユニットでのみシャーシの操作を実行できます。

始める前に

ハイアベイラビリティの場合、フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。高可用性を解除する必要があります（高可用性ペアの解除（315ページ）を参照）。これにより、アクティブユニットの再起動時にダウンタイムが発生するようになります。ユニットの再起動が完了したら、高可用性を再編成できます。

手順

ステップ 1 クラスタリングまたは高可用性の場合は、次の手順を実行します。

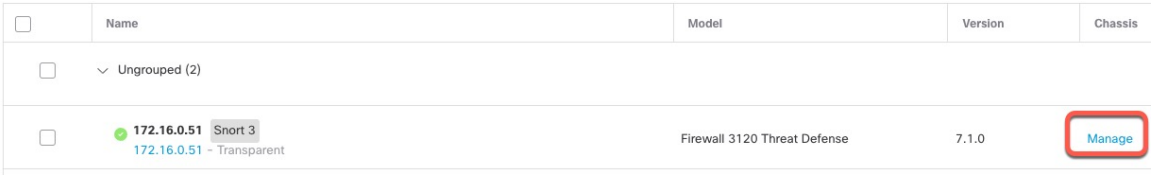
- **クラスタリング**：ネットワークモジュールを交換している間、ダウンタイムを回避するために、各ノードを一度に1つずつ分断し、クラスタから排除することができます。ノードの除外 （357 ページ）を参照してください。

  交換が完了したら、ノードをクラスタに戻します。

- **高可用性**：ネットワークモジュールを交換している間、フェールオーバーを回避するために、ネットワークモジュール上のインターフェイスのインターフェイスモニタリングを無効にします。スタンバイ IP アドレスとインターフェイス モニタリングの設定 （308 ページ）を参照してください。

ステップ 2 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

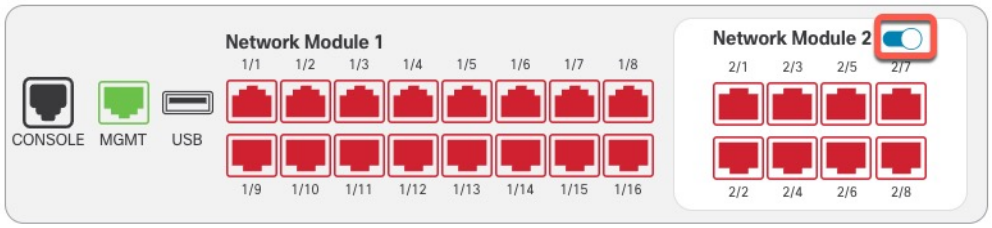
図 *226* : シャーシの管理



デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

ステップ 3 インターフェイスのグラフィックで、スライダ （ ） をクリックしてネットワークモジュールを無効にします。

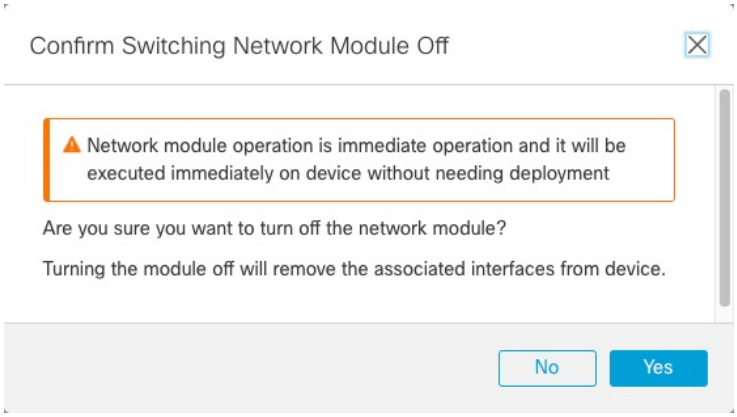
図 *227* : ネットワークモジュールの無効化



[インターフェイス（Interfaces）] ページでは変更を保存しないでください。ネットワークモジュールを交換するため、既存の構成を中断する必要はありません。

ステップ 4 ネットワークモジュールの無効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *228* : 無効化の確認



ステップ 5 ハードウェア設置ガイドに従って、デバイスの古いネットワークモジュールを取り外し、新しいネットワークモジュールと交換します。

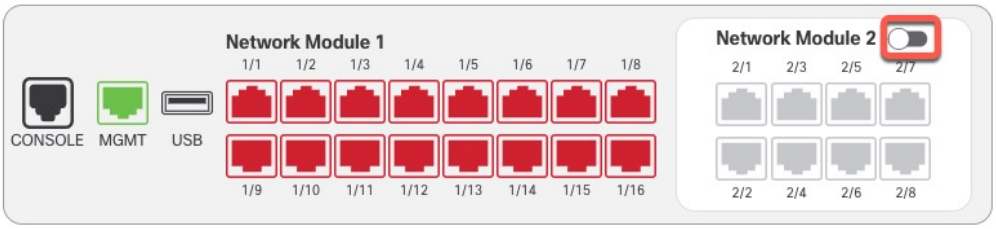
ステップ 6 ファイアウォールを再起動します。デバイスのシャットダウンまたは再起動 （41 ページ）を参照してください。

クラスタリングまたは高可用性の場合は、最初にデータノード/スタンバイユニットを再起動し、それらが復旧するのを待ちます。その後、制御ノード（制御ノードの変更 （360 ページ）を参照）またはアクティブユニット（Firewall Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替え （311 ページ）を参照）を変更し、以前の制御ノードまたはアクティブユニットを再起動できます。

ステップ 7 Firewall Management Center で、[モジュールの同期（Sync Modules）] をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。

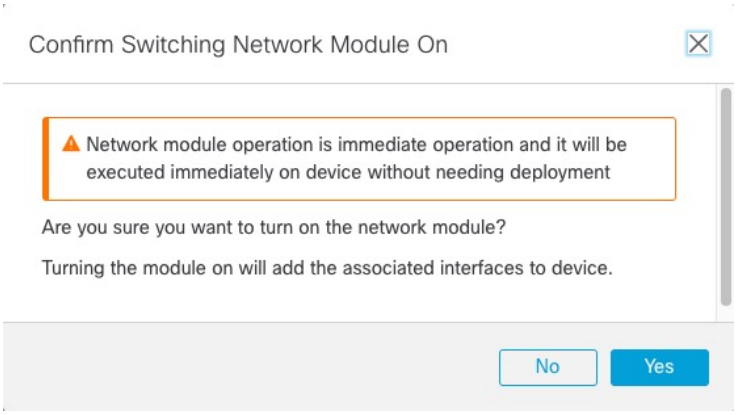
ステップ 8 スライダ （ ） をクリックして新しいモジュールを有効にします。

図 *229* : ネットワークモジュールの有効化



ステップ 9 ネットワークモジュールの有効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *230* : 有効化の確認



ステップ 10 画面上部のメッセージ内のリンクをクリックして[インターフェイス（Interfaces）]ページに移動し、インターフェイスの変更を保存します。

図 *231* : *[インターフェイス（**Interface**）]* ページへの移動

ステップ 11 ネットワークモジュールのインターフェイス数が減少した場合：

a) [インターフェイス（Interfaces）]ページの上部で、[クリックして詳細を表示（Click to know more）]をクリックします。[インターフェイスの変更（Interface Changes）]ダイアログボックスが開きます。

図 *232* : インターフェイスの変更の表示

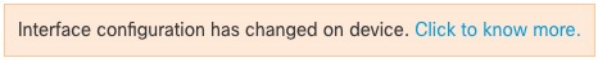
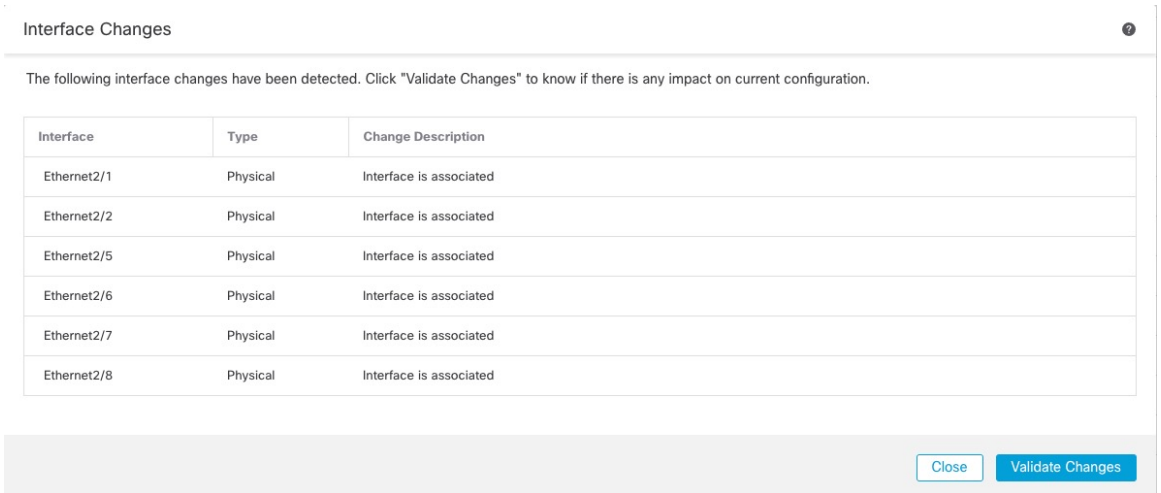


図 *233* : インターフェイスの変更



b) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与える場合があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

c) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。

ステップ 12 インターフェイス速度を変更するには、物理インターフェイスの有効化およびイーサネット設定の構成 （635 ページ）を参照してください。

デフォルトの速度は、[SFPを検出（Detect SFP）]に設定されています。これにより、取り付けられているSFPから適切な速度が検出されます。速度を手動で特定の値に設定しており、その速度の変更が必要になった場合にのみ、速度を修正する必要があります。

ステップ 13 [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。

ステップ 14 構成を変更する必要があった場合は、**[展開（Deploy）] > [展開（Deployment）]**に移動してポリシーを展開します。

ネットワークモジュールの変更を保存するためだけに展開する必要はありません。

ステップ 15 クラスタリングまたは高可用性の場合は、次の手順を実行します。

- **クラスタリング**：ノードをクラスタに追加して戻します。新しいクラスタノードの追加（355 ページ）を参照してください。
- **高可用性**：ネットワークモジュールのインターフェイスのインターフェイスモニタリングを再度有効にします。「スタンバイ IP アドレスとインターフェイス モニタリングの設定（308 ページ）」を参照してください。

ネットワーク モジュールの取り外し

ネットワークモジュールを完全に削除する場合は、次の手順に従います。ネットワークモジュールを削除するには、再起動が必要です。

クラスタリングまたは高可用性の場合、制御ノード/アクティブユニットでのみシャーシの操作を実行できます。

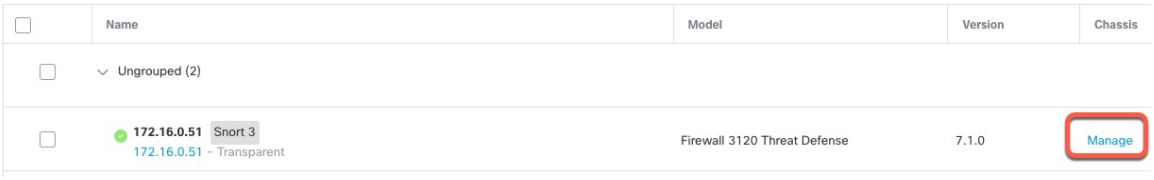
始める前に

クラスタリングまたは高可用性の場合は、クラスタ/フェールオーバーリンクがネットワークモジュール上にないことを確認してください。

手順

ステップ 1 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

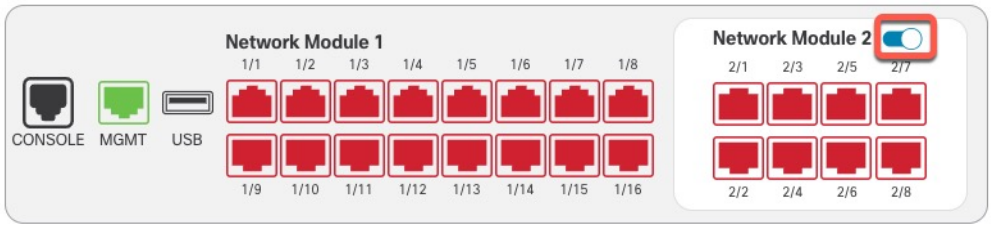
図 *234* : シャーシの管理



デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

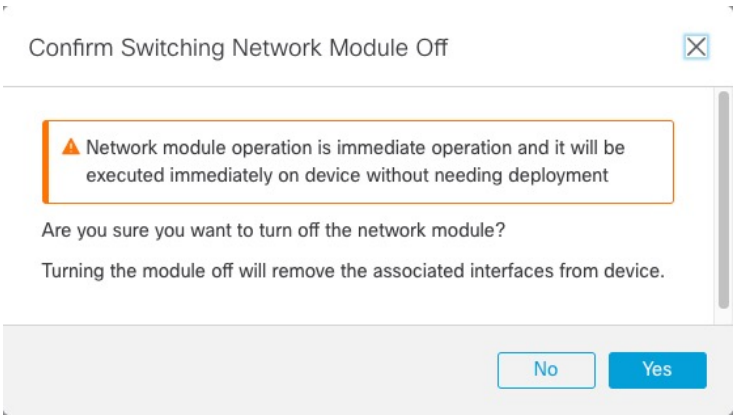
ステップ 2 インターフェイスのグラフィックで、スライダ（ ）をクリックしてネットワークモジュールを無効にします。

図 *235* : ネットワークモジュールの無効化



ステップ 3 ネットワークモジュールの無効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *236* : 無効化の確認

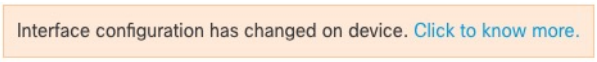


ステップ 4 画面の上部にメッセージが表示されます。リンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

図 *237 : [インターフェイス（Interface）] ページへの移動*

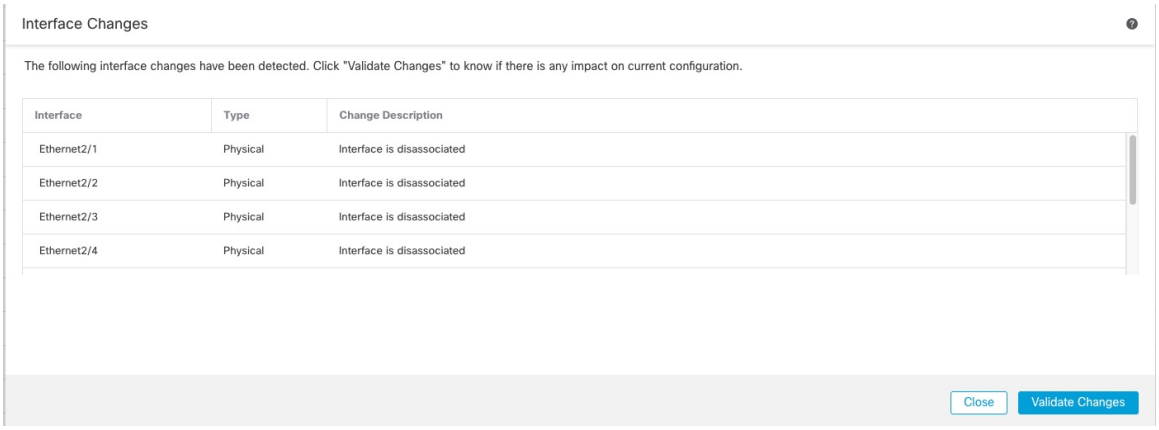
ステップ 5 [インターフェイス（Interfaces）] ページの上部に、インターフェイスの設定が変更されたことを示すメッセージが表示されます。

図 *238 : インターフェイスの変更の表示*



a) [クリックして詳細を表示（Click to know more）] をクリックします。[インターフェイスの変更（Interface Changes）] ダイアログボックスが開き、変更が表示されます。

図 *239 : インターフェイスの変更*



b) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与える場合があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

c) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。

ステップ 6 [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。

ステップ 7 構成を変更する必要があった場合は、**[展開（Deploy）] > [展開（Deployment）]** に移動してポリシーを展開します。

ステップ 8 ファイアウォールを再起動します。デバイスのシャットダウンまたは再起動 （41 ページ）を参照してください。

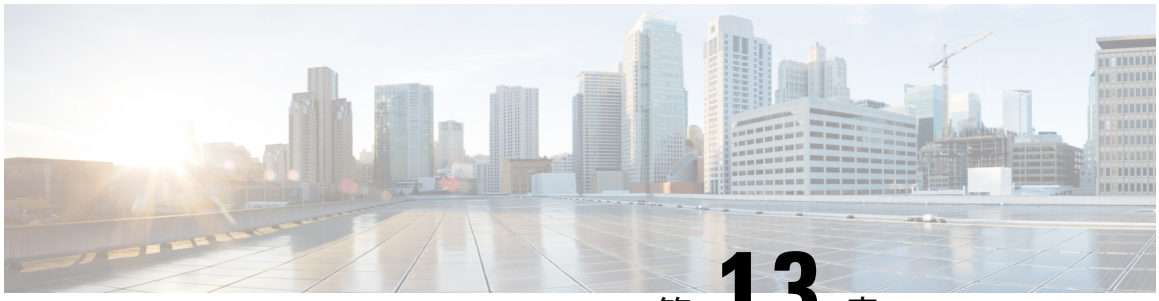
クラスタリングまたは高可用性の場合は、最初にデータノード/スタンバイユニットを再起動し、それらが復旧するのを待ちます。その後、制御ノード（制御ノードの変更 （360 ページ）を参照）またはアクティブユニット（Firewall Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替え （311 ページ）を参照）を変更し、以前の制御ノードまたはアクティブユニットを再起動できます。

インターフェイスの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Cisco Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正（FEC）が、25 GB+ SR、CSR、および LR トランシーバの第 74 条 FC-FEC から第 108 条 RS-FEC に変更されました。	7.2.4	7.2.4	Cisco Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB 以上の SR、CSR、および LR トランシーバのデフォルトタイプが第 74 条 FC-FEC ではなく第 108 条 RS-FEC に設定されるようになりました。
Firepower 2100、Cisco Secure Firewall 3100 で LLDP をサポート。	7.2.0	7.2.0	Firepower 2100 および Cisco Secure Firewall 3100 のインターフェイスで Link Layer Discovery Protocol（LLDP）を有効にすることができます。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [ネットワーク接続（Network Connectivity）]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Cisco Secure Firewall 3100のフロー制御に対応するためのフレームの一時停止	7.2.0	7.2.0	トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を抑制できます。 新規/変更された画面：**[デバイス（Devices）]>[デバイス管理（Device Management）]>[インターフェイス（Interfaces）]>[ハードウェア構成（Hardware Configuration）]>[ネットワーク接続（Network Connectivity）]**
Cisco Secure Firewall 3100 におけるネットワークモジュールのホットスワップのサポート	7.1.0	7.1.0	Cisco Secure Firewall 3100 では、ファイアウォールの電源がオンの状態でネットワークモジュールを追加または削除できます。モジュールを同じタイプの別のモジュールに交換する場合、再起動は必要ありません。最初の起動の後にモジュールを追加するか、モジュールを完全に削除するか、モジュールを新しいタイプのモジュールに交換する場合は、再起動が必要です。 新しい/変更された画面： [デバイス（Devices）]>[デバイス管理（Device Management）]>[シャーシの操作（Chassis Operations）]
Cisco Secure Firewall 3100における前方誤り訂正のサポート	7.1.0	7.1.0	Cisco Secure Firewall 3100 25 Gbps インターフェイスは、前方誤り訂正（FEC）をサポートします。FEC はデフォルトで有効になっており、[自動（Auto）] に設定されています。 新規/変更された画面：**[デバイス（Devices）]>[デバイス管理（Device Management）]>[インターフェイス（Interfaces）]>[インターフェイスの編集（Edit Interface）]>[ハードウェア構成（Hardware Configuration）] [速度（Speed）]**
Cisco Secure Firewall 3100 における SFP に基づく速度設定のサポート	7.1.0	7.1.0	Cisco Secure Firewall 3100 は、インストールされている SFP に基づくインターフェイスの速度検出をサポートします。SFP の検出はデフォルトで有効になっています。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。 新規/変更された画面：**[デバイス（Devices）]>[デバイス管理（Device Management）]>[インターフェイス（Interfaces）]>[インターフェイスの編集（Edit Interface）]>[ハードウェア構成（Hardware Configuration）] [速度（Speed）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firepower 1100 の LLDP サポート。	7.1.0	7.1.0	Firepower 1100 インターフェイスで Link Layer Discovery Protocol（LLDP）を有効にすることができます。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[ハードウェア構成（Hardware Configuration）]** > **[LLDP]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics**
インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになり、インターフェイスの同期が改善されました。	7.1.0	7.1.0	インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになりました。また、Firewall Management Center でインターフェイスを同期すると、ハードウェアの変更がより効果的に検出されます。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]** サポートされるプラットフォーム：Firepower 1000、2100、Cisco Secure Firewall 3100
Firepower 1100/2100 シリーズ ファイバ インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました。	6.7.0	6.7.0	フロー制御とリンク ステータス ネゴシエーションを無効化するように Firepower 1100/2100 シリーズ ファイバ インターフェイスを設定できるようになりました。 以前は、これらのデバイスでファイバインターフェイス速度（1000 または 10000 Mbps）を設定すると、フロー制御とリンク ステータス ネゴシエーションが自動的に有効になり、無効にはできませんでした。 [自動ネゴシエーション（Auto-negotiation）] の選択を解除し、速度を 1000 に設定してフロー制御とリンク ステータス ネゴシエーションを無効化できるようになりました。10000 Mbps でネゴシエーションを無効化することはできません。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [速度（Speed）]



第 13 章

通常のファイアウォール インターフェイス

この章では、 EtherChannel、VLAN サブインターフェイス、IP アドレスなどを含む通常のファイアウォール Firewall Threat Defense インターフェイスの設定について説明します。

（注） Firepower 4100/9300 の最初のインターフェイスの設定については、インターフェイスの設定（254 ページ）を参照してください。

- 通常のファイアウォール インターフェイスの要件と前提条件 （673 ページ）
- Firepower 1010 のスイッチポートの設定 （674 ページ）
- ループバック インターフェイスの設定 （686 ページ）
- VLAN サブインターフェイスと 802.1Q トランキングの設定 （692 ページ）
- VXLAN インターフェイスの設定 （697 ページ）
- ルーテッドモードとトランスペアレントモードのインターフェイスの設定 （713 ページ）
- 高度なインターフェイスの設定 （741 ページ）
- 通常のファイアウォール インターフェイスの履歴 （755 ページ）

通常のファイアウォールインターフェイスの要件と前提条件

モデルのサポート

Threat Defense

ユーザの役割

- 管理者
- アクセス管理者

- ネットワーク管理者

Firepower 1010 のスイッチポートの設定

Firepower 1010 の各インターフェイスは、通常のファイアウォール インターフェイスとしてまたはレイヤ2ハードウェア スイッチ ポートとして実行するように設定できます。この項では、スイッチ モードの有効化と無効化、VLAN インターフェイスの作成、そのインターフェイスのスイッチ ポートへの割り当てなど、スイッチ ポート設定を開始するためのタスクについて説明します。また、サポートされているインターフェイスで Power on Ethernet（PoE）をカスタマイズする方法についても説明します。

スイッチ ポートについて

この項では、Firepower 1010 のスイッチ ポートについて説明します。

スイッチポートおよびインターフェイスについて

ポートとインターフェイス

1010 の物理インターフェイスごとに、その動作をファイアウォール インターフェイスまたはスイッチポートとして設定できます。物理インターフェイスとポートタイプ、およびスイッチポートを割り当てる論理VLANインターフェイスについては、次の情報を参照してください。

- 物理ファイアウォールインターフェイス：ルーテッドモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ3のネットワーク間でトラフィックを転送します。トランスペアレントモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールサービスを適用することによって、レイヤ2の同じネットワーク上のインターフェイス間でトラフィックを転送するブリッジグループメンバーです。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとして、その他のインターフェイスでレイヤ3インターフェイスとして、統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット1/1インターフェイスはファイアウォールインターフェイスとして設定されます。また、これらのインターフェイスを IPS 専用（インラインセットとパッシブインターフェイス）に設定することもできます。

- 物理スイッチポート：スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。同じ VLAN 上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、Firewall Threat Defense セキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、それらを単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数のVLANに属することができます。デフォルトでは、イーサネット 1/2 ～ 1/8 は VLAN 1 のアクセススイッチポートとして設定され

ています。Diagnostic インターフェイスをスイッチポートとして設定することはできません。

- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、IPS 専用インターフェイス（インラインセットおよびパッシブインターフェイス）、または EtherChannel インターフェイスを作成できないという例外があります。スイッチポートが別のネットワークと通信する必要がある場合、Firewall Threat Defense デバイスは VLAN インターフェイスにセキュリティポリシーを適用し、別の論理 VLAN インターフェイスまたはファイアウォール インターフェイスにルーティングします。ブリッジグループメンバーとして VLAN インターフェイスで統合ルーティングおよびブリッジングを使用することもできます。同じ VLAN 上のスイッチポート間のトラフィックに Firewall Threat Defense セキュリティポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、ブリッジグループとスイッチポートを階層化して特定のセグメント間にセキュリティポリシーを適用できます。

Power Over Ethernet

PoE は、IEEE 802.3af（PoE）および 802.3at（PoE+）を使用して、イーサネット 1/7 およびイーサネット 1/8 でポートあたり最大 30 ワットまで供給できます。

PoE + では、リンク層検出プロトコル（Link Layer Discovery Protocol、LLDP）を使用して、電力レベルをネゴシエートします。電力は必要な場合にのみ提供されます。

インターフェイスをシャットダウンすると、デバイスへの電源がディセーブルになります。

Auto-MDI/MDIX 機能

すべてのスイッチポートで、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

スイッチポートの注意事項および制約事項

高可用性 とクラスタリング

- クラスタはサポートされません。
- 高可用性を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性は、トラフィックがスタンバイユニットを通過

するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の 高可用性 のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLANインターフェイスはフェールオーバーによってモニタできますが、スイッチポートはモニタできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、高可用性 を正常に使用することができますが、代わりに物理ファイアウォール インターフェイスを使用する設定の方が簡単です。

- ファイアウォールインターフェイスはフェールオーバーリンクとしてのみ使用できます。

論理 VLAN インターフェイス（SVI）

- 最大 60 個の VLAN インターフェイスを作成できます。
- また、ファイアウォール インターフェイスで VLAN サブインターフェイスを使用する場合、論理 VLAN インターフェイスと同じ VLAN ID は使用できません。
- MAC アドレス：
  - ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが 1 つの MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。MAC アドレスの設定 （749 ページ） を参照してください。
  - トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。MAC アドレスの設定 （749 ページ）を参照してください。

ブリッジ グループ

同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

VLAN インターフェイスおよびスイッチ ポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- 等コストマルチパス（ECMP）ルーティング
- インラインセットまたはパッシブインターフェイス
- EtherChannel：スイッチのポートを EtherChannel の一部にはできません。PoE も、EtherChannel のポートではサポートされません。

- フェールオーバーおよびステートリンク
- セキュリティグループタグ（SGT）

その他の注意事項と制約事項

- Firepower 1010 には、最大 60 個の名前付きインターフェイスを設定できます。
- Diagnostic インターフェイスをスイッチポートとして設定することはできません。

デフォルト設定

- イーサネット 1/1 はファイアウォール インターフェイスです。
- イーサネット 1/2 ～ 1/8 が、VLAN 1 に割り当てられたスイッチ ポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。

スイッチ ポートと Power Over Ethernet の設定

スイッチ ポートおよび PoE を設定するには、次のタスクを実行します。

スイッチ ポート モードの有効化または無効化

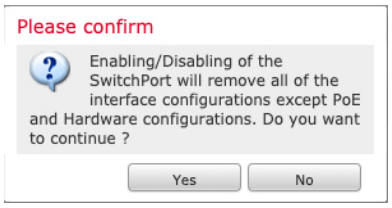
各インターフェイスは、ファイアウォール インターフェイスまたはスイッチ ポートのいずれかになるように個別に設定できます。デフォルトでは、イーサネット 1/1 はファイアウォール インターフェイスで、残りのイーサネット インターフェイスはスイッチ ポートとして設定されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 [スイッチポート（SwitchPort）] 列のスライダをクリックしてスイッチポートモードを設定すると、[有効なスライダ（Slider enabled）]（ ）または[無効なスライダ（Slider disabled）]（ ）と表示されます。

デフォルトでは、スイッチ ポートは VLAN 1 のアクセス モードに設定されています。トラフィックをルーティングし、Firewall Threat Defense セキュリティ ポリシーに参加するには、論理 VLAN 1 インターフェイス（またはこれらのスイッチ ポートに設定した任意の VLAN）を手動で追加する必要があります（VLAN インターフェイスの設定（678 ページ）を参照）。管理インターフェイスをスイッチポートモードに設定することはできません。スイッチ ポート モードを変更すると、サポートされていないすべての設定が削除されます。



さらに、インターフェイスがすでに有効になっている場合は、無効になります。インターフェイスを再度有効にしたことを確認してください。

VLAN インターフェイスの設定

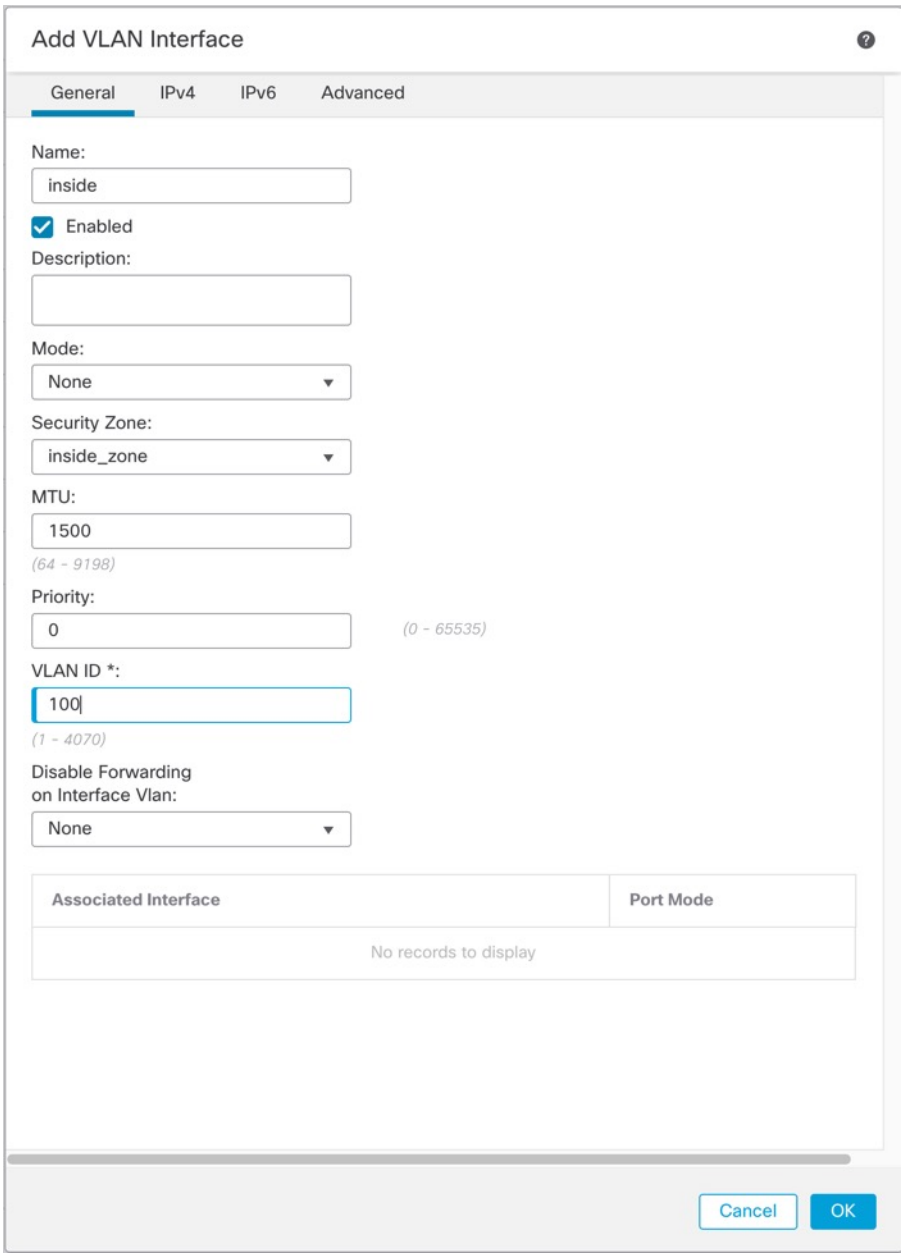
ここでは、関連付けられたスイッチポートで使用するための VLAN インターフェイスの設定方法について説明します。デフォルトでは、スイッチポートは VLAN1 に割り当てられます。トラフィックをルーティングし、Firewall Threat Defense セキュリティポリシーに参加するには、論理VLAN1インターフェイス（またはこれらのスイッチポートに設定した任意のVLAN）を手動で追加する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（ ） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 **[インターフェイスの追加（Add Interfaces）]** > **[VLANインターフェイス（VLAN Interface）]** をクリックします。

ステップ 3 [一般（General）] で、次の VLAN 固有のパラメータを設定します。



既存の VLAN インターフェイスを編集している場合、[関連付けられているインターフェイス（Associated Interface）] テーブルには、この VLAN のスイッチ ポートが表示されます。

a) [VLAN ID] を 1 ー 4070 の範囲に設定します。ただし、内部使用のために予約されている 3968 ー 4047 の範囲の ID は除きます。

インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

b) （任意）[インターフェイスVLANでの転送の無効化（Disable Forwarding on Interface VLAN）] の VLAN ID を選択し、別の VLAN への転送を無効にします。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。自宅のネットワークはビジネス ネットワークにアクセスする必要がないので、自宅の VLAN で転送を無効にできます。ビジネス ネットワークは自宅のネットワークにアクセスできますが、その反対はできません。

ステップ 4 インターフェイス設定を完了するには、次のいずれかの手順を参照してください。

- ルーテッド モードのインターフェイスの設定 （717 ページ）
- ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定 （724 ページ）

ステップ 5 **[OK]** をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

スイッチ ポートのアクセス ポートとしての設定

1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。アクセス ポートは、タグなしのトラフィックのみを受け入れます。では、イーサネット 1/2 ～ 1/8 は、デフォルトで VLAN 1 に割り当てられています。

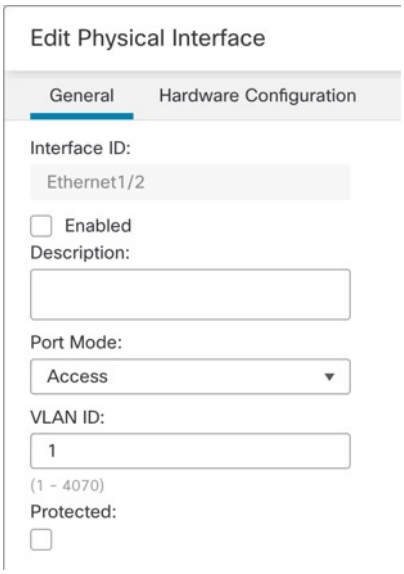
（注） デバイスは、ネットワーク内のループ検出に使用されるスパニングツリープロトコルをサポートしていません。したがって、Firewall Threat Defense とのすべての接続は、ネットワークループ内で終わらないようにする必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

図 *240* : 物理インターフェイスの編集



ステップ 3 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 4 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 [ポートモード（Port Mode）] を [アクセス（Access）] に設定します。

ステップ 6 [VLAN ID] フィールドで、このスイッチ ポートの VLAN を 1 ～ 4070 の範囲で設定します。

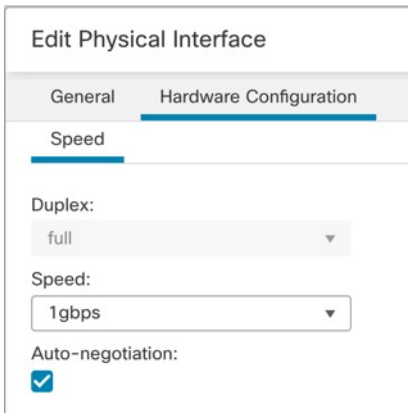
デフォルトの VLAN ID は 1 です。

ステップ 7 （任意） このスイッチ ポートを保護対象として設定するには、[保護済み（Protected）] チェックボックスをオンにします。これにより、スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信するのを防ぐことができます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチ ポートで [保護済み（Protected）] を有効にすると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 8 （任意） [ハードウェア構成（Hardware Configuration）] をクリックして、デュプレックスと速度を設定します。

図 *241* : ハードウェア構成



[自動ネゴシエーション（Auto-negotiation）] チェックボックス（デフォルト）をオンにして、速度とデュプレックスを自動検出します。このチェックボックスをオフにすると、速度とデュプレックスを手動で設定できます。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。
- [速度（Speed）] : [10mbps]、[100mbps]、または [1gbps] を選択します。

ステップ 9 **[OK]** をクリックします。

ステップ 10 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

スイッチ ポートのトランク ポートとしての設定

この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランクポートは、タグなしトラフィックとタグ付きトラフィックを受け入れます。許可された VLAN のトラフィックは、トランクポートを変更せずに通過します。

トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、ASA が正しいスイッチポートにトラフィックを転送したり、別のファイアウォールインターフェイスにルーティングしたりできるようにします。ASA は、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

図 *242*：トランクポートモードの設定

ステップ 3 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 4 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 [ポートモード（Port Mode）] を [トランク（Trunk）] に設定します。

ステップ 6 [ネイティブVLAN ID（Native VLAN ID）] フィールドで、このスイッチ ポートのネイティブ VLAN を 1 ～ 4070 の範囲で設定します。

デフォルトのネイティブVLANは1です。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

ステップ 7 [許可VLAN ID（Allowed VLAN IDs）] フィールドで、このトランク ポートの VLAN を 1 ～ 4070 の範囲で入力します。

次のいずれかの方法で最大 20 個の ID を指定できます。

- 単一の番号（n）
- 範囲（n-x）
- 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。

  5,7-10,13,45-100

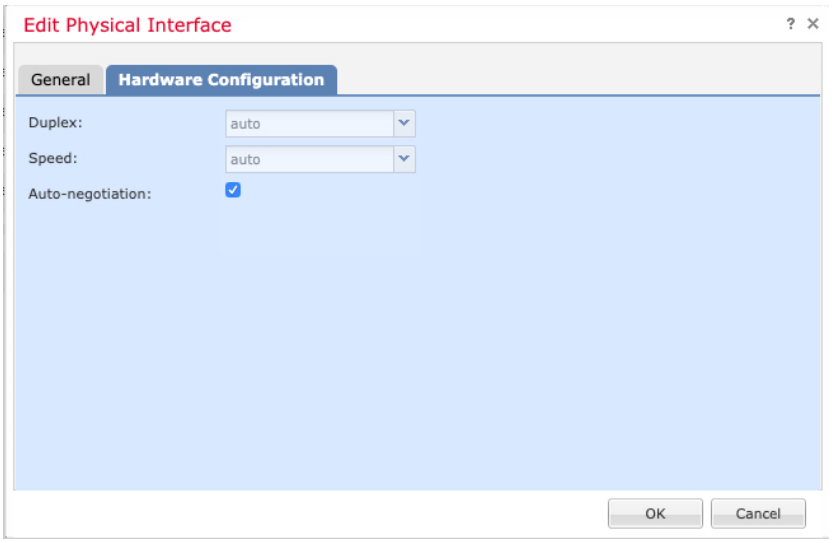
  カンマの代わりスペースを入力できます。

このフィールドにネイティブ VLAN を含めると、無視されます。トランクポートは、ネイティブ VLAN トラフィックをポートから送信するときに、常に VLAN タグを削除します。さらに、ネイティブ VLAN タグ付きのトラフィックは受信されません。

ステップ 8 （任意）このスイッチ ポートを保護対象として設定するには、[保護済み（Protected）] チェックボックスをオンにします。これにより、スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信するのを防ぐことができます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチ ポートで [保護済み（Protected）] を有効にすると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 9 （任意）[ハードウェア構成（Hardware Configuration）] をクリックして、デュプレックスと速度を設定します。



[自動ネゴシエーション（Auto-negotiation）] チェックボックス（デフォルト）をオンにして、速度とデュプレックスを自動検出します。このチェックボックスをオフにすると、速度とデュプレックスを手動で設定できます。

- [デュプレックス（Duplex）]：[全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。
- [速度（Speed）]：[10mbps]、[100mbps]、または [1gbps] を選択します。

ステップ 10 **[OK]** をクリックします。

ステップ 11 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

Power over Ethernet の設定

Power over Ethernet（PoE）ポートは、IP 電話や無線アクセスポイントなどのデバイスに電力を供給します。PoE はデフォルトでイネーブルです。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する方法について説明します。

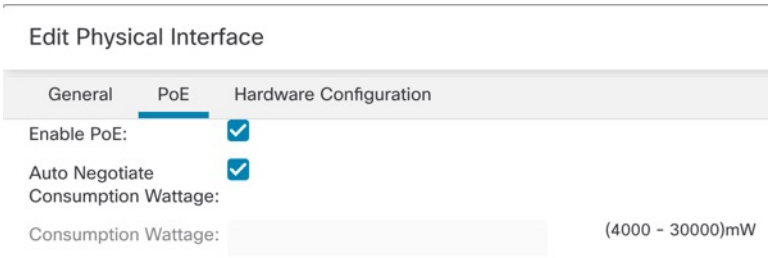
手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 の [編集（Edit）]（✎） をクリックします。

ステップ 3 [PoE] をクリックします。

図 *243 : PoE*



ステップ 4 [PoEを有効にする（Enable PoE）] チェックボックスをオンにします。

PoE はデフォルトでイネーブルです。

ステップ 5 自動ネゴシエーションまたは手動電源を選択します。

- **[消費ワット数の自動ネゴシエート（Auto Negotiate Consumption Wattage）]**：給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。ファイアウォールは LLDP を使用して、さらに適切なワット数をネゴシエートします。特定クラスのデバイスを接続すると、より多くの電力を使用する必要がある場合に備

えて、そのクラスの最大値までプロビジョニングが行われます。たとえば、12.95W を要求するクラス4デバイスを追加した場合、そのデバイスが現在その電力すべてを使用していなくても、30Wが割り当てられます。一部のデバイスは、電力要件を再ネゴシエートできます。デバイスに必要な電力が割り当てられている電力よりも少ないことがわかっている場合は、代わりに **[消費ワット数（Consumption Wattage）]** を手動で設定して、他のデバイス用に電力を解放できます。

- **[消費ワット数（Consumption Wattage）]**：**[消費ワット数の自動ネゴシエート（Auto Negotiate Consumption Wattage）]** チェックボックスをオフにして、手動ワット数を設定し、ワット数を（ミリワット単位）で4000～30000に手動で指定します。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。手動割り当ての場合、 **show power inline** 出力にクラスが **n/a** と表示されます。これは、クラスが消費電力の決定に使用されないためです。

  show power inline コマンドを使用して、現在の PoE ステータスを表示します。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ループバック インターフェイスの設定

ここでは、ループバック インターフェイスを設定する方法について説明します。

ループバック インターフェイスについて

ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア専用インターフェイスであり、複数の物理インターフェイスを介して IPv4 および IPv6 に到達できます。ループバック インターフェイスはパス障害の克服に役立ちます。任意の物理インターフェイスからアクセスできるため、1 つがダウンした場合、別のインターフェイスからループバック インターフェイスにアクセスできます。

ループバック インターフェイスは、次の目的で使用できます。

- スタティックおよびダイナミック VTI トンネル

Firewall Threat Defense は、ダイナミック ルーティング プロトコルを使用してループバックアドレスを配布できます。または、ピアデバイスでスタティックルートを設定して、 Firewall Threat Defense のいずれかの物理インターフェイスを介してループバック IP アドレスに到達できます。Firewall Threat Defense では、ループバック インターフェイスを指定するスタティックルートを設定できません。

関連トピック

ループバック インターフェイスのガイドラインと制限事項 （687 ページ）
ループバック インターフェイスの設定 （687 ページ）

ループバック インターフェイスのガイドラインと制限事項

ファイアウォール モード

- ルーテッド モードのみでサポートされます。

高可用性 とクラスタリング

- クラスタリングはサポートされません。

その他のガイドラインと制限事項

- 物理インターフェイスからループバック インターフェイスへのトラフィックでは、TCP シーケンスのランダム化は常に無効になっています。

ループバック インターフェイスの設定

デバイスのループバック インターフェイスを追加するには、次の手順を実行します。

手順

ステップ 1 **[デバイス（Devices）]>[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 [インターフェイスの追加（Add Interfaces）] ドロップダウンリストから、**[ループバックインターフェイス（Loopback Interface）]** を選択します。

ステップ 3 [一般（General）] タブで、次のパラメータを設定します。

a) [名前（Name）] : ループバック インターフェイスの名前を入力します。
b) [有効（Enabled）] : ループバック インターフェイスを有効にするには、このチェックボックスをオンにします。
c) [ループバック ID（Loopback ID）] : 1 ～ 1024 のループバック ID を入力します。
d) [説明（Description）] : ループバック インターフェイスの説明を入力します。

ステップ 4 ルーテッド モード インターフェイスのパラメータを設定します。「ルーテッド モードのインターフェイスの設定 （717 ページ）」を参照してください。

ループバック インターフェイスへのトラフィックのレート制限

始める前に

システムに過剰な負荷がかからないように、ループバック インターフェイス IP アドレスに送信されるトラフィックのレートを制限する必要があります。グローバルサービスポリシーに接続制限ルールを追加できます。

手順

ステップ 1 ループバック インターフェイス IP アドレスへのトラフィックを識別する拡張アクセスリストを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツテーブルから **[アクセスコントロールリスト（Access Control Lists）] > [拡張（Extended）]** を選択します。

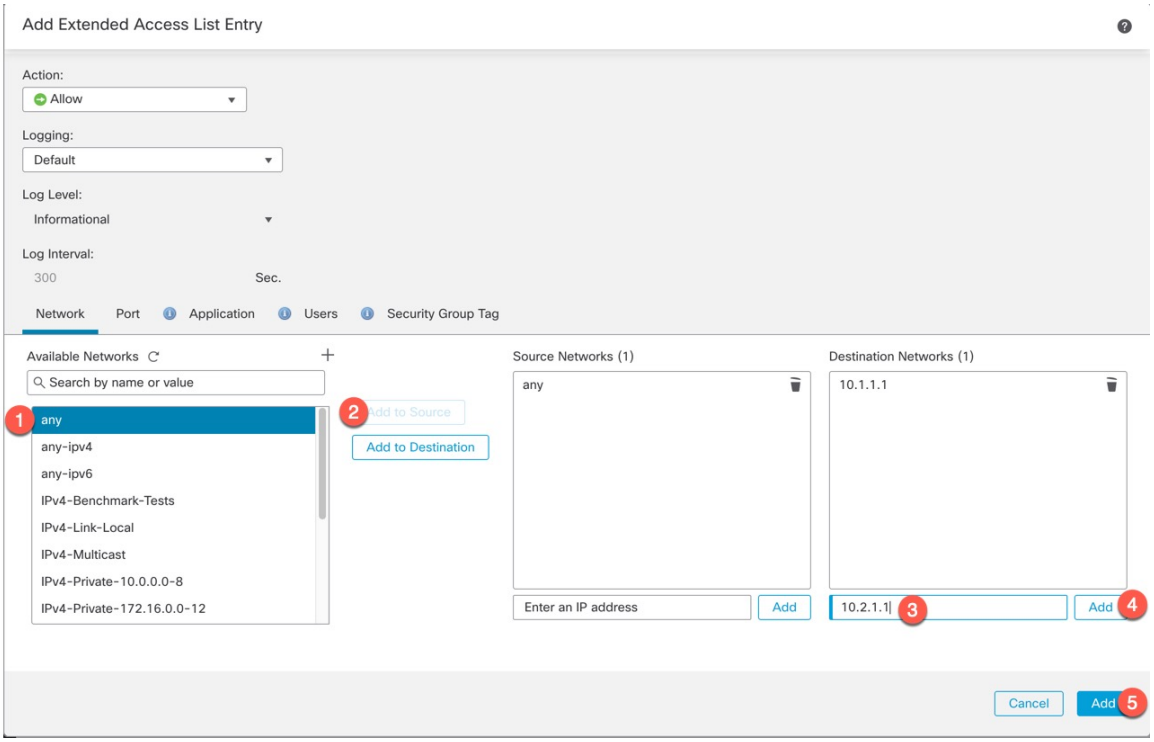
b) [拡張アクセスリストの追加（Add Extended Access List）] をクリックして、新しい ACL を作成します。

c) [新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] ダイアログボックスで、ACL の名前を入力し（スペースは使用不可）、[追加（Add）] をクリックして新しいエントリを作成します。

図 *244 : ACL* の命名とエントリの追加

d) [ネットワーク（Network）] タブで、送信元（任意）および宛先アドレス（ループバック IP アドレス）を設定します。

図 *245 :* 送信元と宛先のネットワーク

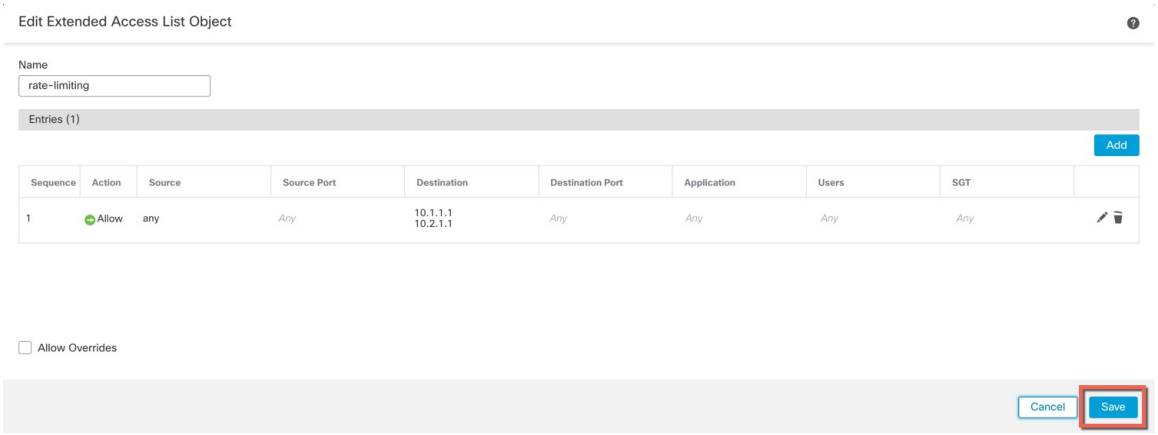


（注）
デフォルトの [アクション（Action）] は [許可（一致）（Allow (match)）] にし、その他の設定はそのままにします。

- [送信元（Source）] : [使用可能なネットワーク（Available Networks）] リストから **any** を選択し、[送信元に追加（Add to Source）] をクリックします。**any** の代わりに送信元 IP アドレスを指定して、このアクセスリストを絞り込むこともできます。
- [宛先（Destination）] : [宛先ネットワーク（Destination Networks）] リストの下の編集ボックスにアドレスを入力し、[追加（Add）] をクリックします。ループバックインターフェイスごとに手順を繰り返します。

e) [追加（Add）] をクリックして、エントリを ACL に追加します。
f) [保存（Save）] をクリックして、ACL を保存します。

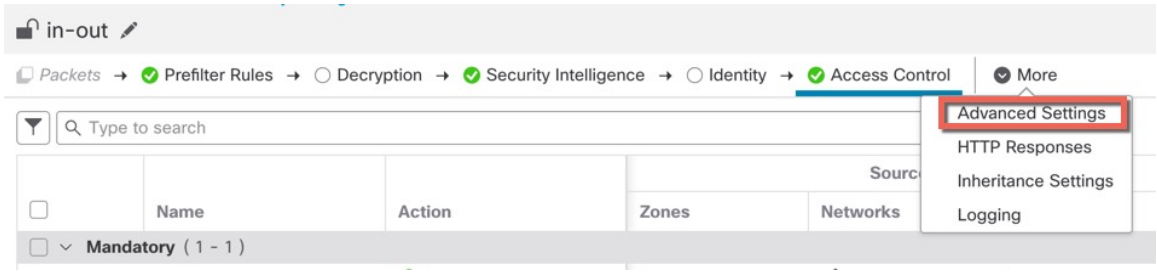
図 *246 : ACL* の保存



ステップ 2 **[ポリシー（Policy）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** の順に選択し、デバイスに割り当てられているアクセス コントロール ポリシーの [編集（Edit）]（✎） をクリックします。

ステップ 3 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。

図 *247 :* 詳細設定

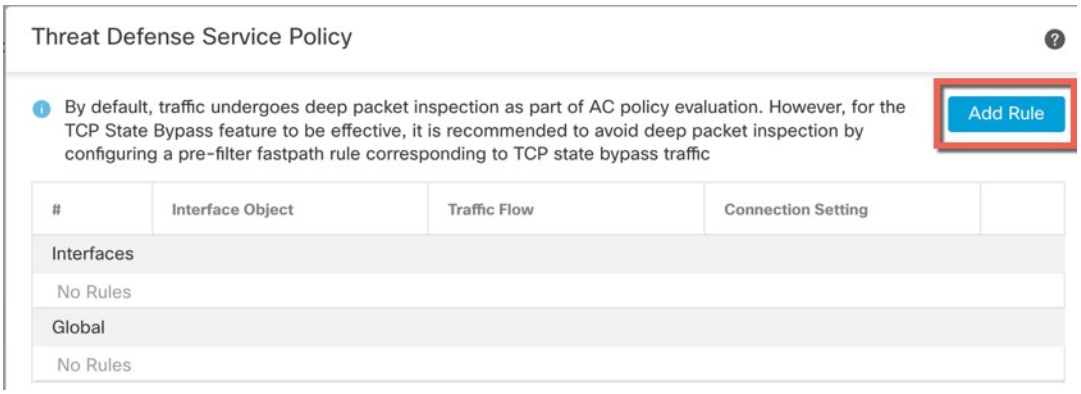


ステップ 4 [Threat Defenseサービスポリシー（Threat Defense Service Policy）] グループで [編集（Edit）]（✎） をクリックします。

図 *248 : Threat Defense* サービス ポリシー

ステップ 5 [ルールの追加（Add Rule）] をクリックして、新しいルールを作成します。

図 *249* : *[*ルールの追加（***Add Rule***）*]*



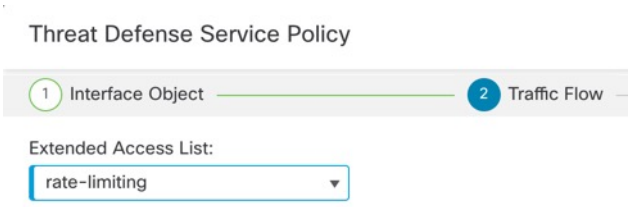
サービス ポリシー ルール ウィザードが開き、ルールの設定プロセスの手順が表示されます。

ステップ 6 [インターフェイス オブジェクト（Interface Object）] ステップで、[グローバル（Global）] をクリックしてすべてのインターフェイスに適用されるグローバルルールを作成し、[次へ（Next）] をクリックします。

図 *250* : グローバルポリシー

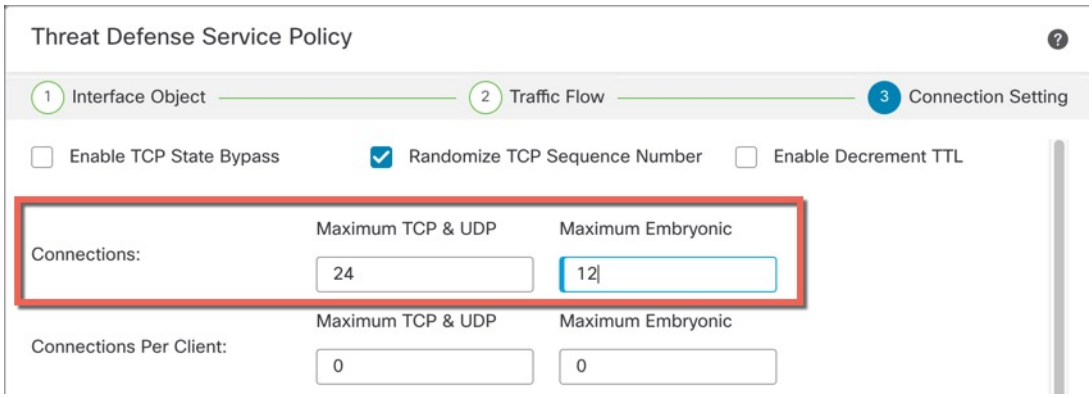
ステップ 7 [トラフィックフロー（Traffic Flow）] ステップで、ステップ 1 （688 ページ） で作成した拡張アクセスリストオブジェクトを選択し、[次へ（Next）] をクリックします。

図 *251* : 拡張アクセスリストの選択



ステップ 8 [接続設定（Connection Setting）] ステップで、[接続制限（Connections limit）] を設定します。

図 *252 :* 接続制限の設定



[最大TCPおよびUDP（Maximum TCP & UDP）] 接続数をループバック インターフェイスの予期される接続数に設定し、[最大初期接続数（Maximum Embryonic）] の接続数をそれよりも低い数に設定します。予期される必要なループバック インターフェイスセッション数に応じて、たとえば、5/2、10/5、または 1024/512 に設定できます。

初期接続制限を設定すると TCP 代行受信が有効になります。この代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃からシステムを保護します。

ステップ 9 [終了（Finish）] をクリックして変更を保存します。

ステップ 10 [OK] をクリックします。

ステップ 11 [詳細設定（Advanced Settings）] ウィンドウで [保存（Save）] をクリックします。

ステップ 12 これで、影響を受けるデバイスに変更を展開できます。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはデバイスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

VLAN サブインターフェイスのガイドラインと制限事項

モデルのサポート

- Firepower 1010：VLAN サブインターフェイスは、スイッチポートおよび VLAN インターフェイスではサポートされていません。

高可用性とクラスタリング

フェールオーバーリンクまたは状態リンクやクラスタ制御リンクのサブインターフェイスを使用することはできません。例外はマルチインスタンスモードの場合です。その場合、これらのリンクにはシャーシ定義サブインターフェイスを使用できます。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイスペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理、冗長、または EtherChannel インターフェイスを有効にする必要があるため、インターフェイスに名前を設定しないことでトラフィックを通過させないようにします。物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常通り名前を設定できます。
- CLI で設定された専用の管理インターフェイスでも、マネージャアクセスに使用されるデータインターフェイスでも、管理インターフェイスにサブインターフェイスを設定することはできません。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- Firewall Threat Defense はダイナミック トランキング プロトコル（DTP）をサポートしないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、Firewall Threat Defense で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、Firewall Threat Defense で特定のインスタンスでのトラフィックの中断を避けることができます。

（注） MAC アドレスを手動で割り当てる場合は、予期しない動作や停止を避けるために、同じ物理インターフェイス上のすべてのサブインターフェイスに MAC アドレスを割り当てるようにしてください。

デバイス モデルによる VLAN サブインターフェイスの最大数

デバイス モデルにより、設定できる VLAN サブインターフェイスの最大数が制限されます。データ インターフェイスでのみサブインターフェイスを設定することができ、管理インターフェイスでは設定できないことに注意してください。

次の表で、各デバイス モデルの制限について説明します。

モデル	VLAN サブインターフェイスの最大数
Firepower 1010	60
Firepower 1120	512
Firepower 1140、1150	1024
Firepower 2100	1024
Cisco Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
Firewall Threat Defense Virtual	50
ISA 3000	100

サブインターフェイスの追加

1 つ以上のサブインターフェイスを物理インターフェイス、冗長インターフェイス、または PortChannel インターフェイスに追加します。

Firepower 4100/9300 の場合、コンテナインターフェイスで使用するためのサブインターフェイスを FXOS で作成します。コンテナ インスタンスの VLAN サブインターフェイスの追加（258 ページ）を参照してください。これらのサブインターフェイスは Firewall Management Center のインターフェイスリストに表示されます。Firewall Management Center にサブインターフェイスを追加することもできますが、FXOS にサブインターフェイスが定義されていない親インターフェイス上に限ります。

（注） 親の物理インターフェイスがタグなしのパケットを渡します。タグなしのパケットを渡さない場合は、セキュリティ ポリシーの親インターフェイスが含まれていないことを確認します。

手順

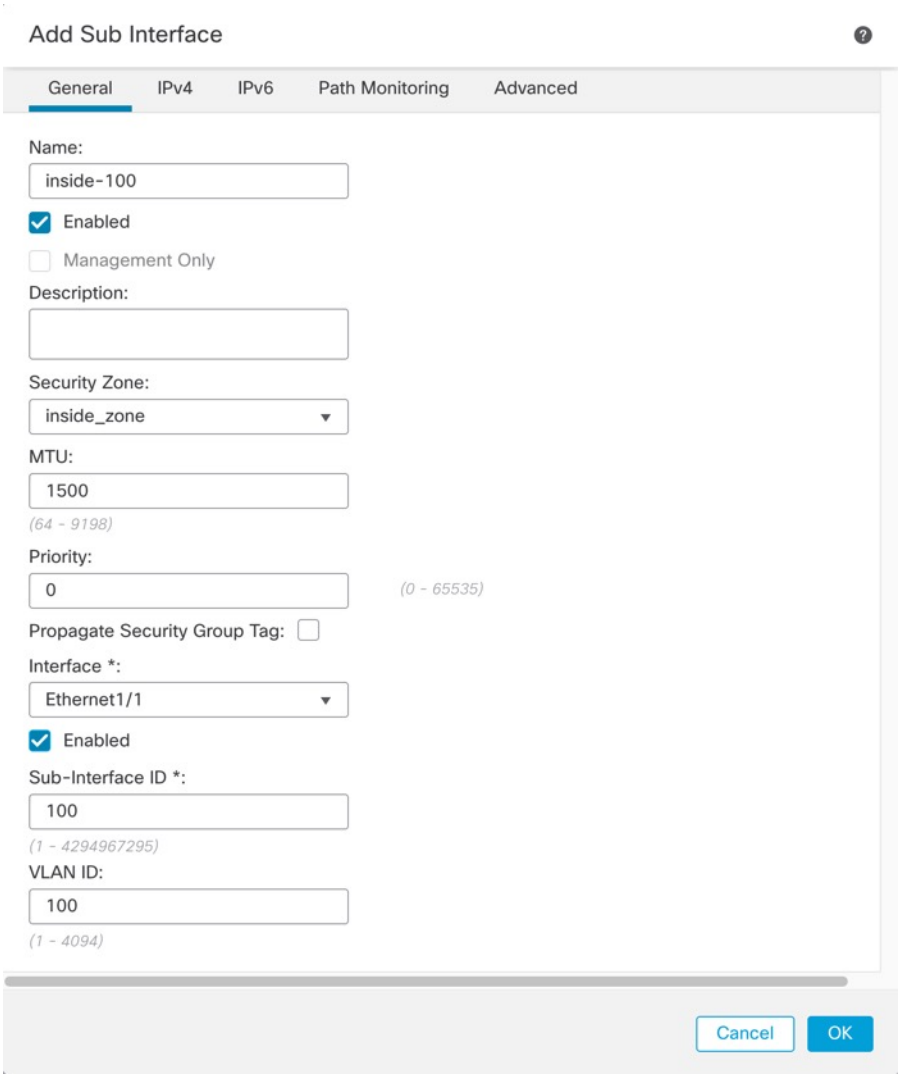
ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（ ） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 物理インターフェイスの有効化およびイーサネット設定の構成（635 ページ）に従って、親インターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）]** > **[サブインターフェイス（Sub Interface）]** をクリックします。

ステップ 4 [全般（General）] で、次のパラメータを設定します。

図 *253* : サブインターフェイスの追加



a) [インターフェイス（Interface）]：サブインターフェイスを追加する物理、冗長、またはポートチャネル インターフェイスを選択します。

b) [サブインターフェイス ID（Sub-Interface ID）]：サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

c) [VLAN ID]：VLAN ID を 1 ～ 4094 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。

この VLAN ID は一意である必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ステップ 7 ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッドモードのインターフェイスの設定（717ページ）またはブリッジグループインターフェイスの設定（724 ページ）を参照してください。

VXLAN インターフェイスの設定

この章では、仮想拡張 LAN（VXLAN）インターフェイスの設定方法について説明します。VXLAN インターフェイスは、レイヤ 2 ネットワークを拡張するために、レイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。

VXLAN インターフェイスについて

VXLAN は、VLAN の場合と同じイーサネットレイヤ 2 ネットワークサービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナントセグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント（最大 1600 万の VXLAN セグメント）に対応するための高度なスケーラビリティ。

ここでは、VXLAN の動作について説明します。VXLAN の詳細については、RFC 7348 を参照してください。Geneve の詳細については、RFC 8926 を参照してください。

カプセル化

Firewall Threat Defense は、次の 2 種類の VXLAN カプセル化をサポートしています。

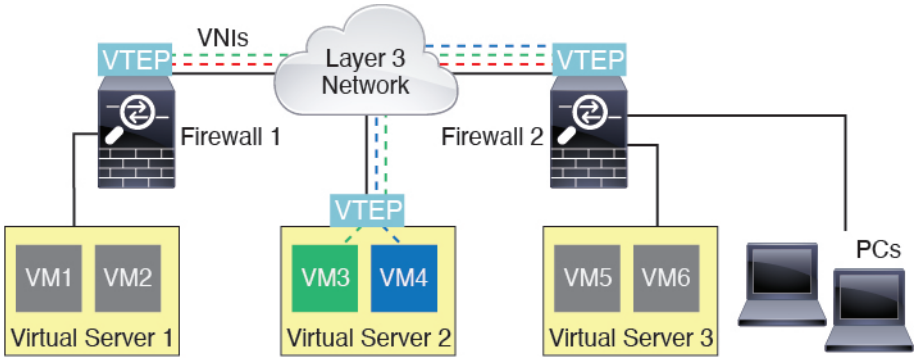
- VXLAN（すべてのモデル）：VXLAN は、MAC Address-in-User Datagram Protocol（MAC-in-UDP）のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。
- Geneve（Firewall Threat Defense Virtual のみ）：Geneve には、MAC アドレスに限定されない柔軟な内部ヘッダーがあります。Geneve カプセル化は、Amazon Web Services（AWS）ゲートウェイロードバランサとアプライアンス間のパケットの透過的なルーティング、および追加情報の送信に必要です。

VXLAN トンネル エンドポイント

VXLAN トンネルエンドポイント（VTEP）デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイス タイプ（セキュリティ ポリシーを適用する VXLAN Network Identifier（VNI）インターフェイスと呼ばれる 1 つ以上の仮想イン

ターフェイスと、 VTEP 間に VNI をトンネリングする VTEP 送信元インターフェイスと呼ばれる通常のインターフェイス）があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

次の図は、2 つの Firewall Threat Defense と、レイヤ 3 ネットワークを介して VTEP として機能し、サイト間の VNI 1、2、3 を拡張する仮想サーバ 2 を示します。Firewall Threat Defense は、VXLAN ネットワークと非 VXLAN ネットワーク間のブリッジまたはゲートウェイとして機能します。



VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。VXLAN カプセル化の場合：宛先 IP アドレスは、リモート VTEP が不明な場合、マルチキャストグループにすることができます。Geneve では、Firewall Threat Defense はスタティックピアのみをサポートします。デフォルトでは、 VXLAN の宛先ポートは UDP ポート 4789 です（ユーザーが設定可能）。Geneve の宛先ポートは 6081 です。

VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、すべての VNI インターフェイスに関連付けられる通常のインターフェイス（物理、EtherChannel、または VLAN）です。Firewall Threat Defense Virtual ごとに 1 つの VTEP 送信元インターフェイスを設定できます。設定できる VTEP 送信元インターフェイスは 1 つだけであるため、VXLAN インターフェイスと Geneve インターフェイスの両方を同じデバイスに設定することはできません。AWS または Azure での Firewall Threat Defense Virtual クラスタリングには例外があり、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、Geneve（AWS）または VXLAN（Azure）インターフェイスはゲートウェイロードバランサに使用できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティ ポリシーを適用できます。ただし、VXLAN トラフィックの場合は、すべてのセキュリティポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレントファイアウォールモードでは、VTEP 送信元インターフェイスは、BVI の一部ではないため、その IP アドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワーク トラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティ ポリシーを直接適用します。

追加できる VTEP インターフェイスは 1 つだけで、すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。AWS または Azure での Firewall Threat Defense Virtual クラスタリングには例外があります。AWS クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、Geneve インターフェイスは AWS ゲートウェイロードバランサに使用できます。Azure クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、2 つ目の VXLAN インターフェイスは Azure ゲートウェイロードバランサに使用できます。

VXLAN パケット処理

VXLAN

VTEP 送信元インターフェイスを出入りするトラフィックは、VXLAN 処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP送信元インターフェイスにより、VXLANヘッダーが含まれている内部MACフレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP がリモート VTEP IP ルックアップによって決定されます。

カプセル化解除については、次の場合に Firewall Threat Defense によって VXLAN パケットのみがカプセル化解除されます。

- これが、宛先ポートが 4789 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- VXLAN パケット形式が標準に準拠します。

Geneve

VTEP送信元インターフェイスを出入りするトラフィックは、Geneve処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP 送信元インターフェイスにより、Geneve ヘッダーが含まれている内部 MAC フレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP には、設定したピア IP アドレスが設定されます。

カプセル化解除については、次の場合に ASA によって Geneve パケットのみがカプセル化解除されます。

- これが、宛先ポートが 6081 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- Geneve パケット形式が標準に準拠します。

ピア VTEP

Firewall Threat Defense がピア VTEP の背後にあるデバイスにパケットを送信する場合、Firewall Threat Defense には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

Firewall Threat Defense は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

VXLAN ピア

Firewall Threat Defense がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを Firewall Threat Defense に静的に設定できます。

  Firewall Threat Defense が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンドノードの MAC アドレスを取得します。

- ピア VTEP IP アドレスのグループを Firewall Threat Defense に静的に設定できます。

  Firewall Threat Defense が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンドノードの MAC アドレスを取得します。

- マルチキャスト グループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

  Firewall Threat Defense は、IP マルチキャストパケット内の VXLAN カプセル化 ARP ブロードキャストパケットを VTEP 送信元インターフェイスを経由して送信します。この ARP

要求への応答により、Firewall Threat Defense はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

このオプションは、Geneve ではサポートされていません。

Geneve ピア

Firewall Threat Defense Virtual は、静的に定義されたピアのみをサポートします。AWS ゲートウェイロードバランサで Firewall Threat Defense Virtual ピアの IP アドレスを定義できます。Firewall Threat Defense Virtual はゲートウェイロードバランサへのトラフィックを開始しないため、Firewall Threat Defense Virtual でゲートウェイロードバランサの IP アドレスを指定する必要はありません。Geneve トラフィックを受信すると、ピア IP アドレスを学習します。マルチキャストグループは、Geneve ではサポートされていません。

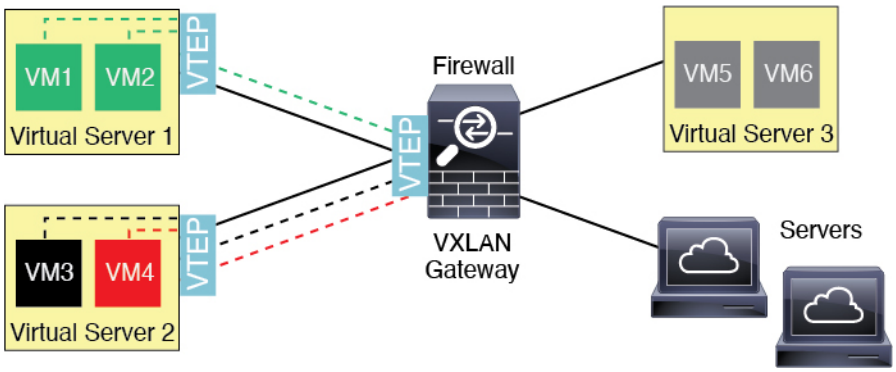
VXLAN 使用例

ここでは、Firewall Threat Defense での VXLAN の実装の使用例について説明します。

VXLAN ブリッジまたはゲートウェイの概要

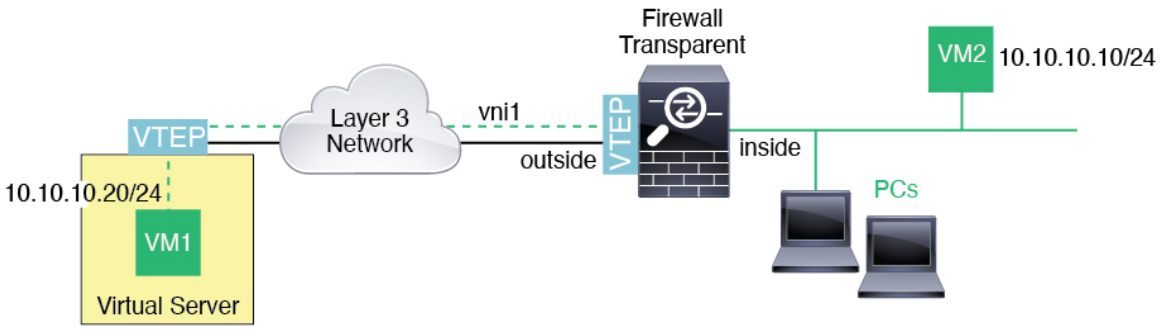
各 Firewall Threat Defense の VTEP は、VM、サーバ、PC、VXLANのオーバーレイ ネットワークなどのエンド ノード間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイスを介して VXLAN カプセル化で受信した受信フレームの場合、Firewall Threat Defense は VXLAN ヘッダーを除去して、内部イーサネット フレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続されている物理インターフェイスに転送します。

Firewall Threat Defense は、常に VXLAN パケットを処理します。つまり、他の 2 つの VTEP 間で VXLAN パケットをそのまま転送する訳ではありません。



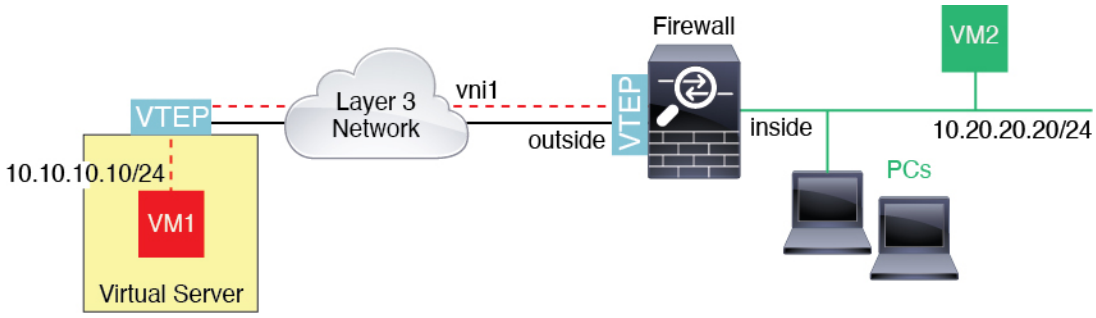
VXLAN ブリッジ

ブリッジグループ（トランスペアレント ファイアウォール モードまたは任意ルーテッドモード）を使用する場合、Firewall Threat Defense は、同じネットワークに存在する（リモート）VXLAN セグメントとローカルセグメント間の VXLAN ブリッジとして機能できます。この場合、ブリッジグループのメンバーは通常インターフェイス 1 つのメンバーが通常のインターフェイスで、もう 1 つのメンバーが VNI インターフェイスです。



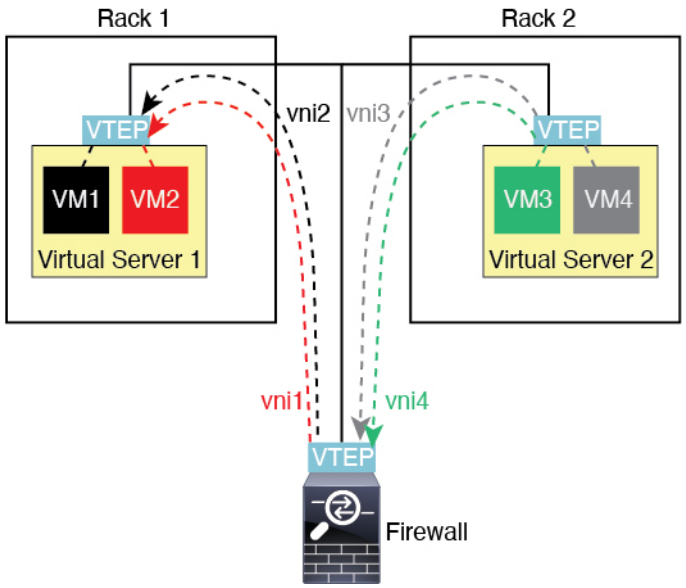
VXLAN ゲートウェイ（ルーテッド モード）

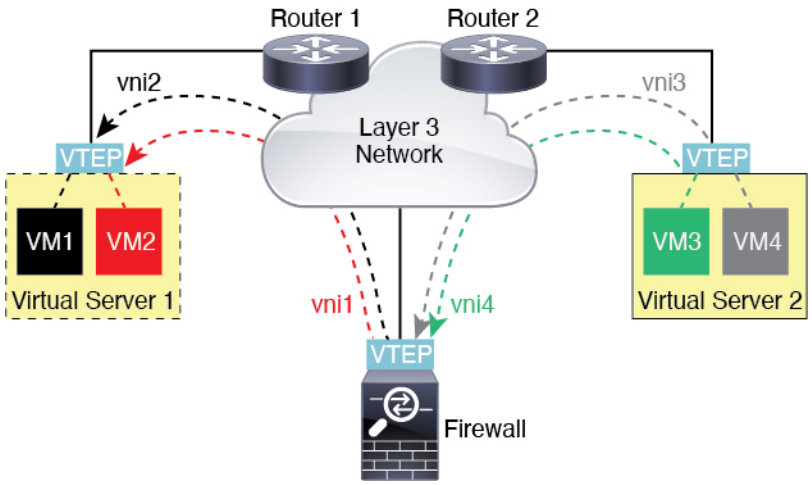
Firewall Threat Defense は、VXLAN ドメインと非 VXLAN ドメイン間のルータとして機能し、異なるネットワーク上のデバイスを接続します。



VXLAN ドメイン間のルータ

VXLAN 拡張 レイヤ 2 ドメインを使用すると、VM は、Firewall Threat Defense が同じラックにないとき、あるいは Firewall Threat Defense がレイヤ 3 ネットワーク上の離れた場所にあるときにsのゲートウェイとして Firewall Threat Defense を指し示すことができます。





このシナリオに関する次の注意事項を参照してください。

1. VM3 から VM1 へのパケットでは、Firewall Threat Defense がデフォルトゲートウェイであるため、宛先 MAC アドレスは Firewall Threat Defense の MAC アドレスです。
2. 仮想サーバー 2 の VTEP 送信元インターフェイスは、VM3 からパケットを受信してから、VNI 3 の VXLAN タグでパケットをカプセル化して Firewall Threat Defense に送信します。
3. Firewall Threat Defense は、パケットを受信すると、そのパケットをカプセル化解除して内部フレームを取得します。
4. Firewall Threat Defense は、ルート ルックアップに内部フレームを使用して、宛先が VNI 2 上であることを認識します。VM1 のマッピングがまだない場合、Firewall Threat Defense は、VNI 2 カプセル化された ARP ブロードキャストを VNI 2 のマルチキャスト グループ IP で送信します。

（注） このシナリオでは複数の VTEP ピアがあるため、Firewall Threat Defense は、複数のダイナミック VTEP ピア ディスカバリを使用する必要があります。

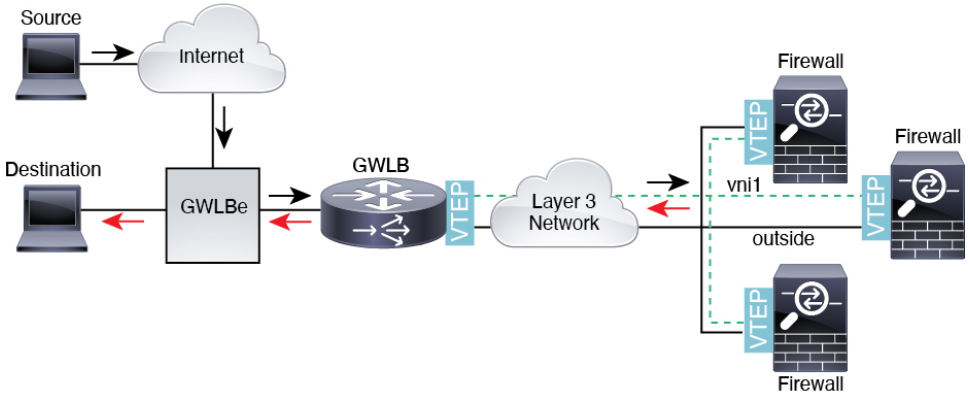
5. Firewall Threat Defense は、VNI 2 の VXLAN タグでパケットを再度カプセル化し、仮想サーバ 1 に送信します。カプセル化の前に、Firewall Threat Defense は、内部フレームの宛先 MAC アドレスを変更して VM1 の MAC にします（Firewall Threat Defense で VM1 の MAC アドレスを取得するためにマルチキャスト カプセル化 ARP が必要な場合があります）。
6. 仮想サーバー 1 は、VXLAN パケットを受信すると、パケットをカプセル化解除して内部フレームを VM1 に配信します。

Geneve シングルアームプロキシの使用例

（注） この使用例は、現在サポートされている Geneve インターフェイスの唯一の使用例です。

AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。Firewall Threat Defense Virtual は、分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。次の図は、ゲートウェイロードバランサのエンドポイントからゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の Firewall Threat Defense Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、ゲートウェイロードバランサに送り返す（U ターントラフィック）前に検査します。ゲートウェイロードバランサは、トラフィックをゲートウェイロードバランサのエンドポイントと宛先に送り返します。

図 *254 : Geneve* シングルアームプロキシ

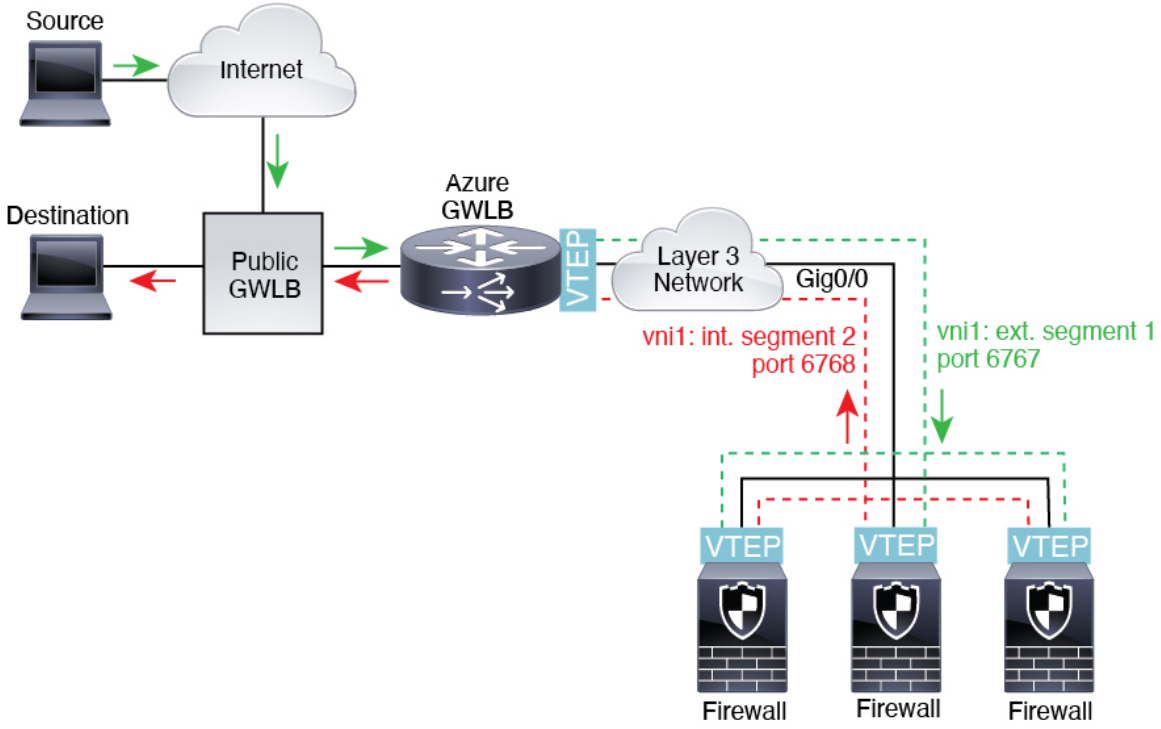


Azure ゲートウェイロードバランサおよびペアプロキシ

Azure サービスチェーンでは、Firewall Threat Defense Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。Firewall Threat Defense Virtual は、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

次の図は、外部 VXLAN セグメント上のパブリックゲートウェイロードバランサから Azure ゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の Firewall Threat Defense Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、外部 VXLAN セグメント上のゲートウェイロードバランサに送り返す前に検査します。Azure ゲートウェイロードバランサは、トラフィックをパブリックゲートウェイロードバランサと宛先に送り返します。

図 *255 :* ペアリングされたプロキシを使用した *Azure Gateway* ロードバランサ



VXLAN インターフェイスの要件と前提条件

モデルの要件

- VXLAN カプセル化は、すべてのモデルでサポートされます。
- Geneve カプセル化は、次のモデルでサポートされます。
  - Amazon Web Services（AWS）の Firewall Threat Defense Virtual
- ペアプロキシモードの VXLAN は、次のモデルでサポートされています。
  - Azure の Firewall Threat Defense Virtual
- Firepower 1010：スイッチポートおよび VLAN インターフェイスは、VTEP インターフェイスとしてサポートされていません。

VXLAN インターフェイスのガイドライン

ファイアウォール モード

- Geneve インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。
- ペアプロキシの VXLAN インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。

IPv6

- VNI インターフェイスは、IPv4 と IPv6 の両方のトラフィックをサポートします。
- VTEP 送信元インターフェイス IP アドレスは、IPv4 のみをサポートします。

クラスタ

- クラスタリングは、クラスタ制御リンク（Firewall Threat Defense Virtual のみ）を除いて、個別インターフェイスモードの VXLAN をサポートしていません。スパンド EtherChannel モードだけが VXLAN をサポートしています。

  GWLB で使用する追加の Geneve インターフェイスを使用できる AWS と、GWLB で使用する追加のペアプロキシの VXLAN インターフェイスを使用できる Azure の場合は例外です。

Routing

- VNI インターフェイスでは、スタティック ルーティングまたはポリシー ベース ルーティングのみをサポートします。ダイナミック ルーティング プロトコルはサポートされません。

VPN

VPN に VTEP 送信元インターフェイスを構成したり、VTI として使用したりすることはできません。

MTU

- VXLAN カプセル化：送信元インターフェイスの MTU が 1,554 バイト未満の場合、Firewall Threat Defense は自動的に MTU を 1,554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU + 54 バイトに設定する必要があります。Firewall Threat Defense Virtual の場合、この MTU は、ジャンボフレーム予約を有効にするためにリスタートする必要があります。

- Geneve カプセル化：送信元インターフェイスの MTU が 1,806 バイト未満の場合、Firewall Threat Defense は自動的に MTU を 1,806 バイトに増やします。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU＋306 バイトに設定する必要があります。この MTU は、ジャンボフレーム予約を有効にするためにリスタートする必要があります。

VXLAN または Geneve インターフェイスの設定

VXLAN または Geneve インターフェイスを設定できます。

VXLAN インターフェイスの設定

VXLAN を設定するには、次の手順を実行します。

（注） VXLAN または Geneve を設定できます（Firewall Threat Defense Virtual のみ）。Geneve インターフェイスについては、Geneve インターフェイスの設定 （710 ページ）を参照してください。

（注） Azure GWLB の場合、ARM テンプレートを使用して VM を展開するときに、VXLAN インターフェイスが設定されます。このセクションを使用して、設定を変更できます。

1. VTEP 送信元インターフェイスの設定 （707 ページ）。
2. VNI インターフェイスの設定 （709 ページ）。
3. （Azure GWLB）ゲートウェイロードバランサのヘルスチェックの許可 （712 ページ）。

VTEP 送信元インターフェイスの設定

Firewall Threat Defense デバイスごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。VXLAN は、デフォルトのカプセル化タイプです。Azure のFirewall Threat Defense Virtual でのクラスタリングには例外があり、1 つの VTEP ソースインターフェイスをクラスタ制御リンクに使用し、2 つ目のソースインターフェイスを Azure GWLB に接続されたデータインターフェイスに使用できます。

手順

ステップ 1 ピア VTEP のグループを指定する場合は、ピア IP アドレスを持つネットワークオブジェクトを追加します。ネットワーク オブジェクトの作成 （1351 ページ） を参照してください。

ステップ 2 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 3 VXLAN を設定するデバイスの横にある [編集（Edit）]（） をクリックします。

ステップ 4 （任意） 送信元インターフェイスが NVE 専用であることを指定します。

ルーテッドモードでは、この設定はオプションです。設定した場合、トラフィックはこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されます。トランスペアレント ファイアウォール モードでは、この設定は自動的に有効になります。

a) [インターフェイス（Interfaces）] をクリックします。

b) VTEP 送信元インターフェイスの [編集（Edit）]（） をクリックします。

c) [全般（General）] ページで、[NVEのみ（NVE Only）] チェックボックスをオンにします。

ステップ 5 まだ表示されていない場合は、[VTEP] をクリックします。

ステップ 6 [NVEの有効化（Enable NVE）] をオンにします。

ステップ 7 [VTEPの追加（Add VTEP）] をクリックします。

ステップ 8 [カプセル化タイプ（Encapsulation Type）] で、[VxLAN] を選択します。

AWS の場合、[VxLAN] と [Geneve] のどちらかを選択できます。他のプラットフォームでは、[VxLAN] が自動的に選択されます。

ステップ 9 [カプセル化ポート（Encapsulation port）] に指定された範囲内で値を入力します。

デフォルト値は 4789 です。

ステップ 10 [VTEP送信元インターフェイス（VTEP Source Interface）] を選択します。

デバイス上にある使用可能な物理インターフェイスのリストから選択します。送信元インターフェイスの MTU が 1554 バイト未満の場合、Firewall Management Center は自動的に MTU を 1554 バイトに増やします。

ステップ 11 [ネイバーアドレス（Neighbor Address）] を選択します。次のオプションを使用できます。

- [なし（None）]：ネイバーアドレスを指定しません。
- [ピアVTEP（Peer VTEP）]：ピア VTP アドレスを指定します。
- [ピアグループ（Peer Group ）]：ピア IP アドレスを持つネットワークオブジェクトを指定します。
- [デフォルトマルチキャスト（Default Multicast）]：関連するすべての VNI インターフェイスのデフォルト マルチキャスト グループを指定します。VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

ステップ 12 [OK] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

ステップ 14 ルーテッドインターフェイスのパラメータを設定します。「ルーテッドモードのインターフェイスの設定」を参照してください。

VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

Azure Firewall Threat Defense Virtual の場合、通常の VXLAN インターフェイスを設定するか、Azure GWLB で使用するペアプロキシモードの VXLAN インターフェイスを設定できます。ペアプロキシモードは、クラスタリングでサポートされる唯一のモードです。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 2 VXLAN を設定するデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [インターフェイスの追加（Add Interfaces）] をクリックし、[VNIインターフェイス（VNI Interface）] を選択します。

ステップ 5 [名前（Name）] と [説明（Description）] にインターフェイスの名前と説明をそれぞれ入力します。.

ステップ 6 [セキュリティゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティゾーンを追加します。

ステップ 7 指定された範囲内で、[優先度（Priority）] フィールドの値を入力します。デフォルトでは、0 が選択されています。

ステップ 8 [VNI ID] には 1 ～ 10000 の間で値を入力します。

この ID は内部インターフェイス識別子です。

ステップ 9 （Azure GWLB のペアプロキシ VXLAN）プロキシペアモードを有効にして、必要なパラメータを設定します。

a) **プロキシのペアリング**を確認します。
b) **内部ポート**を 1024 ～ 65535 に設定します。
c) **内部セグメント ID** を 1 ～ 16777215 の範囲で設定します。
d) **外部ポート**を 1024 ～ 65535 に設定します。
e) **外部セグメント ID** を 1 ～ 16777215 の範囲で設定します。

ステップ 10 （通常の VXLAN）**[VNIセグメントID（VNI Segment ID）]** には 1 ～ 16777215 の間の値を入力します。

セグメント ID は VXLAN タギングに使用されます。

ステップ 11 [マルチキャストグループアドレス（Multicast Group IP Address）] を入力します。

VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP 送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。

ステップ 12 [VTEPインターフェイスにマッピングされているNVE（NVE Mapped to VTEP Interface）] をオンにします。

このオプションにより、インターフェイスがVTEP送信元インターフェイスに関連付けられます。

ステップ 13 [OK] をクリックします。

ステップ 14 [保存（Save）] をクリックして、インターフェイス設定を保存します。

ステップ 15 ルーテッドまたはトランスペアレント インターフェイスのパラメータを設定します。「ルーテッド モードとトランス ペアレント モードのインターフェイスの設定 （713 ページ）」を参照してください。

Geneve インターフェイスの設定

Firewall Threat Defense Virtual の Geneve インターフェイスを設定するには、次の手順を実行します。

（注） VXLAN または Geneve を設定できます。VXLAN インターフェイスの詳細については、「VXLAN インターフェイスの設定 （707 ページ）」を参照してください。

1. VTEP 送信元インターフェイスの設定 （710 ページ）。
2. VNI の設定 （711 ページ）。
3. ゲートウェイロードバランサのヘルスチェックの許可 （712 ページ）。

VTEP 送信元インターフェイスの設定

Firewall Threat Defense Virtual デバイスごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 2 Geneve を設定するデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [VTEP] をクリックします。

ステップ 4 [NVEの有効化（Enable NVE）] をオンにします。

ステップ 5 [VTEPの追加（Add VTEP）] をクリックします。

ステップ 6 [カプセル化タイプ（Encapsulation Type）] で、[Geneve] を選択します。

ステップ 7 [カプセル化ポート（Encapsulation port）] に指定された範囲内で値を入力します。

[Geneveポート（Geneve Port）] を変更することは推奨しません。AWS にはポート 6081 が必要です。

ステップ 8 [VTEP送信元インターフェイス（VTEP Source Interface）] を選択します。

デバイス上にある使用可能な物理インターフェイスのリストから選択できます。送信元インターフェイスの MTU が 1806 バイト未満の場合、Firewall Management Center は自動的に MTU を 1806 バイトに増やします。

ステップ 9 [OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 ルーテッドインターフェイスのパラメータを設定します。「ルーテッドモードのインターフェイスの設定」を参照してください。

VNI の設定

VNI を追加し、その VNI を（VTEP）送信元インターフェイスに関連付けて、基本インターフェイスパラメータを設定します。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 2 Geneve を設定するデバイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [インターフェイスの追加（Add Interfaces）] をクリックし、[VNIインターフェイス（VNI Interface）] を選択します。

ステップ 5 [名前（Name）] フィールドと [説明（Description）] フィールドに、関連情報を入力します。

ステップ 6 [VNI ID] フィールドには 1 ～ 10000 の値を入力します。

（注）
この ID は内部インターフェイス識別子です。

ステップ 7 [プロキシの有効化（Enable Proxy] チェックボックスをオンにします。

（注）
デバイスの VNI インターフェイスで AWS プロキシが有効になっている場合、NAT の設定は許可されません。

このオプションにより、シングルアームプロキシが有効になり、トラフィックは入ったときと同じインターフェイスから出ることができます（U ターントラフィック）。後でインターフェ

イスを編集する場合、シングルアームプロキシを無効にすることはできません。無効にするには、既存のインターフェイスを削除して、新しい VNI インターフェイスを作成する必要があります。

このオプションは、Geneve VTEP でのみ使用できます。

ステップ 8 [VTEPインターフェイスにマッピングされているNVE（NVE Mapped to VTEP Interface）] を選択します。

このオプションにより、インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

ステップ 9 [OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

ルーテッドインターフェイスのパラメータを設定します。「ルーテッドモードのインターフェイスの設定」を参照してください。

ゲートウェイロードバランサのヘルスチェックの許可

AWS または Azure GWLB では、アプライアンスがヘルスチェックに正しく応答する必要があります。GWLBは、正常と見なされるアプライアンスにのみトラフィックを送信します。SSH、HTTP、または HTTPS のヘルスチェックに応答するように Firewall Threat Defense Virtual を設定する必要があります。

次のいずれかの方法を設定します。

手順

ステップ 1 SSH を設定します。「セキュアシェルの設定」を参照してください。

GWLB IP アドレスからの SSH を許可します。GWLB は、Firewall Threat Defense Virtual への接続の確立を試行し、ログインの Firewall Threat Defense Virtual のプロンプトが正常性の証拠として取得されます。SSH ログインの試行は 1 分後にタイムアウトします。このタイムアウトに対応するには、GWLB でより長いヘルスチェック間隔を設定する必要があります。

ステップ 2 ポート変換機能を備えたスタティック インターフェイス NAT を使用した HTTP(S) リダイレクトの設定

ヘルスチェックをメタデータ HTTP(S) サーバーにリダイレクトするように Firewall Threat Defense Virtual を設定できます。HTTP（S）ヘルスチェックの場合、HTTP（S）サーバーは 200 ー 399 の範囲のステータスコードで GWLB に応答する必要があります。Firewall Threat Defense Virtual では同時管理接続の数に制限があるため、ヘルスチェックを外部サーバーにオフロードすることもできます。

ポート変換を設定したスタティック インターフェイス NAT を使用すると、ポート（ポート 80 など）への接続を別の IP アドレスにリダイレクトできます。たとえば、Firewall Threat Defense Virtual 外部インターフェイスの宛先を持つ GWLB からの HTTP パケットを、HTTP サーバーの宛先を持つ Firewall Threat Defense Virtual 外部インターフェイスからのように変換します。次に Firewall Threat Defense Virtual はパケットをマッピングされた宛先アドレスに転送します。HTTP サーバーは Firewall Threat Defense Virtual 外部インターフェイスに応答し、Firewall Threat Defense Virtual は GWLB に応答を転送します。GWLB から HTTP サーバーへのトラフィックを許可するアクセスルールが必要です。

a) GWLB ネットワークから送られた外部インターフェイスの HTTP(S) トラフィックをアクセスルールで許可します。アクセス コントロール ルール （1775 ページ） を参照してください。

b) HTTP(S) の場合、送信元 GWLB の IP アドレスを Firewall Threat Defense Virtual 外部インターフェイスの IP アドレスに変換します。次に、外部インターフェイスの IP アドレスの宛先を HTTP(S) サーバーの IP アドレスに変換します。「スタティック手動 NAT の設定（957 ページ）」を参照してください。

ルーテッド モードとトランス ペアレント モードのインターフェイスの設定

この項では、ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードで、すべてのモデルに対応する標準のインターフェイス設定を完了するためのタスクについて説明します。

ルーテッド モード インターフェイスとトランスペアレント モード インターフェイスについて

ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、IP 最適化、TCP の正規化などのファイアウォール機能の対象となります。オプションで、セキュリティポリシーに従ってこのトラフィックに IPS 機能を設定することもできます。

設定できるファイアウォール インターフェイスのタイプは、ルーテッド モードとトランスペアレント モードのどちらのファイアウォール モードがそのデバイスに設定されているかによって異なります。詳細については、トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード （199 ページ）を参照してください。

- ルーテッド モード インターフェイス（ルーテッド ファイアウォール モードのみ）：ルーティングを行う各インターフェイスは異なるサブネット上にあります。
- ブリッジグループ インターフェイス（ルーテッドおよびトランスペアレント ファイアウォール モード）：複数のインターフェイスをネットワーク上でグループ化することがで

き、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通過させることができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。ルーテッド モードでは、Firepower Threat Defense デバイスは BVI と通常のルーテッド インターフェイス間をルーティングします。トランスペアレント モードでは、各ブリッジグループは分離されていて、相互通信できません。

デュアル IP スタック（IPv4 および IPv6）

Firewall Threat Defense デバイス は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

31 ビット サブネット マスク

ルーテッド インターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの Firewall Threat Defense 間のフェールオーバーリンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP または Syslog を実行する管理ステーションを直接接続することもできます。

31 ビットのサブネットとクラスタリング

管理インターフェイスとクラスタ制御リンクを除き、クラスタインターフェイスの 31 ビットのサブネットマスクを使用できます。

31 ビットのサブネットとフェールオーバー

フェールオーバーに関しては、Firewall Threat Defense インターフェイスの IP アドレスに 31 ビットのサブネットを使用した場合、アドレスが不足しているため、インターフェイス用のスタンバイ IP アドレスは設定できません。通常、アクティブなユニットがインターフェイスのテストを実行し、スタンバイのインターフェイスの健全性を保証できるよう、フェールオーバー インターフェイスはスタンバイ IP アドレスを必要とします。スタンバイ IP アドレスがないと、Firewall Threat Defense はネットワークのテストを実行できず、リンクステートのみしか追跡できません。

ポイントツーポイント接続であるフェールオーバーと任意のステートリンクでは、31 ビットのサブネットも使用できます。

31 ビットのサブネットと管理

直接接続される管理ステーションがあれば、Firewall Threat Defense 上で SSH または HTTP にポイントツーポイント接続を、または管理ステーション上で SNMP または Syslog にポイントツーポイント接続をそれぞれ使用できます。

31 ビットのサブネットをサポートしていない機能

次の機能は、31 ビットのサブネットをサポートしていません。

- ブリッジ グループ用 BVI インターフェイス - ブリッジ グループには BVI、2 つのブリッジ グループ メンバーに接続された 2 つのホスト用に、少なくとも 3 つのホスト アドレスが必要です。/ 29 サブネット以下を使用する必要があります。
- マルチキャスト ルーティング

ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項

高可用性、クラスタリング、およびマルチインスタンス

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、「高可用性」の章を参照してください。
- クラスタインターフェイスの場合は、クラスタリングの章で要件を確認してください。
- マルチインスタンスモードの場合、共有インターフェイスはブリッジ グループ メンバー インターフェイス（トランスペアレントモードまたはルーテッドモード）ではサポートされません。
- 高可用性 を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。**[モニタ対象インターフェイス（Monitored Interfaces）]** 領域の **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[高可用性（High Availability）]** タブで、スタンバイ IP アドレスを設定します。詳細については、高可用性の章も参照してください。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- Firewall Threat Defense デバイスは、IPv6 エニーキャスト アドレスはサポートしません。
- DHCPv6およびプレフィックス委任オプションは、トランスペアレントモード、クラスタリング、または 高可用性 ではサポートされません。

モデルのガイドライン

- ブリッジされた ixgbevf インターフェイスを持つ VMware 上の Firewall Threat Defense Virtual では、 のブリッジグループはサポートされません。
- FirePOWER 2100 シリーズでは、ルーテッド モードのブリッジ グループはサポートされません。

トランスペアレント モードとブリッジ グループのガイドライン

- 64のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Firewall Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- デバイスとデバイス間の管理トラフィック、および Firewall Threat Defense デバイス を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- マルチインスタンスモードの場合、共有インターフェイスはブリッジ グループ メンバー インターフェイス（トランスペアレントモードまたはルーテッドモード）ではサポートされません。
- ブリッジされた ixgbevf インターフェイスを備えた VMware の Firewall Threat Defense Virtual の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードではサポートされていません。
- Firepower 2100 シリーズ では、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower 1010 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。
- Firepower 4100/9300 では、データ共有インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firewall Threat Defense の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークから

の管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は Diagnostic インターフェイスでサポートされません。
- 透過モードは、Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Oracle Cloud Infrastructure にデプロイされた脅威防御仮想インスタンスではサポートされていません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、Firewall Threat Defense 定義の EtherChannel インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、Firewall Threat Defense を介して許可されません。BFD を実行している Firewall Threat Defense の両側に 2 つのネイバーがある場合、Firewall Threat Defense は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

その他のガイドラインと要件

- Firewall Threat Defense では、ファイアウォール インターフェイスについては、パケットで 802.1Q ヘッダーが 1 つだけサポートされ、複数のヘッダー（Q-in-Q）はサポートされません。**注**：インラインセットとパッシブインターフェイスについては、FTD で Q-in-Q がサポートされ、パケットで 802.1Q ヘッダーが 2 つまでサポートされます。ただし、Firepower 4100/9300 は例外で、802.1Q ヘッダーは 1 つだけサポートされます。
- 頻繁なアップ/ダウンステータスの変化などのインターフェイスの問題があると、フローティング接続タイマーが、インターフェイスを通過する接続に正しく適用されない場合があります。インターフェイスのステータスに問題がある場合は、無効な接続をクリアするため、ステータスが安定した後にすべての接続をクリアすることを検討してください。

ルーテッド モードのインターフェイスの設定

この手順では、名前、セキュリティ ゾーン、および IPv4 アドレスを設定する方法について説明します。

（注） すべてのインターフェイスタイプですべてのフィールドがサポートされているわけではありません。

始める前に

- **Firepower 4100/9300**
  1. 物理インターフェイスの設定 （254 ページ）
  2. （任意）特別なインターフェイスを設定します。
     - EtherChannel（ポート チャネル）の追加 （256 ページ）
     - コンテナインスタンスのVLANサブインターフェイスの追加 （258ページ） FXOSで次を実行します。
     - ループバック インターフェイスの設定 （687 ページ）
     - Firewall Management Center でのサブインターフェイスの追加 （694 ページ）
     - VXLAN インターフェイスの設定 （707 ページ）

- （任意）**他のすべてのモデル**：
  - EtherChannel の設定 （644 ページ）
  - ループバック インターフェイスの設定 （687 ページ）
  - サブインターフェイスの追加 （694 ページ）
  - VXLAN インターフェイスの設定 （707 ページ）
  - AWS 上の Firewall Threat Defense Virtual：Geneve インターフェイスの設定 （710 ページ）
  - Firepower 1010：VLAN インターフェイスの設定 （678 ページ）

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

この名前を「cluster」という語句で始めることはできません。その名前は内部で使用するために予約されています。

ステップ 4 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 5 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ルーテッドインターフェイスは、ルーテッドタイプインターフェイスであり、ルーテッドタイプのゾーンにのみ属することができます。

ステップ 9 **MTU** についてはMTU の設定 （747 ページ）を参照してください。

ステップ 10 [優先度（Priority）] フィールドに、0 ～ 65535 の範囲の数値を入力します。

この値は、ポリシーベースのルーティング構成で使用されます。優先度は、複数の出力インターフェイス間でトラフィックをルーティングする方法を決定するために使用されます。詳細については、「ポリシーベース ルーティング ポリシーの設定 （1281 ページ）」を参照してください。

ステップ 11 [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

高可用性、クラスタリング、およびループバック インターフェイスは、静的 IP アドレス構成のみをサポートします。DHCP および PPPoE はサポートされていません。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。ポイントツーポイント接続の場合、31 ビットのサブネットマスク（255.255.255.254 または /31）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。この場合、スタンバイ IP アドレスを設定できません。高可用性の場合は、静的 IP アドレスのみを使用できます。[モニター対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバーからデフォルト ルートを取得します。
  - [DHCPルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。
- [PPPoE を使用（Use PPPoE）]：インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。

- [VPDN グループ名（VPDN Group Name）]：この接続を表すために選択するグループ名を指定します。
- [PPPoE ユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
- [PPPoE パスワード/パスワードの確認（PPPoE Password/Confirm Password）]：ISP によって提供されたパスワードを指定し、確認します。
- [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

  PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。
- [PPPoE ルート メトリック（PPPoE route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は 1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブ ディスタンスは 1 です。
- [ルート設定の有効化（Enable Route Settings）]：手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス（IP Address）] を入力します。

  [ルート設定を有効化（Enable Route Settings）] チェックボックスをオンにして、[IPアドレス（IP Address）] を空欄にした場合、**ip address pppoe setroute** コマンドが次のように適用されます。

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- [フラッシュにユーザー名とパスワードを保存（Store Username and Password in Flash）]：フラッシュ メモリにユーザー名とパスワードを保存します。

  Firewall Threat Defense デバイスは、NVRAM の特定の場所にユーザー名とパスワードを保存します。

ステップ 12 （任意）IPv6 アドレスの設定 （728 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 13 （任意）MAC アドレスの設定 （749 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 14 （任意）**[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]**をクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）]：[全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。SFP インターフェイスは [全二重（Full）] のみをサポートします。
- [速度（Speed）]：速度を選択します（モデルによって異なります）。（Cisco Secure Firewall 3100 のみ）[SFPを検出（Detect SFP）] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。

  （注）
  高可用性（HA）またはクラウド制御リンクインターフェイスの速度は変更できません。
- [自動ネゴシエーション（Auto-negotiation）]：速度、リンクステータス、およびフロー制御をネゴシエートするようにインターフェイスを設定します。
- [前方誤り訂正モード（Forward Error Correction Mode）]：（Cisco Secure Firewall 3100 のみ）25 Gbps 以上のインターフェイスの場合は、前方誤り訂正（FEC）を有効にします。EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。**自動**を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *46*：自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト FEC（イーサネット 1/9 ～ 1/16）	ネットワークモジュールのデフォルト FEC
25G-SR	第 74 条 FC-FEC	第 108 条 RS-FEC
25G-LR	第 74 条 FC-FEC	第 108 条 RS-FEC
10/25G-CSR	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-AOC*x*M	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション

ステップ 15 （任意）[マネージャアクセス（Manager Access）]ページのデータインターフェイスで Firewall Management Center 管理アクセスを有効にします。

Firewall Threat Defense を最初にセットアップするときに、データインターフェイスからマネージャアクセスを有効にできます。Firewall Threat Defense を Firewall Management Center に追加した後にマネージャアクセスを有効または無効にする場合は、次を参照してください。

- マネージャアクセスの有効化：管理アクセスインターフェイスの管理からデータへの変更（92 ページ）

（注）
管理インターフェイスからデータインターフェイスへのマネージャインターフェイスの移行を最初に開始しないと、マネージャアクセスを有効にすることはできません。移行を開始したら、[マネージャアクセス（Manager Access）] ページでマネージャアクセスを有効にし、設定を保存できます。

- マネージャアクセスの無効化：マネージャ アクセス インターフェイスをデータから管理に変更する （96 ページ）

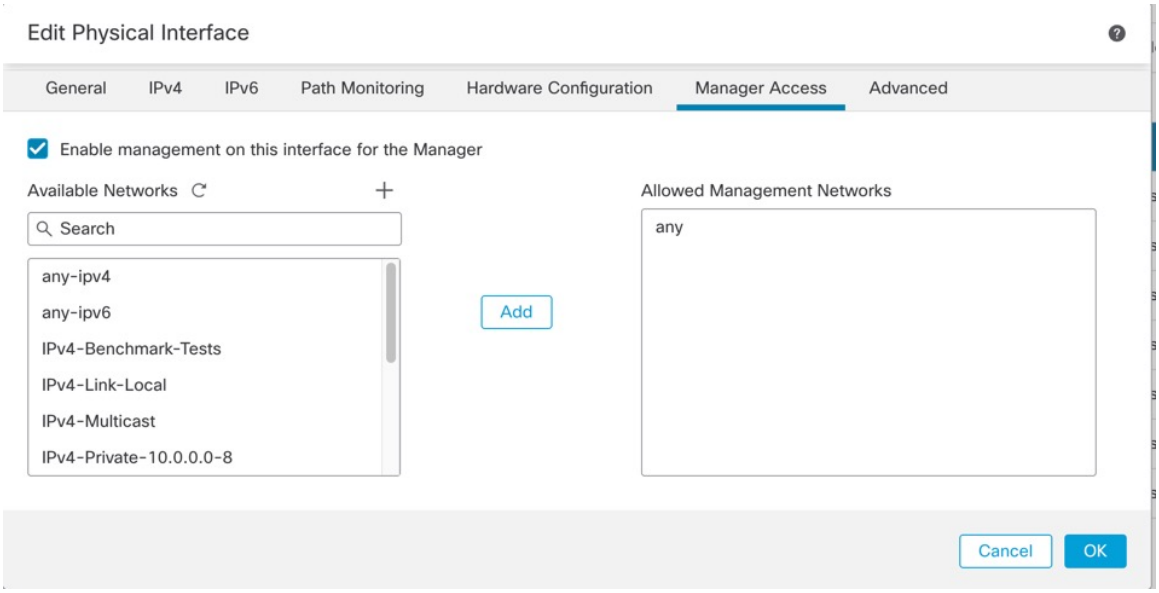
マネージャアクセスインターフェイスをあるデータインターフェイスから別のデータインターフェイスに変更する場合は、元のデータインターフェイスでマネージャアクセスを無効にする必要がありますが、インターフェイス自体はまだ無効にしないでください。展開を実行するには、元のデータインターフェイスを使用する必要があります。新しいマネージャ アクセス インターフェイスで同じ IP アドレスを使用する場合は、元のインターフェイスの IP 設定を削除または変更できます。この変更は展開に影響しません。新しいインターフェイスに別の IP アドレスを使用する場合は、Firewall Management Center に表示されるデバイスの IP アドレスも変更します。Firewall Management Center でのホスト名または IP アドレスの更新 （84 ページ）を参照してください。スタティックルート、DDNS、DNS 設定などの新しいインターフェイスを使用するように、関連する構成も更新してください。

データインターフェイスからのマネージャアクセスには、次の制限があります。

- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスまたは EtherChannel を使用することはできません。マネージャアクセスインターフェイスでサブインターフェイスを作成することもできません。冗長性を目的として、Firewall Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Firewall Threat Defense と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Firewall Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。Amazon Web Services の Firewall Threat Defense Virtual の場合、コンソールポートは使用できないため、管理インターフェイスへの SSH アクセスを維持する必要があります。設定を続行する前に、管理用の静的ルートを追加します。または、マネージャアクセス用のデータインターフェイスを設定する前に、すべての CLI 構成（**configure manager add** コマンドを含む）を終了してから接続を切断します。

- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。
- ハイアベイラビリティはサポートされません。この場合、管理インターフェイスを使用する必要があります。

図 *256* : マネージャアクセス



- Firepower Management Center が専用の管理インターフェイスの代わりにこのデータインターフェイスを管理に使用するには、[このインターフェイス上の管理をマネージャに対して有効にする（Enable management on this interface for the manager） をオンにします。
- （オプション）[許可された管理ネットワーク（Allowed Management Networks）] ボックスで、マネージャアクセスを許可するネットワークを追加します。デフォルトでは、すべてのネットワークが許可されます。

ステップ 16 **[OK]** をクリックします。

ステップ 17 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ブリッジ グループ インターフェイスの設定

ブリッジ グループは、Secure Firewall Threat Defense デバイス がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。ブリッジグループの詳細については、ブリッジグループについて（201 ページ）を参照してください。

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

この手順は、ブリッジ グループ メンバー インターフェイスの名前とセキュリティ ゾーンを設定する方法について説明します。同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、Firepower 1010 VLAN インターフェイス、EtherChannel、冗長インターフェイス）を含めることができます。管理インターフェイスはサポートされていません。 ルーテッド モードでは、EtherChannel はサポートされません。Firepower 4100/9300 では、データ共有タイプのインターフェイスはサポートされていません。

始める前に

- **Firepower 4100/9300**
  1. 物理インターフェイスの設定 （254 ページ）
  2. （任意）特別なインターフェイスを設定します。
     - EtherChannel（ポート チャネル）の追加 （256 ページ）
     - コンテナインスタンスの VLAN サブインターフェイスの追加 （258 ページ） FXOS で次を実行します。
     - Firewall Management Center でのサブインターフェイスの追加 （694 ページ）
- （任意）**他のすべてのモデル**：
  - EtherChannel の設定 （644 ページ）
  - サブインターフェイスの追加 （694 ページ）
  - Firepower 1010：VLAN インターフェイスの設定 （678 ページ）

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

この名前を「cluster」という語句で始めることはできません。その名前は内部で使用するために予約されています。

ステップ 4 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 5 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。このインターフェイスをブリッジ グループに割り当てると、[スイッチド（Switched）] がモードに表示されます。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ブリッジ グループ メンバー インターフェイスは、スイッチドタイプ インターフェイスであり、スイッチドタイプのゾーンにのみ属することができます。このインターフェイスに対して IP アドレス設定は行わないでください。ブリッジ仮想インターフェイス（BVI）に対してのみ IP アドレスを設定します。BVI はゾーンに属しておらず、BVI にはアクセス コントロール ポリシーを適用できないことに注意してください。

ステップ 9 **MTU** についてはMTU の設定 （747 ページ）を参照してください。

ステップ 10 （任意） **[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]**をクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。SFP インターフェイスは [全二重（Full）] のみをサポートします。
- [速度（Speed）] : 速度を選択します（モデルによって異なります）。（Cisco Secure Firewall 3100 のみ）[SFPを検出（Detect SFP）] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。

  （注）
  高可用性（HA）またはクラウド制御リンクインターフェイスの速度は変更できません。
- [自動ネゴシエーション（Auto-negotiation）] : 速度、リンクステータス、およびフロー制御をネゴシエートするようにインターフェイスを設定します。
- [前方誤り訂正モード（Forward Error Correction Mode）] : （Cisco Secure Firewall 3100 のみ）25 Gbps 以上のインターフェイスの場合は、前方誤り訂正（FEC）を有効にします。EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。**自動**を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *47*: 自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト FEC（イーサネット 1/9 ～ 1/16）	ネットワークモジュールのデフォルト FEC
25G-SR	第 74 条 FC-FEC	第 108 条 RS-FEC
25G-LR	第 74 条 FC-FEC	第 108 条 RS-FEC
10/25G-CSR	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-AOCxM	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション

ステップ 11 （任意） IPv6 アドレスの設定 （728 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 12 （任意） MAC アドレスの設定 （749 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 13 **[OK]** をクリックします。

ステップ 14 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。Firewall Threat Defense はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカル アドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

ルーテッドモードの場合、BVI に名前を指定すると、BVI がルーティングに参加します。名前を指定しなければ、ブリッジ グループはトランスペアレント ファイアウォール モードの場合と同じように隔離されたままになります。

（注） 個別の Diagnostic インターフェイスでは、設定できないブリッジ グループ（ID 301）は、設定に自動的に追加されます。このブリッジグループはブリッジグループの制限に含まれません。

始める前に

セキュリティ ゾーンに BVI を追加することはできません。そのため、BVI にアクセス コントロール ポリシーを適用することはできません。ゾーンに基づいてブリッジ グループのメンバー インターフェイスにポリシーを適用する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 **[インターフェイスの追加（Add Interfaces）]** > **[ブリッジ グループ インターフェイス（Bridge Group Interface）]** を選択します。

ステップ 3 （ルーテッド モード）[名前（Name）] フィールドに、名前を 48 文字以内で入力します。

トラフィックをブリッジ グループ メンバーの外部（たとえば、外部インターフェイスや他のブリッジ グループのメンバー）にルーティングする必要がある場合は、BVI に名前を付ける必要があります。名前は大文字と小文字が区別されません。

ステップ 4 [ブリッジ グループ ID（Bridge Group ID）] フィールドに、1 ～ 250 の間のブリッジ グループ ID を入力します。

ステップ 5 （オプション）[説明（Description）] フィールドに、このブリッジ グループの説明を入力します。

ステップ 6 [インターフェイス（Interfaces）] タブでインターフェイスをクリックし、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interfaces）] 領域にそのインターフェイスを移動します。ブリッジ グループのメンバーにするすべてのインターフェイスに対して繰り返します。

ステップ 7 （トランスペアレント モード）[IPv4] タブをクリックします。[IP アドレス（IP Address）] フィールドに IPv4 アドレスおよびサブネット マスクを入力します。

BVI にはホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。Firewall Threat Defense デバイスは、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約済みアドレスを割り当てた場合、Firewall Threat Defense デバイスはダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

高可用性の場合は、[モニター対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[高可用性（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。

ステップ 8 （ルーテッド モード）[IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

高可用性およびクラスタリング インターフェイスは、静的 IP アドレス設定のみをサポートします。DHCP はサポートされていません。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。高可用性の場合は、静的 IP アドレスのみを使用できます。[モニター対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバーからデフォルト ルートを取得します。
  - [DHCPルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

ステップ 9 （任意）IPv6アドレッシングの設定については、IPv6アドレスの設定 （728ページ）を参照してください。

ステップ 10 （任意）スタティック ARP エントリの追加 （750ページ）および静的MACアドレスの追加とブリッジグループの MAC 学習の無効化 （751 ページ）（トランスペアレント モードの場合のみ）を参照して **ARP** と **MAC** を設定します。

ステップ 11 **[OK]** をクリックします。

ステップ 12 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

IPv6 アドレスの設定

ここでは、ルーテッド モードおよびトランスペアレント モードで IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレッシング

IPv6 に対して次の 2 種類のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などのネイバー探索機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ インターフェイスでは、BVI でグローバル アドレスを設定した場合、Firewall Threat Defense デバイスが自動的にメンバーインターフェイスのリンクローカルアドレスを生成します。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。Firewall Threat Defense デバイスでは、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスで有効化されていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。

IPv6 プレフィックス委任クライアントの設定

Firewall Threat Defense は、（ケーブルモデムに接続された外部インターフェイスなどの）クライアント インターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、Firewall Threat Defense はそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。

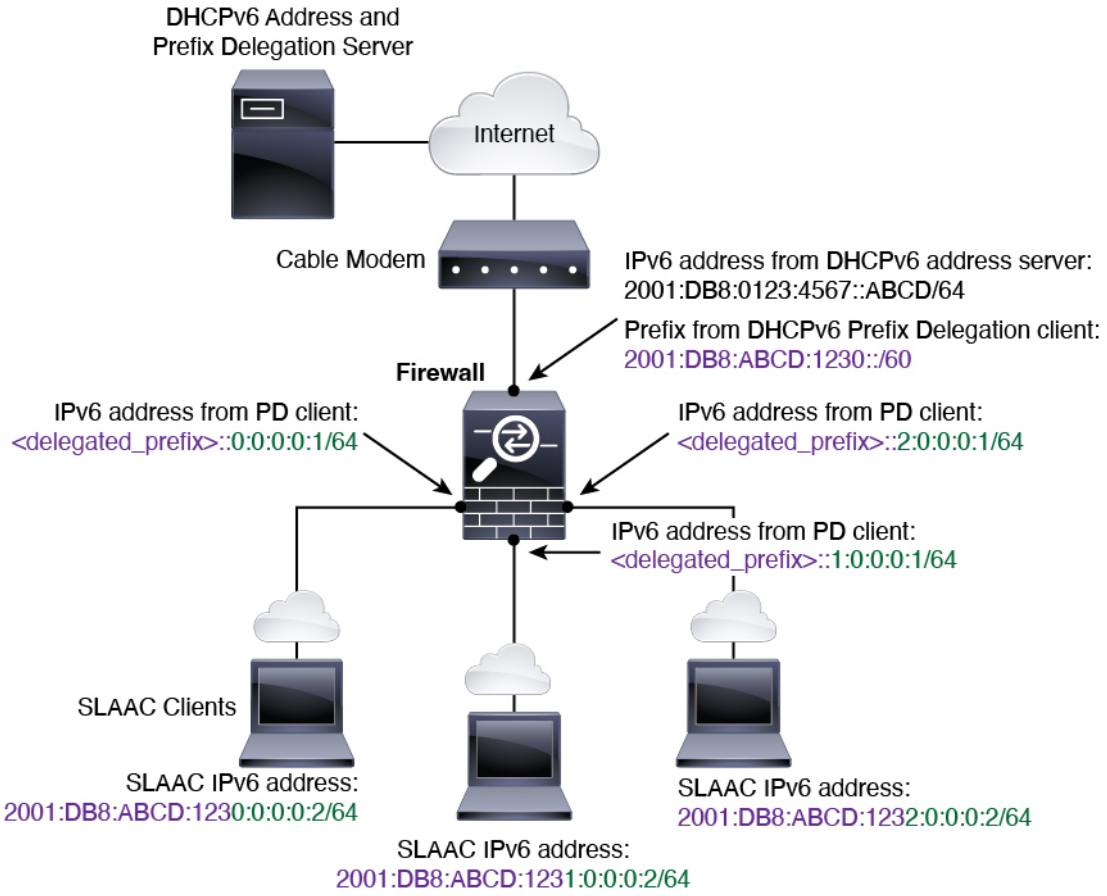
IPv6 プレフィックス委任の概要

Firewall Threat Defense は、（ケーブルモデムに接続された外部インターフェイスなどの）クライアント インターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、Firewall Threat Defense はそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。これにより、内部インターフェイスに接続されているホストは、StateLess Address Auto Configuration（SLAAC）を使用してグローバル IPv6 アドレスを取得できます。ただし、内部 Firewall Threat Defense インターフェイスはプレフィックス委任サーバーとして機能しないため注意してください。Firewall Threat Defense は、SLAAC クライアントにグローバル IP アドレスを提供することしかできません。たとえば、ルータが Firewall Threat Defense に接続されている場合、ASA は SLAAC クライアントとして機能し、IP アドレスを取得できます。しかし、ルータの背後のネットワークに代理プレフィックスのサブネットを使用したい場合、ルータの内部インターフェイス上でそれらのアドレスを手動で設定する必要があります。

Firewall Threat Defense には軽量 DHCPv6 サーバーが含まれており、SLAAC クライアントが情報要求（IR）パケットを Firewall Threat Defense に送信した場合、Firewall Threat Defense は DNS サーバーやドメイン名などの情報を SLAAC クライアントに提供できます。Firewall Threat Defense は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス（Firewall Threat Defense がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

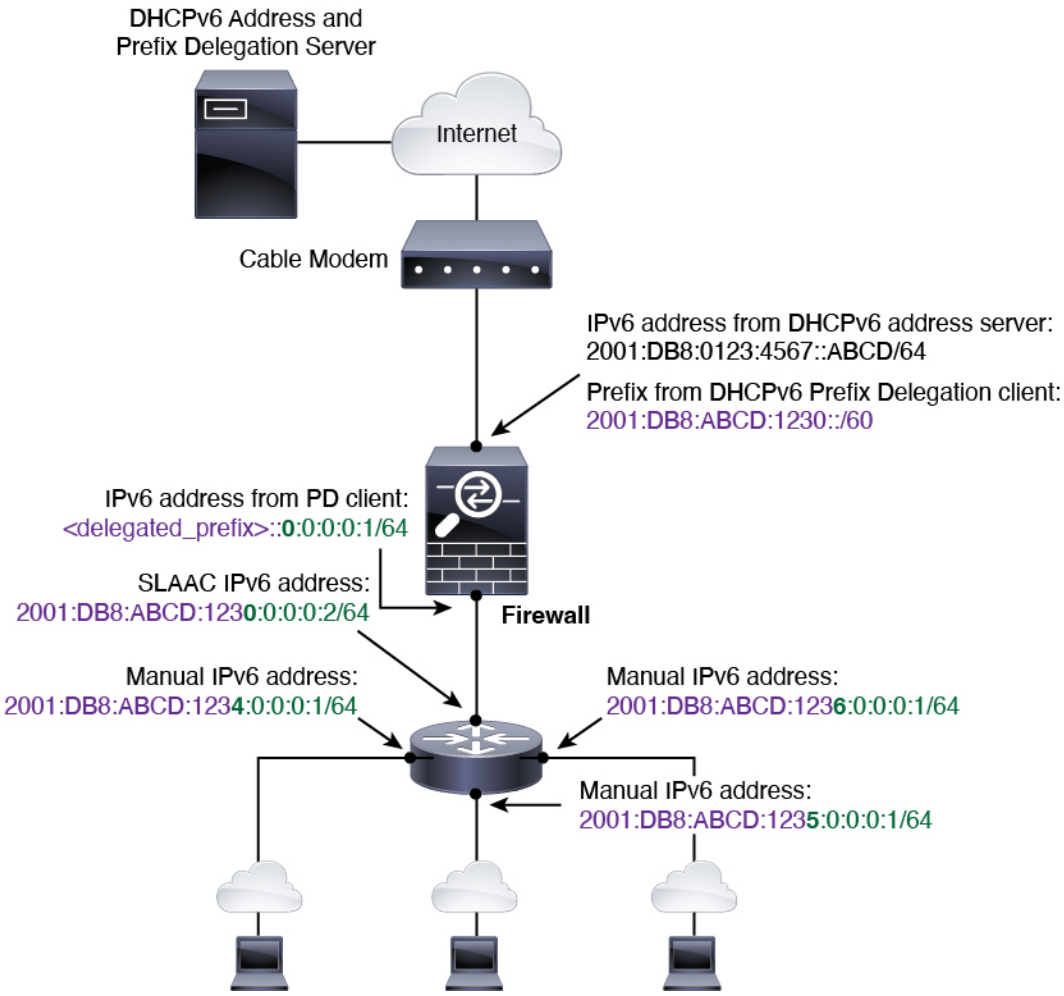
IPv6 プレフィックス委任 */64* サブネットの例

次の例では、Firewall Threat Defense が DHCPv6 アドレスクライアントを使用して、外部インターフェイス上で IP アドレスを受け取るところを示しています。また、ASA は DHCPv6 プレフィックス委任クライアントを使用して代理プレフィックスを取得します。Firewall Threat Defense は、委任されたプレフィックスを /64 ネットワークにサブネット化し、委任されたプレフィックスと手動で設定されたサブネット（::0、::1、または ::2）と各インターフェイスの IPv6 アドレス（0:0:0:1）を使用して、動的に内部インターフェイスにグローバル IPv6 アドレスを割り当てます。これらの内部インターフェイスに接続されている SLAAC クライアントは、各 /64 サブネットの IPv6 アドレスを取得します。



IPv6 プレフィックス委任 */62* サブネットの例

次の例は、Firewall Threat Defense が 4/62 サブネットにプレフィックスをサブネット化するところを示しています。2001:DB8:ABCD:123**0**::/62、2001:DB8:ABCD:123**4**::/62、2001:DB8:ABCD:123**8**::/62、2001:DB8:ABCD:123**C**::/62。Firewall Threat Defense は、内部ネットワーク（::0）に 2001:DB8:ABCD:1230::/62 の利用可能な 64 サブネット 4 つのいずれかを使用します。ダウンストリーム ルータには、手動で追加の /62 サブネットを使用できます。図のルータは、内部インターフェイス（::4, ::5, and ::6）に 2001:DB8:ABCD:1234::/62 の利用可能な 4 つの /64 サブネットのうちの 3 つを使用します。この場合、内部ルータインターフェイスは委任されたプレフィックスを動的に取得できないため、Firewall Threat Defense 上で委任されたプレフィックスを表示し、ルータ設定にそのプレフィックスを使用する必要があります。通常、リースが期限切れになった場合、ISP は既定のクライアントに同じプレフィックスを委任しますが、Firewall Threat Defense が新しいプレフィックスを受け取った場合、新しいプレフィックスを使用するようルータ設定を変更する必要があります。DHCP の一意識別子（DUID）は、再起動後も存続します。



IPv6 プレフィックス委任クライアントの有効化

1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。Firewall Threat Defense は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントを有効にしたインターフェイスは DHCPv6 アドレスクライアントを使用して IP アドレスを取得し、その他の Firewall Threat Defense インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。

この機能は、ルーテッドモードでのみサポートされます。この機能は、クラスタリングまたはハイアベイラビリティではサポートされません。

始める前に

プレフィックス委任を使用する場合は、IPv6 トラフィックの中断を防ぐために、Firewall Threat Defense IPv6 ネイバー探索のルータアドバタイズメント間隔を DHCPv6 サーバーによって割り当てられるプレフィックスの推奨有効期間よりもはるかに小さい値に設定する必要があります。たとえば、DHCPv6 サーバーでプレフィックス委任の推奨有効期間を 300 秒に設定してい

る場合は、Firewall Threat Defense RA の間隔を 150 秒に設定する必要があります。推奨有効期間を設定するには、**show ipv6 general-prefix** コマンドを使用します。Firewall Threat Defense RA の間隔を設定するには、「IPv6 ネイバー探索の設定（738 ページ）」を参照してください。デフォルトは 200 秒です。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [IPv6] ページをクリックしてから、[DHCP] をクリックします。

ステップ 4 [クライアントPDプレフィックス名（Client PD Prefix Name）] をクリックし、このプレフィックスの名前を入力します。

図 *257*: プレフィックス委任クライアントの有効化

名前には最大 200 文字を使用できます。

ステップ 5 （任意）[クライアントPDヒントプレフィックス（Client PD Hint Prefixes）] フィールドにプレフィックスとプレフィックス長を入力し、受信する委任されたプレフィックスに関する DHCP サーバーへのヒントを 1 つ以上指定して [追加（Add）] をクリックします。

通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合は、そのプレフィックスの全体をヒントとして入力できます。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバによって決定されます。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

グローバル IPv6 アドレスの設定

ルーテッド モードの任意のインターフェイスとトランスペアレント モードまたはルーテッド モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジ グループについて、BVI でグローバル アドレスを設定すると、すべてのメンバー インターフェイスのリンクローカル アドレスが自動的に設定されます。

Firewall Threat Defense で定義されているサブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、Firewall Threat Defense で特定のインスタンスでのトラフィックの中断を避けることができます。MAC アドレスの設定 （749 ページ）を参照してください。

始める前に

ブリッジグループの IPv6 ネイバー探索では、双方向アクセスルールを使用して、Firewall Threat Defense ブリッジ グループ メンバー インターフェイスでネイバー送信要求（ICMPv6 タイプ 135）およびネイバーアドバタイズメント（ICMPv6 タイプ 136）パケットを明示的に許可する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [IPv6] ページをクリックします。

ルーテッドモードでは、[基本（Basic）]ページがデフォルトで選択されています。トランスペアレントモードでは、[アドレス（Address）] ページがデフォルトで選択されています。

ステップ 4 （任意） [基本（Basic）] ページで、[IPv6を有効にする（Enable IPv6）] をオンにします。

リンクローカルアドレスのみを設定する場合は、このオプションを使用します。それ以外の場合、IPv6 アドレスを設定すると、IPv6 処理が自動的に有効になります。

ステップ 5 グローバル IPv6 アドレスを次のいずれかの方法で設定します。

フェールオーバーやクラスタリング、およびループバック インターフェイスの場合は、IP アドレスを手動で設定する必要がありますクラスタリングの場合、リンクローカルアドレスの手動設定もサポートされていません。

- （ルーテッドインターフェイス）ステートレス自動設定：[自動設定（Autoconfiguration）] チェックボックスをオンにします。

  インターフェイス上でステートレス自動設定を有効にすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定が有効になっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

  RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、Firewall Threat Defense デバイスがルータ アドバタイズメント メッセージを送信します。**[IPv6]** > **[設定（Settings）]** > **[RA の有効化（Enable RA）]** チェックボックスをオフにして、メッセージを抑制します。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

  1. [アドレス（Address）] ページ、[アドレスの追加（Add Address）]（＋）の順にクリックします。

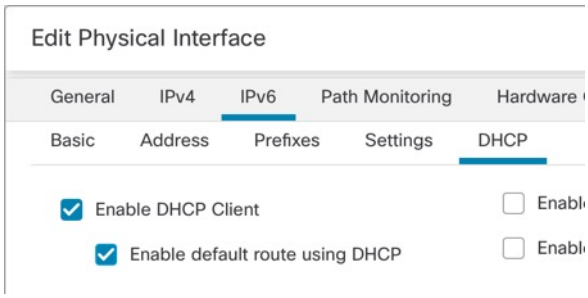
     [アドレスの追加（Add Address）] ダイアログボックスが表示されます。

  2. [アドレス（Address）] フィールドに、インターフェイス ID を含む完全なグローバル IPv6 アドレス、または IPv6 プレフィックス長と IPv6 プレフィックスのいずれかを入力します。（ルーテッドモード）プレフィックスだけを入力した場合は、必ず [EUI-64 を適用（Enforce EUI 64）] チェックボックスをオンにして、Modified EUI-64 形式を使用してインターフェイス ID を生成するようにしてください。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。

     （[EUI 64の適用（Enforce EUI 64）] を設定しなかった場合は）高可用性のために、[モニター対象インターフェイス（Monitored Interfaces）] 領域の **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[高可用性（High Availability）]** ページでスタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

- （ルーテッドインターフェイス）DHCPv6 を使用してアドレスを取得する：DHCPv6 を使用するには、次の手順を実行します。

図 *258 : DHCPv6* クライアントの有効化



  1. [DHCP] ページをクリックします。

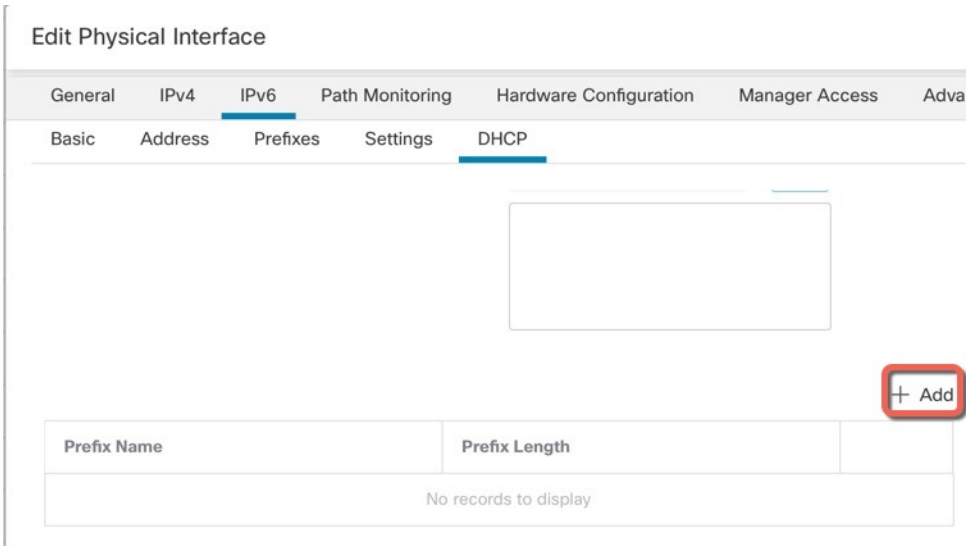
2. [DHCPクライアントの有効化（Enable DHCP Client）] チェックボックスをオンにします。
3. （オプション）ルータアドバタイズメントからデフォルトルートを取得するには、[DHCPを使用してデフォルトルートを有効にする（Enable default route using DHCP）] チェックボックスをクリックします。

- （ルーテッドインターフェイス）委任されたプレフィックスを使用する：委任されたプレフィックスを使用して IPv6 アドレスを割り当てるには、次の手順を実行します。

  この機能は、Firewall Threat Defense に別のインターフェイスで DHCPv6 プレフィックス委任クライアントを有効にさせるために必要です。IPv6 プレフィックス委任クライアントの有効化 （732 ページ） を参照してください。

1. [DHCP] ページをクリックします。
2. （＋） をクリックします。

図 259 : 委任されたプレフィックスの使用

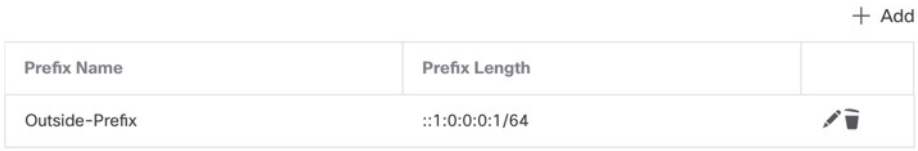


3. IPv6 アドレスと**プレフィックス長**を入力します。

   通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（1:0:0:0:1 など）を指定する必要があります。プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。

4. [OK] をクリックします。

図 260 : プレフィックス委任テーブル



5. 必要に応じて、このインターフェイスで DHCPv6 ステートレスサーバーを有効にします（「DHCPv6 ステートレスサーバーの有効化 （791 ページ）」を参照）。その場合は、[アドレス以外の設定でDHCPを有効にする（Enable DHCP for non-address config）] オプションもオンにすることをお勧めします。

ステップ 6 ルーテッドインターフェイスの場合は、必要に応じて [基本（Basic）] ページで次の値を設定できます。

- ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[EUI-64 を適用（Enforce EUI-64）] チェックボックスをオンにします。
- リンクローカル アドレスを手動で設定するには、[リンクローカル アドレス（Link-Local address）] フィールドにアドレスを入力します。

  リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカルアドレスによりパケットがドロップされることがあります。

  クラスタリングは、手動のリンクローカルアドレスをサポートしていません。

ステップ 7 ルーテッドインターフェイスの場合は、必要に応じて [DHCP] ページで次の値を設定できます。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Managed Address Config フラグを設定します。

  IPv6 ルータ アドバタイズメント内のこのフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Other Address Config フラグを設定します。

IPv6 ルータ アドバタイズメント内のこのフラグは、DHCPv6 から DNS サーバー アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。DHCPv6 プレフィックス委任で DHCPv6 ステートレスサーバーを使用する場合は、このオプションを使用します。

ステップ 8 ルーテッドインターフェイスの場合は、[プレフィックス（Prefixes）]ページと [設定（Settings）] ページでの設定について「IPv6 ネイバー探索の設定（738 ページ）」を参照してください。BVI インターフェイスの場合は、[設定（Settings）] ページの以下のパラメータを参照してください。

- [DAD 試行（DAD attempts）]：DAD 試行の最大数（1 ～ 600）。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。デフォルトでは 1 になっています。
- [NS 間隔（NS Interval）]：インターフェイスでの IPv6 ネイバー要請再送信の間隔（1000 ～ 3600000 ms）。デフォルト値は 1000 ミリ秒です。
- [到達可能時間（Reachable Time）]：到達可能性確認イベントが発生した後でリモートの IPv6 ノードを到達可能とみなす時間（0 ～ 3600000 ms）。デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 9 **[OK]** をクリックします。

ステップ 10 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび要請ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを特定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失われると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

始める前に

ルーテッドモードのみでサポートされます。トランスペアレントモードでサポートされる IPv6 ネイバー設定については、「グローバル IPv6 アドレスの設定（734 ページ）」を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎）をクリックします。

ステップ 3 [IPv6]、[プレフィックス（Prefixes）] の順にクリックします。

ステップ 4 （任意） IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、次の手順を実行します。

a) [プレフィックスの追加（Add Prefix）] をクリックします。（＋）

b) [アドレス（Address）] フィールドに、プレフィックス長の IPv6 アドレスを入力するか、または [デフォルト（Default）] チェックボックスをオンにして、デフォルトのプレフィックスを使用します。

c) （任意） IPv6 プレフィックスをアドバタイズしない場合は、[アドバタイズメント（Advertisement）] チェックボックスをオフにします。**デフォルトの** プレフィックスの場合、この設定はオンリンク プレフィックスにのみ適用されます。特定のオフリンク プレフィックスの **[アドバタイズメント（Advertisement）]** をオフにしない限り、オフリンク プレフィックスは引き続きアドバタイズされます。

d) [オフ リンク（Off Link）] チェックボックスをオンにして、指定したプレフィックスがリンクに割り当てられたことを示します。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。このプレフィックスは、オンリンクの判別には使用しないでください。

e) 指定されているプレフィックスを自動設定に使用する場合、[自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [プレフィックス ライフタイム（Prefix Lifetime）] で、[期間（Duration）] または [失効日（Expiration Date）] をクリックします。

- [期間（Duration）]：プレフィックスの [優先ライフタイム（Preferred Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが有効なものとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～ 4294967295 です。デフォルトは 2592000（30 日間）です。プレフィックスの [有効ライフタイム（Valid Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが優先であるとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～ 4294967295 です。デフォルト設定は、604800（7 日）です。または、[無限大（Infinite）] チェックボックスをオンにして、時間無制限を設定します。

- [失効日（Expiration Date）]：[有効（Valid）]、[優先（Preferred）] 日時を選択します。

g) [OK] をクリックします。

ステップ 5 [設定（Settings）] をクリックします。

ステップ 6 （任意） [DAD 試行（DAD attempts）] の最大数、1 ～ 600 を設定します。デフォルトでは 1 になっています。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。

この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。

ステートレス自動設定プロセス中に、重複アドレス検出は、アドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

ステップ 7 （任意） [NS インターバル（NS Interval）] フィールドで、IPv6 ネイバー勧誘再送信の時間の間隔を、1000 ～ 3600000ms で設定します。

デフォルト値は 1000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャスト アドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

ステップ 8 （任意） 到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能であると見なされる時間を、[到達可能時間（Reachable Time）] フィールドにて、0 ～ 3600000ms で設定します。

デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6

ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 9 （任意）ルータ アドバタイズメントの伝送を抑制にするには、[RA を有効にする（Enable RA）]チェックボックスをオフにします。ルータ アドバタイズメントの伝送を有効にすると、RA ライフタイムと時間間隔を設定できます。

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

Firewall Threat Defenseで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを無効化できます。

- [RA ライフタイム（RA Lifetime）]：IPv6 ルータ アドバタイズメントのルータのライフタイム値を、0 ～ 9000 秒で設定します。

  デフォルトは 1800 秒です。

- [RA インターバル（RA Interval）]：IPv6 ルータ アドバタイズメントの伝送の間の時間間隔を、3 ～ 1800 秒で設定します。

  デフォルトは 200 秒です。

  他の IPv6 ノードとの同期を防ぐために、ファイアウォールは、設定した値（ジッター）をランダムに調整します。

ステップ 10 **[OK]** をクリックします。

ステップ 11 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

高度なインターフェイスの設定

この項では、通常のファイアウォール モードのインターフェイスの MAC アドレスの設定方法、最大伝送ユニット（MTU）の設定方法、およびその他の詳細パラメータの設定方法について説明します。

インターフェイスの詳細設定について

ここでは、インターフェイスの詳細設定について説明します。

MAC アドレスについて

手動でMACアドレスを割り当てて、デフォルトを上書きすることができます。 コンテナインスタンスの場合、FXOS シャーシはすべてのインターフェイスに対して一意の MAC アドレスを自動的に生成します。

（注） 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、Firewall Threat Defense で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、Firewall Threat Defense デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

（注） コンテナ インスタンスでは、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

デフォルトの MAC アドレス

ネイティブインスタンスの場合：

デフォルトのMACアドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスでは、Burned-In MAC Address を使用します。
- VLAN インターフェイス（Firepower 1010 および）：ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。MAC アドレスの設定 （749 ページ）を参照してください。

  トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。MAC アドレスの設定 （749 ページ）を参照してください。
- EtherChannel（Firepower モデル）：EtherChannel の場合、そのチャネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対して透過的になります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャネルインターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。

- EtherChannel（ASA モデル）：ポートチャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポートチャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイスのメンバーシップが変更された場合に備えて、一意の MAC アドレスを設定することをお勧めします。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス(Firewall Threat Defense定義): 物理インターフェイスのすべてのサブインターフェイスは同じBurned-In MAC Addressを使用します。サブインターフェイスに一意のMACアドレスを割り当てることが必要になる場合があります。たとえば、サービスプロバイダーによっては、MACアドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、Firewall Threat Defense で特定のインスタンスでのトラフィックの中断を避けることができます。

コンテナインスタンスの場合：

- すべてのインターフェイスの MAC アドレスは、MAC アドレス プールから取得されます。サブインターフェイスの場合、手動で MAC アドレスを設定する場合は、同じ親インターフェイス上のすべてのサブインターフェイスに一意の MAC アドレスを使用して、正しく分類されるようにしてください。コンテナ インスタンス インターフェイスの自動 MAC アドレス （239 ページ） を参照してください。

MTU について

MTU は、Firewall Threat Defense デバイス が特定のイーサネット インターフェイスで送信可能な最大フレームペイロードサイズを指定します。MTU の値は、イーサネット ヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば、MTU を 1500 に設定すると、予想されるフレーム サイズはヘッダーを含めて 1518 バイトで、VLAN を使用する場合は 1522 です。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

Geneve については、イーサネットデータグラム全体がカプセル化されるため、新しい IP パケットは大きくなり、より大きな MTU が必要となります。そのため、ASA VTEP 送信元インターフェイスの MTU をネットワーク MTU + 306 バイトに設定する必要があります。

パス MTU ディスカバリ

Firewall Threat Defense デバイス は、Path MTU Discovery（RFC 1191 の定義に従う）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

Firewall Threat Defense デバイス のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッド分の 18～22 バイトは含まれません。

MTU とフラグメンテーション

IPv4 の場合、出力 IP パケットが、指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されます。フラグメント化はパフォーマンス低下の原因となります。IPv6 の場合、通常、パケットのフラグメント化は許可されません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内におさめる必要があります。

TCP パケットの場合、通常、エンドポイントが MTU を使用して、TCP 最大セグメント サイズ（たとえば、MTU - 40 など）を判別します。途中で TCP ヘッダーが追加される場合（たとえば、サイト間 VPN トンネルなど）、トンネリング エンティティによって TCP MSS を調整する必要があります。TCP MSS について （744 ページ）を参照してください。

UDP または ICMP の場合、アプリケーションは、フラグメンテーションを避けるために、MTU を考慮する必要があります。

（注） Firewall Threat Defense デバイス はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

MTU とジャンボ フレーム

MTU が大きくなると、より大きなパケットを送信できます。大きなパケットはネットワークにとってより効率的です。次のガイドラインを参照してください。

- トラフィックパスの MTU の一致：すべての Firewall Threat Defense インターフェイスの MTU と、トラフィックパス上のその他のデバイスインターフェイスの MTU を同じ値に設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボフレームへの対応：ジャンボフレームが有効な場合、MTU を 9,000 バイト以上に設定できます。最大値はモデルによって異なります。

TCP MSS について

TCP 最大セグメント サイズ（MSS）とは、あらゆる TCP と IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

FlexConfig の Sysopt_Basic オブジェクトを使用して 」を参照してください。「FlexConfig ポリシー （2687 ページ）」を参照してください。デフォルトで、最大 TCP MSS は 1,380 バイトに設定されます。この設定は、Firewall Threat Defense デバイス が IPsec VPN カプセル化のパケットサイズを大きくする必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、Firewall Threat Defense デバイス の最大 TCP MSS を無効化する必要があります。

最大 TCP MSS を設定すると、接続のいずれかのエンドポイントが Firewall Threat Defense デバイス で設定した値よりも大きな TCP MSS を要求した場合に、Firewall Threat Defense デバイスは要求パケットの TCP MSS を Firewall Threat Defense デバイス の最大値で上書きします。ホストやサーバが TCP MSS を要求しない場合、Firewall Threat Defense デバイス は RFC 793 のデ

フォルト値 536 バイト（IPv4）または 1220 バイト（IPv6）を想定しますが、パケットを変更することはありません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。Firewall Threat Defense デバイス の最大 TCP MSS が 1380（デフォルト）の場合は、Firewall Threat Defense デバイス は TCP 要求パケットの MSS 値を 1380 に変更します。サーバは、1380 バイトのペイロードを含むパケットを送信します。Firewall Threat Defense デバイス はさらに 120 バイトのヘッダーをパケットに追加しますが、それでも 1500 の MTU サイズに収まります。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、Firewall Threat Defense デバイス は値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含む to-the-box トラフィックには、この設定は適用されません。Firewall Threat Defense デバイス は MTU を使用して、TCP MSS を導き出します。MTU - 40（IPv4）または MTU - 60（IPv6）となります。

デフォルト TCP MSS

デフォルトでは、Firewall Threat Defense デバイス の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、Firewall Threat Defense デバイス が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。Firewall Threat Defense デバイス が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして Firewall Threat Defense デバイス を使用しない場合は、FlexConfig の Sysopt_Basic オブジェクトを使用して TCP MSS 設定を変更する必要があります。

（注） MSS を明示的に設定した場合でも、TLS/SSL 復号やサーバ検出などのコンポーネントが特定の MSS を必要とする場合、その MSS はインターフェイス MTU に基づいて設定され、MSS 設定は無視されます。

次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。一般に接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。

- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

ブリッジグループ トラフィックの ARP インスペクション

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARPインスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARPスプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイルータはゲートウェイ ルータのMACアドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションを有効化すると、Firewall Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IPアドレス、MACアドレス、および送信元インターフェイスがARPエントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firewall Threat Defense デバイスはパケットをドロップします。
- ARPパケットがスタティックARPテーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにFirewall Threat Defense デバイスを設定できます。

（注） 専用のDiagnosticインターフェイスは、このパラメータがfloodに設定されている場合でもパケットをフラッディングしません。

MAC アドレス テーブル

ブリッジグループを使用する場合、Firewall Threat Defenseは、通常のブリッジまたはスイッチと同様に、MACアドレスを学習してMACアドレステーブルを作成します。デバイスがブリッジ グループ経由でパケットを送信すると、Firewall Threat Defense が MAC アドレスをアドレステーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、Firewall Threat Defenseは、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジ グループ メンバー間のトラフィックには Firewall Threat Defense セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに

元のパケットをFirewall Threat Defenseがフラッディングすることはありません。代わりに、直接接続されたデバイスまたはリモート デバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：Firewall Threat Defense は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモート デバイスへのパケット：Firewall Threat Defense は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

デフォルト設定

- ARPインスペクションを有効にした場合、デフォルト設定では、一致しないパケットはフラッディングします。
- ダイナミック MAC アドレス テーブル エントリのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、Firewall Threat Defense デバイスは対応するエントリを MAC アドレス テーブルに追加します。

（注） Secure Firewall Threat Defense デバイス はリセットパケットを生成し、ステートフル検査エンジンによって拒否された接続をリセットします。リセットパケットでは、パケットの宛先 MAC アドレスがARPテーブルのルックアップに基づいて決定されるのではなく、拒否されるパケット（接続）から直接取得されます。

ARP インスペクションと MAC アドレス テーブルのガイドライン

- ARP インスペクションは、ブリッジ グループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジ グループでのみサポートされます。

MTU の設定

たとえば、ジャンボ フレームを許可するようにインターフェイスの MTU をカスタマイズします。

、ISA 3000、Firewall Threat Defense Virtualの場合：1500 バイトを超える MTU を変更すると、jumbo-frame reservation が自動的に有効になります。ジャンボフレームを使用するには、システムを再起動する必要があります。クラスタリングをサポートする Firewall Threat Defense Virtual では、Day0 構成で jumbo-frame reservation を有効にすることができるため、その場合は再起動

する必要はありません。再起動後、disable jumbo-frame reservation を無効にすることはできません。Firewall Threat Defense Virtual の場合は例外で、サポートされている場合は Day0 構成で jumbo-frame reservation を無効にできます。インライン セットでインターフェイスを使用する場合、MTU 設定は使用されません。ただし、jumbo-frame reservation の設定はインラインセットに関連します。ジャンボフレームによりインラインインターフェイスは最大 9000 バイトのパケットを受信できます。 jumbo-frame reservation を有効にするには、すべてのインターフェイスの MTU を 1500 バイトより大きい値に設定する必要があります。

ジャンボフレームは、他のプラットフォームではデフォルトで有効化されます。

⚠

注意 デバイス上でデータインターフェイスの最大 MTU 値を変更し、設定の変更を展開すると、Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。インスペクションは、変更したインターフェイスだけでなく、すべてのデータインターフェイスで中断されます。この中断でトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイス タイプに応じて異なります。この注意は、診断インターフェイスまたは管理専用のインターフェイスには適用されません。詳細については、Snort の再起動によるトラフィックの動作（165 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [全般（General）] タブで [MTU] を設定します。最小値と最大値は、プラットフォームによって異なります。

デフォルト値は 1500 バイトです。

ステップ 4 **[OK]** をクリックします。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ステップ 6 ISA 3000、および Firewall Threat Defense Virtual で MTU を 1,500 バイト超に設定する場合は、システムを再起動して jumbo-frame reservation を有効にします。「デバイスのシャットダウンまたは再起動 （41 ページ）」を参照してください。

MAC アドレスの設定

MAC アドレスを手動で割り当てることが必要となる場合があります。また、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定することもできます。両方の画面でインターフェイスの MAC アドレスを設定した場合は、**[インターフェイス（Interfaces）]** > **[詳細（Advanced）]** タブのアドレスが優先されます。

（注） コンテナ インスタンスでは、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックします。
[情報（Information）] タブが選択されています。

ステップ 4 アクティブおよびスタンバイの MAC アドレスを設定します。

a) [アクティブな MAC アドレス（Active MAC Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

b) [スタンバイMACアドレス（Standby MAC Address）] フィールドに、ハイ アベイラビリティで使用する MAC アドレスを入力します。

アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 5 **[OK]** をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

スタティック ARP エントリの追加

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションを有効にします（ARP インスペクション （826 ページ） 参照）。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARPテーブルは、ARP応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定のIPアドレスのMACアドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレント モードの場合、管理トラフィックなどの Firewall Threat Defense デバイスとの間のトラフィックに、Firewall Threat Defense は ARP テーブルのダイナミック ARP エントリのみを使用します。

始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[ARP] タブをクリックします（トランスペアレント モードでは、[ARP と MAC（ARP and MAC）]）。

ステップ 4 [ARP 設定を追加（Add ARP Config）]（＋） をクリックします。
[ARP 設定を追加（Add ARP Config）] ダイアログボックスが表示されます。

ステップ 5 [IP アドレス（IP Address）] フィールドに、ホストの IP アドレスを入力します。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。

ステップ 7 このアドレスでプロキシ ARP を実行するには、[エイリアスを有効にする（Enable Alias）] チェックボックスをオンにします。

Firewall Threat Defense デバイスは、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

ステップ 8 [OK] をクリックし、次にもう一度 [OK] をクリックして、[詳細設定（Advanced settings）] を閉じます。

ステップ 9 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

静的 MAC アドレスの追加とブリッジグループの MAC 学習の無効化

通常、MACアドレスは、特定のMACアドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス ラーニングを無効にすることができます。ただし、MAC アドレスをスタティックにテーブルに追加しないかぎり、トラフィックは Firewall Threat Defense デバイスを通過できません。スタティック MAC アドレスは、MACアドレステーブルに追加することもできます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じMACアドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、Firewall Threat Defense デバイスはトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（スタティック ARP エントリの追加 （750 ページ） を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

始める前に

この画面は、トランスペアレントモードの名前付き BVI でのみ使用できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[ARP と MAC（ARP and MAC）] タブをクリックします。

ステップ 4 （任意） [MAC ラーニングを有効にする（Enable MAC Learning）] チェックボックスをオフにして MAC ラーニングを無効にします。

ステップ 5 スタティック MACアドレスを追加するには、[MAC設定を追加（Add MAC Config）] をクリックします。
[MAC 設定を追加（Add MAC Config）] ダイアログボックスが表示されます。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。[OK] をクリックします。

ステップ 7 [OK] をクリックして詳細設定を終了します。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

セキュリティの設定パラメータの設定

この項では、IP スプーフィングの防止方法、完全フラグメント リアセンブルの許可方法、および [プラットフォーム設定（Platform Settings）] でデバイス レベルで設定されるデフォルトのフラグメント設定のオーバーライド方法について説明します。

アンチ スプーフィング

この項では、インターフェイスでユニキャスト リバース パス フォワーディング（ユニキャスト RPF）を有効にします。ユニキャスト RPF は、ルーティング テーブルに従って、すべてのパケットが正しい送信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、Firewall Threat Defense デバイスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。ユニキャスト RPF は、送信元アドレスも調べるようにデバイスに指示します。そのため、リバース パス フォワーディング（Reverse Path Forwarding）と呼ばれます。Firewall Threat Defense デバイスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをデバイスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、Firewall Threat Defense デバイスはデフォルト ルートを使用してユニキャスト RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、デバイスはデフォルト ルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、Firewall Threat Defense デバイスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、デバイスはパケットをドロップします。

ユニキャスト RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションが含まれているため、初期パケットには逆ルートのルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持

されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

パケットあたりのフラグメント

デフォルトでは、Firewall Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントが Firewall Threat Defense デバイスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

フラグメントのリアセンブル

Firewall Threat Defense デバイスは、次に示すフラグメント リアセンブル プロセスを実行します。

- IP フラグメントは、フラグメント セットが作成されるまで、またはタイムアウト間隔が経過するまで収集されます。
- フラグメントセットが作成されると、セットに対して整合性チェックが実行されます。これらのチェックには、重複、テール オーバーフロー、チェーン オーバーフローはいずれも含まれません。
- Firewall Threat Defense デバイスで終端する IP フラグメントは、常に完全にリアセンブルされます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が無効化されている場合（デフォルト）、フラグメントセットは、さらに処理するためにトランスポート層に転送されます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が有効化されている場合、フラグメント セットは、最初に単一の IP パケットに結合されます。この単一の IP パケットは、さらに処理するためにトランスポート層に転送されます。

始める前に

この画面は、名前付きインターフェイスでのみ使用できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[セキュリティ設定（Security Configuration）] タブをクリックします。

ステップ 4 ユニキャストリバースパスフォワーディングを有効にするには、[アンチスプーフィングの有効化（Enable Anti Spoofing）] チェックボックスをオンにします。

ステップ 5 完全フラグメントリアセンブルを有効化するには、[完全フラグメントリアセンブルを許可（Allow Full Fragment Reassembly）] チェックボックスをオンにします。

ステップ 6 パケットごとに許容するフラグメント数を変更するには、[デフォルトフラグメント設定のオーバーライド（Override Default Fragment Setting）] チェックボックスをオンにして、次に示す値を設定します。

- サイズ（Size）：リアセンブルを待機する IP リアセンブル データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。この値を 1 に設定すると、フラグメントが無効化されます。
- チェーン（Chain）：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。
- タイムアウト（Timeout）：フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケットフラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。

ステップ 7 **[OK]** をクリックします。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

通常のファイアウォール インターフェイスの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
VTI のループバック インターフェイス サポート	7.3	任意（Any）	ループバック インターフェイスを追加できるようになりました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。VTIの場合、送信元インターフェイスとしてループバック インターフェイスを設定するのに加えて、静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されています。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [ループバック インターフェイスの追加（Add Loopback Interface）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
IPv6 DHCP	7.3	任意（Any）	Firewall Threat Defense で IPv6 アドレッシングの次の機能がサポートされるようになりました。 • DHCPv6 アドレスクライアント：Firewall Threat Defense は DHCPv6 サーバーから IPv6 グローバルアドレスとオプションのデフォルトルートを取得します。 • DHCPv6 プレフィックス委任クライアント：Firewall Threat Defense は DHCPv6 サーバーから委任プレフィックスを取得します。Firewall Threat Defense は、委任プレフィックスを使用して他の Firewall Threat Defense インターフェイスのアドレスを設定し、ステートレスアドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレスサーバー：SLAAC クライアントが Firewall Threat Defense に情報要求（IR）パケットを送信すると、Firewall Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Firewall Threat Defense は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの追加/編集（Add/Edit Interfaces）] > [IPv6] > [DHCP]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [DHCP IPv6プール（DHCP IPv6 Pool）]** 新規/変更されたコマンド：**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Azure ゲートウェイロードバランサの Firewall Threat Defense Virtual のペアプロキシ VXLAN	7.3	任意（Any）	Azure ゲートウェイロードバランサ（GWLB）で使用するために、Azure で Firewall Threat Defense Virtual 用のペアプロキシモード VXLAN インターフェイスを設定できます。Firewall Threat Defense Virtual は、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** サポートされているプラットフォーム：Azure の Firewall Threat Defense Virtual
VXLAN のサポート	7.2	任意（Any）	VXLAN カプセル化のサポートが追加されました。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [VTEP]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）]** [物理インターフェイスの編集（edit physical interface）] > [全般（General）] サポートされているプラットフォーム：すべて。

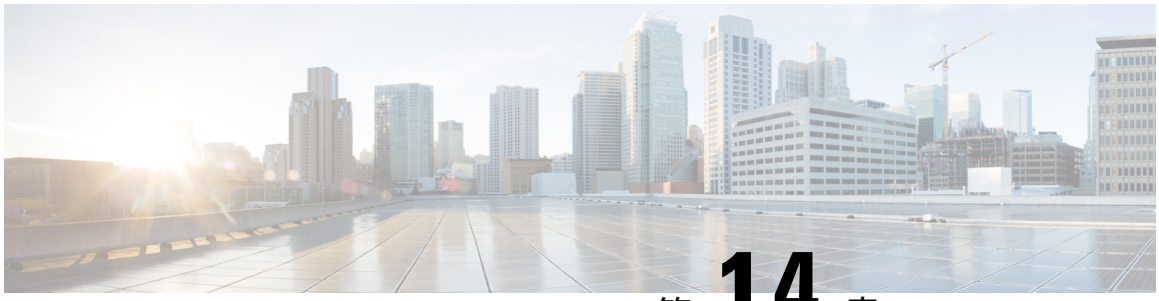
機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firewall Threat Defense Virtual の Geneve サポート	7.1	任意（Any）	Amazon Web Services（AWS）ゲートウェイロードバランサのシングルアームプロキシをサポートするために、Geneveカプセル化サポートが Firewall Threat Defense Virtual に追加されました。AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイ（全トラフィックの唯一の出入口）と、トラフィックを分散し、トラフィックの需要に合わせて Firewall Threat Defense Virtual を拡張するロードバランサを組み合わせます。 この機能には Snort 3 が必要です。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [VTEP]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）]** [物理インターフェイスの編集（edit physical interface）] > [全般（General）] サポートされているプラットフォーム：AWS の Firewall Threat Defense Virtual

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
31 ビット サブネット マスク	7.0	任意（Any）	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの FTD 間のフェールオーバーリンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。この機能は、ブリッジグループ用の BVI、またはマルチキャスト ルーティングではサポートされていません。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firepower 4100/9300 の Firewall Threat Defense 動作リンク状態と物理リンク状態の同期	6.7	いずれか	Firepower 4100/9300 シャーシで、Firewall Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Firewall Threat Defense アプリケーション インターフェイスの管理状態は考慮されません。Firewall Threat Defense からの同期がない場合は、たとえば、Firewall Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、Firewall Threat Defense のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、 Firewall Threat Defense が処理できるようになる前に外部ルータが Firewall Threat Defense へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、またはRadware vDP デコレータを使用する Firewall Threat Defense ではサポートされていません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] 画面：**[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）]** 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされているプラットフォーム：Firepower 4100/9300
Firepower 1010 ハードウェア スイッチのサポート	6.5	任意（Any）	Firepower 1010 では、各イーサネット インターフェイスをスイッチポートまたはファイアウォール インターフェイスとして設定できます。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [VLANインターフェイスの追加（Add VLAN Interface）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	6.5	任意（Any）	Firepower 1010 は、スイッチ ポートとして設定されている場合、イーサネット 1/7 およびイーサネット 1/8 の Power on Ethernet+（PoE+）をサポートします。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）] > [PoE]**
コンテナインスタンスで使用される VLAN サブインターフェイス	6.3.0	いずれか	柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Secure Firewall Management Center 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン > **[インターフェイス（Interfaces）]** タブ 新規/変更された Secure Firewall シャーシマネージャ 画面： **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）]** ドロップダウン メニューの **[サブインターフェイス（Subinterface）]** 新規/変更された FXOS コマンド：**create subinterface、set vlan、show interface、show subinterface** サポートされるプラットフォーム：Firepower 4100/9300
コンテナインスタンスのデータ共有インターフェイス	6.3.0	いずれか	柔軟な物理インターフェイスの使用を可能にするため、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Secure Firewall シャーシマネージャ 画面： **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [タイプ（Type）]** 新規/変更された FXOS コマンド：**set port-type data-sharing、show interface** サポートされるプラットフォーム：Firepower 4100/9300

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
統合ルーティングおよびブリッジング	6.2.0	いずれか	統合ルーティングおよびブリッジングによって、ブリッジグループとルーテッドインターフェイスの間でルーティングする機能が提供されます。ブリッジグループは、Firewall Threat Defense がルーティングではなくブリッジするインターフェイスのグループです。Firewall Threat Defense は、Firewall Threat Defense がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレントファイアウォールモードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッド インターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。Firewall Threat Defense にブリッジ グループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ 2 スイッチを使用するのではない別の方法が提供されます。ルーテッド モードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるクラスタリングの機能は、ルーテッドモードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスを追加（Add Interfaces）] > [ブリッジ グループ インターフェイス（Bridge Group Interface）]** サポートされているプラットフォーム：すべて（Firepower 2100 と Firewall Threat Defense Virtual を除く）



第 14 章

インラインセットとパッシブインターフェイス

IPS 専用のパッシブインターフェイス、パッシブ ERSPAN インターフェイス、インラインセットを設定できます。

- IPS インターフェイスについて （763 ページ）
- インラインセットの要件と前提条件 （767 ページ）
- インライン セットとパッシブ インターフェイスのガイドライン （769 ページ）
- パッシブ インターフェイスの設定 （771 ページ）
- インライン セットを設定します。 （773 ページ）
- インラインセットとパッシブインターフェイスの履歴 （778 ページ）

IPS インターフェイスについて

IPS インターフェイスには、パッシブ インターフェイス、パッシブ ERSPAN インターフェイス、インライン セットが含まれます。IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティポリシー（Snort）のみをサポートします。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティポリシー（Snort）のみをサポートします。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

（注） ファイアウォールモードは通常のファイアウォールインターフェイスにのみ影響を与えます。インライン セットやパッシブ インターフェイスなどの IPS 専用インターフェイスには影響を与えません。IPS 専用インターフェイスは両方のファイアウォール モードで使用可能です。

インライン セット

インラインセットはワイヤ上のバンプのように動作し、1つ以上のインターフェイスペアを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にFirewall Threat Defenseをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインペアの他のインターフェイスから、外部に再送信されます。インラインセットに複数のインラインペアがある場合、トラフィックはペアのインターフェイス間でのみ通過できます。異なるペアのインターフェイス間を渡すことはできません。

タップ モードでは、Firewall Threat Defense はインラインで展開されますが、ネットワーク トラフィック フローは妨げられません。代わりに、Firewall Threat Defenseは各パケットのコピーを作成して、パケットを分析できるようにします。それらのタイプのルールでは、ルールがトリガーされると侵入イベントが生成され、侵入イベントのテーブルビューにはトリガーの原因となったパケットがインライン展開でドロップされたことが示されることに注意してください。インライン展開された FTD でタップモードを使用することには、利点があります。たとえば、Firewall Threat Defense がインラインであるかのように Firewall Threat Defense とネットワーク間の配線をセットアップし、Firewall Threat Defense で生成される侵入イベントのタイプを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更してドロップ ルールを追加できます。Firewall Threat Defenseをインラインで展開する準備ができたら、タップ モードを無効にして、Firewall Threat Defense とネットワーク間の配線を再びセットアップせずに、不審なトラフィックのドロップを開始することができます。

（注） タップモードは、トラフィックによってはFirewall Threat Defenseのパフォーマンスに大きく影響します。

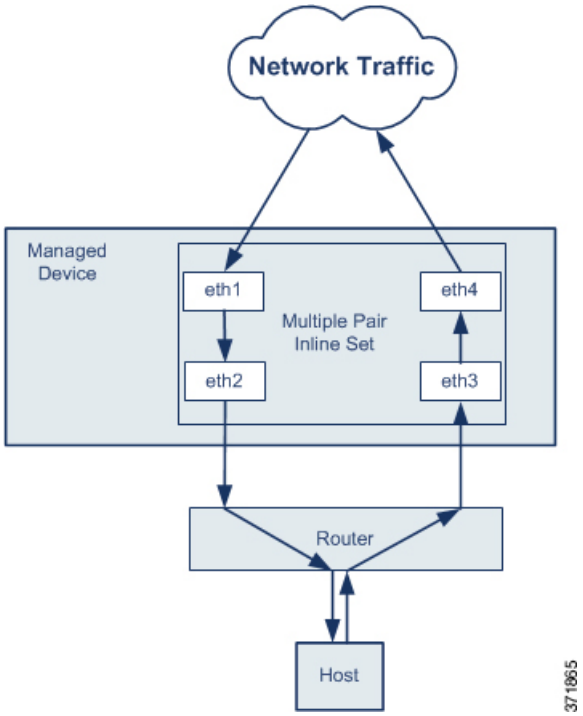
（注） 「透過インライン セット」としてインライン セットに馴染みがある人もいますが、インラインインターフェイスのタイプはトランスペアレントファイアウォールモードやファイアウォール タイプのインターフェイスとは無関係です。

複数のインライン ペアと非同期ルーティング

トラフィックがインバウンドであるかアウトバウンドであるかに応じて、異なるインラインペアを介してネットワーク上のホストと外部ホスト間のトラフィックをルーティングするように、インターフェイスを設定できます。これは非同期ルーティング設定です。非同期ルーティングを展開しても、インライン セットに 1 つのインライン ペアしか含めないと、デバイスがトラフィックの半分しか認識しないため、ネットワーク トラフィックが適切に分析されない可能性があります。

同じインライン セットに複数のインライン ペアを追加すると、システムが着信トラフィックと発信トラフィックを同じトラフィック フローの一部として識別させることができます。パッシブ インターフェイスでのみ、同じセキュリティ ゾーンにインターフェイス ペアを含めることによっても実現できます。

図 *261* : 非同期ルーティング



（注） 複数のインライン ペアを単一のインライン セットに割り当てたときに、重複トラフィックの問題が発生した場合は、個別のインライン セットにインライン ペアを再割り当てするか、セキュリティ ゾーンを変更する必要があります。

パケットのフラグメントが異なるインターフェイス ペアで受信された場合、それらは再構成されず、ドロップされます。パケットのすべてのフラグメントが同じインターフェイス ペアで送受信されるようにしてください。

パッシブ インターフェイス

パッシブ インターフェイスは、スイッチ SPAN またはミラー ポートを使用してネットワーク中のトラフィック フローをモニターします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で Firewall Threat Defense を構成した場合は、Firewall Threat Defense は特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信さ

れたトラフィックは再送されません。Encapsulated Remote Switched Port Analyzer（ERSPAN）インターフェイスは、複数のスイッチに分散された送信元ポートからのトラフィックをモニタし、GREを使用してトラフィックをカプセル化します。ERSPANインターフェイスは、Firewall Threat Defenseがルーテッド ファイアウォール モードになっている場合にのみ許可されます。

（注） 無差別モードの制限により、SR-IOV ドライバを使用する一部の Intel ネットワークアダプタ（Intel X710 や 82599 など）では、SR-IOV インターフェイスを NGFWv のパッシブインターフェイスとして使用することはできません。このような場合は、この機能をサポートするネットワークアダプタを使用してください。Intel ネットワークアダプタの詳細については、『Intel Ethernet Products』[英語] を参照してください。

インライン セットのハードウェア バイパスについて

サポートされているモデルの特定のインターフェイスモジュールでは（インラインセットの要件と前提条件（767ページ）を参照）、ハードウェア バイパス機能を有効にできます。ハードウェア バイパスにより、停電中のインライン インターフェイス ペア間でトラフィックが引き続きフローできるようにします。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

ハードウェア バイパス トリガー

ハードウェア バイパス は次のシナリオでトリガーされることがあります。

- Firewall Threat Defense のクラッシュ
- Firewall Threat Defense の再起動
- セキュリティ モジュールの再起動
- シャーシのクラッシュ
- Chassis reboot
- 手動トリガー
- シャーシの停電
- セキュリティ モジュールの電力損失

（注） ハードウェアバイパスは、計画外の障害または予期しない障害のシナリオのためのものです。計画されたソフトウェアアップグレード中に自動的にトリガーされることはありません。ハードウェアバイパスは、Firewall Threat Defenseアプリケーションの再起動時に、計画されたアップグレードプロセスの最後にのみ関与します。

ハードウェア バイパスのスイッチオーバー

通常の運用からハードウェア バイパスに切り替えたとき、またはハードウェア バイパスから通常の運用に戻したときに、トラフィックが数秒間中断する可能性があります。中断時間の長さに影響を与える可能性があるいくつかの要因があります。たとえば、銅線ポートの自動ネゴシエーション、リンク エラーやデバウンスのタイミングをどのように処理するかなどのオプティカル リンク パートナーの動作、スパニング ツリー プロトコルのコンバージェンス、ダイナミック ルーティング プロトコルのコンバージェンスなどです。この間は、接続が落ちることがあります。

また、通常の操作に戻った後で接続のミッドストリームを分析するときに、アプリケーションの識別エラーが原因で接続が切断されることがあります。

Snort フェール オープンと ハードウェア バイパス

タップ モード以外のインライン セットでは、[Snort フェール オープン（Snort Fail Open）] オプションを使用して、トラフィックをドロップするか、Snort プロセスがビジーまたはダウンしている場合に検査なしでトラフィックの通過を許可します。Snort フェール オープンは、ハードウェア バイパスをサポートするインターフェイス上のみでなく、タップ モードのものを除くすべてのインライン セットでサポートされます。

ハードウェア バイパス機能を使用すると、停電時や特定の限定されたソフトウェア障害などのハードウェア障害時にトラフィックが流れます。Snort フェール オープンをトリガーするソフトウェアの障害は、ハードウェア バイパスをトリガーしません。

ハードウェア バイパス Status

システムの電源が入っている場合、バイパス LED はハードウェア バイパスのステータスを表示します。LED の説明については、Firepower シャーシ ハードウェア インストレーションガイドを参照してください。

インラインセットの要件と前提条件

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

ハードウェア バイパス サポート

Firewall Threat Defense は、以下のモデルの特定のネットワーク モジュールのインターフェイス ペアで ハードウェア バイパス をサポートします。

- Firepower 2130 および 2140

- Cisco Secure Firewall 3100
- Firepower 4100
- Firepower 9300

（注） ISA 3000 にはハードウェアバイパス用の個別の実装があります。これは、FlexConfig のみを使用して有効にできます（FlexConfig ポリシー（2687 ページ）を参照）。この章は、ISA 3000 ハードウェアバイパスの設定には使用しないでください。

（注） ハードウェア バイパス 機能を有効にしなくても、ハードウェア バイパス インターフェイスを標準インターフェイスとして使用できます。

これらのモデルでサポートされている ハードウェア バイパス ネットワーク モジュールは以下のとおりです。

- Firepower 2130 および 2140：
  - Firepower 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド（FPR2K-NM-6X1SX-F）
  - Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR2K-NM-6X10SR-F）
  - Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR2K-NM-6X10LR-F）
- Secure Firewall 3100：
  - 6 ポート 1 G SFP Fail-to-Wire ネットワークモジュール、SX（マルチモード）（FPR3K-XNM-6X1SXF）
  - 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-6X10SRF）
  - 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X10LRF）
  - 6 ポート 25 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-X25SRF）
  - 6 ポート 25 G Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X25LRF）
  - 8 ポート 1 G 銅ケーブル Fail-to-Wire ネットワークモジュール（銅ケーブル）（FPR3K-XNM-8X1GF）

- Firepower 4100：
  - Firepower 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド（FPR4K-NM-6X1SX-F）
  - Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR4K-NM-6X10SR-F）
  - Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR4K-NM-6X10LR-F）
  - Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド（FPR4K-NM-2X40G-F）
  - Firepower 8 ポート 1G Copper FTW ネットワーク モジュール シングルワイド（FPR-NM-8X1G-F）
- FirePOWER 9300：
  - Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR9K-NM-6X10SR-F）
  - Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR9K-NM-6X10LR-F）
  - Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド（FPR9K-NM-2X40G-F）

ハードウェア バイパス では以下のポート ペアのみ使用できます。

- 1 および 2
- 3 および 4
- 5 および 6
- 7 および 8

インラインセットとパッシブインターフェイスのガイドライン

ファイアウォール モード

- ERSPAN インターフェイスは、デバイスがルーテッド ファイアウォール モードになっている場合にのみ許可されます。

クラスタリング

- インラインセットのリンクステートの伝達は、クラスタリングではサポートされていません。

マルチインスタンスモード

- マルチインスタンスの共有インターフェイスはサポートされていません。非共有インターフェイスを使用する必要があります。
- マルチインスタンスのシャーシ定義サブインターフェイスはサポートされていません。物理インターフェイスまたは EtherChannel を使用する必要があります。

一般的な注意事項

- インラインセットとパッシブインターフェイスは物理インターフェイスおよびEtherChannelsのみをサポートし、VLAN、またはその他の仮想インターフェイス（マルチインスタンスのシャーシ定義サブインターフェイスを含む）は使用できません。
- IPS インターフェイスは通常のファイアウォール保護をサポートしていないため、IPS セキュリティ ポリシー（Snort）では、すべてのトラフィックを検査できるようにトラフィック フローが同じ Firewall Threat Defense を通過する必要があります。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、インライン セットを使用するときに、Firewall Threat Defense を介して許可されません。BFD を実行している Firewall Threat Defense の両側に 2 つのネイバーがある場合、Firewall Threat Defense は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。
- インラインセットとパッシブインターフェイスについては、Firewall Threat Defense ではパケットで 802.1Q ヘッダーが 2 つまでサポートされます（Q-in-Q サポートとも呼ばれます）。ただし、Firepower 4100/9300 は例外で、802.1Q ヘッダーは 1 つだけサポートされます。**注**：ファイアウォールタイプのインターフェイスでは Q-in-Q はサポートされず、802.1Q ヘッダーは 1 つだけサポートされます。

ハードウェア バイパス ガイドライン

- ハードウェア バイパス ポートはインライン セットでのみサポートされます。
- ハードウェア バイパス ポートを EtherChannel の一部にはできません。
- ハードウェア バイパス 高可用性モードではサポートされていません。
- ハードウェア バイパス は Firepower 9300 でのシャーシ内クラスタリングでサポートされます。シャーシ内の最後のユニットに障害が発生すると、ポートはハードウェアバイパスモードになります。シャーシ間クラスタリングはサポートされません。これは、シャーシ間クラスタリングがスパンドEtherChannelのみをサポートするためです。ハードウェア バイパス ポートを EtherChannel の一部にすることはできません。

- Firepower 9300 でのシャーシ内クラスタに含まれるすべてのモジュールに障害が発生すると、最終ユニットで ハードウェア バイパス がトリガーされ、トラフィックは引き続き通過します。ユニットが復帰すると、ハードウェア バイパスはスタンバイ モードに戻ります。ただし、アプリケーショントラフィックと一致するルールを使用すると、それらの接続が切断され、再確立する必要がある場合があります。状態情報がクラスタユニットに保持されず、ユニットがトラフィックを許可されたアプリケーションに属するものとして識別できないため、接続は切断されます。トラフィックのドロップを回避するには、アプリケーションベースのルールの代わりにポートベースのルールを使用します（展開に適している場合）。
- ハードウェア バイパス 機能を有効にしなくても、ハードウェア バイパス インターフェイスを標準インターフェイスとして使用できます。

IPS インターフェイスでサポートされていないファイアウォール機能

- DHCP サーバー
- DHCP リレー
- DHCP クライアント
- TCP Intercept
- ルーティング
- NAT
- VPN
- アプリケーション インスペクション
- QoS
- NetFlow
- VXLAN

パッシブ インターフェイスの設定

ここでは、次の方法について説明します。

- インターフェイスを有効にします。デフォルトでは、インターフェイスは無効です。
- インターフェイス モードをパッシブまたはERSPANに設定します。ERSPANインターフェイスの場合は、ERSPAN パラメータと IP アドレスを設定します。
- MTU を交換してください。デフォルトでは、MTU は 1500 バイトに設定されます。MTU の詳細については、MTU について （743 ページ）を参照してください。
- 特定の速度と二重通信（使用できる場合）を設定する。デフォルトでは、速度とデュプレックスは [自動（Auto）] に設定されます。

（注） Secure Firewall Threat Defense（FXOS シャーシに搭載） の場合、Firepower 4100/9300 の基本インターフェイスの設定を行います。詳細については、「物理インターフェイスの設定 （254 ページ）」を参照してください。

始める前に

- EtherChannel を使用している場合は、「EtherChannel の設定 （644 ページ）」に従って追加します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [モード（Mode）] ドロップダウン リストで、[パッシブ（Passive）] または [Erspan] を選択します。

ステップ 4 [有効化（Enable）] チェックボックスをオンにして、インターフェイスを有効にします。

ステップ 5 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 6 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ステップ 7 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 8 （任意） [一般（General）] で、[MTU] を 64 ～ 9198 バイトの間で設定します。Secure Firewall Threat Defense Virtual および Secure Firewall Threat Defense（FXOS シャーシに搭載） の場合、最大値は 9000 バイトです。

デフォルト値は 1500 バイトです。

ステップ 9 ERSPAN インターフェイスの場合は、次のパラメータを設定します:

- [フロー ID（Flow Id）]：ERSPAN トラフィックを特定するために送信元と宛先セッションによって使用される ID を、1 ～ 1023 の間で設定します。この ID は、ERSPAN 宛先セッション設定でも入力する必要があります。
- [ソース IP（Source IP）]：ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。

ステップ 10 ERSPAN インターフェイスの場合は、[IPv4] で IPv4 アドレスとマスクを設定します。

ステップ 11 （任意） [Hardware Configuration] をクリックして、デュプレックスと速度を設定します。

正確な速度とデュプレックスオプションはハードウェアによって異なります。

- [Duplex]：[Full]、[Half]、または[Auto]を選択します。デフォルトは[Auto（自動）]です。
- [速度（Speed）]：[10],[100]、[1000]、または[自動（Auto）]を選択します。デフォルトは[Auto（自動）]です。

ステップ 12 **[OK]** をクリックします。

ステップ 13 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

インライン セットを設定します。

ここでは、インラインセットに追加できるインラインペアごとに2つの物理インターフェイスまたはEtherChannelを有効にして名前を付けます。インラインセットごとに複数のインラインペアを追加できます。また、状況に応じて、サポートされるインラインペアに対して ハードウェア バイパス を有効にすることができます。

（注） Firepower 4100/9300 の場合、シャーシで FXOS の基本インターフェイスの設定を構成します。詳細については、「物理インターフェイスの設定 （254 ページ）」を参照してください。

始める前に

- EtherChannelを使用している場合は、「EtherChannelの設定 （644ページ）」に従って追加します。
- Firewall Threat Defense インライン ペア インターフェイスに接続する STP 対応スイッチに対して STP PortFast を設定することを推奨します。この設定は、ハードウェア バイパスの設定に特に有効でバイパス時間を短縮できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defenseデバイス[編集（Edit）]（✎）をクリックします。[インターフェイス（Interfaces）]タブがデフォルトで選択されます。

ステップ 2 インラインペアの各インターフェイスについて、インターフェイスに名前を付けて有効にします。他のハードウェア設定を指定することもできます。インラインペアの各インターフェイス

のハードウェア設定が一致していることを確認してください。インターフェイスの複数のペアを設定できます。

a) 編集するインターフェイス [編集（Edit）]（） をクリックします。
b) [名前（Name）] フィールドに、48 文字以内で名前を入力します。
c) [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。
d) （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

e) [モード（Mode）] は [なし（None）] のままにします。

このインターフェイスをインラインセットに追加すると、このフィールドにモードのインラインが表示されます。

f) セキュリティゾーンはまだ設定しないでください。後でこの手順でインラインセットを作成してから設定する必要があります。
g) （任意） [Hardware Configuration] をクリックして、デュプレックスと速度を設定します。

正確な速度とデュプレックスオプションはハードウェアによって異なります。

- [Duplex]：[Full]、[Half]、または [Auto] を選択します。デフォルトは [Auto（自動）] です。
- [速度（Speed）]：[10],[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [Auto（自動）] です。

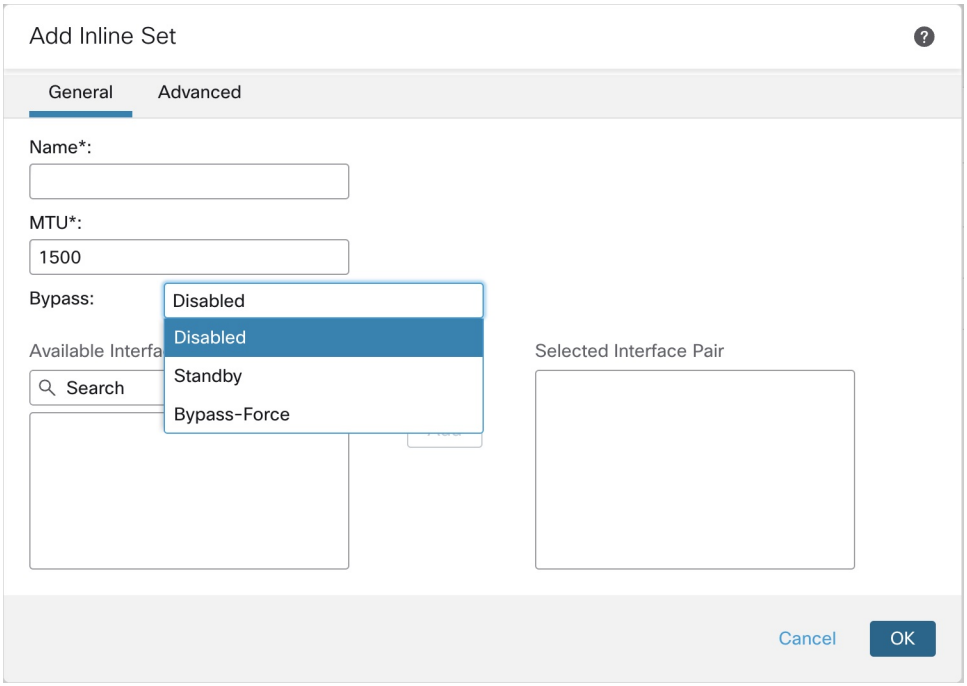
h) [OK] をクリックします。

このインターフェイスに対して他の設定は行わないでください。

ステップ 3 [Inline Sets] をクリックします。

ステップ 4 [Add Inline Set] をクリックします。

図 *262 :* インラインセットの追加



[Add Inline Set] ダイアログボックスが、[General] が選択された状態で表示されます。

ステップ 5 [名前（Name）] フィールドに、セットの名前を入力します。

ステップ 6 （任意） ジャンボフレームを有効にするには、**MTU** を変更します。

インラインセットの MTU の設定は使用されません。ただし、ジャンボフレームの設定はインラインセットに関連します。ジャンボフレームによりインラインインターフェイスは最大9000バイトのパケットを受信できます。ジャンボフレームを有効にするには、デバイスのすべてのインターフェイスの MTU を 1500 バイトより大きい値に設定する必要があります。

ステップ 7 ハードウェア バイパス を設定します。

a) [Bypass] モードの場合、次のいずれかのオプションを選択します。

- [Disabled]：ハードウェア バイパス がサポートされているインターフェイスの場合はハードウェア バイパス を無効にするか、またはハードウェア バイパス がサポートされていないインターフェイスを使用します。
- [Standby]：サポートされているインターフェイスの ハードウェア バイパス をスタンバイ状態に設定します。ハードウェア バイパス インターフェイスのペアのみ表示されます。スタンバイ状態の場合、トリガーイベントが発生するまで、インターフェイスは通常動作を保ちます。
- **[Bypass-Force]**：インターフェイスペアを手動で強制的にバイパス状態にします。**[Inline Sets]** では、[Bypass-Force] モードになっているインターフェイスペアに対して [Yes] が表示されます。

b) [Available Interfaces Pairs] 領域でペアをクリックし、[Add] をクリックして [Selected Interface Pair] 領域にそのペアを移動します。

この領域には、モードが [None] に設定されている名前付きインターフェイスと有効なインターフェイス間で可能なすべてのペアが表示されます。

ステップ 8 （任意） **[Advanced]** をクリックして、次のオプション パラメータを設定します。

- **[Tap Mode]**：インラインタップ モードに設定します。

  同じインライン セットでこのオプションと厳密な TCP 強制を有効にすることはできないことに注意してください。

  （注）
  タップモードを有効または無効にする必要がある場合は、メンテナンス期間中に行う必要があります。デバイスがトラフィックを渡している間にモードを変更すると、トラフィックが中断される可能性があります。

  （注）
  タップモードは、トラフィックによってはFirewall Threat Defenseのパフォーマンスに大きく影響します。

- **[Propagate Link State]**：リンクステートの伝達を設定します。

  インラインセットのインターフェイスの1つが停止した場合、リンク ステート伝播によってインライン インターフェイス ペアのもう一方のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、もう一方のインターフェイスも自動的に起動します。つまり、いずれかのインターフェイスのリンク ステートが変更されると、デバイスがその変更を検知し、もう一方のインターフェイスのリンク ステートを更新して両方のインターフェイスのリンク ステートを一致させるということです。リンク ステートの変更が伝播されるまでに最大4秒かかることに注意してください。障害状態のネットワーク デバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。

  （注）
  クラスタリングを使用する場合は、[リンクステートの伝達（Propagate Link State）] を有効にしないでください。

- [Snort フェール オープン（Snort Fail Open）]：[ビジー（Busy）] オプションと [ダウン（Down）] オプションのいずれか、または両方を有効/無効にして、Snortプロセスがビジーまたはダウンしている場合は新規または既存のトラフィックをインスペクションなしで通過させるか（有効）、またはトラフィックをドロップします（無効）。

  デフォルトでは、Snort プロセスがダウンしている場合はトラフィックをインスペクションなしで通過させ、ビジーの場合はトラフィックをドロップします。

  Snort プロセスの状態には以下の意味があります。

  - ビジー：トラフィック バッファが満杯であるため十分な速度でトラフィックを処理しきれていません。デバイスが処理できる量を上回るトラフィックがあるか、他のソフトウェア リソースに問題があることを意味します。

- ダウン：再起動が必要となる設定を導入したため、再起動が行われています。展開またはアクティブ化された際に Snort プロセスを再起動する設定 （167 ページ）を参照してください。

Snort プロセスは、ダウンしてから再起動すると、新しい接続を検査します。誤検知と検出漏れを防ぐために、Snort プロセスはインライン インターフェイス、ルーテッド インターフェイス、またはトランスペアレントインターフェイス上の既存の接続を検査しません。これは、プロセスのダウン中に初期セッション情報が失われている可能性があるためです。

（注）
Snort プロセスが開始できない場合、Snort プロセスに依存する機能は動作しません。該当する機能には、アプリケーション制御とディープインスペクションが含まれます。システムでは、シンプルかつ容易に判断できるトランスポート層とネットワークの特性を使用して、基本的なアクセスコントロールのみ実行されます。

（注）
[厳密なTCPの適用（Strict TCP Enforcement）] オプションはサポートされていません。

ステップ 9 各インターフェイスのセキュリティゾーンを設定します。

a) [インターフェイス（Interfaces）] をクリックします。

b) メンバーインターフェイスの [編集（Edit）]（✎） をクリックします。

c) **[Security Zone]** ドロップダウン リストからセキュリティ ゾーンを選択するか、**[New]** をクリックして、新しいセキュリティゾーンを追加します。

セキュリティ ゾーンはインターフェイスをインライン セットに追加してからでないと設定できません。インターフェイスをインラインセットに追加すると、モードがインラインに設定されて、インライン タイプのセキュリティ ゾーンを選択できるようになります。

d) **[OK]** をクリックします。

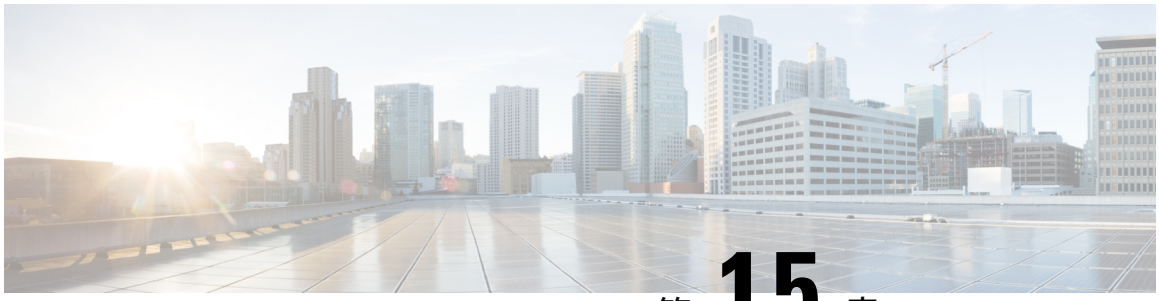
ステップ 10 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

インラインセットとパッシブインターフェイスの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
サポート対象ネットワークモジュールに関する Cisco Secure Firewall 3100 でのハードウェアバイパスのサポート	7.2	任意（Any）	Cisco Secure Firewall 3100 は、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェアバイパス機能をサポートするようになりました。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Cisco Secure Firewall 3100
Firepower 4100/9300 の Firewall Threat Defense 動作リンク状態と物理リンク状態の同期	6.7	いずれか	Firepower 4100/9300 シャーシで、Firewall Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Firewall Threat Defense アプリケーション インターフェイスの管理状態は考慮されません。Firewall Threat Defense からの同期がない場合は、たとえば、Firewall Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、シャットダウン開始後からしばらくの間アップ状態のままになったりすることがあります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、 Firewall Threat Defense が処理できるようになる前に外部ルータが Firewall Threat Defense へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、またはRadware vDP デコレータを使用する Firewall Threat Defense ではサポートされていません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] 画面：**[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）]** 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされているプラットフォーム：Firepower 4100/9300

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
サポート対象ネットワークモジュールに関する Firepower 2130 および 2140 でのハードウェアバイパスのサポート	6.3.0	いずれか	Firepower 2130 および 2140 は、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェアバイパス機能をサポートするようになりました。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Firepower 2130 および 2140
Firewall Threat Defense インラインセットまたはパッシブインターフェイスでの EtherChannel のサポート	6.2.0	いずれか	Firewall Threat Defenseインラインセットまたはパッシブインターフェイスで EtherChannel を使用できるようになりました。
サポート対象ネットワーク モジュールに対する Firepower 4100/9300 でのハードウェア バイパス サポート	6.1.0	いずれか	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Firepower 4100/9300
Firewall Threat Defense のインライン セット リンク ステート伝達サポート	6.1.0	いずれか	Firewall Threat Defense アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、Firewall Threat Defense はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。 新規/変更された FXOS コマンド：**show fault |grep link-down**、**show interface detail**



第 15 章

DHCP および DDNS

次のトピックでは、DHCP サービスと DDNS サービスについて、および Threat Defense デバイスでこれらを設定する方法について説明します。

- DHCP サービスと DDNS サービスについて （781 ページ）
- DHCP および DDNS の要件と前提条件 （783 ページ）
- DHCP サービスと DDNS サービスのガイドライン （783 ページ）
- DHCPv4 サーバーの設定 （785 ページ）
- DHCPv6 ステートレス サーバーの設定 （788 ページ）
- DHCP リレー エージェントの設定 （792 ページ）
- ダイナミック DNS の設定 （794 ページ）
- DHCP および DDNS の履歴 （801 ページ）

DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

DHCPv4 サーバについて

DHCP は、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。Firewall Threat Defense デバイス は、Firewall Threat Defense デバイス インターフェイスに接続されている DHCP クライアントに、DHCP サーバーを提供します。DHCP サーバは、ネットワーク設定パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージをリッスンし、DHCP サーバは UDP ポート 67 でメッセージをリッスンします。

DHCP オプション

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータは DHCP メッセージの Options フィールドにストアされているタグ付けされたア

イテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。
- DHCP オプション 3 では、デフォルト ルートが設定されます。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が Firewall Threat Defense ですでに設定されていると、DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションを使用すれば、DHCP クライアントに DNS、WINS、およびドメイン名の各パラメータを提供できます。DHCP オプション 15 は DNS ドメインのサフィックスに使用されます。DHCP 自動コンフィギュレーションの設定を使用して、これらの値を取得したり、これらを手動で定義したりできます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動構成設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動構成を有効にできます。DHCP 自動構成によって、DNS サーバーおよび WINS サーバーとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバー名および WINS サーバー名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

DHCPv6 ステートレス サーバーについて

ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアント（IPv6 プレフィックス委任クライアントの有効化（732 ページ））については、DHCP IPv6 プールを定義して DHCPv6 サーバーに割り当てることにより、これらのクライアントが情報要求（IR）パケットを Firewall Threat Defense に送信する際に（DNS サーバー、ドメイン名などの）情報を提供するように Firewall Threat Defense を設定できます。Firewall Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス（Firewall Threat Defense がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、Firewall Threat Defense デバイス はブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェントを使用して、ブロードキャストを受信している Firewall Threat Defense デバイス のインターフェイスが DHCP 要求を別のデバイスの DHCP サーバーに転送するように設定できます。

DHCP および DDNS の要件と前提条件

モデルのサポート

Threat Defense

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

DHCP サービスと DDNS サービスのガイドライン

この項では、DHCP および DDNS サービスを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

ファイアウォール モード

- DHCP リレーは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。
- DHCP サーバーは、ブリッジ グループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。 ルーテッド モードでは、DHCP サーバーは BVI インターフェイスでサポートされますが、ブリッジ グループ メンバー インターフェイスではサポートされません。DHCP サーバーを動作させるために、BVI には名前が必要です。
- DDNS は、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。

- DHCPv6 ステートレス サーバーは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。

クラスタリング

- DHCPv6 ステートレス サーバは、クラスタリングではサポートされません。

IPv6

DHCP ステートレス サーバーの IPv6 と DHCP リレーをサポートします。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- 名前と IP アドレスを持つ任意のインターフェイス（物理インターフェイス、サブインターフェイス、ルーテッドモードの BVIなど）で DHCP サーバーを設定できます。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。しかし、DNS サーバー、ドメイン名、オプション、ping のタイムアウト、WINS サーバーなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバーによって使用されます。
- インターフェイスで DHCP サーバーも有効になっている場合、そのインターフェイスを DHCP クライアントとして設定することはできません。スタティック IP アドレスを使用する必要があります。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。
- Firewall Threat Defense は、QIP DHCP サーバーと DHCP プロキシサービスとの併用をサポートしません。
- DHCP サーバーは、BOOTP 要求をサポートしていません。

DHCPv6 サーバ

DHCPv6 ステートレス サーバは、DHCPv6 アドレス、プレフィックス委任クライアントまたは DHCPv6 リレーが設定されているインターフェイス上で設定できません。

DHCP リレー

- 仮想ルータ、グローバルおよびインターフェイス固有のサーバーを合わせて 10 台までの DHCPv4 リレーサーバーを設定できます。インターフェイスごとには、4 台まで設定できます。

- 仮想ルータごとに 10 台までの DHCPv6 リレーサーバーを設定できます。IPv6 のインターフェイス固有のサーバーはサポートされません。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。
- DHCP リレー サービスは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスでは利用できません。ただし、アクセス ルールを使用して DHCP トラフィックを通過させることはできます。DHCP 要求と応答が Firewall Threat Defense を通過できるようにするには、2 つのアクセス ルールを設定する必要があります。1 つは内部インターフェイスから外部（UDP 宛先ポート 67）への DCHP 要求を許可するもので、もう 1 つは逆方向（UDP 宛先ポート 68）に向かうサーバーからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 Firewall Threat Defense に接続する必要があり、他のリレー エージェントやルータを介して要求を送信できません。IPv6 の場合、Firewall Threat Defense は別のリレー サーバーからのパケットをサポートします。
- DHCP クライアントは、Firewall Threat Defense が要求をリレーする DHCP サーバーとは別のインターフェイスに存在する必要があります。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。

DDNS サービス

ファイアウォールの DDNS は、DynDNS サービスのみをサポートします。したがって、DDNS が次のシンタックスの更新 URL で設定されていることを確認します。

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**

DHCPv4 サーバーの設定

DHCPv4 サーバーを設定するには、次の手順を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [DHCP] > [DHCP サーバー（DHCP Server）] を選択します。

ステップ 3 次の DHCP サーバーのオプションを設定します。

- [Ping タイムアウト（Ping Timeout）]：Firewall Threat Defense デバイスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ～ 10000 ミリ秒です。デフォルト値は、50 ミリ秒です。

アドレスの衝突を避けるために、Firewall Threat Defense デバイスは、1 つのアドレスに ICMP ping パケットを 2 回送信してから、そのアドレスを DHCP クライアントに割り当てます。

- [リース長（Lease Length）]：リースの期間が終了する前に、割り当て IP アドレスをクライアントが使用できる秒単位の時間。有効な値の範囲は、300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。
- （ルーテッド モード）[自動設定（Auto-configuration）]：Firewall Threat Defense デバイスで DHCP 自動設定を有効にします。自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動設定にしない場合は、自動設定を無効にして、手順 4 で値を追加することもできます。
- （ルーテッド モード）[インターフェイス（Interface）]：自動設定に使用されるインターフェイスを指定します。 仮想ルーティング機能を備えたデバイスの場合、このインターフェイスはグローバル仮想ルータインターフェイスにしかなれません。

ステップ 4 自動設定をオーバーライドするには、以下を実行します。

- インターフェイスのドメイン名を入力します。たとえば、デバイスは Your_Company ドメインにあるかもしれません。
- ドロップダウン リストから、インターフェイスに設定された DNS サーバ（プライマリおよびセカンダリ）を選択します。DNS サーバを新たに追加する手順については、ネットワーク オブジェクトの作成 （1351 ページ）を参照してください。
- ドロップダウン リストから、インターフェイスに設定された WINS サーバ（プライマリおよびセカンダリ）を選択します。WINS サーバーを新たに追加する手順については、ネットワーク オブジェクトの作成 （1351 ページ）を参照してください。

ステップ 5 [サーバー（Server）]を選択して[追加（Add）]をクリックし、次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウン リストからインターフェイスを選択します。トランスペアレント モードでは、名前付きブリッジ グループ メンバー インターフェイスを指定します。 ルーテッド モードでは、名前付きルーテッド インターフェイスまたは名前付き BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。DHCP サーバーが動作するためには、BVI の各ブリッジ グループ メンバー インターフェイスにも名前を付ける必要があることに注意してください。
- [アドレス プール（Address Pool）]：DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲です。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCP サーバを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバを有効にします。

ステップ 6 [OK] をクリックして、DHCP サーバーの設定を保存します。

ステップ 7 （オプション）[詳細（Advanced）] を選択して、[追加（Add）] をクリックし、DHCP クライアントに戻すオプションの情報のタイプを指定します。

- [オプション コード（Option Code）]：Firewall Threat Defense デバイスは、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（1 ～ 255）がサポートされています。DHCP オプション コードの詳細については、DHCPv4 サーバについて （781 ページ）を参照してください。

  （注）
  Firewall Threat Defense デバイスは、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。オプション コードと、コードに関連付けられたタイプおよび期待値の詳細については、RFC 2132 を参照してください。

- [タイプ（Type）]：DHCP のオプションのタイプ。使用できるオプションには、IP、ASCII、および HEX が含まれます。IP を選択する場合、[IP アドレス（IP Address）] フィールドに IP アドレスを追加する必要があります。ASCII を選択する場合、[ASCII] フィールドに [ASCII] 値を追加する必要があります。HEX を選択する場合、[HEX] フィールドに [HEX] 値を追加する必要があります。
- [IP アドレス 1（IP Address 1）] および [IP アドレス 2（IP Address 2）]：このオプション コードで戻る IP アドレス。IP アドレスを新たに追加する手順については、ネットワーク オブジェクトの作成 （1351 ページ）を参照してください。
- [ASCII]：DHCP クライアントに戻る ASCII 値。文字列にスペースを含めることはできません。
- [HEX]：DHCP クライアントに戻る HEX 値。文字列はスペースなしの偶数でなければなりません。0x プレフィックスを使用する必要はありません。

ステップ 8 [OK] をクリックして、オプション コードの設定を保存します。

ステップ 9 DHCP ページで [保存（Save）] をクリックして変更を保存します。

ステップ 10 DHCP バインディングを表示するには、次のコマンドを使用します。

show dhcpd binding

例：

```
> show dhcpd binding
IP Address Client-id         Lease Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds     automatic
```

DHCPv6 ステートレス サーバーの設定

ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアントについては、これらのクライアントが情報要求（IR）パケットを Firewall Threat Defense に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように Firewall Threat Defense を設定できます。

DHCP IPv6 プールの作成

DHCPv6 サーバーで使用する DHCP IPv6 プールを作成します。クライアントが Firewall Threat Defense に情報要求（IR）パケットを送信すると、DHCPv6 サーバーは、DNS サーバー名やドメイン名などの情報を提供します。DHCP IPv6 プールは、IR メッセージで送信するパラメータを定義します。

この機能は、ルーテッドモードでのみサポートされます。この機能は、クラスタリングまたはハイアベイラビリティではサポートされません。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクトタイプのリストから [DHCP IPv6プール（DHCP IPv6 Pool）]を選択します。

ステップ 3 追加（ ） をクリックします。

ステップ 4 **DNS サーバー**と**ドメイン名**を設定します。

手動で値を定義して [追加（Add）] をクリックするか、[インポート（Import）] をクリックして、プレフィックス委任クライアント インターフェイスで Firewall Threat Defense が DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用します。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じパラメータを手動で設定し、かつ [インポート（Import）] を使用することはできません。

図 *263* : 手動での値の定義

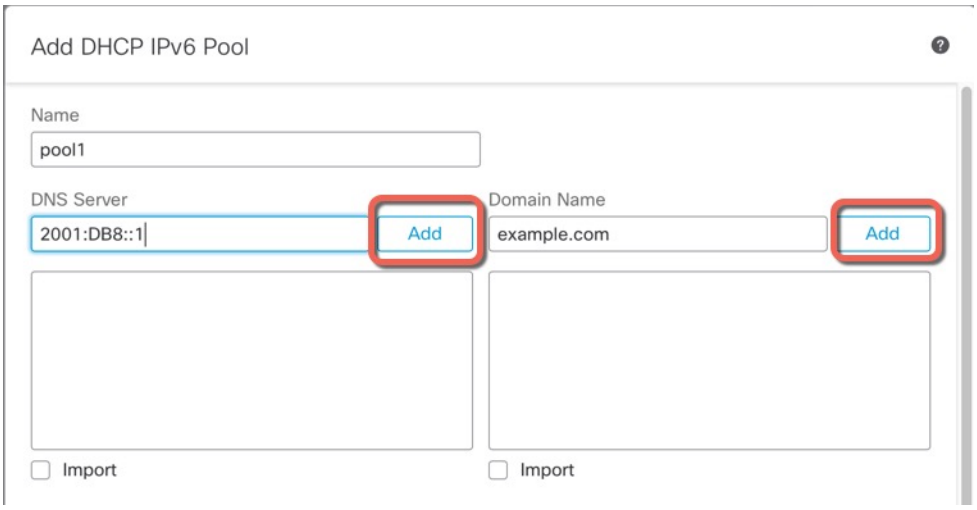
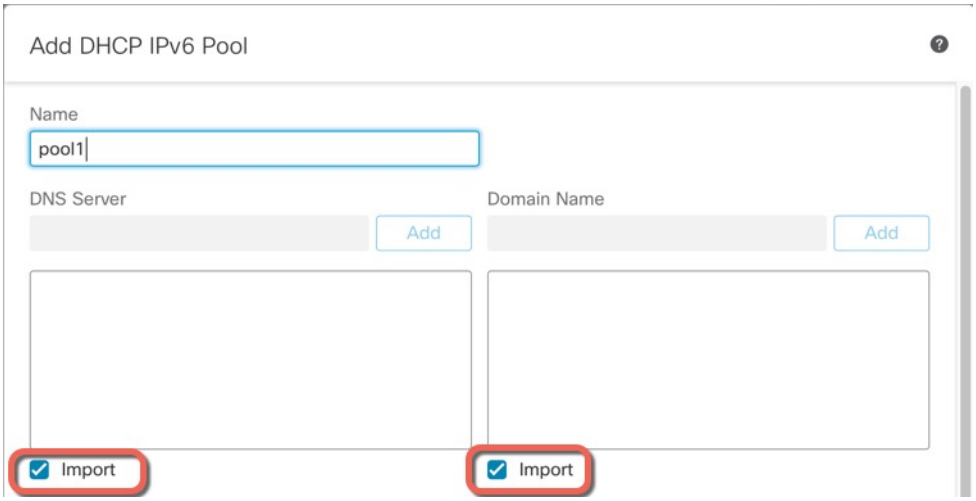


図 *264* : 値のインポート



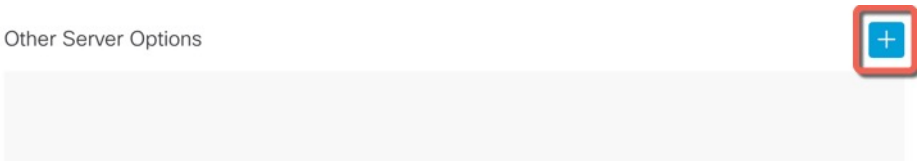
ステップ 5 **その他のサーバーオプション**を定義します。

次のサーバーのドメイン名と IP アドレスを定義できます。

- NIS
- NISP
- SIP
- SNTP

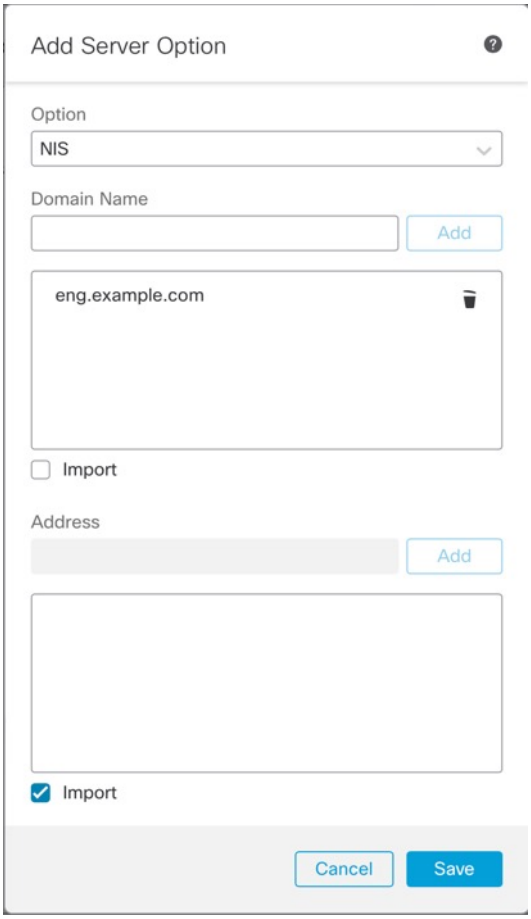
a) 追加（ ） をクリックします。

図 *265 :* その他のサーバーオプション



b) [オプション（Option）] でサーバータイプを選択し、**ドメイン名**と**アドレス**を手動で定義するか、[インポート（Import）] をオンにします。

図 *266 :* サーバーのドメイン名とアドレスの定義



[インポート（Import）] を指定すると、プレフィックス委任クライアント インターフェイスで Firewall Threat Defense が DHCPv6 サーバーから取得した 1 つ以上のパラメータが使用されます。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じパラメータを手動で設定し、かつ [インポート（Import）] を使用することはできません。

c) **[保存（Save）]** をクリックします。
d) 各サーバータイプでこの手順を繰り返します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 このプールはDHCPv6 サーバーで使用します。「DHCPv6 ステートレスサーバーの有効化（791 ページ）」を参照してください。

DHCPv6 ステートレスサーバーの有効化

ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアント（IPv6 プレフィックス委任クライアントの有効化（732 ページ））については、これらのクライアントが情報要求（IR）パケットを Firewall Threat Defense に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように Firewall Threat Defense を設定できます。Firewall Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータアドバタイズメントメッセージで受信したプレフィックス（Firewall Threat Defense がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

この機能は、ルーテッドモードでのみサポートされます。この機能は、クラスタリングまたはハイアベイラビリティではサポートされません。

始める前に

DHCP IPv6 プールオブジェクトを追加します。DHCP IPv6 プールの作成（788 ページ）を参照してください。このオブジェクトは、IR メッセージに含まれるサーバーパラメータを定義します。

手順

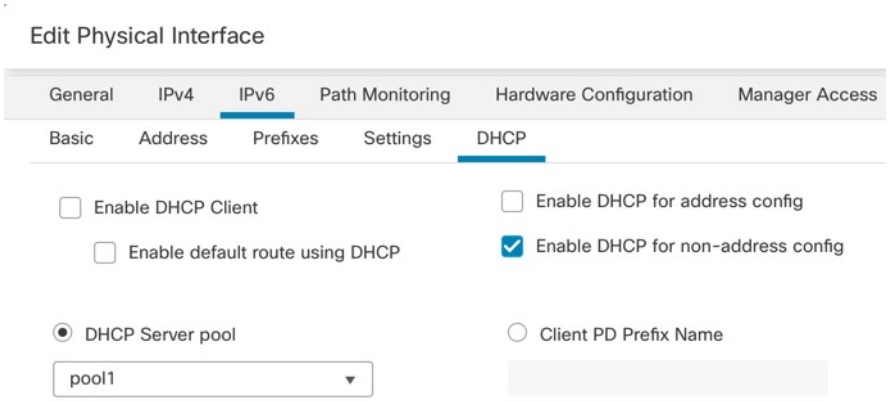
ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎）をクリックします。

ステップ 3 [IPv6] ページをクリックしてから、[DHCP] をクリックします。

ステップ 4 [DHCPサーバープール（DHCP Server Pool）] をクリックし、前に作成したオブジェクトを選択します。

図 *267 : DHCPv6* サーバーの有効化



ステップ 5 DHCPv6 サーバーについて SLAAC クライアントに通知するには、[アドレス以外の設定でDHCP を有効にする（Enable DHCP for non-address config）] をオンにします。

このフラグは、DHCPv6 から DNS サーバー アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

DHCP リレー エージェントの設定

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、Firewall Threat Defense デバイスはブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。

ブロードキャストを受信している Firewall Threat Defense デバイスのインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバーに転送するように設定すると、この状況を改善できます。

（注） 透過型ファイアウォールモードでは DHCP リレーはサポートされていません。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [DHCP] > [DHCP リレー（DHCP Relay）] を選択します。

ステップ 3 [IPv4リレータイムアウト（IPv4 Relay Timeout）] および [IPv6リレータイムアウト（IPv6 Relay Timeout）] フィールドでは、Firewall Threat Defense デバイスが DHCP リレーエージェントのタイムアウトを待つ時間を秒単位で入力します。有効な値の範囲は、1 ～ 3600 秒です。デフォルト値は 60 秒です。

タイムアウトは、ローカル DHCP リレー エージェントを介すアドレス ネゴシエーション用です。

ステップ 4 [DHCPリレーエージェント（DHCP Relay Agent）] で、[追加（Add）] をクリックして、以下のオプションを設定します。

- [インターフェイス（Interface）]：DHCP クライアントに接続されているインターフェイス。
- [IPv4リレーを有効にする（Enable IPv4 Relay）]：このインターフェイスで IPv4 DHCP リレーを有効にします。
- [ルート設定（Set Route）]：（IPv4 用）サーバーからの DHCP メッセージのデフォルト ゲートウェイ アドレスを、元の DHCP 要求をリレーした DHCP クライアントに最も近い Firewall Threat Defense デバイスのインターフェイスのアドレスに変更します。このアクションを行うと、クライアントは、自分のデフォルトルートを設定して、DHCP サーバーで異なるルータが指定されている場合でも、Firewall Threat Defense デバイスをポイントすることができます。パケット内にデフォルトのルータ オプションがなければ、Firewall Threat Defense デバイスは、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。
- [IPv6 リレーを有効にする（Enable IPv6 Relay）]：このインターフェイスで IPv6 DHCP リレーを有効にします。

ステップ 5 [OK] をクリックして、DHCP リレー エージェントの変更を保存します。

ステップ 6 [DHCPサーバー（DHCP Servers）] タブで、[追加（Add）] をクリックして、以下のオプションを設定します。

IPv4 サーバー アドレスおよび IPv6 サーバー アドレスが同じサーバーに属していても、個別のエントリとして追加します。

- [サーバー（Server）]：DHCP サーバーの IP アドレス。ドロップダウン リストから IP アドレスを選択します。新たに加えるには、次を参照してください。 ネットワーク オブジェクトの作成 （1351 ページ）

- [インターフェイス（Interface）]：指定の DHCP サーバーが接続されるインターフェイス。DHCP リレー エージェントと DHCP サーバーを、同じインターフェイスに設定することはできません。

ステップ 7 [OK] をクリックして、DHCP サーバーの変更を保存します。

ステップ 8 DHCP ページで [保存（Save）] をクリックして変更を保存します。

ダイナミック DNS の設定

インターフェイスで DHCP IP アドレッシングを使用している場合、DHCP リースが更新されると、割り当てられた IP アドレスが変更されることがあります。完全修飾ドメイン名（FQDN）を使用してインターフェイスに到達できる必要がある場合、この IP アドレスの変更が原因で DNS サーバーのリソースレコード（RR）が古くなる可能性があります。ダイナミック DNS（DDNS）は、IP アドレスまたはホスト名が変更されるたびに DNS の RR を更新するメカニズムです。DDNS はスタティックまたは PPPoE IP アドレッシングにも使用できます。

DDNS では DNS サーバーの A RR と PTR RR を更新します。A RR には名前から IP アドレスへのマッピングが含まれ、PTR RR でアドレスが名前にマッピングされます。

Firewall Threat Defense では、次の DDNS 更新方式をサポートしています。

- 標準の DDNS：標準の DDNS 更新方式は RFC 2136 で定義されています。

  この方式では、Firewall Threat Defense と DHCP サーバーで DNS 要求を使用して DNS の RR を更新します。Firewall Threat Defense または DHCP サーバーは、ローカル DNS サーバーにホスト名に関する情報を求める DNS 要求を送信し、その応答に基づいて RR を所有するメイン DNS サーバーを特定します。その後、Firewall Threat Defense または DHCP サーバーからメイン DNS サーバーに更新要求が直接送信されます。一般的なシナリオを次に示します。

  - Firewall Threat Defense で A RR を更新し、DHCP サーバーで PTR RR を更新する。

    通常、Firewall Threat Defense が A RR を「所有」し、DHCP サーバーが PTR RR を「所有」するため、両方のエンティティで個別に更新を要求する必要があります。IP アドレスまたはホスト名が変更されると、Firewall Threat Defense から DHCP サーバーに DHCP 要求（FQDN オプションを含む）が送信され、PTR RR の更新を要求する必要があることが通知されます。

  - DHCP サーバーで A RR と PTR RR の両方を更新する。

    このシナリオは、Firewall Threat Defense に A RR を更新する権限がない場合に使用します。IP アドレスまたはホスト名が変更されると、Firewall Threat Defense から DHCP サーバーに DHCP 要求（FQDN オプションを含む）が送信され、A RR と PTR RR の更新を要求する必要があることが通知されます。

セキュリティのニーズやメイン DNS サーバーの要件に応じて、異なる所有権を設定できます。たとえば、静的アドレスの場合、Firewall Threat Defense で両方のレコードの更新を所有します。

- Web：Web 更新方式では、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用します。

  この方式では、IP アドレスまたはホスト名が変更されると、Firewall Threat Defense からアカウントを持っている DNS プロバイダーに HTTP 要求が直接送信されます。

[DDNS] ページは、DDNS に関連する DHCP サーバー設定の設定もサポートしています。

（注） DDNS は BVI またはブリッジグループのメンバーインターフェイスではサポートされません。

始める前に

- **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[DNS サーバーグループ（DNS Server Group）]** で DNS サーバーグループを構成し、**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[DNS]** でインターフェイスのグループを有効にします。DNS （828 ページ）を参照してください。
- デバイスのホスト名を設定します。Firewall Threat Defense の初期セットアップを実行するとき、または **configure network hostname** コマンドを使用して、ホスト名を設定できます。インターフェイスごとにホスト名を指定しない場合は、デバイスのホスト名が使用されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[DHCP]** > **[DDNS]** を選択します。

ステップ 3 標準の DDNS 方式：Firewall Threat Defense からの DNS 要求を有効にするように DDNS 更新方式を設定します。

すべての要求を DHCP サーバーで実行する場合は、DDNS 更新方式を設定する必要はありません。

a) [DDNS更新方式（DDNS Update Methods）] で、[追加（Add）] をクリックします。
b) [メソッド名（Method Name）] を設定します。
c) [DDNS] をクリックします。
d) （任意） [Update Interval] で、DNS 要求の更新間隔を設定します。デフォルトでは、すべての値が 0 に設定され、IP アドレスまたはホスト名が変更されるたびに更新要求が送信されます。要求を定期的に送信するには、[Days]（0 ～ 364）、[Hours]、[Minutes]、[Seconds] で間隔を設定します。

e) Firewall Threat Defense が更新する [更新レコード（Update Records）] を設定します。

この設定は、Firewall Threat Defense から直接更新するレコードにのみ影響します。DHCP サーバーで更新するレコードを指定するには、インターフェイスごとまたはグローバルに DHCP クライアント設定を行います。ステップ 5 （796 ページ）を参照してください。

- [未定義（Not Defined）]：Firewall Threat Defense からの DNS 更新を無効にします。
- [AおよびPTRの両レコード（Both A and PTR Records）]：Firewall Threat Defense で A RR と PTR RR の両方を更新するように設定します。スタティックまたは PPPoE IP アドレッシングには、このオプションを使用します。
- [A レコード（A Records）]：Firewall Threat Defense で A RR のみを更新するように設定します。DHCP サーバーで PTR RR を更新する場合は、このオプションを使用します。

f) [OK] をクリックします。

g) この方式をステップ 5 （796 ページ） でインターフェイスに割り当てます。

ステップ 4 Web 方式：Firewall Threat Defense からの HTTP 更新要求を有効にするように DDNS 更新方式を設定します。

a) [DDNS更新方式（DDNS Update Methods）] で、[追加（Add）] をクリックします。

b) [メソッド名（Method Name）] を設定します。

c) [Web] をクリックします。

d) [Web更新タイプ（Web Update Type）] を、IPv4、IPv6、または両方のタイプのアドレスを更新するように設定します。

e) [Web URL] を設定します。更新 URL を指定します。必要な URL については、DNS プロバイダーに問い合わせてください。

次の構文を使用します。

https://*username***:***password***@***provider-domain/path***?hostname=<h>&myip=<a>**

例：

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) （任意） [Update Interval] で、DNS 要求の更新間隔を設定します。デフォルトでは、すべての値が 0 に設定され、IP アドレスまたはホスト名が変更されるたびに更新要求が送信されます。要求を定期的に送信するには、[Days]（0 ～ 364）、[Hours]、[Minutes]、[Seconds] で間隔を設定します。

g) [OK] をクリックします。

h) この方式をステップ 5 （796 ページ） でインターフェイスに割り当てます。

i) Web タイプ方式の DDNS の場合は、HTTPS 接続用の DDNS サーバ証明書の検証のために DDNS サーバのルート CA も識別する必要があります。ステップ 9（799 ページ）を参照してください。

ステップ 5 DDNS のインターフェイス設定として、このインターフェイスの更新方式、DHCP クライアント設定、ホスト名などを設定します。

a) [DDNSインターフェイス設定（DDNS Interface Settings）] で、[追加（Add）] をクリックします。

b) ドロップダウンリストから [Interface] を選択します。

c) [DDNS更新方式（DDNS Update Methods）] ページで作成した [メソッド名（Method Name）] を選択します。

（標準の DDNS 方式）すべての更新を DHCP サーバーで実行する場合は、方式を割り当てる必要はありません。

d) このインターフェイスの [ホスト名（Host Name）] を設定します。

ホスト名を設定しない場合は、デバイスのホスト名が使用されます。FQDN を指定しない場合、DNS サーバーグループのデフォルトのドメイン（スタティックまたは PPPoE IP アドレッシングの場合）、または DHCP サーバーのドメイン名（DHCP IP アドレッシングの場合）が追加されます。

e) 標準の DDNS 方式：[DHCPクライアントが更新要求をDHCPサーバーに要求（DHCP Client requests DHCP server to update requests）] で、DHCP サーバーで更新するレコードを指定します。

Firewall Threat Defense から DHCP サーバーに DHCP クライアント要求が送信されます。DHCP サーバーも DDNS をサポートするように設定する必要があることに注意してください。サーバーはクライアント要求を受け入れるように設定できるほか、クライアントをオーバーライドすることもできます（この場合、サーバーで実行している更新をクライアントで実行しないようにクライアントに応答します）。

スタティックまたは PPPoE IP アドレッシングの場合、これらの設定は無視されます。

（注）
これらの値は、[DDNS] ページで、すべてのインターフェイスに対してグローバルに設定することもできます。インターフェイスごとの設定は、グローバル設定よりも優先されます。

- [未選択（Not Selected）]：DHCP サーバーへの DDNS 要求を無効にします。クライアントで DDNS 更新を要求しなくても、DHCP サーバーから更新を送信するように設定できます。
- [更新なし（No Update）]：DHCP サーバーで更新を実行しないように要求します。この設定は、[Both A and PTR Records] を有効にした DDNS 更新方式と連携して機能します。
- [PTRのみ（Only PTR）]：DHCP サーバーで PTR RR の更新を実行するように要求します。この設定は、[A Records] を有効にした DDNS 更新方式と連携して機能します。
- [AおよびPTRの両レコード（Both A and PTR Records）]：DHCP サーバーで A RR と PTR RR の両方の更新を実行するように要求します。この設定では、DDNS 更新方式をインターフェイスに関連付ける必要はありません。

f) [OK] をクリックします。

（注）

[ダイナミックDNS更新（Dynamic DNS Update）] 設定は、Firewall Threat Defense で DHCP サーバーを有効にするときのDHCPサーバー設定に関連します。詳細については、ステップ 6（798 ページ）を参照してください。

ステップ 6 Firewall Threat Defense で DHCP サーバーを有効にすると、DDNS の DHCP サーバー設定を構成できます。

DHCP サーバーを有効にするには、DHCPv4 サーバーの設定（785 ページ）を参照してください。DHCP クライアントが標準の DDNS 更新方式を使用する場合のサーバーの動作を構成できます。サーバーが更新を実行する場合に、クライアントのリースが期限切れになる（更新されない）場合、サーバーは、DNS サーバーが担当していた RR を削除するように要求します。

a) サーバー設定は、グローバルに構成することも、インターフェイスごとに構成することもできます。グローバル設定については、メインの [DDNS] ページを参照してください。インターフェイスごとの設定については、[DDNSインターフェイス設定（DDNS Interface Settings）] ページを参照してください。インターフェイス設定は、グローバル設定よりも優先されます。

b) [ダイナミックDNS更新（Dynamic DNS Update）] で、DHCP サーバーが更新する DNS RR を構成します。

- [未選択（Not Selected）]：クライアントが要求した場合でも、DDNS 更新は無効になっています。
- [PTRのみ（Only PTR）]：DDNS 更新を有効にします。[DHCPクライアント要求のオーバーライド（Override DHCP Client Requests）] 設定を有効にすると、サーバーは PTR RR のみを更新します。それ以外の場合、サーバーはクライアントが要求する RR を更新します。クライアントが FQDN オプションで更新要求を送信しない場合、サーバーは DHCP オプション 12 で検出されたホスト名を使用して、A RR と PTR RR の両方の更新を要求します。
- [AおよびPTRの両レコード（Both A and PTR Records）]：DDNS 更新を有効にします。[DHCPクライアント要求のオーバーライド（Override DHCP Client Requests）] 設定を有効にすると、サーバーは A RR と PTR RR の両方を更新します。それ以外の場合、サーバーはクライアントが要求する RR を更新します。クライアントが FQDN オプションで更新要求を送信しない場合、サーバーは DHCP オプション 12 で検出されたホスト名を使用して、A RR と PTR RR の両方の更新を要求します。

c) DHCPクライアントによって要求された更新アクションをオーバーライドするには、[DHCPクライアント要求のオーバーライド（Override DHCP Client Requests）] をオンにします。

サーバーは、要求がオーバーライドされたので、サーバーで実行している更新をクライアントで実行しないようにクライアントに応答します。

ステップ 7 （任意） 一般的な DHCP クライアント設定を構成します。これらの設定は DDNS には関係ありませんが、DHCP クライアントの動作に関係しています。

a) [DDNS] ページで、[DHCPクライアントブロードキャストを有効にする（Enable DHCP Client Broadcast）] をオンにして、DHCP サーバーが DHCP 応答をブロードキャストするように要求します（DHCP オプション 1）。

b) デフォルトの内部生成文字列ではなく、オプション 61 の DHCP 要求パケット内に保存された MAC アドレスを強制するには、**[DDNS]** > **[DHCPクライアントIDインターフェイス（DHCP Client ID Interface）]**で、[使用可能なインターフェイス（Available Interfaces）] リストからインターフェイスを選択し、[追加（Add）]をクリックして、それを [選択したインターフェイス（Selected Interfaces）] リストに移動します。

いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。この設定は DDNS とは直接関係ありませんが、一般的な DHCP クライアントの設定です。

ステップ 8 [デバイス（Device）] ページで [保存（Save）] をクリックして変更を保存します。

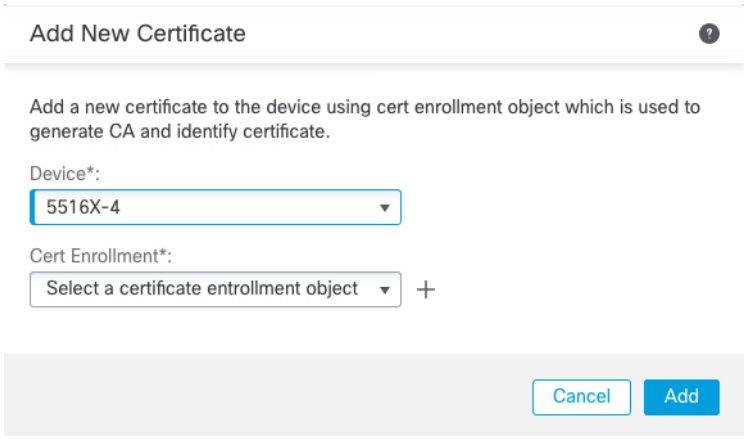
ステップ 9 Web 方式の DDNS の場合は、HTTPS 接続用の DDNS サーバ証明書の検証のために DDNS サーバのルート CA も識別する必要があります。

次に、DDNS サーバの CA をトラストポイントとして追加する例を示します。

a) DDNS サーバーの CA 証明書を取得します。この手順では、PEM 形式を使用した手動インポートを示していますが、PKCS12 を使用することもできます。

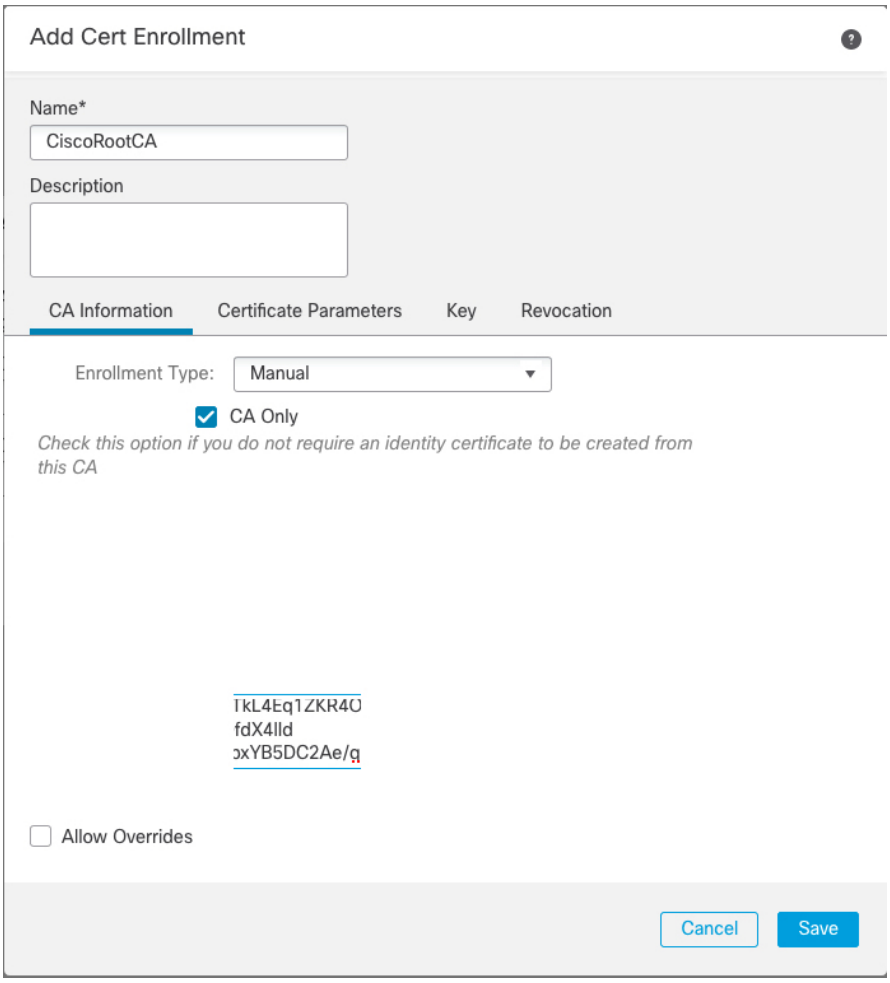
b) Firewall Management Center で、**[デバイス（Devices）]** > **[証明書（Certificates）]** を選択し、[追加（Add）] をクリックします。

c) [デバイス（Device）] を選択し、[追加（Add）] (+) をクリックします。



[証明書の登録の追加（Add Cert Enrollment）] ダイアログボックスが表示されます。

d) 次のフィールドに入力し、[保存（Save）] をクリックします。

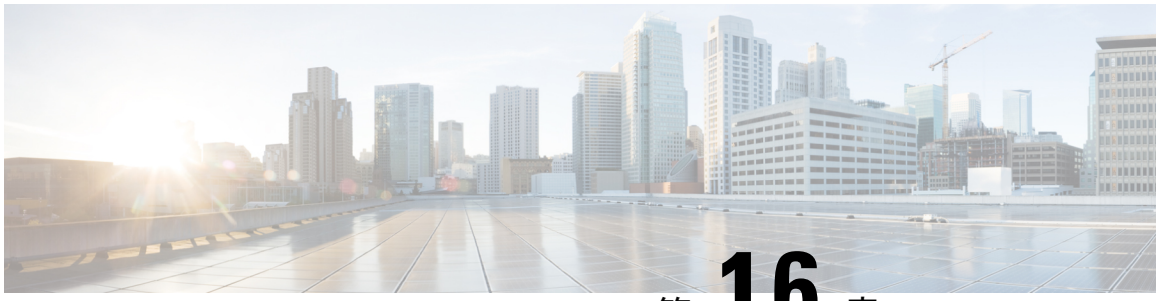


- 名前を入力します。
- **[登録タイプ（Enrollment Type）] > [手動（Manual）]**を選択します。
- [CAのみ（CA Only）] をクリックします。
- ステップ 9.a （799 ページ） の CA テキストを貼り付けます。

e) [保存（Save）] をクリックします。

DHCP および DDNS の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
DHCPv6 ステートレスサーバー	7.3.0	7.3.0	Firewall Threat Defense は、DHCPv6 プレフィックス委任クライアントを使用するときに、軽量の DHCPv6 ステートレスサーバーをサポートするようになりました。SLAAC クライアントが Firewall Threat Defense に情報要求（IR）パケットを送信すると、Firewall Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Firewall Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの追加/編集（Add/Edit Interfaces）] > [IPv6] > [DHCP]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [DHCP IPv6プール（DHCP IPv6 Pool）]** 新規/変更されたコマンド：**show ipv6 dhcp**



第 16 章

Firepower 1000/2100 の SNMP

この章では、Firepower 1000/2100 の SNMP を設定する方法について説明します。

- Firepower 1000/2100 の SNMP について （803 ページ）
- Firepower 1000/2100 の SNMP の有効化と SNMP プロパティの設定 （804 ページ）
- Firepower 1000/2100 の SNMP トラップの作成 （806 ページ）
- Firepower 1000/2100 の SNMP ユーザーの作成 （807 ページ）

Firepower 1000/2100 の SNMP について

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：Firepower シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに報告する Firepower 1000/2100 シャーシ内のソフトウェアコンポーネント。Firepower シャーシには、エージェントと一連の MIB が含まれています。SNMP エージェントを有効にし、マネージャとエージェント間のリレーションシップを作成するには、Firewall Management Center で SNMP を有効にし、設定します。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower 1000/2100 シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。。

Firepower 1000/2100 の SNMP の有効化と SNMP プロパティの設定

（注） この手順は Firepower 1000/2100 にのみ該当します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 次のフィールドに入力します。

名前	説明
[管理状態（Admin State）] チェックボックス	SNMP を有効にするか無効にするか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。
[ポート（Port）] フィールド	Firepower のシャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。

名前	説明
[コミュニティ（Community）] フィールド	Firepower シャーシが SNMP ホストに送信するトラップメッセージに含まれるデフォルトの SNMPv1 または v2 コミュニティの名前、あるいは SNMP v3 のユーザー名およびパスワード。 SNMPv1 および SNMPv2 の有効なコミュニティ文字列を入力します。 • 1 ー 32 文字までの英数字および特殊文字 !（感嘆符）、-（ハイフン）、~（チルダ）、&&（二重アンパサンド）、[ ]（角カッコ）、^（カラ）、'（引用符）、"（二重引用符）、および <>（山カッコ）。 • @（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。 • 文字列は、0x21 から 0x7E の範囲内の ASCII 文字でも指定できますが、HTML挿入ベクター、つまり引用符（'）、二重引用符（"）、および山括弧（<>）は除外されます。 有効な SNMPv3 のユーザー名およびパスワードを入力します。 • ユーザー名には英数字を使用でき、@（アットマーク）、\（バックスラッシュ）、.（ピリオド）、_（下線）、および -（ハイフン）を含めることができます。 • パスワードの制限は、コミュニティ文字列の制限と同じです。 [コミュニティ（Community）] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [設定：はい（Set: Yes）] となることに注意してください。[コミュニティ（Community）] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [設定：いいえ（Set: No）] となります。
[システム管理者名（System Admin Name）] フィールド	SNMP の実装担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[Location] フィールド	SNMP エージェント（サーバ）が動作するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 4 [保存] をクリックします。

次のタスク

SNMP トラップおよびユーザを作成します。

Firepower 1000/2100 の SNMP トラップの作成

（注） この手順は Firepower 1000/2100 にのみ該当します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMP トラップ設定（SNMP Traps Configuration）] 領域で、[追加（Add）] をクリックします。

ステップ 4 [SNMP トラップ設定（SNMP Trap Configuration）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Host Name] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[コミュニティ（Community）] フィールド	Firepower シャーシがトラップを SNMP ホストに送信するときに含める SNMP v1 または v2 のコミュニティ名または SNMP v3 のユーザー名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。
[ポート（Port）] フィールド	Firepower のシャーシがトラップのために SNMP ホストと通信するポート。 1 ～ 65535 の整数を入力します。
[バージョン（Version）] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **V1** • **[V2]** • **V3**

名前	説明
[タイプ（Type）] フィールド	バージョンとして [V2] または [V3] を選択した場合に、送信するトラップのタイプ。次のいずれかになります。 • **[Traps]** • **情報**
[特権（Privilege）] フィールド	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。 • [認証（Auth）]：認証あり、暗号化なし • [認証なし（Noauth）]：認証なし、暗号化なし • [秘密（Priv）]：認証あり、暗号化あり

ステップ 5 [OK] をクリックして、[SNMP トラップ設定（SNMP Trap Configuration）] ダイアログボックスを閉じます。

ステップ 6 [保存（Save）] をクリックします。

Firepower 1000/2100 の SNMP ユーザーの作成

（注） この手順は Firepower 1000/2100 にのみ該当します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMP ユーザー設定（SNMP Users Configuration）] 領域で、[追加（Add）] をクリックします。

ステップ 4 [SNMP ユーザー設定（SNMP User Configuration）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ユーザー名（Username）] フィールド	SNMP ユーザーに割り当てられるユーザー名。 32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、-（ハイフン）も指定できます。

名前	説明
[認証アルゴリズム タイプ（Auth Algorithm Type）] フィールド	許可タイプ：**SHA**。
[AES-128 を使用（Use AES-128）] チェックボックス	オンにすると、このユーザーに AES-128 暗号化が使用されます。 （注） SNMPv3 は DES をサポートしていません。[AES-128] ボックスをオフのままにすると、プライバシーの暗号化は行われず、設定されたプライバシーパスワードは無効になります。
[認証パスワード（Authentication Password）] フィールド	ユーザーのパスワード。
[確認（Confirm）] フィールド	確認のためのパスワードの再入力。
[暗号化パスワード（Encryption Password）] フィールド	ユーザーのプライバシー パスワード。
[確認（Confirm）] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 5 [OK] をクリックして、[SNMP ユーザー設定（SNMP User Configuration）] ダイアログボックスを閉じます。

ステップ 6 [保存（Save）] をクリックします。

第 17 章

QoS

以下のトピックでは、Firewall Threat Defenseデバイスを使ってネットワーク トラフィックを管理するために Quality of Service（QoS）機能を使用する方法について説明します。

- QoS の概要 （809 ページ）
- QoS ポリシーについて （810 ページ）
- QoS の要件と前提条件 （810 ページ）
- QoS ポリシーによるレート制限 （811 ページ）
- QoS の履歴 （822 ページ）

QoS の概要

Quality of Service（QoS）は、アクセス制御によって許可または信頼されている（ポリシーの）ネットワーク トラフィックをレート制限します。システムはファストパスされたトラフィックにレート制限は行いません。

QoS は Firewall Threat Defense デバイスのルーテッドインターフェイスでのみサポートされていますが、サイト間 VPN および VTI インターフェイスではサポートされていません。

レート制限された接続のロギング

QoS 用のロギング設定はありません。接続はロギングなしでレート制限することができ、またレート制限されているという理由だけで接続をロギングすることはできません。接続イベントで QoS 情報を表示するには、適切な接続の終了を Firewall Management Center データベースに個別にロギングする必要があります。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Other Connections You Can Log」を参照してください。

レート制限された接続の接続イベントには、どの程度のトラフィックがドロップされ、どの QoS の設定がトラフィックを制限したかについての情報が含まれています。この情報はイベント ビューア（ワークフロー）、ダッシュボード、レポートで確認できます。

QoS ポリシーについて

管理対象デバイスに展開する QoS ポリシーによりレート制限が決まります。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

システムは指定した順序で QoS ルールをトラフィックと照合します。システムは、すべての条件がトラフィックに一致する最初のルールに従ってトラフィックをレート制限します。どのルールにも一致しないトラフィックは、レート制限を受けません。

（注） デバイス上の QoS ルールを含むルールの総数は 255 以下である必要があります。このしきい値に達すると、展開警告メッセージが表示されます。正常に展開するには、ルールの数を減らす必要があります。

QoS ルールは、送信元または接続先（ルーティング先）インターフェイスによって制約を設ける必要があります。システムは、これらの個別のインターフェイスでそれぞれ独立したレート制限を行います。複数のインターフェイスにまとめてレート制限を指定することはできません。

QoS ルールでは、その他のネットワーク特性や、アプリケーション、URL、ユーザ ID、およびカスタム セキュリティ グループ タグ（SGT）などのコンテキスト情報によってトラフィックのレート制限を行うこともできます。

ダウンロード トラフィックとアップロード トラフィックは、それぞれ独立してレート制限が可能です。システムは、接続イニシエータを基準としてダウンロードかアップロードかを判別します。

（注） QoS はメインアクセス制御設定に従属するものではありません。QoS は個別に設定します。ただし、同じデバイスに展開されたアクセス コントロール ポリシーおよび QoS ポリシーはアイデンティティ設定を共有します。アクセス制御への他のポリシーの関連付け（1765 ページ）を参照してください。

QoS の要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

QoS ポリシーによるレート制限

ポリシー ベースのレート制限を実行するために、管理対象デバイスに QoS ポリシーを設定して展開します。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

ポリシーの編集は、1 つのブラウザウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[QoS]** を選択します。

ステップ 2 [新規ポリシー（New Policy）] をクリックして、新しい QoS ポリシーを作成して、必要に応じてターゲットデバイスを割り当てます。詳細については、QoS ポリシーの作成（812 ページ）を参照してください。

既存のポリシーを [コピー（Copy）]（ ）または [編集（Edit）]（）することもできます。

ステップ 3 QoS ルールを設定します。QoS ルールの設定（813 ページ）またはQoS ルール条件（816 ページ）を参照してください。

QoS ポリシーエディタの [ルール（Rules）] には、各ルールが評価順にリストされ、ルール条件とレート制限の設定の概要が表示されます。右クリックのメニューには、ルールの管理オプション（移動、有効化、無効化など）があります。

大規模な展開では、特定のデバイスまたはデバイスのグループに影響するルールのみを表示する、[デバイス基準のフィルタ（Filter by Device）] が役に立ちます。また、ルールの検索とルール内の検索も可能です。システムは、[ルールの検索（Search Rules）] フィールドに入力されたテキストをルールの名前および条件値と照合します。これには、オブジェクトとオブジェクトグループが含まれます。

（注）
ルールを適切に作成して順序付けることは複雑なタスクですが、効果的な展開を構築する上で不可欠なタスクです。慎重に計画していないと、ルールが別のルールをプリエンプション処理したり、追加のライセンスが必要になったり、ルールに無効な設定が含まれる場合がありま

す。アイコンにより、コメント、警告、およびエラーが表されます。問題があれば、[警告の表示（Show Warnings）] をクリックしてリストを表示します。詳細については、アクセス制御ルールのベストプラクティス （1736 ページ）を参照してください。

ステップ 4 [ポリシーの割り当て（Policy Assignments）] をクリックして、ポリシーがターゲットにしている管理対象デバイスを特定します。詳細については、QoS ポリシーのターゲット デバイスの設定 （813 ページ）を参照してください。

ポリシーの作成中にデバイス ターゲットを特定した場合は、選択内容を確認します。

ステップ 5 QoS ポリシーを保存します。

ステップ 6 この機能では一部のパケットを通過させる必要があるため、これらのパケットを検査するようにシステムを設定する必要があります。トラフィック識別の前に通過するパケットを処理するためのベストプラクティス （2746 ページ）およびトラフィック識別の前に通過するパケットを処理するためのポリシーの指定 （2747 ページ）を参照してください。

ステップ 7 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

QoS ポリシーの作成

ルールのない新規 QoS ポリシーは、レート制限を実行しません。

手順

ステップ 1 **[デバイス（Devices）] > [QoS]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 （オプション）ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリックするか、[選択されたデバイス（Selected Devices）] にドラッグ アンド ドロップします。表示されるデバイスを絞り込むには、[検索（Search）] フィールドに検索文字列を入力します。

ポリシーを展開する前に、デバイスを割り当てる必要があります。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- QoS ポリシーを設定および展開します。QoS ポリシーによるレート制限 （811 ページ）を参照してください。

QoS ポリシーのターゲット デバイスの設定

各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

手順

ステップ 1 QoS ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 ターゲット リストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。
- 削除：1 つのデバイスの横にある [削除（Delete）]（） をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。検索をクリアするには、[クリア（Clear）]（） をクリックします。

ステップ 3 [OK] をクリックしてポリシーの割り当てを保存します。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

QoS ルールの設定

ルールを作成または編集するときに、一般的なルール プロパティを設定するには、ルール エディタの上部を使用します。ルール条件とコメントを設定するには、ルールエディタの下部を使用します。

手順

ステップ 1 QoS ポリシーエディタの [ルール（Rules）] で、次の操作を実行します。

- ルールの追加：[ルールの追加（Add Rule）] をクリックします。
- ルールの編集：[編集（Edit）]（） をクリックします。

ステップ 2 [名前（Name）]を入力します。

ステップ 3 ルール コンポーネントを設定します。

- [有効化（Enabled）]：ルールを有効にするかどうかを指定します。
- [QoS の適用（Apply QoS On）]：レート制限するインターフェイス（[宛先インターフェイス オブジェクトのインターフェイス（Interfaces in Destination Interface Objects）] または [送信元インターフェイス オブジェクトのインターフェイス（Interfaces in Source Interface Objects）]）を選択します。選択するインターフェイスは、入力されたインターフェイス制約（任意ではなく）と一致する必要があります。
- [インターフェイスごとのトラフィック制限（Traffic Limit Per Interface）]：ダウンロード制限とアップロード制限を Mbits/sec 単位で入力します。[無制限（Unlimited）] のデフォルト値にすると、一致するトラフィックはその方向でレート制限されません。
- [条件（Conditions）]：追加する対応条件をクリックします。[QoS の適用（Apply QoS On）] の選択内容に対応する、送信元インターフェイスまたは宛先インターフェイスの条件を設定する必要があります。
- [コメント（Comments）]：[コメント（Comments）] をクリックします。コメントを追加するには、[新規コメント（New Comment）] をクリックしてコメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ルール コンポーネントの詳細については、QoS ルール コンポーネント （814 ページ）を参照してください。

ステップ 4 ルールを保存します。

ステップ 5 ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。

ルールには 1 から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

アクセス制御ルールのベストプラクティス （1736 ページ）

QoS ルール コンポーネント

状態（有効/無効）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

インターフェイス（QoS の適用対象）

すべてのトラフィックがレート制限されている QoS のルールは保存できません。QoS のルールごとに、次のいずれかに QoS を適用する必要があります：

- 送信元インターフェイス オブジェクトのインターフェイス：レートは、ルールの送信元インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少なくとも 1 つの送信元インターフェイスの制約を追加する必要があります（**どんな**制約であってもよいわけではありません）。
- 宛先インターフェイス オブジェクト：レートは、ルールの宛先インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少なくとも 1 つの宛先インターフェイスの制約を追加する必要があります（**どんな**制約であってもよいわけではありません）。

インターフェイスごとのトラフィック制限

QoS ルールでは、[QoS の適用対象（Apply QoS On）] オプションで指定するインターフェイスごとに個別にレートを制限します。インターフェイスのセットに対して集約レート制限を指定することはできません。

トラフィックのレート制限を M ビット/秒とします。[無制限（Unlimited）] のデフォルト値では、一致したトラフィックのレートは制限されません。

ダウンロード トラフィックとアップロード トラフィックは、それぞれ独立してレート制限が可能です。システムは、接続イニシエータを基準としてダウンロードかアップロードかを判別します。

インターフェイスの最大スループットを超える制限を指定すると、システムは一致しているトラフィックのレート制限は行いません。最大スループットはインターフェイスのハードウェア構成による影響を受ける可能性があり、各デバイス（**[デバイス（Devices）] > [デバイス管理（Device Management）]**）のプロパティに指定します。

条件

条件は、ルールが処理する特定のトラフィックを指定します。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。各条件の種類には、ルール エディタ内に独自のタブがあります。詳細については、QoS ルール条件 （816 ページ）を参照してください。

説明

ルールで変更を保存するたびに、コメントを追加することができます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ポリシー エディタでは、システムがそのルールのコメント数を表示します。ルール エディタでは、[コメント（Comments）] タブを使用して、既存のコメントを表示し、新しいコメントを追加します。

QoS ルール条件

条件は、ルールが処理する特定のトラフィックを指定します。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。各条件の種類には、ルールエディタ内に独自のタブがあります。以下を使用して、トラフィックをレート制限できます：

詳細については、次の項を参照してください。

関連トピック

インターフェイスルール条件 （816 ページ）
ネットワークルール条件 （816 ページ）
ユーザールール条件 （817 ページ）
アプリケーションルール条件 （817 ページ）
ポートルールの条件 （819 ページ）
URL ルール条件 （821 ページ）
カスタム SGT ルール条件 （821 ページ）

インターフェイスルール条件

インターフェイスルールの条件は送信元インターフェイスと宛先インターフェイスによってトラフィックを制御します。

ルールタイプと導入環境でのデバイスにより、セキュリティゾーンやインターフェイスグループと呼ばれる定義済みのインターフェイスオブジェクトを使用してインターフェイス条件を構築できます。インターフェイスオブジェクトはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することによってトラフィックフローを制御し、分類しやすくします。インターフェイス（Interface）（1346 ページ）を参照してください。QoS ルールは、ルーテッドインターフェイスのみに適用できます。

ヒント　インターフェイスによってルールを制約するのは、システムパフォーマンスを改善するための最適な方法の 1 つです。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

ネットワークルール条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注） アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

ユーザールール条件

接続を開始したユーザー、またはユーザーが属するグループに基づいてトラフィックが照合されます。たとえば、財務グループの全員がネットワークリソースにアクセスすることを禁止するブロックルールを設定できます。

Microsoft Active Directory レルムのユーザーに対してのみユーザー ルール条件を設定できます。

設定されたレルムのユーザーとグループの設定に加えて、次の特殊なアイデンティティユーザーのポリシーを設定できます。

- [失敗した認証（Failed Authentication）]：キャプティブポータルでの認証に失敗したユーザー。
- [ゲスト（Guest）]：キャプティブポータルでゲストユーザーとして設定されたユーザー。
- [認証不要（No Authentication Required）]：アイデンティティの [認証不要（No Authentication Required）] ルールアクションに一致するユーザー。
- [不明（Unknown）]：識別できないユーザー。たとえば、設定されたレルムによってダウンロードされていないユーザー。

アクセス制御ルールのみの場合、ID ポリシーをアクセス コントロール ポリシーに最初に関連付ける必要があります（アクセス制御への他のポリシーの関連付け （1765 ページ）を参照）。

アプリケーションルール条件

システムはIP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザー定義の再利用可能フィルタを作成できます。

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザー定義ディテクタが有効になります。アプリケーション ディテクタの詳細については、アプリケーション ディテクタの基本 （2633 ページ）を参照してください。

アプリケーションフィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

アプリケーション フィルタの利点

アプリケーションフィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザーがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーションフィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーショントラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーショントラフィックは常に最新のディテクタによってモニターされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *48 :* アプリケーションの特性

特性	説明	例
タイプ	アプリケーション プロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲーム アプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。	Facebook はソーシャル ネットワーキングのカテゴリに含まれます。

特性	説明	例
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオストリーミングWebアプリケーションには、ほとんどの場合、`high bandwidth`と`displays ads`というタグが付けられます。

関連トピック

アプリケーション制御の設定のベストプラクティス （1732 ページ）

ポートルールの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTD など）にも推奨されます。ポートベースのアクセス コントロールルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

ポート、プロトコル、および ICMP コードルールの条件

ポート条件により、送信元ポートと宛先ポートに基づいてトラフィックが照合されます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP と UDP のトラフィックは、ポートに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- プロトコル：ポートを使用しないその他のプロトコルを使用してトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。なお、プレフィルタルールではアプリケーション フィルタリングを使用できません。

アプリケーション フィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTP など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP と DNS over UDP の両方を 1 つのアクセスコントロールルールの宛先ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

ポートベースではないプロトコルを照合できます。デフォルトでは、ポート条件を指定しない場合は IP トラフィックを照合します。非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：クラシック デバイスの場合、GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して

すべてのトラフィックを照合します。Firewall Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。

- 復号ルール：これらのルールは TCP ポート条件のみをサポートします。
- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

URL ルール条件

URL 条件を使用してネットワークのユーザーがアクセスできる Web サイトを制御します。

詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについて（1816 ページ）を参照してください。

カスタム SGT ルール条件

ID ソースとして ISE/ISE-PIC を設定しない場合、ISE によって指定**されていない**セキュリティ グループ タグ（SGT）使用してトラフィックを制御できます。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。

カスタム SGT ルールの条件では、システムが ISE サーバとの接続によって取得した ISE SGT ではなく、手動で作成された SGT オブジェクトを使ってトラフィックをフィルタ処理します。この手動で作成された SGT オブジェクトは、制御するトラフィックの SGT 属性に対応します。カスタム SGT を使用したトラフィック制御は、ユーザ制御とは見なされません。

ISE SGT とカスタム SGT ルール条件との比較

ルールの中には、割り当てられた SGT に基づいてトラフィックを制御するために使用できるものがあります。ルールのタイプ、およびアイデンティティ ソースの設定によって、ISE 割り当ての SGT またはカスタム SGT のいずれかを使用して、トラフィックを割り当て済み SGT 属性と照合することができます。

（注） ISE SGT を使用してトラフィックを照合する場合、パケットに SGT 属性が割り当てられていないとしても、パケットの送信元 IP アドレスが ISE 内で既知であれば、そのパケットは ISE SGT ルールと照合されます。

条件タイプ	要件	ルール エディタにリストされている SGT
ISE SGT	ISE アイデンティティ ソース	ISE サーバをクエリして取得され、メタデータが自動的に更新される SGT
カスタム SGT	ISE/ISE-PIC アイデンティティ ソースなし	ユーザーが作成するスタティック SGT オブジェクト

カスタムセキュリティグループタグ（SGT）からISEセキュリティグループタグ（SGT）への自動遷移

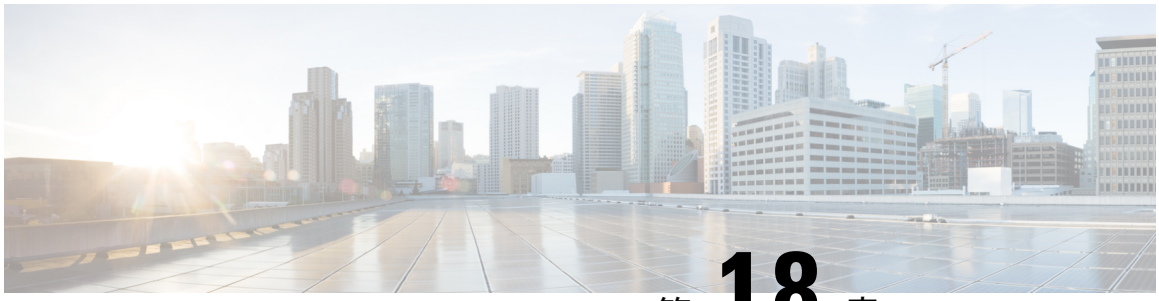
カスタム SGT に一致するルールを作成し、ISE/ISE-PIC を ID ソースに設定すると、システムは次の動作をします。

- オブジェクト マネージャの [セキュリティ グループ タグ（Security Group Tag）] オプションを無効にします。システムは既存の SGT オブジェクトをそのまま保持しますが、それらの変更や、新しいオブジェクトの追加はできません。
- カスタム SGT 条件の既存のルールを保持します。ただし、これらのルールはトラフィックの照合を行いません。また、既存のルールにカスタム SGT 基準を追加することや、カスタム SGT 条件を含む新しいルールを作成することはできません。

ISE を設定する場合は、カスタム SGT 条件を含む既存のルールは削除するか、無効にすることを推奨します。SGT 属性を持つトラフィックを照合するには、代わりに ISE 属性条件を使用します。

QoS の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
廃止：FlexConfig での priority-queue。	7.2.5	7.2.5	FlexConfig は、Threat Defense で priority-queue を設定するために使用されていました。このコマンドは削除されました。
レピュテーションが不明な URL の処理を指定する機能。	6.7.0	いずれか	詳細については、URL フィルタリングの履歴（1848 ページ）を参照してください。 新しい/変更された画面：QoS ルールエディタ
レート制限の増大。	6.2.1	いずれか	最大レート制限が 1,000 Mbps から 100,000 Mbps に増やされました。 新しい/変更された画面：QoS ルールエディタ
カスタム SGT および元のクライアントネットワーク フィルタリング。	6.2.1	いずれか	カスタム セキュリティ グループ タグ（SGT）および元のクライアントネットワーク情報（XFF、True-Client-IP、またはカスタム定義の HTTP ヘッダー）を使用した、トラフィックのレート制限。 新しい/変更された画面：QoS ルールエディタ
QoS（レート制限）の導入。	6.1.0	いずれか	FTD は、アクセス制御によって許可または信頼されている（ポリシーの）ネットワークトラフィックをレート制限します。 新しい/変更された画面：**[デバイス（Devices）] > [QoS]**



第 18 章

プラットフォーム設定

Firewall Threat Defense デバイス用のプラットフォーム設定では、互いに関連しないさまざまな機能を設定して、いくつかのデバイス間でその値を共有できます。デバイスごとに異なる設定が必要な場合でも、共有ポリシーを作成し、該当するデバイスにそれを適用する必要があります。

- プラットフォーム設定の概要 （824 ページ）
- プラットフォーム設定ポリシーの要件と前提条件 （824 ページ）
- プラットフォーム設定ポリシーの管理 （824 ページ）
- ARP インスペクション （826 ページ）
- バナー （827 ページ）
- DNS （828 ページ）
- 外部認証 （832 ページ）
- フラグメント設定 （838 ページ）
- **HTTP** （840 ページ）
- **ICMP** （841 ページ）
- **Shell**の確保 （843 ページ）
- SMTP サーバー （845 ページ）
- SNMP （846 ページ）
- SSL （862 ページ）
- Syslog （867 ページ）
- タイムアウト （888 ページ）
- 時刻の同期 （890 ページ）
- タイムゾーン （892 ページ）
- UCAPL/CC コンプライアンス （892 ページ）
- パフォーマンス プロファイル （893 ページ）
- プラットフォーム設定の履歴 （895 ページ）

プラットフォーム設定の概要

プラットフォーム設定ポリシーは、時刻の設定や外部認証など、展開内の他の管理対象デバイスと同様になる可能性の高い、管理対象デバイスの側面を定義する共有の機能またはパラメータのセットです。

共有ポリシーによって同時に複数の管理対象デバイスを設定することができ、これによって展開に一貫性をもたらし、管理の手間を合理化することができます。プラットフォーム設定ポリシーへの変更は、ポリシーを適用したすべての管理対象デバイスに影響します。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

たとえば、組織のセキュリティポリシーではユーザのログイン時にアプライアンスに「無断使用禁止」のメッセージを表示する必要があるとします。プラットフォーム設定を使えば、プラットフォーム設定ポリシー内で一度ログイン バナーを設定するだけで完了します。

また、単一の Firewall Management Center で複数のプラットフォーム設定ポリシーを活用することもできます。たとえば、さまざまな状況で別々のメール リレー ホストを使用する場合や、さまざまなアクセス リストをテストする場合は、単一のポリシーを編集するのではなく、いくつかのプラットフォーム設定ポリシーを作成し、それらを切り替えることができます。

プラットフォーム設定ポリシーの要件と前提条件

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

プラットフォーム設定ポリシーの管理

[プラットフォームの設定（Platform Settings）]ページ（**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]**）を使用して、プラットフォーム設定ポリシーを管理します。このページには、各ポリシーのデバイスのタイプが示されます。[ステータス（Status）]列で、ポリシーのデバイスターゲットが示されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**を選択します。

ステップ 2 既存のポリシーの場合は、ポリシーを [コピー（Copy）]（）、[編集（Edit）]（）、または[削除（Delete）]（） できます。

注意
どのターゲットデバイスでも、最後に展開したポリシーは期限切れであっても削除しないでください。ポリシーを完全に削除する前に、それらのターゲットに別のポリシーを展開するようにしてください。

ステップ 3 新しいポリシーを作成するには、[新しいポリシー（New Policy）] をクリックします。

a) ドロップダウン リストから、デバイス タイプを選択します。

- [Firepower設定（Firepower Settings）]：従来型の管理対象デバイス用の共有ポリシーを作成します。
- [脅威に対する防御設定（Threat Defense Settings）]：Firewall Threat Defenseの管理対象デバイス用の共有ポリシーを作成します。

b) 新しいポリシーの [名前（Name）]、および必要に応じて [説明（Description）] を入力します。

c) 必要に応じて、ポリシーを適用する [使用可能なデバイス（Available Devices）] を選択し、[追加（Add）] をクリック（またはドラッグアンドドロップ）して、選択したデバイスを追加します。 [検索（Search）] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。

d) [保存（Save）] をクリックします。

システムにより、ポリシーが作成され、編集のために開かれます。

ステップ 4 ポリシーのターゲットデバイスを変更するには、編集するプラットフォーム設定ポリシーの横にある [編集（Edit）]（） をクリックします。

a) [ポリシーの割り当て（Policy Assignment）] をクリックします。

b) デバイス、高可用性ペア、またはデバイスグループをポリシーに割り当てるには、[使用可能なデバイス（Available Devices）] リストで選択し、[Add] をクリックします。ドラッグアンド ドロップを使用することもできます。

c) デバイスの割り当てを削除するには、[選択されたデバイス（Selected Devices）] リストのデバイス、高可用性ペア、またはデバイスグループの横にある [削除（Delete）]（） をクリックします。

d) **[OK]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ARP インスペクション

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARPインスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイルータはゲートウェイ ルータのMACアドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションを有効化すると、Firewall Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IPアドレス、MACアドレス、および送信元インターフェイスがARPエントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firewall Threat Defense デバイスはパケットをドロップします。
- ARPパケットがスタティックARPテーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにFirewall Threat Defense デバイスを設定できます。

（注） 専用のDiagnosticインターフェイスは、このパラメータがfloodに設定されている場合でもパケットをフラッディングしません。

手順

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [ARP インスペクション（ARP Inspection）] を選択します。

ステップ 3 ARP インスペクション テーブルにエントリを追加します。

a) [追加（Add）] をクリックして新しいエントリを作成するか、エントリがすでにある場合は、[編集（Edit）] をクリックします。

b) 任意のオプションを選択します。

- [インスペクション有効（Inspect Enabled）]：選択されているインターフェイスとゾーンの ARP インスペクションを実行します。
- [フラッディング有効（Flood Enabled）]：静的 ARP エントリに一致しない ARP 要求を元のインターフェイスまたは専門の管理インターフェイス以外のすべてのインターフェイスにフラッディングします。これはデフォルトの動作です。

  ARP 要求のフラッディングを選択しない場合、静的 ARP エントリに一致する要求のみが許可されます。
- [セキュリティ ゾーン（Security Zones）]：選択されているアクションを実行するインターフェイスを含むゾーンを追加します。ゾーンはスイッチドゾーンにする必要があります。ゾーンにないインターフェイスでは、選択されたセキュリティ ゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 スタティック ARP エントリの追加（750 ページ）に従って、静的 ARP エントリを追加します。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

バナー

デバイスの CLI（コマンド ライン インターフェイス）に接続するユーザーを表示するよう、メッセージを設定できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [バナー（Banner）] を選択します。

ステップ 3 バナーを設定します。

以下は、バナーのコツと要件です。

- 使用できる文字はASCII文字のみです。回線返品（Enterを押します）を使用できますが、タブを使用できません。
- デバイスのホスト名またはドメイン名は、**$(hostname)** 変数と **$(domain)** 変数を組み込むことによってダイナミックに追加できます。
- バナーに長さの制限はありませんが、バナー メッセージの処理に十分なシステム メモリがない場合、Telnet または SSH セッションは閉じます。
- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。侵入者を招き入れる可能性があるので、「ようこそ」や「お願いします」などの言葉は使用しないでください。次のバナーは、不正アクセスに対する適切な基調を定めます。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

DNS

ドメイン ネーム システム（DNS）サーバは、IP アドレスのホスト名の解決に使用されます。2つのDNSサーバー設定があり、異なるタイプのトラフィック（データトラフィックと特別な管理トラフィック）に適用されます。データトラフィックには、アクセスコントロールルールやリモートアクセス VPN など、DNS ルックアップが必要な FQDN を使用するサービスが含まれます。特別な管理トラフィックには、構成やデータベースの更新など、管理インターフェイスで発生するトラフィックが含まれます。この手順は、データ DNS サーバーにのみ適用されます。管理 DNS 設定については、CLI コマンドの **configure network dns servers** と **configure network dns searchdomains** を参照してください。

DNS サーバー通信の正しいインターフェイスを決定するために、管理対象デバイスではルーティングルックアップが使用されますが、使用されるルーティングテーブルは、DNSを有効にするインターフェイスによって異なります。詳細については、以下のインターフェイス設定を参照してください。

必要に応じて、複数のDNSサーバーグループを構成し、それらを使用してさまざまなDNSドメインを解決できます。たとえば、インターネットへの接続で使用するために、パブリック DNS サーバーを使用するキャッチオールのデフォルトグループを作成できます。次に、example.com ドメイン内のマシンへの接続など、内部トラフィックに内部DNSサーバーを使用する別のグループを構成できます。したがって、組織のドメイン名を使用したFQDNへの接続は、内部 DNS サーバーを使用して解決されますが、パブリックサーバーへの接続は外部 DNS

サーバーを使用します。これらの解決は、NAT やアクセスコントロールルールなど、データ DNS 解決を使用する機能によって使用されます。

[信頼されたDNSサーバー（Trusted DNS Servers）] タブを使用して、DNS スヌーピング用の信頼された DNS サービスを構成できます。DNS スヌーピングは、アプリケーションドメインを IP にマッピングして、最初のパケットでアプリケーションを検出するために使用されます。信頼された DNS サーバーの構成とは別に、構成済みのサーバーを、DNS グループ、DHCP プール、DHCP リレー、および DHCP クライアントに、信頼された DNS サーバーとして含めることができます。

（注） アプリケーションベースの PBR の場合、信頼された DNS サーバーを構成する必要があります。また、ドメインを解決してアプリケーションを検出できるように、DNS トラフィックがクリアテキスト形式で Firewall Threat Defense を通過するようにする必要があります（暗号化された DNS はサポートされていません）。

始める前に

- 1 つ以上の DNS サーバーグループを作成していることを確認します。詳細については、DNS サーバー グループ オブジェクトの作成 （1335 ページ）を参照してください。
- DNS サーバーに接続するためのインターフェイス オブジェクトが作成されていることを確認します。
- 管理対象デバイスに、DNS サーバーにアクセスするための適切なスタティックルートまたはダイナミックルートがあることを確認します。

手順

ステップ 1 **[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]** を選択し、Threat Defense ポリシーを作成または編集します。

ステップ 2 [DNS] をクリックします。

ステップ 3 [DNS設定（DNS Settings）] タブをクリックします。

ステップ 4 [Enable DNS name resolution by device] をオンにします。

ステップ 5 DNS サーバーグループを設定します。

a) DNS サーバーグループリストで次のいずれかを実行します。

- グループをリストに追加するには、[追加（Add）]をクリックします。サーバーグループの既存のリスト内に 30 のフィルタドメインが構成されている場合、別のグループを追加することはできません。
- グループの設定を編集するには、グループの横にある [編集（Edit）]（✎） をクリックします。

- グループを削除するには、グループの横にある [削除（Delete）]（ ）をクリックします。グループを削除しても、DNS サーバー グループ オブジェクトは削除されません。このリストから削除されるだけです。

b) グループを追加または編集するときは、次の設定を構成し、[OK] をクリックします。

- [DNSグループの選択（Select DNS Group）]：既存の DNS サーバー グループ オブジェクトを選択するか、[+] をクリックして新しいオブジェクトを作成します。
- [デフォルトに設定（Make as default）]：このオプションを選択して、このグループをデフォルトのグループにします。他のグループのフィルタに一致しない DNS 解決要求は、このグループのサーバーを使用して解決されます。
- [ドメインのフィルタ処理（Filter Domains）]：デフォルト以外のグループの場合のみ、example.com、example2.com などのドメイン名のカンマ区切りリスト。スペースは使用できません。

  グループは、これらのドメインの DNS 解決にのみ使用されます。この DNS プラットフォーム設定ポリシーに追加されたすべてのグループで、最大 30 の個別のドメインを入力できます。それぞれの名前は最大 127 文字です。

  これらのフィルタドメインは、グループのデフォルトドメイン名とは関係がないことに注意してください。フィルタリストは、デフォルトドメインとは異なる場合があります。

ステップ 6 （任意）[Expiry Entry Timer] と [Poll Timer] の値を分単位で入力します。

これらのオプションは、ネットワークオブジェクトにのみ指定されている FQDN に適用されます。これらは、他の機能で使用される FQDN には適用されません。

- [Expire Entry Timer] は、DNS エントリの最小存続可能時間（TTL）を分単位で指定します。有効期限タイマーがエントリの TTL よりも長い場合、TTL は有効期限エントリ時間値まで増加します。TTL が有効期限タイマーよりも長い場合、有効期限エントリ時間値は無視されます。この場合、TTL に追加の時間は追加されません。有効期限が切れると、DNS ルックアップテーブルからエントリが削除されます。エントリの削除にはテーブルをコンパイルする必要があります。したがって、削除を頻繁に行うとデバイス上の処理負荷が増加する可能性があります。DNS エントリによっては TTL が極端に短い（3 秒程度）場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です（つまり、すべての解像度の最小 TTL は 1 分です）。指定できる範囲は 1 ～ 65535 分です。

  7.0 以前を実行しているシステムでは、有効期限が実際に TTL に追加されることに注意してください。最小値は指定されません。

- [Poll Timer] では、ネットワークオブジェクトに定義されている FQDN を解決するために、デバイスが DNS サーバーにクエリを行うまでの制限時間を指定します。FQDN は、ポール タイマーの期限切れ、または解決された IP エントリの TTL の期限切れのいずれかが発生すると定期的に解決されます。

ステップ 7 すべてのインターフェイスまたは特定のインターフェイスで DNS ルックアップを有効にします。これらの選択は、使用されるルーティングテーブルにも影響します。

インターフェイスで DNS ルックアップを有効にすることは、ルックアップの送信元インターフェイスを指定することとは異なるので注意してください。Firewall Threat Defense は、常にルートルックアップを使用して送信元インターフェイスを決定します。専用の管理インターフェイス以外の管理専用インターフェイスは使用できません。

- [インターフェイスの選択なし（No interfaces selected）]：管理インターフェイスと管理専用インターフェイスを含む、すべてのインターフェイスで DNS ルックアップを有効にします。Firewall Threat Defense はデータルーティングテーブルのみチェックし、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックします。
- [特定のインターフェイスが選択されました（Specific interfaces selected）] ただし [診断インターフェイス経由のDNSルックアップも有効にする（Enable DNS Lookup via diagnostic/management interface also）] オプションはなし：指定したインターフェイスで DNS ルックアップを有効にします。Firewall Threat Defense はデータルーティングテーブルのみチェックします。
- [特定のインターフェイスが選択されました（Specific interfaces selected）] に加えて [診断インターフェイス経由のDNSルックアップも有効にする（Enable DNS Lookup via diagnostic/management interface also）] オプション：指定したインターフェイスと [診断（Diagnostic）] インターフェイスで DNS ルックアップを有効にします。Firewall Threat Defense はデータルーティングテーブルをチェックし、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックします。
- [Enable DNS Lookup via diagnostic interface also] オプションのみ：[診断（Diagnostic）] で DNS ルックアップを有効にします。Firewall Threat Defense は、管理専用ルーティングテーブルのみチェックします。[Devices] > [Device Management] > [edit device] > [Interfaces] ページで診断インターフェイスの IP アドレスを設定してください。

ステップ 8 信頼された DNS サーバーを構成するには、[信頼されたDNSサーバー（Trusted DNS Servers）] タブをクリックします。

ステップ 9 デフォルトでは、DHCP プール、DHCP リレー、DHCP クライアント、または DNS サーバーグループで構成されている既存の DNS サーバーは、信頼された DNS サーバーとして含まれています。それらのいずれかを除外する場合は、該当するチェックボックスをオフにします。

ステップ 10 信頼された DNS サーバーを追加するには、[DNSサーバーの指定（Specify DNS Servers）] で [編集（Edit）] をクリックします。

ステップ 11 [DNSサーバーの選択（Select DNS Servers）] ダイアログボックスで、信頼された DNS サーバーとしてホストオブジェクトを選択するか、信頼された DNS サーバーの IP アドレスを直接指定します。

a) 既存のホストオブジェクトを選択するには、[使用可能なホストオブジェクト（Available Host Objects）] で必要なホストオブジェクトを選択し、[追加（Add）] をクリックしてそれを [選択済みDNSサーバー（Selected DNS Servers）] に含めます。ホストオブジェクトの追加については、ネットワーク オブジェクトの作成 （1351 ページ）を参照してください。

b) 信頼された DNS サーバーの IP アドレス（IPv4 または IPv6）を直接指定するには、所定のテキストフィールドにアドレスを入力し、[追加（Add）] をクリックして、[選択済みDNSサーバー（Selected DNS Servers）] に追加します。

c) [保存（Save）] をクリックします。追加された DNS サーバーは、[信頼されたDNSサーバー（Trusted DNS Servers）] ページに表示されます。

（注）
最大で 12 の DNS サーバーを設定できます。

ステップ 12 （オプション）ホスト名または IP アドレスを使用して、追加された DNS サーバーを検索するには、[DNSサーバーの指定（Specify DNS Servers）] の下の検索フィールドを使用します。

ステップ 13 [保存（Save）] をクリックします。

次のタスク

アクセス制御ルールの FQDN オブジェクトを使用するには、アクセス制御ルールに割り当て可能な FQDN ネットワーク オブジェクトを作成します。手順については、ネットワーク オブジェクトの作成 （1351 ページ）を参照してください。

外部認証

（注） このタスクを実行するには、管理者特権が必要です。

管理ユーザーの外部認証を有効にすると、Firewall Threat Defense により外部認証オブジェクトで指定された LDAP または RADIUS サーバーを使用してユーザー クレデンシャルが検証されます。

外部認証オブジェクトの共有

外部認証オブジェクトは、Firewall Management Center および Firewall Threat Defense デバイスで使用できます。同じオブジェクトを Firewall Management Center とデバイス間で共有することも、別々のオブジェクトを作成することもできます。Firewall Threat Defense は RADIUS サーバーでのユーザーの定義をサポートしますが、Firewall Management Center では外部認証オブジェクトのユーザー リストを事前定義する必要があることに注意してください。Firewall Threat Defense には事前に定義されているリスト方式を使用できますが、RADIUS サーバーでユーザーを定義する場合は Firewall Threat Defense と Firewall Management Center に個別のオブジェクトを作成する必要があります。

（注） タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（LDAP の場合は 1 ー 30 秒、RADIUS の場合は 1 ー 300 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense 外部認証設定が機能しません。

デバイスへの外部認証オブジェクトの割り当て

Firewall Management Center では、**[システム（System）] > [ユーザー（Users）] > [外部認証（External Authentication）]** で外部認証オブジェクトを直接有効にします。この設定は、Firewall Management Center の使用にのみ影響します。管理対象デバイスを使用する場合は、有効にする必要はありません。Firewall Threat Defense のデバイスでは、デバイスに展開するプラットフォーム設定で外部認証オブジェクトを有効にする必要があり、ポリシーごとにアクティブ化できる外部認証オブジェクトは1つのみです。CAC認証を有効にしたLDAPオブジェクトは、CLIアクセスでも使用することはできません。オブジェクトを共有していない場合でも、Firewall Threat Defense と Firewall Management Center の両方が LDAP サーバーに到達できることを確認します。Firewall Management Center は、ユーザーリストを取得してデバイスにダウンロードするために必要です。

Firewall Threat Defense サポート対象フィールド

Firewall Threat Defense SSH アクセスでは、外部認証オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを Firewall Management Centerにも使用する場合は、それらのフィールドが使用されます。この手順は、Firewall Threat Defense でサポートされているフィールドのみを対象とします。 その他のフィールドについては、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Configure External Authentication for the Firewall Management Center*」を参照してください。

ユーザー名

ユーザー名は Linux で有効な名前で、かつ、小文字のみである必要があり、英数文字とピリオド（.）およびハイフン（-）を使用できます。アットマーク（@）やスラッシュ（/）など、その他の特殊文字はサポートされていません。外部認証に **admin** ユーザーを追加することはできません。外部ユーザーは、Firewall Management Center で（外部認証オブジェクトの一部として）追加することしかできません。CLI では追加できません。内部ユーザーは、Firewall Management Center ではなく、CLI でしか追加できないことに注意してください。

configure user add 内部ユーザーとして同じユーザー名がコマンドを使用して設定されていた場合は、Firewall Threat Defense は最初にその内部ユーザーのパスワードをチェックし、それが失敗した場合はAAAサーバーをチェックします。後から外部ユーザーと同じ名前の内部ユーザーを追加できないことに注意してください。既存の内部ユーザーしかサポートされません。RADIUS サーバーで定義されているユーザーの場合は、内部ユーザーの権限レベルと同じに設定してください。そうしないと、外部ユーザー パスワードを使用してログインできません。

Privilege Level

LDAP ユーザーには常に Config 権限があります。RADIUS ユーザーは、Config ユーザーまたは Basic ユーザーとして定義できます。

始める前に

- SSHアクセスは管理インターフェイス上でデフォルトで有効になります。データインターフェイス上でSSHアクセスを有効にするには、Shellの確保（843ページ）を参照してください。SSH は診断インターフェイスに対してサポートされていません。
- RADIUS ユーザーに次の動作を通知し、適切に動作するようにします。
  - 外部ユーザーが初めてログインすると、Firewall Threat Defense は必要な構造体を作成しますが、ユーザー セッションを同時に作成することはできません。ユーザがセッションを開始するには、再度認証する必要があるだけです。ユーザには次のようなメッセージが表示されます。「New external username identified. Please log in again to start a session.」
  - ユーザーの Service-Type 属性が RADIUS サーバーで定義されていないか、正しく設定されていない場合、RADIUS で定義されたユーザーを認証に使用すると、次のようなメッセージがユーザーに表示されます。「Your username is not defined with a service type that is valid for this system. You are not authorized to access the system?」

    場合により、失敗メッセージを表示する前でも、SSH クライアントは失敗した SSH 接続の CLI ウィンドウを閉じます。したがって、ユーザーの Service-Type 属性が RADIUS サーバーで正しく定義されていることを確認してください。
  - 同様に、最後のログイン以降にユーザーの Service-Type 認証が変更された場合、ユーザーを再認証する必要があります。ユーザには次のようなメッセージが表示されます。「Your authorization privilege has changed. セッションを開始するにはもう一度ログインしてください。（Please log in again to start a session.）」

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [外部認証（External Authentication）] をクリックします。

ステップ 3 [外部認証サーバーの管理（Manage External Authentication Server）] リンクをクリックします。

[システム（System）] > **[ユーザー（Users）]** > **[外部認証（External Authentication）]**をクリックして、[外部認証（External Authentication）] 画面を開くこともできます。

ステップ 4 LDAP 認証オブジェクトを設定します。

a) [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。
b) [認証方式（Authentication Method）] を [LDAP] に設定します。
c) [名前（Name）] とオプションの [説明（Description）] を入力します。
d) ドロップダウン リストから [サーバタイプ（Server Type）] を選択します。
e) [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

（注）
証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

f) （任意）[ポート（Port）] をデフォルトから変更します。
g) （任意）[バックアップサーバ（Backup Server）] パラメータを入力します。
h) [LDAP固有のパラメータ（LDAP-Specific Parameters）] を入力します。

- [ベースDN（Base DN）]：アクセスする LDAP ディレクトリのベース識別名を入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。または、[DNの取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。
- （オプション）[基本フィルタ（Base Filter）]：たとえば、ディレクトリ ツリー内のユーザ オブジェクトに `physicalDeliveryOfficeName` 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。
- [ユーザ名（User Name）]：LDAP サーバを参照するために十分なクレデンシャルを持つユーザの識別名を入力します。たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。
- [パスワード（Password）] と [パスワードの確認（Confirm Password）]：ユーザのパスワードを入力して確認します。
- （オプション）[詳細オプションを表示（Show Advanced Options）]：次の詳細オプションを設定します。
  - **[暗号化（Encryption）]**：**[なし（None）]**、**[TLS]**、または **[SSL]** をクリックします。

    （注）
    ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされます。[なし（None）] または [TLS] の場合、ポートはデフォルト値の 389 にリセットされます。[SSL] 暗号化を選択した場合、ポートは 636 にリセットされます。

  - [SSL証明書アップロードパス（SSL Certificate Upload Path）]：SSL または TLS 暗号化の場合は、[ファイルの選択（Choose File）] をクリックして証明書を選択する必要があります。
  - （未使用）[ユーザー名テンプレート（User Name Template）]：Firewall Threat Defense では使用されていません。

- [タイムアウト（Timeout）]：バックアップ接続にロールオーバーするまでの秒数（1 ー 30 秒）を入力します。デフォルトは 30 です。

  （注）
  タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（1 ー 30 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense 外部認証設定が機能しません。

i) （任意）ユーザー識別タイプ以外のシェルアクセス属性を使用する場合は、[CLIアクセス属性（CLI Access Attribute）] を設定します。たとえば、Microsoft Active Directory Server で `sAMAccountName` シェルアクセス属性を使用してシェルアクセスユーザーを取得するには、[CLIアクセス属性（CLI Access Attribute）] フィールドに `sAMAccountName` と入力します。

j) [CLIアクセスフィルタ（CLI Access Filter）] を設定します。

次のいずれかの方法を選択します。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] を選択します。
- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

LDAP サーバー上の名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

k) [保存（Save）] をクリックします。

ステップ 5 LDAP の場合、LDAP サーバーで後からユーザーを追加または削除する場合は、ユーザー リストを更新し、プラットフォーム設定を再展開する必要があります。

a) **[システム（System）] > [ユーザー（Users）] > [外部認証（External Authentication）]** を選択します。

b) LDAP サーバーの横にある [更新（Refresh）]（ ）をクリックします。

ユーザー リストが変更された場合は、デバイスの設定変更を展開するように促すメッセージが表示されます。Firepower Threat Defense のプラットフォーム設定には、「x 台の対象デバイスで古くなっている」ことも表示されます。

c) 設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

ステップ 6 RADIUS 認証オブジェクトを設定します。

a) Service-Type 属性を使用して RADIUS サーバー上のユーザーを定義します。

次に、Service-Type 属性でサポートされている値を示します。

- Administrator (6)：CLI への config アクセス認証を提供します。これらのユーザーは、CLI ですべてのコマンドを使用できます。
- NAS Prompt (7) または 6 以外のレベル：CLI への基本的なアクセス認証を提供します。これらのユーザーは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

または、外部認証オブジェクトにユーザーを事前定義できます（ステップ 6.j（838 ページ） を参照）。Firewall Threat Defense に対して Service-Type 属性メソッドを使用しているときに Firewall Threat Defense および Firewall Management Center に同じ RADIUS サーバーを使用するには、同じ RADIUS サーバーを識別する外部認証オブジェクトを 2 つ作成します。一方のオブジェクトには事前に定義した [CLIアクセスフィルタ（CLI Access Filter）] ユーザーを含め（Firewall Management Center で使用）、もう一方のオブジェクトの [CLIアクセスフィルタ（CLI Access Filter）] は空のままにします（Firewall Threat Defense で使用）。

b) Firewall Management Center で [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

c) [認証方式（Authentication Method）] を [RADIUS] に設定します。

d) [名前（Name）] とオプションの [説明（Description）] を入力します。

e) [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

（注）
証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

f) （任意） [ポート（Port）] をデフォルトから変更します。

g) [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

h) （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。

i) [RADIUS固有のパラメータ（RADIUS-Specific Parameters）] を入力します。

- [タイムアウト（秒）（Timeout (Seconds)）]：バックアップ接続にロールオーバーするまでの秒数を入力します。デフォルトは 30 です。

- [再試行（Retries）]：バックアップ接続にロールオーバーする前にプライマリ サーバ接続を試行する回数を入力します。デフォルトは 3 です。

j) （オプション）RADIUS 定義ユーザーを使用する代わりに、[CLIアクセスフィルタ（CLI Access Filter）] の下で、[管理者CLIアクセスユーザーリスト（Administrator CLI Access User List）] フィールドに、カンマ区切りのユーザー名のリストを入力します。たとえば、**`jchrichton, aerynsun, rygel`** と入力します。

Firewall Threat Defense で [CLIアクセスフィルタ（CLI Access Filter）] メソッドを使用すると、Firewall Threat Defense およびその他のプラットフォームタイプで同一の外部認証オブジェクトを使用できます。RADIUS 定義ユーザーを使用する場合は、[CLIアクセスフィルタ（CLI Access Filter）] を空のままにする必要があります。

これらのユーザー名が RADIUS サーバーのユーザー名と一致していることを確認します。名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アット マーク（@）、またはスラッシュ（/）は使用不可

（注）
RADIUS サーバーでユーザーのみを定義する場合は、このセクションを空のままにしておく必要があります。

k) [保存（Save）] をクリックします。

ステップ 7 **[デバイス（Devices）] > > [プラットフォーム設定（Platform Settings）] > [外部認証（External Authentication）]** に戻ります。

ステップ 8 [更新（Refresh）]（ ）をクリックして、新しく追加したオブジェクトを表示します。

LDAP の場合は、SSL 暗号化または TLS 暗号化を指定するときに、その接続用の証明書をアップロードする必要があります。アップロードしない場合は、このウィンドウにサーバーがリストされません。

ステップ 9 使用する外部認証オブジェクトの横にある [有効なスライダ（Slider enabled）]（ ）をクリックします。有効にできるのは、1 つのオブジェクトのみです。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

フラグメント設定

デフォルトでは、Firewall Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP

など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、[チェーン（Chain）] を 1 に設定してフラグメントを許可しないようにすることをお勧めします。フラグメント化されたパケットは、サービス妨害（DoS）攻撃によく使われます。

（注） これらの設定は、このポリシーが割り当てられたデバイスのデフォルトになります。インターフェイス構成で [デフォルト フラグメント設定のオーバーライド（Override Default Fragment Setting）] を選択することで、デバイスの特定のインターフェイスでこれらの設定をオーバーライドできます。インターフェイスを編集する際、**[詳細（Advanced）]** > **[セキュリティ設定（Security Configuration）]** でオプションを確認できます。**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択して、Firewall Threat Defense デバイスを編集し、[インターフェイス（Interfaces）] タブを選択して、インターフェイスのプロパティを編集します。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [フラグメント設定（Fragment Settings）] を選択します。

ステップ 3 次のオプションを設定します。デフォルト設定を使用する場合は、[デフォルトにリセット（Reset to Defaults）] をクリックします。

- [サイズ（ブロック（Size (Block)）] : リアセンブルを待機可能な、すべての集合的な接続からのパケット フラグメントの最大数。デフォルトは 200 フラグメントです。
- [チェーン（フラグメント）（Chain (Fragment)）] : 1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。フラグメントを許可しない場合は、このオプションを 1 に設定します。
- [タイムアウト（秒）（Timeout (Sec)）] : フラグメント化されたパケット全体の到着を待機する最大秒数を設定します。デフォルトは 5 秒です。すべてのフラグメントがこの時間内に受信されなかった場合、すべてのフラグメントが破棄されます。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

HTTP

HTTPSサーバーを有効にして、アプリケーションロードバランサを使用するAWS上のFirewall Threat Defense Virtualなど、クラウドロードバランサのヘルスチェックメカニズムを提供できます。

Firewall Threat Defenseでの HTTPS のその他の用途はサポートされていません。たとえば、Firewall Threat Defenseは、この管理モードでの設定用の Web インターフェイスを備えていません。

この設定は、管理専用として設定したものも含め、データインターフェイスにのみ適用されます。専用管理インターフェイスには適用されません。物理管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイス間で共有されます。この設定は、使用されている診断論理インターフェイスまたはその他のデータインターフェイスにのみ適用されます。管理論理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Firewall Management Centerにデバイスを設定し、登録するために使用されます。これには、個別の IP アドレスとスタティック ルーティングがあります。

HTTPS の使用で、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、HTTPS アクセスを設定する必要があるだけです。

到達可能なインターフェイスにのみ HTTPS を使用できます。HTTPS ホストが外部インターフェイスにある場合は、外部インターフェイスへの直接的な管理接続のみ開始できます。

始める前に

- 同じ TCP ポートに関して、同じインターフェイスに HTTPS と Cisco Secure Client の AnyConnect VPN モジュール の両方を設定することはできません。たとえば、外部インターフェイスにリモート アクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。同じインターフェイスに両方の機能を設定する必要がある場合は、別々のポートを使用します。たとえば、ポート 4443 で HTTPS を開きます。
- デバイスへの HTTPS 接続に許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択して、オブジェクトを設定します。

（注） システム提供の **any** ネットワーク オブジェクト グループは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[HTTP]** を選択します。

ステップ 3 [HTTPサーバーを有効にする（Enable HTTP Server）] チェックボックスをオンにして HTTP サーバーを有効にします。

ステップ 4 （任意） HTTP ポートを変更します。デフォルトは 443 です。

ステップ 5 HTTP 接続を許可するインターフェイスと IP アドレスを指定します。

このテーブルを使用して、HTTP 接続および HTTP 接続が許可されているクライアントの IP アドレスを承認するインターフェイスを制限します。個々の IP アドレスはなく、ネットワークアドレスを使用できます。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

- [IPアドレス（IP Address）]：HTTP 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- **[セキュリティゾーン（Security Zones）]**：HTTP 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、**[選択したセキュリティゾーン（Selected Security Zones）]** リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) **[OK]** をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ICMP

デフォルトでは、IPv4 または IPv6 を使用して任意のインターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- Firewall Threat Defense は、ブロードキャスト アドレス宛ての ICMP エコー要求に応答しません。
- Firewall Threat Defenseは、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセスルールと同様に順序があり、パケットに最初に一致したルールのアクションが適用されます。

インターフェイスに対して any ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージ タイプだけを拒否する場合は、残りのメッセージ タイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP 到達不能メッセージタイプ（タイプ 3）の権限を常に付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになり、IPsec および PPTP トラフィックが停止することがあります。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスに使用されます。

始める前に

ルールに必要なオブジェクトがすでに存在していることを確認します。**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択して、オブジェクトを設定します。任意のホストまたはネットワークを定義するネットワークオブジェクトまたはグループ、あるいは制御する ICMP メッセージタイプを定義するポートオブジェクトが必要です。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[ICMP]** を選択します。

ステップ 3 ICMP ルールを設定します。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] をクリックして既存のルールを編集します。

b) 次のルール プロパティを設定します。

- [アクション（Action）]：一致するトラフィックを許可または拒否（ドロップ）するかどうかを指定します。
- [ICMP サービス（ICMP Service）]：ICMP メッセージ タイプを識別するポート オブジェクト。
- [ネットワーク（Network）]：アクセスを制御しているホストまたはネットワークを識別するネットワークオブジェクトまたはグループ。

- **[セキュリティゾーン（Security Zones）]**保護しているインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、**[選択したセキュリティゾーン（Selected Security Zones）]** リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 （オプション）。ICMPv4 到達不能メッセージをレート制限します。

- [レート制限（Rate Limit）]：到達不能メッセージのレート制限を、1 秒あたり 1 ～ 100 の範囲で設定します。デフォルトは、1 秒あたり 1 メッセージです。
- [バースト サイズ（Burst Size）]：バースト レートを 1 ～ 10 の範囲で設定します。この数の応答は送信されますが、それ以降の応答は、レート制限に達するまで送信されません。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

Shellの確保

外部インターフェイスなどのデータインターフェイスでFirewall Management Centerアクセスを有効にした場合は、この手順に従ってそのインターフェイスで SSH を有効にする必要があります。ここでは、Firewall Threat Defense で 1 つ以上のデータインターフェイスに対して SSH 接続を有効にする方法について説明します。 SSHは診断論理インターフェイスに対してサポートされません。

Firewall Threat Defense は、OpenSSH に基づく CiscoSSH スタックを使用します。CiscoSSH は、FIPSの順守と、シスコおよびオープンソースコミュニティからの更新を含む定期的な更新をサポートします。

（注） SSH は管理インターフェイス上でデフォルトで有効になっていますが、この画面は管理 SSH アクセスに影響しません。

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Firewall Management Centerにデバイスを設定し、登録するために使用されます。データ インターフェイスの SSH は、管理インターフェイスの SSH と内部および外部ユーザ リストを共有します。その他の設定は個別に設定されます。データインターフェイスでは、この画面を使用してSSH とアクセス リストを有効にします。データ インターフェイスの SSH トラフィックは通常のルーティング設定を使用し、設定時に設定されたスタティック ルートや CLI で設定されたスタティック ルートは使用しません。

管理インターフェイスの場合、SSH アクセスリストを構成するには Cisco Secure Firewall Threat Defense コマンドリファレンス の **configure ssh-access-list** コマンドを参照してください。スタティック ルートを設定するには、**configure network static-routes** コマンドを参照してください。デフォルトでは、初期設定時に管理インターフェイスからデフォルト ルートを設定します。

SSH を使用するには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

SSH は、到達可能なインターフェイスにのみ使用できます。SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみを開始できます。

SSH は、次の暗号およびキー交換をサポートしています。

- 暗号化：aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr
- 完全性：hmac-sha2-256
- キー交換：dh-group14-sha256

（注） SSH を使用した CLI へのログイン試行が 3 回連続して失敗すると、デバイスの SSH 接続は終了します。

始める前に

- SSH 内部ユーザーは、**configure user add** コマンドを使用して CLI でのみ設定できます。を参照してくださいCLI での内部ユーザーの追加 （134 ページ）。デフォルトでは、初期設定時にパスワードを設定した**Admin**ユーザーが存在します。LDAP または RADIUS 上の外部ユーザーは、プラットフォーム設定で [外部認証（External Authentication）] を設定することによっても設定できます。外部認証 （832 ページ）を参照してください。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]** を選択して、オブジェクトを設定します。

（注） システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[セキュアシェル（Secure Shell）]** を選択します。

ステップ 3 SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワーク アドレスを使用できます。

a) [追加（Add）]をクリックして新しいルールを追加するか、[編集（Edit）]をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

- [IP Address]：SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- **[セキュリティゾーン（Security Zones）]**：SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、**[選択したセキュリティゾーン（Selected Security Zones）]** リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。 選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) **[OK]** をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

SMTP サーバー

Syslog 設定で電子メール アラートを設定する場合は、SMTP サーバを指定する必要があります。Syslog で設定する送信元電子メールアドレスは、SMTP サーバの有効なアカウントである必要があります。

始める前に

プライマリおよびセカンダリ SMTP サーバーのホスト アドレスを定義するネットワーク オブジェクトが存在することを確認します。**[オブジェクト（Objects）]**>**[オブジェクト管理（Object**

Management）] を選択してオブジェクトを定義します。または、ポリシーの編集時にオブジェクトを作成することもできます。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [SMTP サーバ（SMTP Server）] をクリックします。

ステップ 3 [プライマリ サーバーの IP アドレス（Primary Server IP Address）]、およびオプションで、[セカンダリ サーバーの IP アドレス（Secondary Server IP Address）] を特定するネットワーク オブジェクトを選択します。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）] > [展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

SNMP

簡易ネットワーク管理プロトコル（SNMP）は、PC またはワークステーションで実行されているネットワーク管理ステーションが、スイッチ、ルータ、セキュリティアプライアンスなどのさまざまなタイプのデバイスのヘルスとステータスをモニターするための標準的な方法を定義します。[SNMP] ページを使用して、SNMP 管理ステーションによってモニターされるようにファイアウォール デバイスを設定できます。

簡易ネットワーク管理プロトコル（SNMP）は、集中管理する場所からのネットワークデバイスのモニタリングをイネーブルにします。Cisco セキュリティアプライアンスでは、SNMP バージョン 1、2c、および 3 を使用したネットワーク モニタリングに加えて、トラップおよび SNMP 読み取りアクセスがサポートされます。SNMP 書き込みアクセスはサポートされません。

SNMPv3 は、読み取り専用ユーザーと、DES（廃止）、3DES、AES256、AES192、および AES128 による暗号化をサポートします。

（注） DES オプションは廃止されました。展開に、DES 暗号化を使用する SNMP v3 ユーザーが含まれていて、そのユーザーが 6.5 より前のバージョンを使用して作成された場合、それらのユーザーを 6.6 以前を実行する Firewall Threat Defense で引き続き使用できます。ただし、これらのユーザーを編集した後も DES 暗号化を維持したり、DES 暗号化を使用する新しいユーザーを作成したりすることはできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、DES 暗号化を使用するプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。

（注） SNMP構成は、ルーテッドインターフェイスと診断インターフェイスのみをサポートします。

（注） 外部 SNMP サーバーでアラートを作成するには、**[ポリシー（Policies）]** > **[アクション（Action）]** > **[アラート（Alerts）]** にアクセスします。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [SNMP] を選択します。

ステップ 3 SNMP を有効にし、基本オプションを設定します。

- [SNMP サーバーを有効にする（Enable SNMP Servers）]：設定された SNMP ホストに SNMP 情報を提供するかどうかを指定します。このオプションの選択を解除すると、設定情報を保持したまま、SNMP モニタリングをディセーブルにできます。
- [コミュニティ ストリングの表示（Read Community String）]、[確認（Confirm）]：SNMP 管理ステーションが Firewall Threat Defense デバイスに要求を送信する際に使用するパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。セキュリティ デバイスでは、このパスワードを使用して、着信 SNMP 要求が有効かどうかを判断します。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースと特殊文字は使用できません。
- [システム管理者名（System Administrator Name）]：デバイス管理者またはその他の担当者の名前を入力します。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [場所（Location）]：このセキュリティ デバイスの場所を入力します（Building 42, Sector 54 など）。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [ポート（Port）]：着信要求が受け入れられる UDP ポートを入力します。デフォルトは 161 です。

ステップ 4 （SNMPv3 のみ）SNMPv3 ユーザーの追加 （854 ページ）。

ステップ 5 SNMP ホストの追加 （857 ページ）。

ステップ 6 SNMP トラップの設定 （859 ページ）。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

SNMP について

SNMP は、ネットワークデバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコルスイートの一部です。Firewall Threat Defense は、SNMP バージョン 1、2c、および 3 を使用したネットワーク監視に対するサポートを提供し、3 つのバージョンの同時使用をサポートします。Firewall Threat Defense のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム（NMS）を使用してネットワークデバイスを監視できます。Firewall Threat Defense は GET 要求の発行を通じて SNMP 読み取り専用アクセスをサポートします。SNMP 書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS（ネットワーク管理システム）に特定のイベント（イベント通知）を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように Firewall Threat Defense を設定したり、NMS を使用してセキュリティ デバイス上で管理情報ベース（MIB）を検索できます。MIB は定義の集合であり、Firewall Threat Defenseは各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

SNMP エージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクが稼働状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別する SNMP OID が含まれています。エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 *49 : SNMP* の用語

用語	説明
エージェント	Secure Firewall Threat Defenseで稼働する SNMP サーバー。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。

用語	説明
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニターすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIB は、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMP イベントのモニターやデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニターおよび表示される情報の源をユーザーに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。 **coldStart**：coldStart トラップは、SNMP の設定後に SNMP エージェントが起動したときに発生します。このトラップは、システムの再起動後にエージェントが起動したときにも発生します。 （注） クラスタノードと HA ノードの場合、リロード後、インターフェイスのリブート時間が 5 分（プリセットしきい値）を超えると、トラップはドロップされます。クラスタおよび HA ノードが正常に再起動すると、他のすべてのトラップが想定どおりに送信されます。 **snmp-server enable traps snmp coldstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

MIB およびトラップ

MIB は、標準またはエンタープライズ固有です。標準 MIB はインターネット技術特別調査委員会（IETF）によって作成され、さまざまな Request for Comment（RFC）に記載されています。トラップは、ネットワークデバイスで発生する重要なイベント（多くの場合、エラーまたは障害）を報告します。SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、ASA ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードすることもできます。

http://www.ietf.org/

SNMP オブジェクトナビゲータを参照し、次の場所から Cisco MIB、トラップ、および OID を検索してください。

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

また、Cisco OID を次の場所から FTP でダウンロードしてください。

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

MIB でサポートされるテーブルおよびオブジェクト

以下に、指定された MIB でサポートされるテーブルおよびオブジェクトを示します。

リモートアクセス VPN のポーリング

表 *50 : CISCO-REMOTE-ACCESS-MONITOR-MIB*

カウンタ	OID	説明
アクティブセッション（Active Sessions）	crasNumSessions（1.3.6.1.4.1.9.9.392.1.3.1）	現在アクティブなセッションの数。
ユーザー	crasNumUsers（1.3.6.1.4.1.9.9.392.1.3.3）	アクティブなセッションを持つユーザーの数。
ピークセッション数（Peak Sessions）	crasNumPeakSessions（1.3.6.1.4.1.9.9.392.1.3.41）	システムが起動してからのピーク RA セッションの数。

サイト間 VPN トンネルのポーリング

表 *51 : CISCO-REMOTE-ACCESS-MONITOR-MIB*

カウンタ	OID	説明
LAN 間セッション（LAN to LAN Sessions）	crasL2LNumSessions（1.3.6.1.4.1.9.9.392.1.3.29）	現在アクティブなLAN間セッションの数。
ピーク LAN 間セッション（Peak LAN to LAN Sessions）	crasL2LPeakConcurrentSessions（1.3.6.1.4.1.9.9.392.1.3.31）	システムが起動してからのピーク同時 LAN 間セッションの数。

接続のポーリング

表 *52 : CISCO-FIREWALL-MIB*

カウンタ	OID	説明
Active Connections	cfwConnectionActive （1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6）	ファイアウォール全体で現在使用されている接続の数。
Peak Connections	cfwConnectionPeak （1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7）	システムが起動してからの、一度に使用された接続の最大数。
1 秒あたりの接続数（Connections Per Second）	cfwConnectionPerSecond （1.3.6.1.4.1.9.9.147.1.2.2.3）	ファイアウォールでの現在の 1 秒あたりの接続数。
1 秒あたりのピーク接続数（Peak Connections Per Second）	cfwConnectionPerSecondPeak （1.3.6.1.4.1.9.9.147.1.2.2.4）	システムが起動してからの、ファイアウォールでの 1 秒あたりの最大接続数。

NAT 変換のポーリング

表 *53 : CISCO-NAT-EXT-MIB*

カウンタ	OID	説明
アクティブな変換（Active Translations）	cneAddrTranslationNumActive （1.3.6.1.4.1.9.9.532.1.1.1.1）	NATデバイスで現在使用可能なアドレス変換エントリの総数。これは、スタティックアドレス変換メカニズムとダイナミックアドレス変換メカニズムの両方から作成された変換エントリの合計を示しています。

カウンタ	OID	説明
ピークアクティブ変換（Peak Active Translations）	cneAddrTranslationNumPeak （1.3.6.1.4.1.9.9.532.1.1.1.2）	システムが起動してから、一度にアクティブになったアドレス変換エントリの最大数。これは、システムの起動以降に一度にアクティブになったアドレス変換エントリの高水準点を示しています。 このオブジェクトには、スタティックアドレス変換メカニズムとダイナミックアドレス変換メカニズムの両方から作成された変換エントリが含まれます。

ルーティング テーブル エントリのポーリング

表 *54 : IP-FORWARD-MIB*

カウンタ	OID	説明
アクティブな変換（Active Translations）	inetCidrRouteNumber （1.3.6.1.2.1.4.24.6）	現在の有効な inetCidrRouteTable エントリの総数。

インターフェイス デュプレックス ステータスのポーリング

表 *55 : CISCO-IF-EXTENSION-MIB*

カウンタ	OID	説明
デュプレックスステータス（Duplex Status）	cieIfDuplexCfgStatus （1.3.6.1.4.1.9.9.276.1.1.2.1.20）	このオブジェクトは、特定のインターフェイスで設定されたデュプレックスステータスを示します。
検出されたデュプレックスステータス（Detected Duplex Status）	cieIfDuplexDetectStatus （1.3.6.1.4.1.9.9.276.1.1.2.1.21）	このオブジェクトは、特定のインターフェイスで検出されたデュプレックスステータスを示します。

Snort 3 侵入イベントレートのポーリング

表 *56 : CISCO-UNIFIED-FIREWALL-MIB*

カウンタ	OID	説明
Snort 3 侵入イベントレート（Snort 3 Intrusion Event Rate）	cufwAaicIntrusionEvtRate（1.3.6.1.4.1.9.9.491.1.5.3.2.1）	このファイアウォールで Snort によって記録された侵入イベントのレート（過去 300 秒間の平均値）。

BGP ピアフラップトラップ通知

表 *57 : BGP4-MIB*

カウンタ	OID	説明
BGP ピアフラップ（BGP Peer-flap）	bgpBackwardTransition（1.3.6.1.4.1.9.9.491.1.5.3.2.1）	BGPBackwardTransition イベントは、BGP FSM が大きい番号が付いた状態から小さい番号が付いた状態に移行した場合に生成されます。

CPU 使用率ポーリング

表 *58 : CISCO-PROCESS-MIB*

カウンタ	OID	説明
CPU Total Utilization	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	過去 1 分間のシステムプロセスの合計 CPU 使用率。

カウンタ	OID	説明
個々の CPU コア使用率	cpmCPUTotal1minRev の関連パラメータと値 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 ～ 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	過去 1 分間の個々の CPU コア使用率の値。「n」はコアの数を表します。 例： • 3.6.1.4.1.99.109.1.1.1.7(n+2) - 集約システム CPU使用率（この値は、シングルコンテキストモードの 3.6.1.4.1.9.9.109.1.1.1.1.7.1 のシステム CPU使用率と同じです）。 • 3.6.1.4.1.99.109.1.1.1.7(n+3) - Snort 平均 CPU 使用率（すべての snort インスタンスの合計値） • 3.6.1.4.1.99.109.1.1.1.7(n+4) - システムプロセス平均 %（「Sysproc」コアの平均）

（注） CPU のモニタリング（hrProcessorTable および hrNetworkTable）に関連する SNMP OID 1.3.6.1.2.1.25.3.3 および 1.3.6.1.2.1.25.3.4 は、ASA FirePOWER では削除されています。デバイスの CPU 正常性の詳細情報は、デバイスマネージャを介してのみ、表示およびモニタリングできます。

SNMPv3 ユーザーの追加

（注） SNMPv3 でのみユーザーを作成できます。以下の手順は、SNMPv1 または SNMPv2c には適用されません。

SNMPv3 は読み取り専用ユーザーのみをサポートすることに注意してください。

SNMPユーザーには、ユーザー名、認証パスワード、暗号化パスワードおよび使用する認証アルゴリズムと暗号化アルゴリズムが指定されています。

（注） クラスタリングまたは高可用性でSNMPv3を使用する場合、最初のクラスタ形成後に新しいクラスタユニットを追加するか、高可用性ユニットを交換すると、SNMPv3ユーザーは新しいユニットに複製されません。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいユニットに強制的にレプリケートする必要があります。

認証アルゴリズムのオプション

認証アルゴリズムのオプションはMD5（廃止、6.5 より前のみ）、SHA、SHA224、SHA256、および SHA384 です。

（注） MD5 オプションは廃止されました。展開に、6.5 より前のバージョンを使用して作成されたMD5認証アルゴリズムを使用するSNMP v3ユーザーが含まれている場合、6.7以前のバージョンを実行する FTD でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 認証アルゴリズムを保持したり、MD5 認証アルゴリズムを使用して新しいユーザーを作成したりすることはできません。管理センターでバージョン 7.0 以降を実行している Threat Defense を管理している場合、MD5 認証アルゴリズムを使用するプラットフォーム設定ポリシーをそれらの Threat Defense に展開すると失敗します。

暗号化アルゴリズムのオプションはDES（廃止、6.5 より前のみ）、3DES、AES256、AES192、および AES128 です。

（注） DES オプションは廃止されました。6.5 より前のバージョンを使用して作成されたDES暗号化を使用する SNMP v3 ユーザーが展開に含まれている場合は、6.7 以前のバージョンを実行する Threat Defense でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集した後も DES 暗号化を維持したり、DES 暗号化を使用する新しいユーザーを作成したりすることはできません。管理センターでバージョン 7.0 以降を実行している Threat Defense を管理している場合、DES 暗号化を使用するプラットフォーム設定ポリシーをそれらの Threat Defense に展開すると失敗します。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[SNMP]** > **[ユーザー（Users）]** をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [セキュリティ レベル（Security Level）] ドロップダウン リストからユーザーに適したセキュリティ レベルを選択します。

- **Auth**：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- **No Auth**：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- **Priv**：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

ステップ 5 [ユーザー名（Username）] フィールドに SNMP ユーザーの名前を入力します。このユーザー名は 32 文字以下であることが必要です。

ステップ 6 [暗号化パスワード タイプ（Encryption Password Type）] ドロップダウン リストから使用するパスワードのタイプを選択します。

- **Clear text**：Firewall Threat Defense デバイスは、デバイスへの導入時を待ってパスワードを暗号化します。
- **Encrypted**：Firewall Threat Defense デバイスは、暗号化を済ませたパスワードを直接展開します。

ステップ 7 [認証アルゴリズム タイプ（Auth Algorithm Type）] ドロップダウンリストから、SHA、SHA224、SHA256、SHA384 のうち、使用する認証タイプを選択します。

（注）
MD5 オプションは廃止されました。展開に、6.5 より前のバージョンを使用して作成された MD5 認証アルゴリズムを使用する SNMP v3 ユーザーが含まれている場合、6.7 以前のバージョンを実行する FTD でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 認証アルゴリズムを保持したり、MD5 認証アルゴリズムを使用して新しいユーザーを作成したりすることはできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、MD5 認証アルゴリズムを使用するプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。

ステップ 8 認証に使用するパスワードを、[認証パスワード（Authentication Password）] フィールドに入力します。暗号化パスワードタイプに [暗号化（Encrpted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。

（注）
パスワードの長さは、選択した認証アルゴリズムによって異なります。すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリア テキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。

ステップ 9 [暗号化タイプ（Encryption Type）] ドロップダウン リストで、AES128、AES192、AES256、3DES の中から使用する暗号化タイプを選択します。

（注）
AES または 3DES 暗号化を使用するには、デバイスに適切なライセンスをインストールしておく必要があります。

（注）
DES オプションは廃止されました。6.5 より前のバージョンを使用して作成された DES 暗号化を使用する SNMP v3 ユーザーが展開に含まれている場合は、6.7 以前のバージョンを実行する Firewall Threat Defense でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集した後も DES 暗号化を維持したり、DES 暗号化を使用する新しいユーザーを作成したりすることはできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、DES 暗号化を使用するプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。

ステップ 10 [暗号化パスワード（Encryption Password）] フィールドに暗号化で使用するパスワードを入力します。暗号化パスワードタイプに [暗号化（Encrpted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。暗号化を行う場合のパスワードの長さは選択された暗号化のタイプにより異なります。パスワードの長さは次のとおりです（各 xx は 1 つのオクテットを示します）。

- AES 128 では 16 オクテットとする必要があります
- AES 192 では 24 オクテットとする必要があります
- AES 256 では 32 オクテットとする必要があります
- 3DES では 32 オクテットとする必要があります
- DES の長さはさまざまです。

（注）
すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリアテキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。

ステップ 11 **[OK]** をクリックします。

ステップ 12 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

SNMP ホストの追加

[ホスト（Host）] を使用して、[SNMP] ページにある [SNMPホスト（SNMP Hosts）] テーブルのエントリを追加または編集します。これらのエントリは、Firewall Threat Defense デバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

最大 8,192 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。

始める前に

SNMP管理ステーションを定義するネットワーク オブジェクトが存在することを確認します。[デバイス（Device）] > [オブジェクト管理（Object Management）] を選択し、ネットワークオブジェクトを設定します。 >

（注） サポートされているネットワーク オブジェクトには、IPv6 ホスト、IPv4 ホスト、IPv4 範囲および IPv4 サブネット アドレスが含まれます。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[SNMP]** > **[ホスト（Hosts）]** をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [IP アドレス（IP Address）] フィールドに、有効な Ipv6 ホストまたは IPv4 ホストを入力するか、SNMP管理ステーションのホストアドレスを定義するネットワーク オブジェクトを選択します。

IP アドレスには、IPv6 ホスト、IPv4 ホスト、IPv4 範囲または IPv4 サブネットを使用できます。

ステップ 5 [SNMP バージョン（SNMP Version）] ドロップダウン リストから、適切な SNMP バージョンを選択します。

ステップ 6 （SNMPv3 のみ）[ユーザー名（User Name）] ドロップダウン リストから設定した SNMP ユーザーのユーザー名を選択します。

（注）
SNMP ホストごとに 23 人までの SNMP ユーザーを関連付けることができます。

ステップ 7 （SNMPv1、2c のみ）[Read コミュニティ ストリング（Read Community String）] フィールドに、デバイスの読み取りアクセスのためにすでに設定してあるコミュニティ ストリングを入力します。確認のためにこの文字列を再入力します。

（注）
この文字列は、この SNMP ステーションで使用されている文字列が [SNMP サーバーを有効にする（Enable SNMP Server）] セクションに定義済みのものと異なる場合のみ必須です。

ステップ 8 デバイスとSNMP管理ステーションの間の通信タイプを選択します。両方のタイプを選択できます。

- **[ポーリング（Poll）]**：管理ステーションは定期的にデバイスに情報を要求します。

- **[トラップ（Trap）]**：デバイスは、イベント発生時にこれをトラップし、管理ステーションに送信します。

（注）
SNMP ホストの IP アドレスが IPv4 範囲または IPv4 サブネットのいずれかである場合、[ポーリング（Poll）] と [トラップ（Trap）] の両方ではなく、いずれかを設定できます。

ステップ 9 [ポート（Port）] フィールドに、SNMP ホストの UDP ポート番号を入力します。デフォルト値は 162 です。有効な範囲は 1 ～ 65535 です。

ステップ 10 [次でアクセス可能（Reachable By）] オプションで、デバイスと SNMP 管理ステーションの間の通信インターフェイスタイプを選択します。デバイスの管理インターフェイスまたは使用可能なセキュリティゾーン/名前付きインターフェイスのいずれかを選択できます。

- **デバイスの管理インターフェイス**：デバイスと SNMP 管理ステーション間の通信は、管理インターフェイスを介して行われます。
  - SNMPv3 ポーリングにこのインターフェイスを選択すると、設定されたすべての SNMPv3 ユーザーがポーリングを許可され、ステップ 6（858 ページ）で選択したユーザーに制限されません。ここでは、SNMPv3 ホストからの SNMPv1 および SNMPv2c は許可されていません。
  - SNMPv1 および SNMPv2c ポーリングにこのインターフェイスを選択すると、ポーリングはステップ 5（858 ページ）で選択したバージョンにまったく制限されません。
- **セキュリティゾーンまたは名前付きインターフェイス**：デバイスと SNMP 管理ステーション間の通信は、セキュリティゾーンまたはインターフェイスを介して行われます。
  - [使用可能なゾーン（Available Zones）] フィールドでゾーンを検索します。
  - [選択したゾーン/インターフェイス（Selected Zones/Interfaces）] リストに、デバイスが管理ステーションと通信するインターフェイスを含むゾーンを追加します。ゾーン内にないインターフェイスの場合は、[選択したゾーン/インターフェイス（Selected Zone/Interface）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。 デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

ステップ 11 **[OK]** をクリックします。

ステップ 12 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

SNMP トラップの設定

[SNMP トラップ（SNMP Traps）] を使用して、Firewall Threat Defense デバイスの SNMP トラップ（イベント通知）を設定します。トラップは参照とは異なります。トラップは、生成される

リンクアップ イベント、リンクダウン イベント、Syslog イベントなど、特定のイベントに対する Firewall Threat Defense デバイスから管理ステーションへの割り込み「コメント」です。デバイスの SNMP オブジェクト ID（OID）は、デバイスから送信される SNMP イベント トラップに表示されます。

一部のトラップは、特定のハードウェア モデルに適用できません。これらのトラップは、これらのモデルの 1 つのポリシーを適用すると無視されます。たとえば、すべてのモデルに現場交換可能ユニットがあるわけではありません。そのため、[現場交換可能ユニット挿入/削除（Field Replaceable Unit Insert/Delete）] トラップはこれらのモデルで設定されません。

SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、Firewall Threat Defense ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードできます。

http://www.ietf.org/

次の場所から Cisco MIB、トラップ、および OID の完全なリストを参照してください。

SNMP Object Navigator

また、Cisco OID を次の場所から FTP でダウンロードしてください。

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[SNMP]** > **[SNMP トラップ（SNMP Traps）]** をクリックして、Firewall Threat Defense デバイスの SNMP トラップ（イベント通知）を設定します。

ステップ 3 適切な [Enable Traps] オプションを選択します。いずれかまたは両方のオプションを選択できます。

a) [すべての SNMP トラップを有効にする（Enable All SNMP Traps）] にマークを付けて、連続する 4 セクションですべてのトラップを素早く選択します。

b) [すべての Syslog トラップを有効にする（Enable All Syslog Traps）] にマークを付けて、トラップ関連の Syslog メッセージの伝送を有効にします。

（注）
SNMP トラップはリアルタイムに近いことが期待されるため、Firewall Threat Defense からの他の通知メッセージよりも優先順位が高いです。すべての SNMP トラップまたは syslog トラップを有効にすると、SNMP プロセスがエージェントとネットワーク内で過剰にリソースを消費し、システムがハングアップする可能性があります。システムの遅延、未完了の要求、またはタイムアウトが発生した場合は、SNMP トラップと syslog トラップを選択して有効にすることができます。また、syslog メッセージの生成レートは、シビラティ（重大度）レベルまたはメッセージ ID によって制限できます。たとえば、212 で始まる syslog メッセージ ID はすべ

て、SNMP クラスに関連しています。syslog メッセージの生成レートの制限 （882 ページ）を参照してください。

ステップ 4 [標準（Standard）] セクションのイベント通知トラップは、既存のポリシーでは、デフォルトで有効になっています。

- [認証（Authentication）]：未認可の SNMP アクセス。この認証エラーは、間違ったコミュニティ ストリングが付いたパケットによって発生します。
- [リンクアップ（Link Up）]：通知に示されているとおり、デバイスの通信リンクの 1 つが使用可能になりました。
- [リンクダウン（Link Down）]：通知に示されているとおり、デバイスの通信リンクの 1 つにエラーが発生しました。
- [コールドスタート（Cold Start）]：デバイスが自動で再初期化しているときに、その設定またはプロトコルエンティティの実装が変更されることがあります。
- [ウォームスタート（Warm Start）]：デバイスが自動で再初期化しているときに、その設定またはプロトコルエンティティの実装が変更されることはありません。

ステップ 5 [エンティティ MIB（Entity MIB）] セクションで好きなイベント通知トラップを選択します。

- [現場交換可能ユニット挿入（Field Replaceable Unit Insert）]：示されているとおり、現場交換可能ユニット（FRU）が挿入されました（FRU には電源装置、ファン、プロセッサ モジュール、インターフェイス モジュールなどの組み立て部品が含まれます）。
- [現場交換可能ユニット除外（Field Replaceable Unit Remove）]：通知に示されているとおり、現場交換可能ユニット（FRU）が取り外されました。
- [設定変更（Configuration Change）]：通知に示されているとおり、ハードウェアに変更がありました。

ステップ 6 [リソース（Resource）] セクションで好きなイベント通知トラップを選択します。

- [接続制限到達（Connection Limit Reached）]：このトラップは、設定した接続制限に達したため、接続試行が拒否されたことを示します。

ステップ 7 [その他（Other）] セクションで好きなイベント通知トラップを選択します。

- [NAT パケット破棄（NAT Packet Discard）]：IP パケットが NAT 機能により廃棄されると、この通知が生成されます。ネットワーク アドレス変換の使用可能なアドレスまたはポートが、設定したしきい値を下回りました。
- [CPU上昇しきい値（CPU Rising Threshold）]：この通知は、設定された期間の CPU 使用率の上昇が、事前定義されたしきい値を超えた場合に生成されます。CPU 上昇しきい値通知を有効にするには、このオプションをオンにします。
  - [割合（Percentage）]：上限しきい値通知のデフォルト値は 70% です。範囲は 10 ～ 94% です。クリティカルしきい値は、95% にハードコードされています。

- [期間（Period）]：デフォルトのモニタリング期間は1分です。範囲は1～60分です。

- [メモリ上昇しきい値（Memory Rising Threshold）]：この通知は、メモリ使用率の上昇が事前定義されたしきい値を超え、使用可能なメモリが減少している場合に生成されます。メモリ上昇しきい値通知を有効にするには、このオプションをオンにします。
  - [割合（Percentage）]：上限しきい値通知のデフォルト値は 70% です。範囲は 50 ～ 95% です。

- [フェールオーバー（Failover）]：この通知は、CISCO-UNIFIED-FIREWALL-MIB によってレポートされたフェールオーバー状態に変化があった場合に生成されます。

- [クラスタ（Cluster）]：この通知は、CISCO-UNIFIED-FIREWALL-MIB によってレポートされたクラスタの正常性に変化があった場合に生成されます。

- [ピアフラップ（Peer Flap）]：この通知は、BGP ルートフラッピングが発生した場合に生成されます。これは、BGP システムが、ネットワークの到達可能性情報をアドバタイズするために過剰な数の更新メッセージを送信する状況です。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

SSL

（注） このタスクを実行するには、管理者権限があり、リーフドメインに属している必要があります。

完全にライセンス供与されたバージョンの Secure Firewall Management Center を実行していることを確認する必要があります。評価モードで Secure Firewall Management Center を実行している場合は、[SSL 設定（SSL Settings）] は無効になります。また、ライセンス供与された Secure Firewall Management Center のバージョンがエクスポートのコンプライアンス基準を満たしていない場合、[SSL 設定（SSL Settings）] は無効になります。SSL でリモート アクセス VPN を使用している場合、スマート アカウントで強力な暗号化機能が有効になっている必要があります。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*License Types and Restrictions*」を参照してください。

手順

ステップ 1 [デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [SSL] を選択します。

ステップ 3 エントリを、[SSL 設定の追加（Add SSL Configuration）] テーブルに追加します。

a) [追加（Add）] をクリックして新しいエントリを作成するか、エントリがすでにある場合は、[編集（Edit）] をクリックします。

b) ドロップダウン リストから必要なセキュリティ設定を選択します。

- [**プロトコル バージョン（Protocol Version**）]：リモート アクセス VPN セッションを設定するときに使用する TLS プロトコルを指定します。
- [**セキュリティ レベル（Security Level**）]：SSL で設定するセキュリティ ポジショニングのタイプを指定します。

ステップ 4 選択するプロトコル バージョンに基づく [使用可能なアルゴリズム（Available Algorithms）] を選択し、[追加（Add）] をクリックして選択したプロトコルに含めます。詳細については、SSL 設定について （863 ページ）を参照してください。

アルゴリズムは、選択するプロトコル バージョンに基づいてリストされます。それぞれのセキュリティ プロトコルは、セキュリティ レベルの設定の一意のアルゴリズムを識別します。

ステップ 5 [OK] をクリックして変更を保存します。

次のタスク

[展開（Deploy）] > [展開（Deployment）] を選択し、[展開（Deploy）] をクリックして、割り当てられたデバイスにポリシーを展開します。

SSL 設定について

Firewall Threat Defense デバイスでは、セキュ ソケットレイヤ（SSL）プロトコルと Transport Layer Security（TLS）を使用して、リモートクライアントからのリモートアクセス VPN のセキュアメッセージ伝送をサポートします。[SSL 設定（SSL Settings）] ウィンドウでは、SSL でのリモート VPN アクセス中に、ネゴシエートとメッセージ伝送に使用される SSL バージョンと暗号化アルゴリズムを設定できます。

（注） セキュリティ認証（UCAPL、CC、または FIPS）準拠モードで動作するように Firewall Management Center と Firewall Threat Defense が構成されていても、Firewall Management Center はサポートされていない暗号の構成を許可します。たとえば、FIPS 対応モードでは、Management Center は FIPS に準拠していない DH グループ 5 の構成を許可します。ただし、非準拠の暗号が使用されるため、VPN トンネルはネゴシエートしません。

SSL 設定は、次の場所で構成します。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SSL]

フィールド

[Minimum SSL Version Server]：Firewall Threat Defense デバイスがサーバーとして動作するときに使用する最小バージョンの SSL/TLS プロトコルを指定します。たとえば、リモート アクセス VPN ゲートウェイとして機能する場合です。

[TLSバージョン（TLS Version）]：ドロップダウンリストから、次のいずれかの TLS バージョンを選択します。

TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
TLSV1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。
TLSV1.3	SSLv2 クライアントの hello を受け入れ、TLSv1.3（以降）をネゴシエートします。

（注） リモートアクセス VPN の TLS 1.3 には、Cisco Secure Client バージョン 5.0 以降が必要です。

[DTLSバージョン（DTLS Version）]：選択した TLS バージョンに基づいて、ドロップダウンリストから DTLS バージョンを選択します。デフォルトでは、DTLSv1 は Firewall Threat Defense デバイスで設定されており、要件に応じて DTLS バージョンを選択できます。

（注） TLS プロトコルのバージョンが、選択した DTLS プロトコルバージョン以上であることを確認します。TLS プロトコルバージョンでは、次の DTLS バージョンがサポートされています。

TLS V1	DTLSv1
TLSV1.1	DTLSv1

TLSV1.2	DTLSv1、DTLSv 1.2
TLSV1.3	DTLSv1、DTLSv 1.2

[Diffie-Hellman グループ（Diffie-Hellman Group）]：ドロップダウンリストからグループを選択します。使用可能なオプションは、[Group1]（768 ビット絶対値）、[Group2]（1024 ビット絶対値）、[Group5]（1536 ビット絶対値）、[Group14]（2048 ビット絶対値、224 ビット素数位数）、および [Group24]（2048 ビット絶対値、256 ビット素数位数）です。デフォルト値は [Group1] です。

[楕円曲線Diffie-Hellmanグループ（Elliptical Curve Diffie-Hellman Group）]：ドロップダウンリストからグループを選択します。使用可能なオプションは、[Group19]（256 ビット EC）、[Group20]（384 ビット EC）、および [Group21]（521 ビット EC）です。デフォルト値は [Group19] です。

TLSv1.2 では、次の暗号方式のサポートが追加されています。

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

（注） 優先度が最も高いのは ECDSA 暗号方式と DHE 暗号方式です。

TLSv1.3 では、次の暗号方式のサポートが追加されています。

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384

Secure Firewall Threat Defense デバイスでサポートしたいプロトコル バージョン、セキュリティ レベル、および暗号アルゴリズムを指定するために、SSL 設定テーブルを使用できます。

[プロトコル バージョン（Protocol Version）]：Secure Firewall Threat Defense デバイスでサポートされ、SSL接続に使用されるプロトコルバージョンを一覧表示します。利用可能なプロトコル バージョンは次のとおりです。

- デフォルト
- TLSV1
- TLSV1.1
- TLSV1.2
- TLSV1.3
- DTLSv1
- DTLSv1.2

[セキュリティ レベル（Security Level）]：Firewall Threat Defense デバイスでサポートされ、SSL接続に使用される暗号セキュリティ レベルを一覧表示します。

評価ライセンスを使用しているFirewall Threat Defenseデバイスがある場合、デフォルトではセキュリティレベルが低くなります。Firewall Threat Defense スマートライセンスでは、デフォルトのセキュリティレベルは[高（High）]です。次のオプションのいずれかを選択して、必要なセキュリティレベルを設定できます。

- [All]：NULL-SHA を含むすべての暗号。
- [Low]：NULL-SHA を除くすべての暗号。
- [Medium]：NULL-SHA、DES-CBC-SHA、RC4-SHA、および RC4-MD5 を除くすべての暗号（これがデフォルトです）。
- [FIPS]：NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、DES-CBC3-SHA、TLS_CHACHA20_POLY1305_SHA256 を除く FIPS 準拠のすべての暗号方式を含む。
- [高（High）]：SHA-2 暗号を使用する AES-256 のみを含み、TLS バージョン 1.2 およびデフォルト バージョンに適用される。
- [Custom]：[Cipher algorithms/custom string] ボックスで指定する 1 つ以上の暗号。このオプションでは、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。

[Cipher Algorithms/Custom String]：Firewall Threat Defense デバイスでサポートされ、SSL 接続に使用される暗号アルゴリズムを一覧表示します。OpenSSL を使用した暗号の詳細については、https://www.openssl.org/docs/apps/ciphers.html を参照してください。 https://www.openssl.org/docs/apps/ciphers.html

Firewall Threat Defense デバイスでは、サポートされる暗号方式の優先度が次のように指定されています。

TLSv1.2 のみでサポートされる暗号方式

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384

DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

TLSv1.1 または TLSv1.2 でサポートされない暗号方式

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

Syslog

Firewall Threat Defense デバイスのシステム ロギング（syslog）を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。また、一部のセキュリティ イベントを syslog サーバーに送信することもできます。ここでは、ロギングとその設定方法について説明します。

Syslog について

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央syslogサーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslogサービスは、簡単なコンフィギュレーション ファイルに従って、メッセージを受

信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。

表 *59* : のシステム ログ *Secure Firewall Threat Defense*

関連ログ	詳細	設定
デバイスとシステム ヘルス、ネットワーク構成	この syslog 設定では、データ プレーン上で実行されている機能、つまり **show running-config** コマンドで表示できる CLI 設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データ インターフェイス、DHCP サーバー、NAT などの機能が含まれます。データ プレーンの syslog メッセージには番号が付けられており、ASA ソフトウェアを実行しているデバイスで生成されるものと同じです。ただし、Secure Firewall Threat Defense は、必ずしも ASA ソフトウェアで使用可能なすべてのメッセージタイプを生成するとは限りません。これらのメッセージの詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html の『*Cisco Secure Firewall Threat Defense Syslog Messages*』を参照してください。この構成については、次のトピックで説明します。	**プラットフォームの設定**
セキュリティ イベント	この syslog の設定では、ファイルとマルウェア、接続、セキュリティ インテリジェンス、および侵入イベントのアラートが生成されます。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「About Sending Syslog Messages for Security Events」およびサブトピックを参照してください。	アクセス コントロール ポリシーの [プラットフォーム設定（Platform Settings）] と [ロギング（Logging）]
（すべてのデバイス） ポリシー、ルール、およびイベント	この syslog 設定では、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Configurations Supporting Alert Responses*」で説明されているように、アクセス制御ルール、侵入ルール、およびその他のアドバンスドサービスに関するアラートが生成されます。これらのメッセージには番号が付けられていません。このタイプの syslog の設定については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Creating a Syslog Alert Response*」を参照してください。	アクセス コントロール ポリシーの [アラート応答（Alert Responses）] と [ロギング（Logging）]

複数の syslog サーバーを設定し、各サーバーに送信されるメッセージとイベントを制御できます。また、コンソール、電子メール、内部バッファなどの異なる宛先を構成することもできます。

重要度レベル

次の表に、syslog メッセージのシビラティ（重大度）の一覧を示します。

表 *60 : Syslog*メッセージのシビラティ（重大度）

レベル番号	重要度	説明
0	**致命的**	システムが使用不可能です。
1	**Alert**（警告）	すぐに措置する必要があります。
2	**深刻**	深刻な状況です。
3	**エラー**	エラー状態です。
4	**warning**	注意状態。
5	**Notification**（通告）	正常ですが、注意を必要とする状況です。
6	**情報**	情報メッセージです。
7	**デバッグ**	デバッグメッセージ。 問題をデバッグするときに、このレベルで一時的にのみログに記録します。このログレベルでは、非常に多くのメッセージが生成される可能性があるため、システムパフォーマンスに影響を与える可能性があります。

（注） ASA および Firewall Threat Defense は、重大度 0（緊急）の syslog メッセージを生成しません。

syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、Firewall Threat Defense デバイスを設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号

  （これは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

- syslog メッセージの重大度

- syslog メッセージ クラス（機能エリアと同等）

  （これは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

これらの基準は、出力先を設定するときに指定可能なメッセージ リストを作成して、カスタマイズできます。あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するように Firewall Threat Defense デバイス を設定することもできます。

（メッセージ リストは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

syslog メッセージ クラス

（注） このトピックは、セキュリティ イベント（接続、侵入など）のメッセージには適用されません。

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。
- メッセージ クラスを指定するメッセージ リストを作成します。

syslog メッセージ クラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

表 *61 : syslog* メッセージのクラスおよび関連付けられているメッセージ *ID* 番号

クラス	定義	Syslog メッセージ ID 番号
auth	ユーザ認証	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
—	ボットネット トラフィック フィルタ	338
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
citrix	Citrix クライアント	723
—	クラスタリング	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	セキュアなデスクトップ	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロール用の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレスの割り当て	735
ips	侵入防御システム	400、401、420

クラス	定義	Syslog メッセージ ID 番号
—	IPv6	325
—	ライセンシング	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用するための NAC 設定	732
—	NAT および PAT	305
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	Phone Proxy	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722

クラス	定義	Syslog メッセージ ID 番号
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tag-switching	サービス タグ スイッチング	779
transactional-rule-engine-tre	トランザクション ルール エンジン	780
uc-ims	UC-IMS	339
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN と セキュアクライアント	716

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

- IPv6 がサポートされます。Syslog は、TCP または UDP を使用して送信できます。
- syslog 送信用に設定されたインターフェイスが有効であること、IPv6 対応であること、および syslog サーバが指定インターフェイス経由で到達できることを確認します。
- IPv6 上でのセキュア ロギングはサポートされません。

その他のガイドライン

- Firewall Management Center をプライマリ syslog サーバーとして設定しないでください。Firewall Management Center は、いくつかの syslog をログに記録できます。ただし、特に複数のセンサーが使用され、すべてのセンサーから syslog が送信される場合、すべてのセンサーの接続イベントから送信される大量の情報を格納するのに十分なストレージのプロビジョニングはありません。
- syslog サーバでは、syslogd というサーバプログラムを実行する必要があります。Windows では、オペレーティング システムの一部として syslog サーバを提供しています。
- syslog サーバーは、ファイアウォールシステムの syslog-ng プロセスに基づいて動作します。SecureWorks の *scwx.conf* ファイルなどの外部設定ファイルは使用しないでください。このようなファイルは、デバイスと互換性がありません。これらを使用すると、解析エラーが発生し、最終的に syslog-ng プロセスが失敗します。
- Firewall Threat Defense デバイスが生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、Firewall Threat Defense デバイスはメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。
- トランスポートプロトコルとして TCP を使用する場合、メッセージが失われないように syslog サーバーへの接続が 4 つ開きます。syslog サーバーを使用して非常に多数のデバイスからメッセージを収集する場合、接続オーバーヘッドの合計がサーバーに対して大きすぎる場合は、代わりに UDP を使用します。
- 2 つの異なるリストまたはクラスを、異なる syslog サーバーまたは同じロケーションに割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。
- syslog サーバは、Firewall Threat Defense デバイス 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスが ICMP 到達不能メッセージを拒否し、同じサーバに syslog を送信するように設定する必要があります。すべてのシビラティ（重大度）に対してロギングがイネーブルであることを確認します。syslog サーバーがクラッシュしないようにするため、syslog 313001、 313004、および 313005 の生成を抑制します。
- syslog の UDP 接続の数は、ハードウェア プラットフォームの CPU の数と、設定する syslog サーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定する syslog サーバの数を乗算した値と同じになります。これは予期されている動作です。グローバル UDP 接続アイドル タイムアウトはこれらのセッションに適用され、デフォルトは 2 分であることに注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトは syslog だけでなくすべての UDP 接続に適用されます。
- Firewall Threat Defense デバイス が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。

- TCP ロギングホストがダウンすると、接続ステータスが *[*接続済み（*Connected*）*]* から *[*接続されていない（*Not connected*）*]* に変わるまで約 6 分かかります。ロギングは TCP を使用してチャネルステートを検出します。それまでは、ロギングはチャネルを介してログを送信します。この間に、**show log**を実行すると、出力に TCP ロギングホストが接続済みであると表示されます。TCP チャネルが閉じられると、TCP ロギング ホストの状態は *[*接続されていません（*Not connected*）*]* に更新されます。

Firewall Threat Defense デバイスの syslog ロギングの設定

ヒント　セキュリティイベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの Firewall Threat Defense プラットフォーム設定がこれらのメッセージに適用されません。セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （876 ページ）を参照してください。

Syslog の設定を行うには、以下の手順を実行します。

始める前に

ロギングのガイドライン （873 ページ）で要件を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 目次の [Syslog] をクリックします。

ステップ 3 [ロギング設定（Logging Setup）] をクリックしてロギングを有効にし、FTP サーバーの設定を指定し、フラッシュの使用を指定します。詳細については、ロギングの有効化および基本設定の構成 （876 ページ）を参照してください。

ステップ 4 [ロギング接続先（Logging Destinations）] をクリックして、特定の接続先へのロギングを有効にし、メッセージ重要度、イベントクラスまたはカスタムイベントリストでフィルタリングを指定します。詳細については、ロギング接続先の有効化 （879 ページ）を参照してください。

ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。

ステップ 5 [電子メール設定（E-mail Setup）] をクリックして、Syslog メッセージを電子メールとして送信する際に、その送信元アドレスとして使用する電子メールアドレスを指定します。詳細については、電子メールアドレスへの syslog メッセージの送信 （880 ページ）を参照してください。

ステップ 6 [イベントリスト（Events List）] をクリックして、イベントクラス、重要度、イベント ID を含むカスタムイベントリストを定義します。詳細については、カスタム イベント リストの作成 （881 ページ）を参照してください。

ステップ 7 [レート制限（Rate Limit）] をクリックして、設定されているすべての宛先に送信されるメッセージの量を指定し、レート制限を割り当てるメッセージのシビラティ（重大度）を定義します。詳細については、syslog メッセージの生成レートの制限 （882 ページ）を参照してください。

ステップ 8 [Syslog設定（Syslog Settings）] タブをクリックして、サーバーを Syslog 接続先として設定するために、ロギング機能を指定し、タイムスタンプの包含を有効にし、他の設定を有効にします。詳細については、Syslog 設定 （883 ページ）を参照してください。

ステップ 9 [Syslogサーバー（Syslog Servers）] をクリックして、ロギング接続先として指定される Syslog サーバーの IP アドレス、使用されているプロトコル、形式、およびセキュリティゾーンを指定します。詳細については、Syslog サーバーの設定 （885 ページ）を参照してください。

セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定

「セキュリティ イベント」には、接続、セキュリティ インテリジェンス、侵入、ファイルとマルウェアのイベントが含まれます。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense設定（Threat Defense Settings）] > [Syslog] ページとそのタブの syslog 設定の一部はセキュリティ イベントの syslog メッセージに適用されますが、多くの場合は、システム ヘルスとネットワークに関連するイベントのメッセージに適用されるだけです。

セキュリティ イベントの syslog メッセージには、次の設定が適用されます。

- [ロギング セットアップ（Logging Setup）] タブ：
  - **EMBLEM 形式で syslog を送信**
- [Syslog 設定（Syslog Settings）] タブ：
  - **syslog メッセージのタイムスタンプを有効化**
  - **タイムスタンプ形式**
  - **Enable Syslog Device ID**
- [Syslog サーバー（Syslog Servers）] タブ：
  - [Syslog サーバーを追加（Add Syslog Server）] 形式（および設定済みサーバーのリスト）のすべてのオプション

ロギングの有効化および基本設定の構成

データプレーンイベントの syslog メッセージを生成するには、システムでロギングを有効にし、基本設定を構成します。また、ローカルバッファがいっぱいになると、フラッシュまたはFTP サーバー上のアーカイブを保存場所として設定することもできます。ログデータは保存後に操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別な

アクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

次の手順では、基本的な syslog 設定の一部について説明します。

ヒント セキュリティイベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの Firewall Threat Defense プラットフォーム設定がこれらのメッセージに適用されません。セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （876 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[syslog]** > **[ロギングの設定（Logging Setup）]** を選択します。

ステップ 3 ロギングを有効にし、基本のロギング設定を構成します。

- [ロギングの有効化（Enable Logging）]：Firewall Threat Defense デバイスのデータ プレーン システム ロギングをオンにします。
- フェールオーバー スタンバイ ユニットでのロギングの有効化（Enable Logging on the Failover Standby Unit）：Firewall Threat Defense デバイスのスタンバイのロギングをオンにします。
- EMBLEM 形式での syslog の送信（Send syslogs in EMBLEM format）：すべてのロギング宛先に対して、EMBLEM 形式のロギングを有効にします。EMBLEM を有効にする場合は、UDP プロトコルを使用して syslog メッセージをパブリッシュする必要があります。EMBLEM は TCP と互換性がありません。

  EMBLEM syslog フォーマットは、RFC 3164 および RFC 5424 の標準に基づいて構築されたシスコ固有の規則です。したがって、EMBLEM が有効になっている場合、syslog メッセージは、<PRI> フィールドの後にコロン（:）を出力します。これは RFC 5424 フォーマットとは対照的です。

  （注）
  RFC5424 形式の syslog メッセージには、通常、プライオリティ値（PRI）が表示されます。ただし、Firewall Management Center では、管理対象 Firewall Threat Defense デバイスの syslog メッセージに PRI 値を表示する場合、EMBLEM 形式を有効にしてください。また、EMBLEM フォーマットの syslog メッセージにデバイス ID は表示されません。

- デバッグ メッセージを syslog として送信（Send debug messages as syslogs）：すべてのデバッグ トレース出力を syslog にリダイレクトします。このオプションが有効になっている場合、syslog メッセージはコンソールに表示されません。したがって、デバッグ メッセージを表示するには、コンソールでロギングを有効にし、デバッグ syslog メッセージ番号とログ レベルの宛先として設定する必要があります。使用される syslog メッセージ番号は 711001 です。この syslog のデフォルトログレベルは [デバッグ（debug）] です。

- 内部バッファのメモリ サイズ（Memory Size of Internal Buffer）：ロギング バッファが有効の場合にsyslogメッセージが保存される内部バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは4096バイトです。範囲は4096～52428800です。

ステップ 4 （任意）Firewall Management Center への syslog メッセージロギングを設定します。

a) **[（Cisco Secure Firewall Management Center へのロギングを有効化（Enable Logging to Secure Firewall Management Center）]** チェックボックスをオンにして、VPN ロギングを有効にします。

b) [ログレベル（Logging Level）] ドロップダウンリストから、ロギングメッセージの syslog セキュリティレベルを選択します。

- VPN メッセージのロギングレベルは、デフォルトで [エラー（Errors）] に設定されます。

  VPN トラブルシューティング syslog により、Firewall Management Center に過度の負荷がかかる場合があります。そのため、このオプションを有効にするには注意が必要です。また、サイト間 VPN またはリモートアクセス VPN を設定してデバイスを設定すると、VPN syslog はデフォルトで自動的に Management Center に送信されます。特に複数のデバイスが関係する RAVPN の場合は、Firewall Management Center への syslog の過剰なフローを制限するために、ログレベルを [エラー（Error）] 以上に制限することをお勧めします。

レベルについては、重要度レベル （869 ページ） を参照してください。

ステップ 5 （オプション）バッファが上書きされる前に、サーバーにログ バッファの内容を保存するには、FTP サーバーを設定します。FTP サーバー情報を指定します。

- FTP サーバーバッファラップ（FTP Server Buffer Wrap）：バッファの内容が上書きされる前にFTPサーバーに保存するには、このボックスをオンにし、次のフィールドに必要な宛先情報を入力します。FTP 設定を削除するには、このオプションを選択解除します。
- IP アドレス（IP Address）：FTP サーバーの IP アドレスを含むホスト ネットワーク オブジェクトを選択します。
- ユーザ名（UserName）：FTPサーバーに接続するときに使用するユーザ名を入力します。
- パス（Path）：バッファの内容を保存するパスを FTP ルートからの相対で入力します。
- パスワードの確認（Password Confirm）：FTP サーバーへのユーザー名の認証に使用されるパスワードを入力および確認します。

ステップ 6 （オプション）バッファが上書きされる前に、サーバーにログ バッファの内容を保存するには、フラッシュ サイズを指定します。

- フラッシュ（Flash）：バッファの内容が上書きされる前にフラッシュ メモリに保存するには、このチェックボックスをオンにします。
- ロギングに使用する最大フラッシュ（KB）（Maximum flash to be used by logging (KB)）：フラッシュメモリ内でロギングに使用される最大領域を指定します（キロバイト単位）。範囲は、4 ～ 8044176 KB です。

- 保持する最小空き領域（KB）（Minimum free space to be preserved (KB)）：フラッシュ メモリに保持する最小空き領域を指定します（KB）。範囲は、0 ～ 8044176 KB です。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

ロギング接続先の有効化

ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。接続先を有効にするとき、その接続先に適用するメッセージフィルタも指定する必要があります。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （876 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [Syslog] > [ロギング接続先（Logging Destinations）] を選択します。 >

ステップ 3 接続先を有効にし、ロギング フィルタを適用するか、または既存の接続先を編集するには、[追加（Add）] をクリックします。

ステップ 4 [ロギング接続先（Logging Destinations）] ダイアログボックスで、接続先を選択し、接続先で使用するフィルタを設定します。

a) [ロギング接続先（Logging Destination）] ドロップダウンリストで、有効にする接続先を選択します。コンソール、メール、内部バッファ、SNMP トラップ、SSH セッション、Syslog サーバのそれぞれの接続先に各自のフィルタを作成できます。

（注）
コンソールおよびSSHセッションロギングは、診断CLIでのみ機能します。**system support diagnostic-cli** を入力します。

b) [イベントクラス（Event Class）] で、テーブルに表示されていないすべてのクラスに適用するフィルタを選択します。

次のフィルタを設定できます。

- [シビラティ（重大度）によるフィルタ（Filter on severity）]：シビラティ（重大度）のレベルを選択します。設定したレベル以上のメッセージが接続先に送られます。
- [イベントリスト使用（Use Event List）]：フィルタを定義するイベントリストを選択します。このイベントリストは[イベントリスト（Event Lists）]ページで作成します。
- [ロギング無効（Disable Logging）]：この接続先へのメッセージ送信を停止します。

c) イベントクラスごとのフィルタを作成するには、[追加（Add）]をクリックして新しいフィルタを作成するか、既存のフィルタを編集し、そのクラスでのメッセージを制限するイベントクラスとシビラティ（重大度）レベルを選択します。[OK]をクリックして、フィルタを保存します。

イベントクラスの説明については、syslog メッセージ クラス （870 ページ） を参照してください。

d) [OK] をクリックします。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

電子メール アドレスへの syslog メッセージの送信

電子メールとして送信される syslog メッセージの受信者リストを設定できます。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （876 ページ）を参照してください。

始める前に

- SMTP サーバのプラットフォーム設定ページで SMTP サーバを設定します
- ロギングの有効化および基本設定の構成 （876 ページ）
- ロギングの宛先として電子メールを設定します

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[Syslog]** > **[電子メールの設定（Email Setup）]** を選択します。

ステップ 3 電子メール メッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メール アドレスを指定します。

ステップ 4 [追加（Add）] をクリックして、指定した syslog メッセージの受信者の新しい電子メール アドレスを入力します。

ステップ 5 その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウンリストから選択します。

宛先の電子メール アドレスに対して適用される syslog メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。レベルについては、重要度レベル（869 ページ） を参照してください。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

カスタム イベント リストの作成

イベントリストは、ロギング接続先に適用して接続先に送信するメッセージを制御できるカスタム フィルタです。通常、シビラティ（重大度）のみに基づいて接続先へのメッセージをフィルタリングしますが、イベントリストを使用して、イベントクラス、シビラティ（重大度）、およびメッセージ識別子（ID）の組み合わせに基づいて送信されるメッセージを微調整できます。

カスタム イベント リストの作成は、2 段階のプロセスです。[イベントリスト（Event Lists）] でカスタムリストを作成し、イベントリストを使用して、[宛先のロギング（Logging Destinations）] で各種宛先のロギングフィルタを定義します。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （876 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[Syslog]** > **[イベント リスト（Events List）]** を選択します。

ステップ 3 イベント リストを設定します。

a) [追加（Add）] をクリックして新規リストを追加したり、既存のリストを編集したりします。

b) [名前（Name）] フィールドにイベント リストの名前を入力します。スペースは使用できません。

c) シビラティ（重大度）またはイベント クラスに基づいてメッセージを識別するには、[シビラティ（重大度）/イベント クラス（Severity/Event Class）] タブを選択して、項目を追加または編集します。

使用可能なクラスの詳細については、syslog メッセージ クラス （870 ページ） を参照してください。

レベルについては、重要度レベル （869 ページ） を参照してください。

特定のイベント クラスは、トランスペアレント モードのデバイスには適用されません。そのようなオプションが設定された場合、オプションは無視され、展開されません。

d) メッセージ ID を指定してメッセージを識別するには、[メッセージID（Message ID）] を選択し、ID を追加または編集します。

ハイフンを使用して ID 範囲を入力できます（たとえば、100000-200000）。ID は 6 桁の数字です。最初の 3 桁が機能にどのようにマップされるかについては、syslog メッセージ クラス （870 ページ） を参照してください。

特定のメッセージ番号については、『Cisco ASA Series Syslog Messages』を参照してください。

e) [OK] をクリックして、イベント リストを保存します。

ステップ 4 [ロギング接続先（Logging Destinations）] をクリックし、フィルタを使用する必要がある接続先を追加または編集します。

「ロギング接続先の有効化 （879 ページ）」を参照してください。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートは、シビラティ（重大度）レベルまたはメッセージ ID によって制限できます。ロギング レベルごと、および Syslog メッセージ ID ごとに個別の制限を指定できます。設定が競合する場合は、Syslog メッセージ ID の制限が優先されます。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （876 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[Syslog]** > **[レート制限（Rate Limit）]** を選択します。

ステップ 3 シビラティ（重大度）レベルによりメッセージの生成を制限するには、**[ログレベル（Logging Level）]** > **[追加（Add）]** をクリックして、次のオプションを設定します。

- ログ レベル（Logging Level）：レートを制限するシビラティ（重大度）レベル。レベルについては、重要度レベル （869 ページ） を参照してください。
- メッセージ数（Number of messages）：指定した時間内に許容される指定したタイプのメッセージの最大数。
- 間隔（Interval）：レート制限カウンタがリセットされるまでの秒数。

ステップ 4 [OK] をクリックします。

ステップ 5 syslog のメッセージ ID によりメッセージの生成を制限するには、**[Syslogレベル（Syslog Level）]** > **[追加（Add）]** をクリックし、次のオプションを設定します。

- [Syslog ID]：レートを制限する syslog のメッセージ ID。特定のメッセージ番号については、『Cisco ASA Series Syslog Messages』を参照してください。
- メッセージ数（Number of messages）：指定した時間内に許容される指定したタイプのメッセージの最大数。
- 間隔（Interval）：レート制限カウンタがリセットされるまでの秒数。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

Syslog 設定

一般的な Syslog 設定を設定して、Syslog サーバーに送信される Syslog メッセージに含めるファシリティ コードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージのシビラティ（重大度）レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、このページの一部の設定がこれらのメッセージに適用されません。Cisco Secure Firewall Management Center アドミニストレーション ガイド の「セキュリティイベントの *syslog* メッセージに適用する *Threat Defense* プラットフォームの設定」を参照してください。

手順

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [Syslog] > [Syslog 設定（Syslog Settings）] を選択します。 >

ステップ 3 ファイル メッセージのベースとして使用する Syslog サーバーのシステム ログ機能を、[ファシリティ（Facility）] ドロップダウンリストから選択します。

デフォルトは LOCAL4(20) です。これは UNIX システムで最も可能性の高いコードです。ただし、ネットワーク デバイス間では使用可能なファシリティが共用されているため、システム ログではこの値を変更しなければならない場合があります。

通常、ファシリティの値はセキュリティイベントとは関係ありません。メッセージにファシリティ値を含める必要がある場合は、Cisco Secure Firewall Management Center アドミニストレーション ガイド の「セキュリティイベントの *Syslog* メッセージのファシリティ」を参照してください。

ステップ 4 [タイムスタンプを各 Syslog メッセージで有効にする（Enable timestamp on each syslog message）] チェックボックスをオンにして、メッセージ生成日時を Syslog メッセージに含めます。

ステップ 5 syslog メッセージの [タイムスタンプの形式（Timestamp Format）] を選択します。

- [レガシー（Legacy）]（MMM dd yyyy HH:mm:ss）形式は、syslog メッセージのデフォルト形式です。

  このタイムスタンプ形式を選択すると、メッセージには常に UTC であるタイム ゾーンが表示されません。

- [RFC 5424]（yyyy-MM-ddTHH:mm:ssZ）は RFC 5424 syslog 形式で指定されている ISO 8601 タイムスタンプ形式を使用します。

  RFC 5424 形式を選択すると、「Z」が各スタンプの末尾に追加され、タイムスタンプが UTC タイム ゾーンを使用していることを示します。

ステップ 6 デバイス識別子を Syslog メッセージに追加する場合は（これはメッセージの先頭に配置されます）、[Syslog デバイス ID を有効にする（Enable Syslog Device ID）] チェックボックスをオンにし、ID のタイプを選択します。

- [インターフェイス（Interface）]：アプライアンスがメッセージの送信に使用するインターフェイスに関係なく、選択されたインターフェイスの IP アドレスを使用します。インターフェイスを識別するセキュリティ ゾーンを選択します。ゾーンは、単一のインターフェイスにマッピングされる必要があります。
- [ユーザー定義 ID（User Defined ID）]：選択したテキスト文字列を使用します（最大 16 文字）。
- [ホスト名（Host Name）]：デバイスのホスト名を使用します。

ステップ 7 [Syslog Message] テーブルを使用して、特定の Syslog メッセージのデフォルト設定を変更します。デフォルト設定を変更する場合にだけ、このテーブルでルールを設定する必要がありま

す。メッセージに割り当てられているシビラティ（重大度）を変更したり、メッセージの生成を無効にしたりできます。

デフォルトでは、NetFlow が有効になり、エントリはテーブルに表示されます。

a) NetFlow が原因で冗長している Syslog メッセージを抑制にするには、[ネットフロー同等 Syslog（Netflow Equivalent Syslogs）] を選択します。

これにより、メッセージが抑止されたメッセージとしてテーブルに追加されます。

（注）
これらの同等の Syslog メッセージがすでにテーブルにある場合、既存のルールは上書きされません。

b) ルールを追加するには、[追加（Add）] をクリックします。
c) 設定変更するメッセージ番号を [Syslog ID] ドロップダウンリストから選択し、新しいシビラティ（重大度）を [ロギング レベル（Logging Level）] ドロップダウンリストから選択するか、または [抑制（Suppressed）] を選択してメッセージの生成を無効にします。通常は、シビラティ（重大度）レベルの変更やメッセージのディセーブル化は行いませんが、必要に応じて両方のフィールドを変更できます。
d) [OK] をクリックしてテーブルにルールを追加します。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

Syslog サーバーの設定

システムから生成されたメッセージを処理するように syslog サーバーを設定するには、次の手順を実行します。

この syslog サーバーに接続イベントや侵入イベントなどのセキュリティイベントを受信させる場合は、セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （876 ページ）も参照してください。

始める前に

- ロギングのガイドライン （873 ページ）で要件を参照してください。
- デバイスからネットワーク上の syslog コレクタに到達できることを確認します。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [Syslog] > [Syslog サーバー（Syslog Server）] > を選択します。

ステップ 3 [TCP syslogサーバーがダウンしているときにユーザートラフィックの通過を許可する（推奨）（Allow user traffic to pass when TCP syslog server is down (Recommended)）] チェックボックスをオンにして、TCPプロトコルを使用するsyslogサーバーがダウンしている場合にトラフィックを許可するようにします。

（注）

- このオプションは、デフォルトで有効です。必要な場合を除き、デバイスが外部TCP syslogサーバーに到達できない場合は、脅威防御デバイスを介した接続を許可することをお勧めします。
- Firewall Management Center バージョン 6.2.x 以前で [TCP syslogサーバーがダウンしているときにユーザートラフィックの通過を許可する（Allow user traffic to pass when TCP syslog server is down）] オプションが無効になっている場合、このオプションはバージョン 6.3 以降にアップグレードした後も無効状態になります。手動で有効にしてください。
- このオプションが無効で、デバイスに複数のTCP syslogサーバーが設定されている場合、少なくとも1つのサーバーが脅威防御デバイスから到達可能であれば、ユーザートラフィックの通過が許可されます。そのため、無効化オプションは、デバイスに設定されているTCP syslog サーバーに到達できない場合にのみ適用されます。デバイスは、デバイスを介して拒否されたトラフィックの根本原因を説明する次の syslog を生成します。

```
%FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. New
connections are denied based on logging permit-hostdown policy
```

ステップ 4 [メッセージキューサイズ（メッセージ）（Message queue size (messages)）] フィールドに、syslog サーバーがビジー状態の場合に syslog メッセージをセキュリティアプライアンスに保存するキューのサイズを入力します。最小件数は 1 件です。デフォルトは 512 です。無制限の数のメッセージをキューに入れる場合は、0 を指定します（使用可能なブロック メモリによって制限されます）。

メッセージが指定されたキューのサイズを超えると、メッセージは破棄され、syslog が失われます。最適なキューサイズを決定するには、使用可能なブロックメモリを特定する必要があります。**show blocks** コマンドを使用して、現在のメモリ使用率を確認します。コマンドと属性の詳細については、『*Cisco Secure Firewall ASA Series Command Reference Guide*』を参照してください。さらにサポートが必要な場合は、Cisco TAC にお問い合わせください。

ステップ 5 [追加（Add）] をクリックして、新しい Syslog サーバーを追加します。

a) [IP アドレス（IP Address）] ドロップダウン リストで、Syslog サーバーの IP アドレスを含むネットワーク ホスト オブジェクトを選択します。

b) プロトコル（TCP または UDP）を選択し、Firewall Threat Defense デバイスと Syslog サーバーの間の通信のポート番号を入力します。

UDP は高速で、TCP よりもデバイス上のリソースが減少します。

UDP のデフォルトポートは 514 です。TCP 用にポート 1470 を手動で設定する必要があります。有効な非デフォルトのポート値は、どちらのプロトコルでも 1025 ～ 65535 です。

c) [Cisco EMBLEM 形式でのログ メッセージ（UDP のみ）（Log messages in Cisco EMBLEM format (UDP only)）] チェックボックスをオンにして、Cisco の EMBLEM 形式でメッセージをログに記録するかどうかを指定します（プロトコルとして UDP が選択されている場合に限る）。

EMBLEM syslog フォーマットは、RFC 3164 および RFC 5424 の標準に基づいて構築されたシスコ固有の規則です。したがって、EMBLEM が有効になっている場合、syslog メッセージは、<PRI> フィールドの後にコロン（:）を出力します。

（注）
RFC5424 形式の syslog メッセージには、通常、プライオリティ値（PRI）が表示されます。ただし、Firewall Management Centerでは、Cisco EMBLEM 形式でのロギングを有効にした場合にのみ、管理対象 Firewall Threat Defense の syslog メッセージに PRI 値が表示されます。また、EMBLEM フォーマットの syslog メッセージにデバイス ID は表示されません。

d) [セキュア Syslog を有効にする（Enable Secure Syslog）] チェックボックスをオンにして、デバイスとサーバーの間の接続を TCP の SSL/TLS を使用して暗号化します。

（注）
このオプションを使用するには、プロトコルとして TCP を選択し、1025 ～ 65535 の範囲のポート値を選択する必要があります。また、**[Devices]** > **[Certificates]** ページで、syslog サーバーとの通信に必要な証明書をアップロードする必要があります。最後に、Firewall Threat Defense デバイスから syslog サーバーに証明書をアップロードして、セキュアな関係を完成させ、トラフィックの復号を許可します。デバイス管理インターフェイスでは、[Enable Secure Syslog] オプションはサポートされていません。

e) Syslog サーバーと通信するための [デバイス管理インターフェイス（Device Management Interface）] または [セキュリティ ゾーンまたは名前付きインターフェイス（Security Zones or Named Interfaces）] を選択します。

- [Device Management Interface]：管理インターフェイスから syslog を送信します。Snort イベントで Syslog を設定する場合は、このオプションを使用することをお勧めします。

  （注）
  [Device Management Interface] オプションでは、[Enable Secure Syslog] オプションをサポートされていません。

- [セキュリティ ゾーンまたは名前付きインターフェイス（Security Zones or Named Interfaces）]：[使用可能ゾーン（Available Zones）] のリストからインターフェイスを選択して、[追加（Add）] をクリックします。

重要
Firewall Threat Defense データプレーン（Lina）の syslog メッセージは、診断インターフェイスを介して送信できません。データプレーンの syslog メッセージを送信するように、他のインターフェイスまたは管理インターフェイス（Br1/Management0）を設定します。

f) **[OK]** をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

タイムアウト

さまざまなプロトコルの接続スロットと変換スロットのグローバル アイドル タイムアウト期間を設定できます。指定したアイドル時間の間スロットが使用されなかった場合、リソースはフリー プールに戻されます。

また、デバイスのコンソール セッションでタイムアウトを設定できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [タイムアウト（Timeouts）] を選択します。

ステップ 3 変更するタイムアウトを設定します。

任意の設定で、[カスタム（Custom）] を選択して自分の値を定義し、[デフォルト（Default）] を選択してシステムのデフォルト値に戻します。ほとんどの場合、最大タイムアウトは 1193 時間です。

[無効（Disable）] を選択して、タイムアウトを無効にできます。

- [コンソール タイムアウト（Console Timeout）]：コンソールへの接続が閉じられるまでのアイドル時間。範囲は 、5 ～ 1440 分です。デフォルトは 0 で、セッションがタイムアウトしないことを示します。値を変更すると、既存のコンソールセッションで古いタイムアウト値が使用されます。新しい値は新しい接続にのみ適用されます。

- [変換スロット（Translation Slot (xlate)）]：NAT 変換スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。
- [接続（Connection (Conn)）]：接続スロットが解放されるまでのアイドル時間。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [ハーフクローズ（Half-Closed）]：TCP ハーフクローズ接続を閉じるまでのアイドル時間。FIN と FIN-ACK の両方が検出された場合、接続はハーフクローズ状態と見なされます。FIN のみが検出された場合は、通常の接続タイムアウトが適用されます。最小は 30 秒です。デフォルトは 10 分です。
- [UDP]：UDP 接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。
- [ICMP]：全般的な ICMP 状態が終了するまでのアイドル時間。デフォルト（および最小）は 2 秒です。
- [RPC/Sun RPC]：SunRPC スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 10 分です。

  Sun RPC ベースの接続では、親接続が削除またはタイムアウトされると、新しい子接続が親子接続の一部と見なされないことがあるため、システムで設定されているポリシーまたはルールに従って新しい接続が評価される可能性があります。親接続がタイムアウトになると、既存の子接続はタイムアウトの設定値になるまで有効です。
- [H.225]：H.225 シグナリング接続を閉じるまでのアイドル時間。デフォルトは 1 時間です。すべての呼び出しがクリアされた後に接続をすぐにクローズするには、タイムアウト値を 1 秒（0:0:1）にすることを推奨します。
- [H.323]：H.245（TCP）および H.323（UDP）メディア接続が終了するまでのアイドル時間。デフォルト（および最小）は 5 分です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。
- [SIP]：SIP シグナリング ポート接続を閉じるまでのアイドル時間。この期間は 5 分以上にする必要があります。デフォルトは 30 分です。
- [SIP メディア（SIP Media）]：SIP メディア ポート接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。SIP メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
- [SIP 接続解除（SIP Disconnect）]：CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間（0:0:1 ～ 00:10:0）。デフォルトは 2 分（0:2:0）です。
- [SIP インバイト（SIP Invite）]：暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間（0:1:0 ～ 00:30:0）。デフォルトは、3 分（0:3:0）です。
- [SIP 暫定メディア（SIP Provisional Media）]：SIP 暫定メディア接続のタイムアウト値（1 ～ 30 分）。デフォルトは 2 分です。

- [フローティング接続（Floating Connection）]：同じネットワークへの複数のルートが存在し、それぞれメトリックが異なる場合、システムは接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは0です（接続はタイムアウトしません）。より良いルートを使用できるようにするには、タイムアウト値を 0:0:30 ～ 1193:0:0 の間で設定します。このタイマーは、仮想トンネルインターフェイス（VTI）を介した接続には適用されません。VTI を介した接続がスタックした場合は、手動でクリアする必要があります。
- [Xlate PAT]：PAT 変換スロットが解放されるまでのアイドル時間（0:0:30～ 0:5:0）。デフォルトは 30 秒です。前の接続がアップストリーム デバイスで引き続き開いている可能性があるため、開放された PAT ポートを使用する新しい接続をアップストリーム ルータが拒否する場合、このタイムアウトを増やすことができます。
- [TCP Proxy Reassembly]：再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウト（0:0:10 ～ 1193:0:0）。デフォルトは、1 分（0:1:0）です。
- [ARPタイムアウト（ARP Timeout）]：ARP テーブルを再構築する間隔の秒数（60 ～ 4,294,967）。デフォルトは 14,400 秒（4 時間）です。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

時刻の同期

Network Time Protocol（NTP）サーバーを使用して、デバイスのクロック設定を同期します。Firewall Management Center と同じ NTP サーバーを使用するように、Firewall Management Center によって管理されるすべての Firewall Threat Defense を設定することをお勧めします。Firewall Threat Defense は、設定された NTP サーバーから時刻を直接取得します。Firewall Threat Defense の設定済み NTP サーバーが何らかの理由で到達できない場合は、その時刻を Firewall Management Center と同期します。

デバイスは NTPv4 をサポートします。

（注） Firepower 4100/9300 シャーシに Firewall Threat Defense を導入する場合は、スマート ライセンスが正しく機能し、デバイス登録に適切なタイムスタンプを確保するように、Firepower 4100/9300 シャーシで NTP を設定する必要があります。Firepower 4100/9300 シャーシと Firewall Management Center には、同じ NTP サーバーを使用する必要があります。

始める前に

- 組織に Firewall Threat Defense からアクセスできる 1 台以上の NTP サーバーがある場合は、Firewall Management Center の [System] > [Configuration] ページで、時刻の同期用に設定したデバイスと同じ NTP サーバーを使用します。
- Firewall Management Center の 1 つまたは複数の NTP サーバーを設定する場合に [認証されたNTPサーバーのみを使用する（Use the authenticated NTP server only）] を選択すると、デバイスでは、Firewall Management Center を使用して認証するように設定された 1 つまたは複数の NTP サーバーのみが使用されます。（管理対象デバイスは、Firewall Management Center と同じ NTP サーバーを使用しますが、その NTP 接続では認証を使用しません）。
- デバイスが NTP サーバーに到達できない場合または組織に NTP サーバーがない場合は、次の手順で説明するように、[ディフェンスセンターの NTP 使用（Via NTP from Defense Center）] オプションを使用する必要があります。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [時間の同期化（Time Synchronization）] を選択します。

ステップ 3 次のいずれかのクロック オプションを設定します。

- [ディフェンスセンターの NTP 使用（Via NTP from Defense Center）]：（デフォルト）。管理対象デバイスは、Firewall Management Center 用に設定された NTP サーバー（認証されたNTPサーバーを除く）から時刻を取得し、それらのサーバーと時刻を直接同期します。ただし、次のいずれかに該当する場合、管理対象デバイスは Firewall Management Center と時刻を同期します。
  - Firewall Management Center の NTP サーバーに、デバイスからアクセスできない。
  - Firewall Management Center には、認証されていないサーバーはありません。
- [Via NTP from]：Firewall Management Center がネットワーク上の NTP サーバーを使用している場合は、このオプションを選択して、[System] > [Configuration] > [Time Synchronization] で指定した NTP サーバーと同じ完全修飾 DNS 名（ntp.example.com など）か IPv4 または IPv6 アドレスを入力します。NTP サーバーに到達できない場合は、Firewall Management Center が NTP サーバーとして機能します。

複数の NTP サーバーが設定されている場合、デバイスは、RFC で定義されている基準に基づいて適切と見なされる NTP サーバーを使用します。したがって、特定の NTP サーバーの [使用中（Being used）] のステータスは、そのサーバーがデバイスによって現在使用されていることを示します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

タイムゾーン

デフォルトでは、システムは UTC タイムゾーンを使用します。デバイスに別のタイムゾーンを指定するには、次の手順を実行します。

指定したタイムゾーンは、この機能をサポートするポリシーの時間ベースのポリシーアプリケーションにのみ使用されます。

（注） 時間ベースの ACL は、Firewall Management Center 7.0 以降の Snort 3 でもサポートされています。

手順

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[タイムゾーン（Time Zone）] ページからタイムゾーンオブジェクトを作成することもできます。

ステップ 2 [+] をクリックして、新しいタイムゾーンオブジェクトを作成します。

ステップ 3 タイムゾーンを選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 時間範囲オブジェクトを作成して、アクセス制御およびプレフィルタールールで適用可能な時間範囲を選択し、正しいタイムゾーンに関連付けられているデバイスに親ポリシーを割り当てます。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

UCAPL/CC コンプライアンス

この設定と、Firewall Management Center で有効にする方法の詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイド を参照 してください。

⚠

注意 この設定を有効にした後に無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

始める前に

- Secure Firewall Threat Defense デバイスは評価ライセンスを使用できません。輸出管理機能を有効にするには、Smart Software Manager アカウントを有効にする必要があります。
- Secure Firewall Threat Defense デバイスはルーテッド モードで展開する必要があります。
- このタスクを実行するには、管理者ユーザーである必要があります。
- Firewall Threat Defense デバイスが高可用性の場合、セキュリティ認定準拠モードは変更できません。高可用性ペアを形成する前に、セキュリティ認定準拠モードを変更してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [UCAPL/CC コンプライアンス（UCAPL/CC Compliance）] をクリックします。

ステップ 3 アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2 つの選択肢があります。

- [コモン クライテリア（Common Criteria）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [CC] を選択します。
- [Unified 機能承認製品リスト（Unified Capabilities Approved Products List）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [UCAPL] を選択します。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

パフォーマンス プロファイル

パフォーマンスプロファイルにより、デバイスの CPU コアがデータプレーン（Lina）と Snort の 2 つのメインシステムプロセスに割り当てられる方法が決定されます。データプレーンは、VPN 接続、ルーティング、およびその他の基本的なレイヤ 3/4 処理を処理します。Snort は、侵入とマルウェアの防止、URL フィルタリング、アプリケーション フィルタリング、および

詳細なパケットインスペクションを必要とするその他の機能を含む、高度なインスペクションを提供します。

基本機能と高度な機能をバランスよく使用する場合は、パフォーマンスプロファイルを変更しないでください。システムは、それらのプロセスにコアをバランスよく割り当てるように設計されています。割り当ては、ハードウェアモデルによって異なります。

ただし、デバイスを主に VPN や、侵入などの高度な検査に使用する場合は、パフォーマンスプロファイルを変更して、頻繁に使用される機能に多くのコアが割り当てられるようにすることができます。これにより、システムのパフォーマンスが向上する可能性があります。

始める前に

- これらの設定は、リリース 7.3 以降を実行しているシステムにのみ適用されます。
- パフォーマンスプロファイルは、次のデバイスタイプでサポートされています。
  - Firepower 4100/9300
  - Secure Firewall Threat Defense Virtual
- パフォーマンスプロファイルの変更は、クラスタまたは高可用性グループ内のユニット、またはマルチインスタンス用に設定されたユニットではサポートされません。スタンドアロンデバイス以外にプロファイルを割り当てると、展開はブロックされます。
- コア割り当ての最小数は2です。コアは、選択したパフォーマンスプロファイルに基づいて偶数単位で割り当てられます。

手順

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [パフォーマンスプロファイル（Performance Profile）] を選択します。

ステップ 3 プロファイルを選択します。

- [デフォルト（Default）]：これは推奨設定であり、VPNと侵入検査の両方を設定する場合に最適なオプションです。
- [プレフィルタfastpathによるVPNヘビー（VPN Heavy with prefilter fastpath）]：デバイスを主にVPNエンドポイントまたはヘッドエンドとして使用し、プレフィルタポリシーでVPNトラフィックの fastpath のルールを設定する場合は、このオプションを選択して、CPU コアの大部分をデータプレーンに割り当てることができます。90%をデータプレーン、10%を Snort に割り当てます。
- [検査によるVPNヘビー（VPN Heavy with inspection）]：デバイスを主に VPN エンドポイントまたはヘッドエンドとして使用するが、プレフィルタポリシーを使用して VPN トラフィックの fastpath を実行しない場合は、このオプションを選択して、CPU コアの大部分をデータプレーンに割り当てることができます。このオプションは、Snort を使用した侵

入検査、URLフィルタ処理などの高度な機能をネットワーク内の別のデバイスに任せることを前提としています。60% をデータプレーン、40% を Snort に割り当てます。

- [IPSヘビー（IPS Heavy）]：VPN を設定しないが、侵入防御のためにデバイスを使用する場合は、このオプションを選択して、CPU コアの大部分を Snort プロセスに割り当てることができます。30% をデータプレーン、70% を Snort に割り当てます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ポリシーを展開します。

ステップ 6 展開が完了したら、影響を受ける各デバイスを再起動して、新しいコアの割り当てを行えるようにする必要があります。

プラットフォーム設定の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
CPU コア割り当てのパフォーマンスプロファイル。	7.3.0	7.3.0	データプレーンと Snort に割り当てられたシステムコアの割合を調整して、システムパフォーマンスを調整できます。この調整は、VPN と侵入ポリシーの相対的な使用に基づいています。両方を使用する場合は、コア割り当てをデフォルト値のままにします。システムを主に VPN（侵入ポリシー適用なし）または IPS（VPN 設定なし）として使用する場合、コア割り当てをデータプレーン（VPN の場合）または Snort（侵入インスペクションの場合）にスキューできます。 [パフォーマンスプロファイル（Performance Profile）] ページがプラットフォーム設定ポリシーに追加されました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
リモートアクセスVPNの TLS 1.3。	7.3.0	7.3.0	TLS 1.3 を使用して、リモートアクセス VPN 接続を暗号化できます。 デバイスがリモートアクセスVPNサーバーとして機能する場合、Threat Defense プラットフォーム設定を使用して、そのデバイスでは TLS 1.3 プロトコルを使用する必要があることを指定します。 TLS 1.3 では、次の暗号方式のサポートが追加されています。 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 この機能には、Cisco Secure Client バージョン 5.0 以降が必要です。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[新しいポリシー（New Policy）]** > **[Threat Defense 設定の追加/編集（Add/Edit Threat Defense Settings）]** > **[SSL]** > **[TLS バージョン（TLS Version）]**
DNS要求を解決するための複数の DNS サーバーグループ。	7.2.0	7.2.0	クライアントシステムからのDNS要求を解決するために、複数のDNSグループを設定できます。これらの DNS サーバー グループを使用して、さまざまな DNS ドメインの要求を解決できます。たとえば、インターネットへの接続で使用するために、パブリック DNS サーバーを使用するキャッチオールのデフォルトグループを作成できます。次に、example.com ドメイン内のマシンへの接続など、内部トラフィックに内部 DNS サーバーを使用する別のグループを構成できます。したがって、組織のドメイン名を使用したFQDNへの接続は、内部DNSサーバーを使用して解決されますが、パブリックサーバーへの接続は外部 DNS サーバーを使用します。 **[プラットフォーム設定（Platform Settings）]** > **[DNS]**ページを変更しました。
HTTP、ICMP、およびSSHプラットフォーム設定のネットワークオブジェクトのサポート。	7.1.0	7.1.0	Threat Defense プラットフォーム設定ポリシーで IP アドレスを設定するときに、ホストまたはネットワークのネットワークオブジェクトを含むネットワーク オブジェクト グループを使用できるようになりました。 サポートされているプラットフォーム： Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
信頼された DNS サーバの指定のサポート。	7.1.0	7.1.0	直接インターネットアクセスの使用中にアドレス解決のために信頼できる DNS サーバを指定するオプションが導入されました。 直接インターネットアクセスの設定時に、信頼された DNS サーバーを設定するための新しいタブ（**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** > **[DNS]** > **[信頼されたDNSサーバー（Trusted DNS Servers）]**）を追加しました。 サポートされているプラットフォーム： Firewall Threat Defense
SNMPv3 ユーザーの MD5認証アルゴリズムまたは DES 暗号化を使用するプラットフォーム設定は、バージョン 7.0 以降を実行している Firewall Threat Defense デバイスに展開できません。	7.0.0	7.0.0	バージョン 6.5 では、Firewall Threat Defense における SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化が廃止されました。展開に、6.4 以前のバージョンを使用して作成された MD5 認証アルゴリズムまたは DES 暗号化を使用する SNMPv3 ユーザーが含まれている場合、バージョン 6.7 以前を実行している Firewall Threat Defense デバイスでは、それらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 または DES の設定を保持することはできません。また、MD5 または DES の設定を使用して新しいユーザーを作成することもできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、MD5 認証アルゴリズムまたは DES 暗号化を使用する SNMP v3 ユーザーを持つプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** > **[ホスト（Host）]** サポートされているプラットフォーム： Firewall Threat Defense
SNMPv3 ユーザーの認証アルゴリズムの SHA224 または SHA384 を指定します。	7.0.0	7.0.0	SNMPv3 ユーザーの認証アルゴリズムとして、SHA224 または SHA384 を選択できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** > **[ユーザー（Users）]** サポートされているプラットフォーム： Firewall Threat Defense
デバイスのタイムゾーンを指定します。	6.6.0	6.6.0	時間ベースのポリシーの適用で使用する、管理対象デバイスのローカルタイムゾーンを指定します。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[タイムゾーン（Time Zone）]** サポートされているプラットフォーム： Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
SNMP 通信の管理インターフェイスを指定します。	6.6.0	6.6.0	デバイスとSNMP管理ステーションの間の通信に管理インターフェイスを選択できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ホスト（Host）]** サポートされているプラットフォーム： Firewall Threat Defense
SNMPv3 ユーザーの認証アルゴリズムの SHA256 を指定します。	6.6.0	6.6.0	SNMPv3 ユーザーの認証アルゴリズムとして、SHA256 を選択できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）]** サポートされているプラットフォーム： Firewall Threat Defense
Firewall Threat Defense における SNMPv3 ユーザー向けの DES 暗号化と MD5 認証アルゴリズムは廃止されました。	6.5.0	いずれか	Firewall Threat Defense デバイスでは、SNMPv3 ユーザーに MD5 認証アルゴリズムまたはDES暗号化を使用しないことを推奨します。これらのオプションは廃止されているためです。展開に、6.4 以前のバージョンを使用して作成された MD5 認証アルゴリズムまたは DES 暗号化を使用する SNMPv3 ユーザーが含まれている場合、それらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 または DES の設定を保持することはできません。また、MD5 またはDES の設定を使用して新しいユーザーを作成することもできません。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）]** サポートされているプラットフォーム： Firewall Threat Defense
TCP syslog サーバーがダウンしているときにユーザートラフィックの通過を許可します。	6.3.0	6.3.0	デバイスが外部 TCP syslog サーバーに到達できない場合は、Threat Defense デバイスを介した接続を許可することを推奨します。[プラットフォーム設定（Platform Settings）] の [TCP syslogサーバーがダウンしているときにユーザートラフィックの通過を許可する（有効にすることを推奨）（Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)）] オプションはデフォルトで有効になっています。
SSH ログイン失敗の制限数。	6.3.0	6.3.0	ユーザーが SSH 経由でデバイスにアクセスし、ログイン試行を 3 回続けて失敗すると、デバイスは SSH セッションを終了します。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
SSH用の外部認証が追加されました。	6.2.3	6.2.3	LDAP または RADIUS認証を使用して Firewall Threat Defense への SSH の外部認証を設定できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [外部認証（External Authentication）]** サポートされているプラットフォーム： Firewall Threat Defense
UC/APPL 準拠モードのサポート。	6.2.1	6.2.1	セキュリティ認定コンプライアンスは、CCモードまたはUCAPLモードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティモードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順についての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [UC/APPL準拠（UC/APPL Compliance）]** サポートされているプラットフォーム：すべてのデバイス
リモートアクセスVPNの SSL 設定。	6.2.1	6.2.1	Firewall Threat Defense デバイスでは、セキュ ソケットレイヤ（SSL）プロトコルと Transport Layer Security（TLS）を使用して、リモートクライアントからのリモートアクセス VPN のセキュアメッセージ伝送をサポートします。SSL でのリモート VPNアクセス中に、ネゴシエートとメッセージ伝送に使用されるSSLバージョンと暗号化アルゴリズムを設定できます。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SSL]** サポートされているプラットフォーム： Firewall Threat Defense
SSH および HTML 用の外部認証は削除されました。	6.1.0	6.1.0	統合管理アクセスをサポートするための変更により、データ インターフェイスに対するSSHおよびHTML ではローカル ユーザのみがサポートされます。また、論理診断インターフェイスに対するSSHは使用できなくなりました。代わりに、（同じ物理ポートを共有する）論理管理インターフェイスに対するSSHを使用できます。以前は、診断およびデータ インターフェイスに対する SSH および HTML アクセスでは外部認証のみがサポートされていましたが、管理インターフェイスに対してはローカル ユーザのみがサポートされていました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [外部認証（External Authentication）]** サポートされているプラットフォーム： Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firepower Threat Defense のサポート。	6.0.1	6.0.1	この機能が導入されました。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** サポートされているプラットフォーム： Firewall Threat Defense

第 19 章

ネットワーク アドレス変換

ここでは、ネットワーク アドレス変換（NAT）について、および Firewall Threat Defense デバイスでそれを設定する方法について説明します。

- NAT を使用する理由 （901 ページ）
- NAT の基礎 （902 ページ）
- NAT ポリシーの要件と前提条件 （912 ページ）
- NAT のガイドライン （913 ページ）
- NAT ポリシーの管理 （921 ページ）
- 脅威に対する防御のための NAT の設定 （923 ページ）
- IPv6 ネットワークの変換 （975 ページ）
- NAT のモニタリング （989 ページ）
- NAT の例 （990 ページ）
- Firewall Threat Defense NAT の履歴 （1049 ページ）

NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アド

レスを節約します。これは、ネットワーク全体に対して1つのパブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるからです。

NAT の他の機能は、次のとおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換：IPv6 ネットワークを IPv4 ネットワークに 接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

（注） NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常どおりに適用されます。

NAT の基礎

ここでは、NAT の基礎について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけでなく、デバイスに接続された任意のネットワークを変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」ネットワークは、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピング アドレス/ホスト/ネットワーク/インターフェイス：マッピング アドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。

（注） アドレスの変換時、デバイスのインターフェイス用に設定された IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、双方向に接続を開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。
- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向です。このガイドでは、特定の接続が「宛先」アドレスから発生する場合でも、コマンドや説明に「送信元」および「宛先」が使用されるので注意してください。

NAT タイプ

NAT は、次の方法を使用して実装できます。

- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。ダイナミック NAT （931 ページ）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この時、この IP アドレスの一意の送信元ポートが使用されます。ダイナミック PAT （937 ページ）を参照してください。
- スタティック NAT：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。スタティック NAT （950 ページ）を参照してください。
- アイデンティティ NAT：実際のアドレスがスタティックにそのアドレス自身に変換されます。基本的に NAT を回避します。大規模なアドレス グループは変換し、小さいアドレス グループは除外する場合、NAT をこの方法で設定します。「アイデンティティ NAT （961 ページ）」を参照してください。

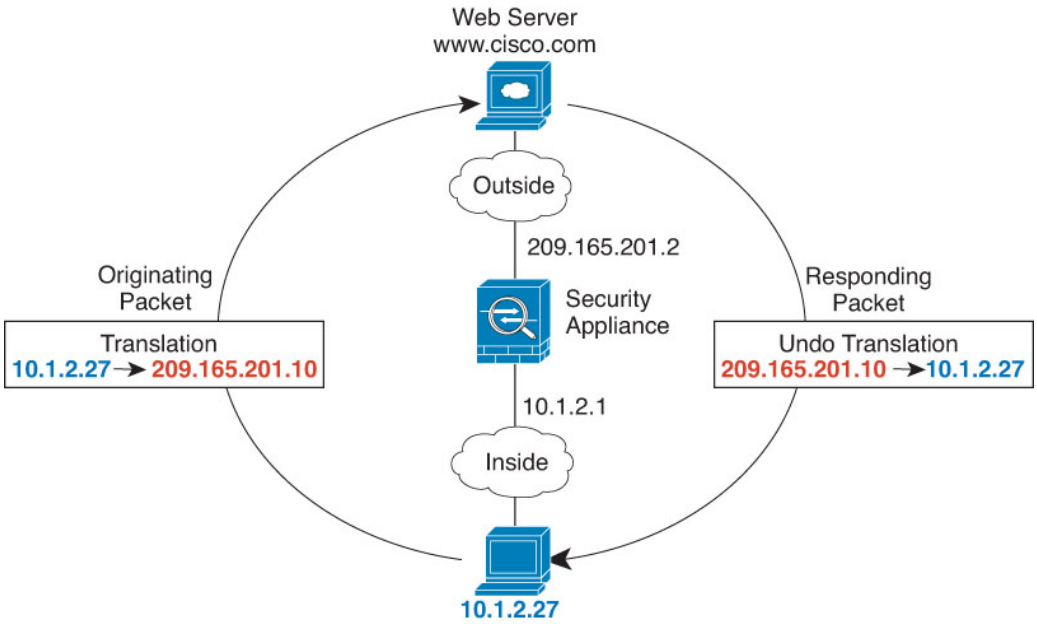
ルーテッド モードとトランスペアレント モードの NAT

NAT は、ルーテッド モードおよびトランスペアレント ファイアウォール モードの両方に設定できます。インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。次の項では、各ファイアウォール モードの一般的な使用方法について説明します。

ルーテッド モードの NAT

次の図は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。

図 *268 : NAT* の例：ルーテッド モード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピング アドレス 209.165.201.10 に変換されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.10 に応答を送信し、Firewall Threat Defense デバイス がそのパケットを受信します。これは、Firewall Threat Defense デバイス がプロキシ ARP を実行してパケットを要求するためです。
3. Firewall Threat Defense デバイス はその後、パケットをホストに送信する前に、マッピング アドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

トランスペアレント モードまたはブリッジ グループ内の NAT

NAT をトランスペアレント モードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータが必要なくなります。これによりルーテッド モードでブリッジ グループ内で同様の機能を実行できます。

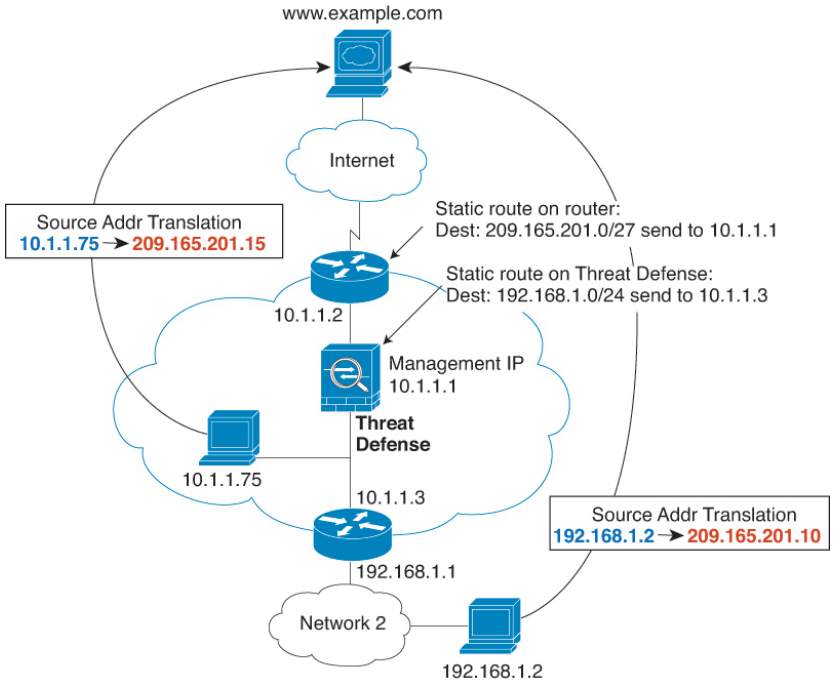
トランスペアレント モードまたは同じブリッジ グループのメンバー間のルーテッド モードの NAT には、以下の要件および制限があります。

- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジ グループ メンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- ARP インスペクションはサポートされていません。また、何らかの理由で、一方の Firewall Threat Defense のホストがもう一方の Firewall Threat Defense のホストに ARP 要求を送信し、開始ホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされる場合、実際のアドレスは ARP 要求で可視のままになります。

- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレント モードの一般的な NAT のシナリオを示します。このシナリオのトランスペアレント ファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 *269 : NAT* の例：トランスペアレント モード



1. 内部ホスト 10.1.1.75 が Web サーバーにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピング アドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.15 に応答を送信し、Firewall Threat Defense がそのパケットを受信します。これは、アップストリーム ルータには、Firewall Threat Defense の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。
3. その後、Firewall Threat Defenseはマッピング アドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.1.75 に戻します。実際のアドレスは直接接続されているため、Firewall Threat Defenseはそのアドレスを直接ホストに送信します。
4. ホスト 192.168.1.2 の場合も、リターン トラフィックを除き、同じプロセスが発生します。Firewall Threat Defense はルーティング テーブルでルートを検索し、192.168.1.0/24 の Firewall Threat Defense スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。

自動 NAT および 手動 NAT

自動 *NAT* および 手動 *NAT* という 2 種類の方法でアドレス変換を実装できます。

手動 NATの追加機能を必要としない場合は、自動 NATを使用することをお勧めします。自動 NAT の設定が容易で、Voice over IP（VoIP）などのアプリケーションでは信頼性が高い場合があります（VoIP では、ルールで使用されるオブジェクトのいずれにも属さない間接アドレスの変換が失敗することがあります）。

自動 NAT

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは 自動 *NAT* ルールとみなされます。これは、ネットワーク オブジェクトに NAT を設定するための迅速かつ簡単な方法です。ただし、これらのルールをグループ オブジェクトに対して作成できません。

これらのルールはオブジェクト自体の一部として設定されますが、オブジェクト マネージャからオブジェクト定義内の NAT 設定は確認できません。

パケットがインターフェイスに入ると、送信元 IP アドレスと宛先 IP アドレスの両方が 自動 NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないので、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、手動 NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

手動 NAT

手動 NAT では、1 つのルールで送信元アドレスと宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイド内でのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポートアドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

自動 NAT と 手動 NAT の比較

これら 2 つの NAT タイプの主な違いは、次のとおりです。

- 実際のアドレスの定義方法
  - 自動 NAT：NAT ルールがネットワーク オブジェクトのパラメータになります。ネットワーク オブジェクトの IP アドレスは元の（実際の）アドレスとして機能します。
  - 手動 NAT：実際のアドレスとマッピングアドレス両方のネットワークオブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT コンフィギュレーションのパラメータです。実際のアドレスのネットワーク オブジェクト グループを使用できることは、手動 NAT がよりスケーラブルであることを意味します。
- 送信元および宛先 NAT の実装方法
  - 自動 NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。つまり、送信元 IP アドレスに 1 つ、宛先 IP アドレスに 1 つと、2 つのルールが使用されることがあります。これらの 2 つのルールを相互に結び付けて、送信先と宛先の組み合わせに特定の変換を適用することはできません。
  - 手動 NAT：1 つのルールにより送信元と宛先の両方が変換されます。パケットは 1 つのルールにのみ一致し、それ以上のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは、1 つの 手動 NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるので、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、sourceA/destinationA には、sourceA/destinationB とは異なる変換を設定できます。
- NAT ルールの順序
  - 自動 NAT：NAT テーブルで自動的に順序付けされます。
  - 手動 NAT：NAT テーブルで手動で順序付けします（自動 NAT ルールの前または後）。

NAT ルールの順序

自動 NAT および 手動 NAT ルールは、3 つのセクションに分割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

（注） セクション 0 もあり、このセクションには、システムが使用するために作成される NAT ルールが含まれています。これらのルールは、他のすべてのルールよりも優先されます。これらのルールはシステムで自動的に作成され、必要に応じて xlate がクリアされます。セクション 0 では、ルールの追加、編集、または変更はできません。

表 *62 : NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	手動 NAT	コンフィギュレーションに登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、手動 NAT ルールはセクション 1 に追加されます。 「固有のルールを前に」とは、次のことを意味します。 • 静的ルールは動的ルールの前に配置する必要があります。 • 宛先変換を含むルールは、送信元変換のみのルールの前に配置する必要があります。 送信元アドレスまたは宛先アドレスに基づいて複数のルールが適用される可能性がある重複するルールを排除できない場合は、これらの推奨事項に従うように特に注意してください。

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 2	自動 NAT	セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。 **1.** スタティック ルール **2.** ダイナミック ルール **各ルールタイプでは、次の順序のガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、アドレス番号（低から高の順）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。
セクション 3	手動 NAT	まだ一致が見つからない場合、セクション 3 のルールは、コンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）
- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（ダイナミック）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

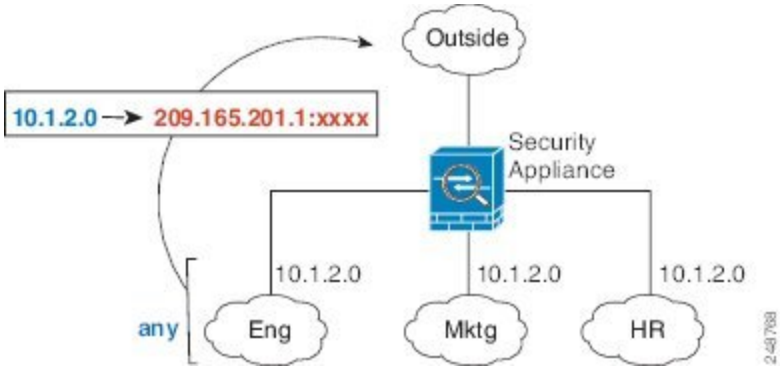
- 192.168.1.1/32（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 192.168.1.0/24（ダイナミック）

NAT インターフェイス

ブリッジ グループ メンバー インターフェイスを除き、NAT ルールを設定して任意のインターフェイス（つまり、すべてのインターフェイス）に適用できます。または、特定の実際のインターフェイスおよびマッピング インターフェイスを識別できます。実際のアドレスには任意のインターフェイスを指定できます。マッピング インターフェイスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベート アドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバル プールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピング アドレスには外部インターフェイスを指定します。

図 *270*：任意のインターフェイスの指定



ただし、「任意の」インターフェイスの概念は、ブリッジ グループ メンバーのインターフェイスには適用されません。「任意の」インターフェイスを指定する場合、すべてのブリッジ グループ メンバー インターフェイスは除外されます。このため、NAT をブリッジ グループ メンバーに適用するには、メンバー インターフェイスを指定する必要があります。したがって、ただ 1 つのインターフェイスが異なるだけで多数の類似したルールができる可能性があります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできませんが、メンバーのインターフェイスのみに NAT を設定することはできます。

（注） インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。インターフェイスを指定する場合は、そのインターフェイスを含むインターフェイス オブジェクトを選択することで間接的に行います。

NAT 用のルーティングの設定

Firewall Threat Defense デバイスは、変換された（マッピング）アドレスに送信されるパケットの宛先である必要があります。

パケットを送信する際、デバイスは宛先インターフェイスを使用するか（指定した場合）、またはルーティング テーブル ルックアップ（指定しない場合）を使用して、出力インターフェイスを決定します。アイデンティティ NAT の場合は、宛先インターフェイスを指定した場合でもルート ルックアップを使用することができます。

以下で説明するように、必要なルーティング設定はマッピング アドレスによって異なります。

マッピング インターフェイスと同じネットワーク上のアドレス

宛先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用する場合、Firewall Threat Defense デバイス はプロキシ ARP を使用してマッピング アドレスの ARP 要求に応答し、マッピング アドレス宛てのトラフィックを代行受信します。この方法では、Firewall Threat Defense デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるので、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

（注） マッピング インターフェイスを任意のインターフェイスとして設定し、マッピング インターフェイスの 1 つと同じネットワーク上のマッピング アドレスを指定すると、そのマッピング アドレスの ARP 要求を別のインターフェイスで受信する場合、入力インターフェイスでそのネットワークの ARP エントリを手動で設定し、その MAC アドレスを指定する必要があります。通常、マッピング インターフェイスに任意のインターフェイスを指定して、マッピング アドレスの固有のネットワークを使用すると、この状況は発生しません。入力インターフェイスの [Advanced] 設定で、ARP テーブルを設定します。

固有のネットワーク上のアドレス

宛先（マッピングされた）インターフェイス ネットワークで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを識別できます。アップストリーム ルー

タには、Firewall Threat Defenseデバイス を指しているマッピング アドレスのスタティック ルートが必要です。

また、ルーテッド モードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピング アドレスの Firewall Threat Defense デバイス にスタティック ルートを設定し、ルーティング プロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク（10.1.1.0/24）に NAT を使用し、マッピング IP アドレス 209.165.201.5 を使用する場合は、209.165.201.5 255.255.255.255（ホスト アドレス）のスタティック ルートを再配布可能な 10.1.1.99 ゲートウェイに設定できます。

トランスペアレント モードの場合は、実際のホストが直接接続されてる場合は、Firewall Threat Defense デバイス をポイントするようにアップストリーム ルータのスタティック ルートを設定します。ブリッジ グループの IP アドレスを指定します。トランスペアレント モードのリモート ホストの場合は、アップストリーム ルータのスタティック ルートで、代わりにダウンストリーム ルータの IP アドレスを指定できます。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。また、必要に応じて通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできます。その場合には、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。

アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、「any」の IP アドレスに対して広範囲のアイデンティティ NAT ルールを設定した場合は、プロキシ ARP をイネーブルのままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストに問題が発生する可能性があります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（任意のアドレスと一致する）NAT ルールと一致します。このとき、実際にはFirewall Threat Defense デバイス 向けのパケットでない場合でも、Firewall Threat Defense デバイス はこのアドレスの ARP をプロキシします（この問題は、手動 NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に Firewall Threat Defense デバイス の ARP 応答を受信した場合、トラフィックは誤って Firewall Threat Defense デバイス に送信されます。

NAT ポリシーの要件と前提条件

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

NAT のガイドライン

ここでは、NAT の実装に関する詳細なガイドラインについて説明します。

NAT のファイアウォール モードのガイドライン

NAT は、ルーテッド モードとトランスペアレント ファイアウォール モードでサポートされています。

ただし、ブリッジグループ メンバーのインターフェイス（ブリッジグループ仮想インターフェイスの一部であるインターフェイス、BVI）での NAT 設定には次の制限があります。

- ブリッジ グループのメンバーの NAT を設定するときは、メンバー インターフェイスを指定します。ブリッジ グループ インターフェイス（BVI）自体に NAT を設定することはできません。
- ブリッジ グループ メンバーのインターフェイス間で NAT を実行するときには、実際のおよびマッピングされたアドレスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。
- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジ グループ メンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- 送信元と宛先のインターフェイスが同じブリッジグループのメンバーである場合、IPv4 と IPv6 ネットワーク（NAT64/46）の間での変換はできません。スタティック NAT/PAT 44/66、ダイナミック NAT44/66、およびダイナミック PAT44 のみが使用可能な方式であり、ダイナミック PAT66 はサポートされていません。ただし、異なるブリッジグループのメンバー間、またはブリッジグループ メンバー（送信元）と標準ルーテッド インターフェイス（宛先）間では、NAT64/46 を行うことは可能です。

（注） インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。

IPv6 NAT ガイドライン

NAT では、次のガイドラインと制御事項に基づいて IPv6 をサポートしています。

- 標準ルーテッド モード インターフェイスの場合、IPv4 と IPv6 の間の変換も可能です。

- 同一ブリッジ グループのメンバーであるインターフェイスの IPv4 と IPv6 間の変換はできません。2 つの IPv6 または 2 つの IPv4 ネットワーク間でのみ変換できます。この制限は、インターフェイスが異なるブリッジ グループのメンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- 同じブリッジ グループのインターフェイス間で変換するときは、IPv6 のダイナミック PAT（NAT66）を使用できません。この制限は、インターフェイスが異なるブリッジ グループのメンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

IPv6 NAT のベスト プラクティス

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます （手動 NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（手動 NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0 が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目 IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。
- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

検査対象プロトコルの NAT サポート

セカンダリ接続を開いたり、パケットに IP アドレスを埋め込んだりする、一部のアプリケーション層プロトコルは、次のサービスを提供するために検査されます。

- ピンホール作成：一部のアプリケーション プロトコルは標準ポートまたはネゴシエートポートのどちらかでセカンダリ TCP または UDP 接続を開きます。検査により、これらのセカンダリ ポートに対してピンホールが開かれるため、アクセス制御ルールを作成する必要はありません。
- NAT リライト：FTP などのプロトコルは、セカンダリ接続用の IP アドレスとポートをプロトコルの一部としてパケットデータに埋め込みます。いずれかのエンドポイントに対して NAT 変換が含まれている場合、インスペクション エンジンはパケット データを書き換えて、埋め込まれたアドレスとポートの NAT 変換を反映させます。NAT リライトなしでは、セカンダリ接続は機能しません。
- プロトコル強制：一部の検査は、検査対象プロトコルの RFC に対して一定の準拠を強制します。

次の表は、NAT リライトが適用される検査対象プロトコルとそれらの NAT 制限を示します。これらのプロトコルを含むNATルールを作成する場合は、これらの制限に留意してください。ここに示されていない検査対象プロトコルには NAT リライトが適用されません。こうしたインスペクションには GTP、HTTP、IMAP、POP、SMTP、SSH および SSL があります。

（注） NAT リライトは示されているポートでのみサポートされます。これらのプロトコルの一部に対して、ネットワーク分析ポリシーを使用して検査を他のポートに拡張できますが、NAT リライトはそれらのポートに拡張されません。これには、DCERPC、DNS、FTP、およびSun RPC インスペクションが含まれます。これらのプロトコルを非標準ポートで使用する場合、接続で NAT を使用しないでください。

表 *63 : NAT* がサポートするアプリケーション インスペクション

アプリケーション	検査対象のプロトコル、ポート	NAT の制限	ピンホールの作成
DCERPC	TCP/135	NAT64 はサポートされません。	はい
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	いいえ
ESMTP	TCP/25	NAT64 はサポートされません。	いいえ
FTP	TCP/21	（クラスタリング）スタティック PAT はサポートされません。	○

アプリケーション	検査対象のプロトコル、ポート	NAT の制限	ピンホールの作成
H.323 H.225（発呼信号） H.323 RAS	TCP/1720 UDP/1718 RAS の場合、UDP/1718 ～ 1719	（クラスタリング）スタティック PAT はサポートされません。 拡張 PAT はサポートされません。 NAT64 はサポートされません。	はい
ICMP ICMP Error	ICMP （デバイス インターフェイスに転送される ICMP トラフィックは検査されません）	制限なし。	いいえ
IP オプション	RSVP	NAT64 はサポートされません。	いいえ
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	拡張 PAT はサポートされません。 NAT64 はサポートされません。	いいえ
RSH	TCP/514	PAT はサポートされません。 NAT64 はサポートされません。 （クラスタリング）スタティック PAT はサポートされません。	○
RTSP	TCP/554 （HTTP クローキングは処理されません）	拡張 PAT はサポートされません。 NAT64 はサポートされません。 （クラスタリング）スタティック PAT はサポートされません。	○
SIP	TCP/5060 UDP/5060	拡張 PAT はサポートされません。 NAT64 または NAT46 はなし。 （クラスタリング）スタティック PAT はサポートされません。	○
Skinny（SCCP）	TCP/2000	拡張 PAT はサポートされません。 NAT64、NAT46、または NAT66 はなし。 （クラスタリング）スタティック PAT はサポートされません。	○

アプリケーション	検査対象のプロトコル、ポート	NAT の制限	ピンホールの作成
SQL*Net （バージョン 1 および 2）	TCP/1521	拡張 PAT はサポートされません。 NAT64 はサポートされません。 （クラスタリング）スタティック PAT はサポートされません。	○
Sun RPC	TCP/111 UDP/111	拡張 PAT はサポートされません。 NAT64 はサポートされません。	はい
TFTP	UDP/69	NAT64 はサポートされません。 （クラスタリング）スタティック PAT はサポートされません。 ペイロード IP アドレスは変換されません。	はい
XDMCP	UDP/177	拡張 PAT はサポートされません。 NAT64 はサポートされません。 （クラスタリング）スタティック PAT はサポートされません。	はい

FQDN 宛先のガイドライン

IP アドレスの代わりに完全修飾ドメイン名（FQDN）ネットワークオブジェクトを使用して、手動 NAT ルールに変換済み（マッピング）宛先を指定できます。たとえば、www.example.com Web サーバを宛先とするトラフィックに基づいてルールを作成できます。

FQDN を使用すると、システムは DNS 解決を取得し、返されたアドレスに基づいて NAT ルールを書き込みます。複数の DNS サーバーグループを使用している場合は、フィルタドメインが優先され、フィルタに基づいて適切なグループからアドレスが要求されます。DNS サーバから複数のアドレスを取得する場合、使用されるアドレスは次の情報に基づきます。

- 指定したインターフェイスと同じサブネット上にアドレスがある場合は、そのアドレスが使用されます。同じサブネットに存在しない場合は、最初に返されたアドレスが使用されます。
- 変換後の送信元と変換後の宛先の IP タイプは一致している必要があります。たとえば、変換後の送信元アドレスが IPv6 の場合、FQDN オブジェクトはアドレスタイプとして IPv6 を指定する必要があります。変換後の送信元が IPv4 の場合、FQDN オブジェクトはアドレスタイプとして IPv4 を指定する必要があります。変換後の送信元が IPv4 の場合、FQDN オブジェクトは IPv4 または IPv4 と IPv6 の両方を指定できます。この場合、IPv4 アドレスが選択されます。

手動 NAT 宛先に使用されるネットワークグループに FQDN オブジェクトを含めることはできません。NAT では、1 つの宛先ホストだけがこのタイプの NAT ルールに適しているため、FQDN オブジェクトは単独で使用する必要があります。

FQDN を IP アドレスに解決できない場合、DNS 解決が取得されるまでルールは機能しません。

NAT のガイドラインの補足

- NAT ルールは、デバイスを通過するトラフィックにのみ適用され、RADIUS 認証など、デバイスによって開始されるトラフィックには適用されません。
- ブリッジ グループ メンバーであるインターフェイスに対しては、NAT ルールを作成します。ブリッジ仮想インターフェイス（BVI）自体には、 NAT ルールは作成できません
- サイト間 VPN で使用される仮想トンネルインターフェイス（VTI）の NAT ルールは作成できません。VTI の送信元インターフェイスのルールを作成すると、NAT は VPN トンネルに適用されません。VTI でトンネリングされた VPN トラフィックに適用される NAT ルールを作成するには、インターフェイスとして [任意（any）] を使用する必要があります。インターフェイス名を明示的に指定することはできません。
- （自動 NATのみ）。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- VPN がインターフェイスで定義されると、インターフェイスの着信 ESP トラフィックに NAT ルールは適用されません。システムでは、確立されている VPN トンネルの ESP トラフィックだけが許可され、既存のトンネルに関連付けられていないトラフィックはドロップされます。この制約は ESP と UDP ポート 500 および 4500 に適用されます。
- ダイナミック PAT を適用しているデバイスの背後にあるデバイスでサイト間 VPN を定義する場合、UDP ポート 500 および 4500 は実際に使用されないため、PAT デバイス背後のデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンダはセキュリティ アソシエーション（SA）を開始できません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションを使用できるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

  既存の接続（VPNトンネルなど）に適用する新しい NAT ルールを作成する場合は、**clear conn** を使用して接続を終了する必要があります。その後、接続を再確立しようとすると、NAT ルールが適用され、接続が正しく NAT 変換されます。

（注） ダイナミック NAT または PAT ルールを削除し、削除したルールに含まれるアドレスと重複するマッピングアドレスを含む新しいルールを追加すると、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** または **clear conn** コマンドを使用してクリアされるまで、新しいルールは使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- アドレスやサブネットの範囲内で明示的に指定するか暗黙的に指定するかにかかわらず、NAT で使用されるネットワークオブジェクトに 131,838 を超える IP アドレスを含めることはできません。アドレス空間をより狭い範囲に分割し、小さなオブジェクトに対して個別のルールを作成します。
- （手動 NATのみ）。発信元アドレスとして **any** を NAT ルールで使用する場合、「any」トラフィックの定義（IPv4 と IPv6）はルールによって異なります。Firewall Threat Defense デバイス がパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Firewall Threat Defense デバイスは、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定し、送信元をインターフェイスの IPv4 アドレスにマッピングする場合、**any** は「任意の IPv4 トラフィック」を意味します。これは、マッピングされたインターフェイス アドレスが、宛先も IPv4 であることを暗示しているためです。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールには、次のアドレスを含めることはできません。
  - マッピング インターフェイスの IP アドレス。ルールに「any」インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合は、インターフェイス アドレスの代わりにインターフェイス名を指定します。
  - フェールオーバー インターフェイスの IP アドレス。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN が有効な場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate

ではなくスタティック xlate にヒットした場合、PPTP 接続の確立に失敗する可能性があります。

- NAT ルールの送信元アドレスとリモートアクセス VPN アドレスプールの重複アドレスは使用できません。
- ルールで宛先インターフェイスを指定すると、ルーティングテーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただしアイデンティティ NAT の場合は、代わりにルート ルックアップを使用することもできます。
- NFS サーバへの接続に使用される Sun RPC トラフィックで PAT を使用する場合、PAT の対象となるポートが 1024 を超えると、NFS サーバが接続を拒否する可能性があることに注意してください。NFS サーバのデフォルト設定では、1024 を超えるポートからの接続は拒否されます。エラーメッセージは、通常「Permission Denied（権限が拒否されました）」です。PAT プールのポート範囲に予約済みポート（1 ー 1023）を含めるオプションを選択しない場合、1024 を超えるポートのマッピングが発生します。この問題を回避するには、NFS サーバの設定をすべてのポート番号を許可するように変更します。
- NAT はトラフィックを介してのみ適用されます。システムによって生成されたトラフィックは、NAT の対象外です。
- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- 単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。
- Protocol Independent Multicast（PIM）レジスタの内部ペイロードで NAT を使用することはできません。
- （手動 NAT）デュアル ISP インターフェイス セットアップ（ルーティング設定でサービス レベルアグリーメントを使用するプライマリインターフェイスとバックアップインターフェイス）の NAT ルールを作成する場合は、ルールで宛先基準を指定しないでください。プライマリインターフェイスのルールがバックアップインターフェイスのルールよりも前にあることを確認してください。これにより、デバイスは、プライマリ ISP が利用できない場合に、現在のルーティング状態に基づいて正しい NAT 宛先インターフェイスを選択できます。宛先オブジェクトを指定すると、NAT ルールは、指定しない場合には重複するルールのプライマリインターフェイスを常に選択します。
- インターフェイスに定義された NAT ルールと一致しないトラフィックについて ASP ドロップ理由 nat-no-xlate-to-pat-pool が示される場合は、影響を受けるトラフィックのアイデンティティ NAT ルールを設定して、トラフィックが変換されずに通過できるようにします。
- GRE トンネルエンドポイントの NAT を設定する場合は、エンドポイントでキープアライブを無効にする必要があります。無効にしないと、トンネルを確立できません。エンドポイントは、キープアライブを元のアドレスに送信します。

- DHCP と BOOTP はポート UDP/67 ～ 68 を共有します。BOOTP は廃止されているため、DHCPも実行している場合、BOOTP ポートの NAT ルールを作成するとポート割り当ての問題が発生する可能性があります。ネットワークセグメント間でDHCP要求を送信する場合は、代わりに DHCP リレーを使用することを検討してください。

NAT ポリシーの管理

ネットワークアドレス変換（NAT）では、着信パケットの IP アドレスが発信パケットの別のアドレスに変換されます。NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT では、プライベート IP アドレスがパブリック IP に置き換えられ、内部プライベートネットワーク内のプライベートアドレスがパブリックインターネットで使用可能でルーティング可能なアドレスに変換されます。NAT では、xlate とも呼ばれる変換が追跡され、リターントラフィックが正しい未変換のホストアドレスに確実に送信されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]**を選択します。

ステップ 2 NAT ポリシーを管理します。

- [作成（Create）]：[新しいポリシー（New Policy）] をクリックして、[Threat Defense NAT] を選択します。NAT ポリシーの作成 （922 ページ）を参照してください。
- [コピー（Copy）]：コピーするポリシーの横にある [コピー（Copy）]（） をクリックします。コピーに新しい一意の名前を付けるように求められます。コピーには、すべてのポリシールールと設定が含まれますが、デバイスの割り当ては含まれません。
- [レポート（Report）]：ポリシーの **[レポート（Report）]**（） をクリックします。ポリシー属性、デバイスの割り当て、ルール、およびオブジェクト使用情報を含むPDF レポートを保存するように求められます。
- [編集（Edit）]：編集するポリシーの横にある [編集（Edit）]（） をクリックします。脅威に対する防御のための NAT の設定 （923 ページ）を参照してください。
- [削除（Delete）]：削除するポリシーの横にある [削除（Delete）]（） をクリックして、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザーの未保存の変更が存在するかどうかも通知されます。

  注意
  管理対象デバイスに NAT ポリシーを展開した後は、デバイスからそのポリシーを削除できません。その代わりに、ルールを持たない NAT ポリシーを展開して、すでに管理対象デバイスに存在する NAT ルールを削除する必要があります。また、どのターゲット デバ

イスでも、最後に展開したポリシーは期限切れであっても削除できません。ポリシーを完全に削除する前に、それらのターゲットに異なるポリシーを展開する必要があります。

NAT ポリシーの作成

新しい NAT ポリシーを作成する場合、少なくとも一意の名前を付ける必要があります。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、ポリシーを展開する前に、この手順を実行する必要があります。ルールを持たない NAT ポリシーをデバイスに適用すると、そのデバイスからすべての NAT ルールが削除されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]**を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックし、ドロップダウンリストで、Firewall Threat Defense デバイスの [Threat Defense NAT] を選択します。

Firepower NAT は、このマニュアルで説明されていない古いデバイス用です。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 ポリシーを展開するデバイスを選択します。

- [使用可能なデバイス（Available Devices）] リストでデバイスを選択し、[ポリシーに追加（Add to Policy）] をクリックします。
- [使用可能なデバイス（Available Devices）] リストから [選択されたデバイス（Selected Devices）] リストに、デバイスをクリックしてドラッグします。
- デバイスの横にある[削除（Delete）]（）をクリックして、[選択されたデバイス（Selected Devices）] リストからデバイスを削除します。

ステップ 6 [保存（Save）] をクリックします。

NAT ポリシーの対象の設定

ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイスおよび高可用性ペアのリストを検索して、選択したデバイスのリストに追加できます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ポリシー割り当て（Policy Assignments）] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、高可用性ペア、またはデバイスグループをポリシーに割り当てるには、[使用可能なデバイス（Available Devices）] リストで選択し、[ポリシーに追加（Add to Policy）] をクリックします。ドラッグ アンド ドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス（Selected Devices）] リストのデバイス、高可用性ペア、またはデバイスグループの横にある [削除（Delete）]（） をクリックします。

ステップ 5 **[OK]** をクリックします。

脅威に対する防御のための NAT の設定

ネットワークアドレス変換は非常に複雑になることがあります。変換の問題が発生したり、トラブルシューティングが難しい状況にならないよう、ルールはできるだけ単純にすることを推奨します。NAT を実装する前に、慎重に計画を立てることが非常に重要です。以下の手順では、基本的なアプローチを説明します。

NAT ポリシーは、共有ポリシーです。同様の NAT ルールを持つべきデバイスに、ポリシーを割り当てます。

割り当てられたデバイスにポリシーの特定のルールが適用されるかどうかは、ルールで使用されるインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）によって決定されます。インターフェイスオブジェクトにデバイスのインターフェイスが 1 つ以上含まれている場合、ルールがデバイスに導入されます。したがって、注意深くインターフェイスオブジェクトを設計することで、単一の共有ポリシー内のデバイスのサブセットに適用されるルールを設定できます。「任意」のインターフェイスオブジェクトに適用されるルールは、すべてのデバイスに導入されます。

インターフェイスのタイプを、そのインターフェイスがあるデバイスを対象とする NAT ポリシーでの使用が無効なタイプに変更した場合、ポリシーはそのインターフェイスに削除済みのラベルを付けます。NAT ポリシーの [保存（Save）] をクリックすると、インターフェイスはポリシーから自動的に削除されます。

デバイスのグループにさまざまなルールが必要な場合は、複数の NAT ポリシーを設定できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** を選択します。

- 新しいポリシーを作成するには、**[新しいポリシー（New Policy）]** > **[Threat Defense NAT]** をクリックします。ポリシーに名前を付け、オプションでデバイスを割り当て、[保存（Save）] をクリックします。

  デバイスの割り当てを後で変更するには、ポリシーを編集して、[ポリシー割り当て（Policy Assignments）] をクリックします。

- 既存の Threat Defense NAT ポリシーを編集するには、[編集（Edit）]（✎）をクリックします。このページには、Firewall Threat Defense デバイスでは使用されない Firepower NAT ポリシーも表示されます。

  代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 必要となるルールのタイプを決定します。

作成できるルールには、ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールがあります。概要については、NAT タイプ（903 ページ）を参照してください。

ステップ 3 手動 NAT または自動 NAT として実装するルールを決定します。

この 2 つの実装オプションの比較については、自動 NAT および 手動 NAT （906 ページ）を参照してください。

ステップ 4 デバイスごとにカスタマイズするルールを決定します。

複数のデバイスに 1 つの NAT ポリシーを割り当てることができるため、多くのデバイスに 1 つのルールを設定できます。ただし、各デバイスによって異なる解釈が必要なルールや、デバイスのサブセットにのみ適用すべきルールの場合もあります。

インターフェイス オブジェクトを使用して、ルールを設定するデバイスを制御します。次に、ネットワーク オブジェクトでオブジェクトのオーバーライドを使用して、デバイスごとに使用されるアドレスをカスタマイズします。

詳細については、複数のデバイスの NAT ルールのカスタマイズ （925 ページ）を参照してください。

ステップ 5 以下の項で説明している手順に従ってルールを作成します。

- ダイナミック NAT （931 ページ）
- ダイナミック PAT （937 ページ）

- スタティック NAT （950 ページ）
- アイデンティティ NAT （961 ページ）

ステップ 6 NAT ポリシーおよびルールを管理します。

以下の操作によって、ポリシーとそのルールを管理できます。

- ポリシーの名前または説明を編集するには、これらのフィールドをクリックし、変更を入力して、フィールドの外側をクリックします。
- 特定のデバイスに適用されるルールのみを表示するには、[デバイスによるフィルタ（Filter by Device）] をクリックし、目的のデバイスを選択します。ルールがデバイスのインターフェイスを含むインターフェイス オブジェクトを使用している場合、そのデバイスにルールが適用されます。
- ポリシーの警告またはエラーを表示するには、[Show warnings] をクリックして、[Device] を選択します。警告とエラーによって、トラフィックフローに悪影響を及ぼしたり、ポリシーの展開を妨げたりする構成がマークされます。
- ポリシーが割り当てられているデバイスを変更するには、[ポリシー割り当て（Policy Assignments）] リンクをクリックし、必要に応じて選択したデバイス リストを変更します。
- ルールが有効であるか、または無効であるかを変更するには、ルールを右クリックし、[状態（State）] コマンドから目的のオプションを選択します。これらのコントロールを使用して、ルールを削除しないで一時的に無効にすることができます。
- ルールを追加するには、[ルールの追加（Add Rule）] ボタンをクリックします。
- ルールを編集するには、ルールの[編集（Edit）]（）をクリックします。
- ルールを削除するには、ルールの[削除（Delete）]（）をクリックします。
- ページに表示するルールの数を変更するには、[Rows Per Page] ドロップダウンリストを使用します。
- 有効化、無効化、または削除する複数のルールを選択するには、各ルールのチェックボックスまたはヘッダーのチェックボックスをクリックしてから、アクションを実行します。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

複数のデバイスの NAT ルールのカスタマイズ

NAT ポリシーは共有されるため、複数のデバイスに特定のポリシーを割り当てることができます。ただし、指定したオブジェクトに設定できる自動 NAT ルールは 1 つまでです。そのた

め、変換を実行する特定のデバイスに基づいてオブジェクトにさまざまな変換を設定する場合は、インターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）を注意深く設定し、変換済みアドレスのネットワーク オブジェクトのオーバーライドを定義する必要があります。

インターフェイス オブジェクトでは、ルールを設定するデバイスを決定します。ネットワーク オブジェクトのオーバーライドでは、そのオブジェクトの特定のデバイスで使用する IP アドレスを決定します。

次のような例が考えられます。

- FTD-A と FTD-B に、「inside」という名前のインターフェイスに接続される内部ネットワーク 192.168.1.0/24 があります。
- FTD-A では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.100.10.10 ～ 10.100.10.200 の範囲の NAT プールに変換する必要があります。
- FTD-B では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.200.10.10 ～ 10.200.10.200 の範囲の NAT プールに変換する必要があります。

このように変換するには、次の手順を実行します。この例のルールはダイナミック自動 NAT 用ですが、任意のタイプの NAT ルールにこのテクニックを一般化できます。

手順

ステップ 1 内部インターフェイスと外部インターフェイスのセキュリティ ゾーンを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) コンテンツのテーブルから [インターフェイス オブジェクト（Interface Objects）] を選択し、**[追加（Add）]** > **[セキュリティ ゾーン（Security Zone）]** をクリックします。（ゾーンの代わりにインターフェイス グループを使用できます）。
c) 内部ゾーンのプロパティを設定します。
   - [名前（Name）]：**inside-zone** などの名前を入力します。
   - [タイプ（Type）]：ルーテッド モードのデバイスの場合は [ルーテッド（Routed）]、トランスペアレント モードの場合は [スイッチド（Switched）] を選択します。
   - [選択したインターフェイス（Selected Interfaces）]：選択済みリストに FTD-A/内部および FTD-B/内部インターフェイスを追加します。
d) [保存（Save）] をクリックします。
e) **[追加（Add）]** > **[セキュリティ ゾーン（Security Zone）]** をクリックし、外部ゾーンのプロパティを定義します。
   - [名前（Name）]：**outside-zone** などの名前を入力します。

- [インターフェイスタイプ（Interface Type）]：ルーテッドモードのデバイスの場合は[ルーテッド（Routed）]、トランスペアレントモードの場合は[スイッチド（Switched）]を選択します。
- [選択したインターフェイス（Selected Interfaces）]：選択済みリストに FTD-A/外部および FTD-B/外部インターフェイスを追加します。

f) [保存（Save）] をクリックします。

ステップ 2 [オブジェクト管理（Object Management）] ページで、元の内部ネットワーク内のネットワークオブジェクトを作成します。

a) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークの追加（Add Network）] > [Add Object（オブジェクトの追加）]** をクリックします。

b) 内部ネットワークのプロパティを設定します。

- [名前（Name）]：**inside-network** などの名前を入力します。
- [ネットワーク（Network）]：**192.168.1.0/24** などのネットワーク アドレスを入力します。

c) [保存（Save）] をクリックします。

ステップ 3 変換済み NAT プールのネットワーク オブジェクトを作成し、オーバーライドを定義します。

a) **[ネットワークの追加（Add Network）] > [Add Object（オブジェクトの追加）]** をクリックします。

b) FTD-A の NAT プールのプロパティを設定します。

- [名前（Name）]：**NAT-pool** などの名前を入力します。
- [ネットワーク（Network）]：**10.100.10.10-10.100.10.200** などの FTD-A のプールに含めるアドレスの範囲を入力します。

c) [オーバーライドを許可（Allow Overrides）] を選択します。

d) [オーバーライド（Override）] の見出しをクリックして、オブジェクト オーバーライドのリストを開きます。

e) [追加（Add）] をクリックして、[オブジェクト オーバーライドの追加（Add Object Override）] ダイアログボックスを開きます。

f) FTD-B を選択し、[選択されたデバイス（Selected Devices）] リストに追加します。

g) [オーバーライド（Override）] をクリックし、[ネットワーク（Network）] を [10.200.10.10-10.200.10.200] に変更します

h) [追加（Add）] をクリックして、オーバーライドをデバイスに追加します。

FTD-B のオーバーライドを定義すると、FTD-B のこのオブジェクトが設定されるたびに、元のオブジェクトに定義されている値の代わりにオーバーライド値が使用されます。

i) [保存（Save）] をクリックします。

ステップ 4 NAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。
b) [ルールの追加（Add Rule）] をクリックします。
c) 次のプロパティを設定します。
   - [NAT ルール（NAT Rule）] = 自動 NAT ルール。
   - [タイプ（Type）] = Dynamic。
d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。
   - [送信元インターフェイス オブジェクト（Source Interface Objects）]：inside-zone。
   - [宛先インターフェイス オブジェクト（Destination Interface Objects）]：outside-zone。

   （注）
   インターフェイス オブジェクトはルールが設定されるデバイスを制御します。この例ではゾーンに FTD-A と FTD-B のインターフェイスのみが含まれているため、NAT ポリシーが追加のデバイスに割り当てられた場合でも、ルールはこれらの 2 つのデバイスにのみ展開されます。
e) [変換（Translation）] で、次の項目を設定します。
   - [元の送信元（Original Source）]：inside-network オブジェクト。
   - **[変換済み送信元（Translated Source）] > [アドレス（Address）]**：NAT-pool オブジェクト。
f) [保存（Save）] をクリックします。

   各ファイアウォールによって保護される内部ネットワークに固有の変換を指定して、1 つのルールを FTD-A と FTD-B で異なるように解釈できるようになりました。

NAT ルールテーブルの検索とフィルタリング

NAT ルールテーブルを検索およびフィルタ処理して、変更または表示する必要があるルールを見つけることができます。テーブルをフィルタ処理すると、一致するルールのみが表示されます。ルール番号は1、2、というように連続的に変化しますが、フィルタ処理によって、実際のルール番号や、非表示のルールに相対するテーブル内のルールの位置は変更されないことに注意してください。フィルタ処理では、関心のあるルールを見つけるのに役立つように、表示されるものを変更するだけです。

NAT ポリシーを編集するときは、テーブルの上にあるフィールドを使用して、次のタイプの検索/フィルタ処理を実行できます。

- **デバイスによるフィルタ**：[デバイスによるフィルタ（Filter by Device）] をクリックし、ルールを表示するデバイスを選択して、[OK] をクリックします。ルールがデバイスに適

用されるかどうかは、ルールのインターフェイス制約によって決まります。送信元または宛先インターフェイスのいずれかにセキュリティゾーンまたはインターフェイスグループを指定した場合、デバイスの少なくとも1つのインターフェイスがゾーンまたはグループにあると、ルールがデバイスに適用されます。NAT ルールが任意の送信元および任意の宛先インターフェイスに適用される場合、すべてのデバイスに適用されます。

テキストまたは複数属性検索も実行すると、結果は選択したデバイスに限定されます。

このフィルタを削除するには、[デバイスによるフィルタ（Filter by Device）] をクリックしてデバイスの選択を解除するか、[すべて（All）] を選択して [OK] をクリックします。

- **単純なテキスト検索**：[フィルタ（Filter）] ボックスに文字列を入力し、Enter キーを押します。文字列は、ルール内のすべての値と比較されます。たとえば、ネットワークオブジェクトの名前である「network-object-1」を入力すると、送信元、宛先、およびPAT プール属性でそのオブジェクトを使用するルールが取得されます。

  ネットワークオブジェクトとポートオブジェクトの場合、文字列はルールで使用されるオブジェクトの内容とも比較されます。たとえば、PAT プールオブジェクトに 10.100.10.3 ～ 10.100.10.100 の範囲が含まれている場合、10.100.10.3 または 10.100.10.100（または部分的に 10.100.10）で検索すると、その PAT プールオブジェクトを使用するルールが含まれます。ただし、完全に一致する必要があります。10.100.10.5 での検索は、この IP アドレスがオブジェクトの IP アドレス範囲内にある場合でも、この PAT プールオブジェクトと一致しません。

  フィルタを削除するには、[フィルタ（Filter）] ボックスの右側にある [x] をクリックします。

- **複数属性検索**：単純なテキスト検索でヒット数が多すぎる場合は、検索に複数の値を設定できます。[フィルタ（Filter）]ボックスをクリックして属性のリストを開き、検索する属性の文字列を選択または入力して、[フィルタ（Filter）]ボタンをクリックします。これらの属性は、NAT ルール内で構成する属性と同じです。属性は AND 結合されているため、フィルタ処理された結果には、構成したすべての属性に一致するルールのみが含まれます。

  - ルールの状態（有効/無効）、PAT プールが構成されているか（有効/無効）、ルールの方向（単方向/双方向）、ルールタイプ（静的/動的）などのバイナリ属性については、必要に応じてボックスをオンまたはオフにします。属性値を気にしない場合は、両方のボックスをオンにしてください。両方のボックスをオフにすると、どのルールもフィルタに一致しません。
  - 文字列属性の場合、その属性に関連する文字列の全体または一部を入力します。これらは、セキュリティゾーン/インターフェイスグループ、ネットワークオブジェクト、またはポートオブジェクトのいずれかのオブジェクト名になります。また、ネットワークオブジェクトまたはポートオブジェクトのコンテンツである場合もあり、単純なテキスト検索の場合と同じ方法で照合されます。

  フィルタを削除するには、[フィルタ（Filter）] ボックスの右側にある [x] をクリックするか、[フィルタ（Filter）] ボックスをクリックしてドロップダウンリストを開き、[クリア（Clear）] ボタンをクリックします。

複数ルールの有効化、無効化、または削除

手動 NAT ルールを有効または無効にしたり、NAT ルールを 1 つずつ削除することができます。複数のルールを選択して、それらのすべてに一度に変更を適用することもできます。有効化/無効化は手動 NAT にのみ適用されるため、複数のルールタイプを組み合わせて選択した場合は、それらのみを削除できます。

ルールを有効または無効にする場合、すでに有効または無効になっているいくつかのルールを選択しても問題ないことに注意してください。たとえば、すでに有効になっているルールを有効にすると、そのルールは有効のままになります。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** を選択し、Threat Defense の NAT ポリシーを編集します。

ステップ 2 （オプション）NAT ルールをフィルタ処理して、変更するものを見つけます。

フィルタ処理は、大規模な NAT ポリシーがある場合に特に役立ちます。たとえば、無効になっているルールを検索して、有効にする必要があるルールを見つけることができます。

ステップ 3 変更するルールを選択します。

- 個々のルールを選択（または選択解除）するには、ルールの左側の列にあるチェックボックスをクリックします。
- 現在表示されているページのすべてのルールを選択するには、テーブルの見出しにあるチェックボックスをクリックします。

ページ間を移動しても、選択内容は保持されます。ただし、実際には、次のページに移動する前に、ページで選択したルールに対してアクションを実行することが最も合理的です。

ステップ 4 目的のアクションを実行します。複数のルールを選択する場合、アクションの確認を求められます。

これらのアクションは、右クリックメニューでも実行できることに注意してください。

- すべてのルールを有効にするには、**[一括アクションの選択（Select Bulk Action）]** > **[有効化（Enable）]** をクリックします。
- すべてのルールを無効にするには、**[一括アクションの選択（Select Bulk Action）]** > **[無効化（Disable）]** をクリックします。
- すべてのルールを削除にするには、**[一括アクションの選択（Select Bulk Action）]** > **[削除（Delete）]** をクリックします。

ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

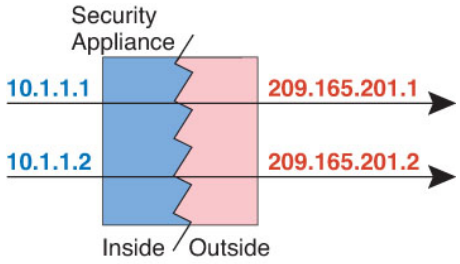
ダイナミック NAT について

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、マッピングされたプールから IP アドレスが、NAT によって、そのホストに割り当てられます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス ルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

（注） 変換の実施中、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。リモートホストからの接続が成功すると、接続のアイドルタイマーがリセットされます。

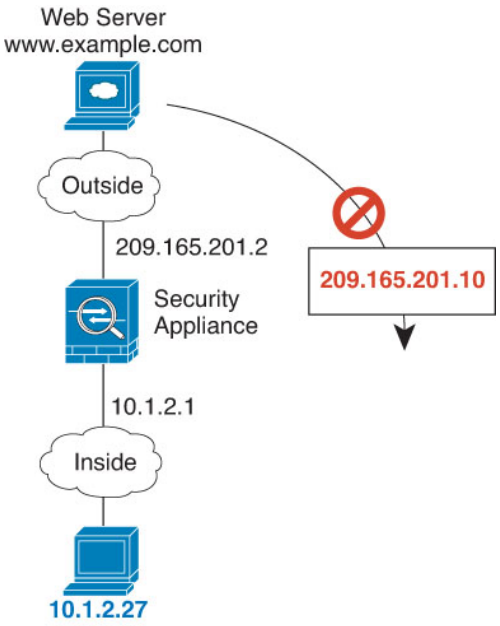
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 *271* : ダイナミック *NAT*



次の図に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。

図 *272 :* マッピング アドレスへの接続開始を試みているリモート ホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  この事象が発生した場合には、PAT または PAT フォールバック方式を使用します。PAT では、単一アドレスのポートを使用して 64,000 を超える変換を処理できるためです。

- マッピング プールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルで PAT を使用できないことです。たとえば、PAT は以下において機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコル。
- 1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持つオープンスタンダードではないアプリケーション。

ダイナミック自動 NAT の設定

ダイナミック自動 NAT ルールを使用して、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件を満たす必要があります：

- [元の送信元（Original Source）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲またはサブネットも可能です。
- [変換済み送信元（Translated Source）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（ ） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）] : [自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [ダイナミック（Dynamic）] を選択します。

ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）] :（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [変換（Translation）] で、次のオプションを設定します。

- [元の送信元（Original Source）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。

ステップ 6 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、NAT を使用した DNS クエリと応答の書き換え （1033 ページ）を参照してください。
- [インターフェイスPATへのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT (Destination Interface）]：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段として宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）を指定します。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

ダイナミック手動 NAT の設定

ダイナミック手動 NAT ルールは、自動 NAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。ダイナミック NAT は、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件も満たしている必要があります。

- [元の送信元（Original Source）]：ネットワークオブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。

- [変換済み送信元（Translated Source）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワークオブジェクトまたはグループを作成できます。

ダイナミック NAT では、宛先でポート変換を行うこともできます。オブジェクト マネージャで、[元の宛先アドレス（Original Destination Address）] および [変換後の宛先アドレス（Translated Destination Address）] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（✎） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[手動 NAT ルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。
- [有効化（Enable）]：ルールをアクティブにするかどうかを指定します。ルールページで右クリック メニューを使用することにより、後からルールをアクティブ化または非アクティブ化できます。
- [挿入（Insert）]：ルールを追加する場所を指定します。You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

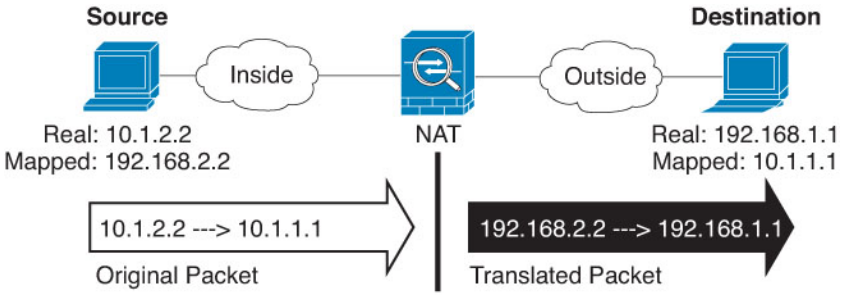
ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、

ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 （[変換（Translation）] ページ上。）元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。空白のままにすると、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [送信元インターフェイスIP（Source Interface IP）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。
- [変換済み宛先（Translated Destination）]：（オプション）。変換後のパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループを指定します。[変換前の宛先（Original Destination）] にオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT（つまり、変換なし）を設定します。

ステップ 7 （オプション）[元の宛先ポート（Original Destination Port）]、[変換後の宛先ポート（Translated Destination Port）] で、サービス変換の宛先サービス ポートを指定します。

ダイナミック NAT ではポート変換がサポートされないため、[元の送信元ポート（Original Source Port）] および [変換後の送信元ポート（Translated Source Port）] フィールドを空のままにします。ただし、宛先の変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- （送信元変換の場合のみ）[このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、NAT を使用した DNS クエリと応答の書き換え （1033 ページ）を参照してください。
- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段として宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）を指定します。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 9 [保存（Save）] をクリックしてルールを追加します。

ステップ 10 NAT ページで [保存（Save）] をクリックして変更を保存します。

ダイナミック PAT

ここでは、ダイナミック PAT について説明します。

ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図に、一般的なダイナミック PAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピング アドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 *273 :* ダイナミック *PAT*

変換が継続している間、アクセスルールで許可されていれば、宛先ネットワーク上のリモートホストは変換済みホストへの接続を開始できます。実際のポート アドレスおよびマッピングポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も有効期限切れになります。

（注） インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイスに同じプールを使用する場合（特に「任意の」インターフェイスに使用する場合）は、プールが短時間で使い尽くされ、新しい変換に使用できるポートがなくなる可能性があります。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、Firewall Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用できます。

同じブリッジ グループのインターフェイス間で変換するときは、IPv6 のダイナミック PAT（NAT66）を使用できません。この制限は、インターフェイスが異なるブリッジ グループのメンバーである場合、またはブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。詳細については、検査対象プロトコルの NAT サポート（915 ページ）を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。 アドレスの PAT プールを設定して、PAT アドレスのラウンドロビン割り当てを使用すると、この状況を緩和できます。

PAT プール オブジェクトの注意事項

PAT プールのネットワーク オブジェクトを作成する場合は、次のガイドラインに従ってください。

PAT プールの場合

- ポートは、1024 ー 65535 の範囲の使用可能なポートにマッピングされます。必要に応じ、1024 番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。

  クラスタで動作する場合、アドレスごとに 512 個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当ても有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも 512 です。クラスタ ユニットの制限（クラスタのサイズ）を変更する場合は、xlate をクリアするか、デバイスを再起動して、PAT プールをクラスタ ユニットに適切に再割り当てできるようにしてください。

- PAT プールに対してブロック割り当てを有効にする場合、ポートブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションに低いポート番号（1 ～ 1023）が必要な場合は、機能しない可能性があります。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内のホストに割り当てられたブロック内でマッピングされたポートを取得します。

- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT が指定される場合は、もう一方のルールでも拡張 PAT が指定される必要があります。

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します。使用可能なポートがない場合、接続が妨げられる可能性があります。この問題を回避するには、ラウンドロビンオプションを使用します。

- パフォーマンスを最大にするには、PAT プール内の IP アドレスの数を 10,000 に制限します。

PAT プールの拡張 PAT の場合

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。

- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合、PAT プールのアドレスを、ポート トランスレーション ルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーション ルールを持つスタティック NAT は作成できません。

- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。

- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

- クラスタ内のユニットで拡張 PAT を使用することはできません。

- 拡張 PAT は、デバイスでのメモリ使用率が増加します。

PAT プールのラウンド ロビン方式の場合

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。ただし、この「粘着性」は、フェールオーバーが発生すると失われます。デバイスがフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- PAT プール ルール/ラウンド ロビン ルールとインターフェイス PAT ルールが同じインターフェイス上で混在していると、IPアドレスの「粘着性」も影響を受けます。指定したインターフェイスで PAT プールまたはインターフェイス PAT のいずれかを選択します。競合する PAT ルールは作成しないでください。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時NATプールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

ダイナミック自動 PAT の設定

ダイナミック自動 PAT ルールを使用して、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。1 つのアドレス（宛先インターフェイスまたは他のアドレスのいずれか）に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件を満たす必要があります：

- [元の送信元（Original Source）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲またはサブネットも可能です。
- [変換済み送信元（Translated Source）]：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。
  - [単一 PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。
  - [PAT プール（PAT pool）]：範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクト グループを作成します。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（ ） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）] : [自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [ダイナミック（Dynamic）] を選択します。

ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）] :（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [変換（Translation）] で、次のオプションを設定します。

- [元の送信元（Original Source）] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）] : 次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、[宛先インターフェイスIP（Destination Interface IP）] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] で [IPv6] オプションを選択する必要があります。PAT プールの設定ステップを飛ばします。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。
  - PAT プールを使用するには、[変換済み送信元（Translated Source）] を空にしておきます。

ステップ 6 PAT プールを使用している場合は、[PATプール（PAT Pool）] ページを選択して、次の手順を実行します。

a) [PATプールの有効化（Enable PAT pool）] を選択します。

b) **[PAT]** > **[アドレス（Address）]** フィールドで、プールのアドレスを保持するネットワークオブジェクト グループを選択します。

または、インターフェイス PAT を実装する別の方法として、[宛先インターフェイスIP（Destination Interface IP）] を選択できます。

c) （オプション）必要に応じて、次のオプションを選択します。

- [ラウンドロビン割り当てを使用（Use Round Robin Allocation）]：アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に2番目のアドレスというように順に使用されます。

- [拡張 PAT テーブル（Extended PAT Table）]：拡張 PAT を使用します。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IPアドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。インターフェイス PAT やインターフェイス PAT フォールバックとこのオプションを併用することはできません。

- [フラットなポート範囲（Flat Port Range）]、[予約済みポートを含む（Include Reserved Ports）]：TCP/UDP ポートを割り当てる際に、ポート範囲（1024 ～ 65535）を単一のフラットな範囲として使用します。（6.7 より前）変換のマッピングポート番号を選択すると、PAT は実際の送信元ポート番号を使用できます（使用可能な場合）。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含む（Include Reserved Ports）] オプションも選択します。バージョン 6.7 以降を実行している Firewall Threat Defense デバイスの場合、オプションを選択するかどうかにかかわらず、フラットなポート範囲が常に設定されます。これらのシステムには、**[予約済みポートを含む（Include Reserved Ports）]** オプションを選択しても、その設定が適用されます。

- [ブロック割り当て（Block Allocation）]：ポートのブロック割り当てを有効にする場合。キャリア グレードまたは大規模 PAT では、NATに 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、元のブロックにすべてのポートに対するアクティブな接続がホストにある場合は、追加のブロックが割り当てられます。ポートのブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。ポー

トのブロック割り当てはラウンド ロビンと互換性がありますが、拡張 PAT またはフラットなポート範囲のオプションと一緒に使用することはできません。また、インターフェイス PAT フォールバックも使用できません。

ステップ 7 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段として宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）を指定します。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 8 [保存（Save）] をクリックしてルールを追加します。

ステップ 9 NAT ページで [保存（Save）] をクリックして変更を保存します。

ダイナミック手動 PAT の設定

ダイナミック手動 PAT ルールは、自動 PAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。ダイナミック PAT は、アドレスを複数の IP アドレスだけに変換するのではなく、固有の IP アドレス/ポートの組み合わせに変換します。1 つのアドレス（宛先インターフェイスまたは他のアドレスのいずれか）に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件も満たしている必要があります。

- [元の送信元（Original Source）]：ネットワークオブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元（Translated Source）]：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。

- [単一 PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。
- [PAT プール（PAT pool）]：範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクト グループを作成します。サブネットを含めることはできません。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワークオブジェクトまたはグループを作成できます。

ダイナミック NAT では、宛先でポート変換を行うこともできます。オブジェクト マネージャで、[元の宛先アドレス（Original Destination Address）]および[変換後の宛先アドレス（Translated Destination Address）] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[手動 NAT ルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。
- [有効化（Enable）]：ルールをアクティブにするかどうかを指定します。ルールページで右クリック メニューを使用することにより、後からルールをアクティブ化または非アクティブ化できます。
- [挿入（Insert）]：ルールを追加する場所を指定します。You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

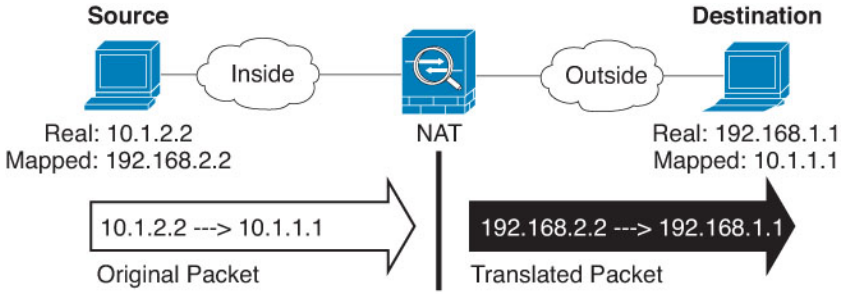
ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイ

スを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 （[変換（Translation）] ページ上。）元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。空白のままにすると、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [送信元インターフェイスIP（Source Interface IP）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] で [IPv6] オプションを選択する必要があります。PAT プールの設定ステップを飛ばします。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。

- PAT プールを使用するには、[変換済み送信元（Translated Source）] を空にしておきます。

- [変換済み宛先（Translated Destination）] :（オプション）。変換後のパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループを指定します。[変換前の宛先（Original Destination）] にオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT（つまり、変換なし）を設定します。

ステップ 7 （オプション）[元の宛先ポート（Original Destination Port）]、[変換後の宛先ポート（Translated Destination Port）] で、サービス変換の宛先サービス ポートを指定します。

ダイナミック NAT ではポート変換がサポートされないため、[元の送信元ポート（Original Source Port）] および [変換後の送信元ポート（Translated Source Port）] フィールドを空のままにします。ただし、宛先の変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 PAT プールを使用している場合は、[PATプール（PAT Pool）] ページを選択して、次の手順を実行します。

a) [PATプールの有効化（Enable PAT pool）] を選択します。

b) **[PAT]** > **[アドレス（Address）]** フィールドで、プールのアドレスを保持するネットワーク オブジェクト グループを選択します。

または、インターフェイス PAT を実装する別の方法として、[宛先インターフェイスIP（Destination Interface IP）] を選択できます。

c) （オプション）必要に応じて、次のオプションを選択します。

- [ラウンドロビン割り当てを使用（Use Round Robin Allocation）] : アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に2番目のアドレスというように順に使用されます。

- [拡張 PAT テーブル（Extended PAT Table）] : 拡張 PAT を使用します。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IPアドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。インターフェイス PAT やインターフェイス PAT フォールバックとこのオプションを併用することはできません。

- [フラットなポート範囲（Flat Port Range）]、[予約済みポートを含む（Include Reserved Ports）]：TCP/UDP ポートを割り当てる際に、ポート範囲（1024 ～ 65535）を単一のフラットな範囲として使用します。（6.7 より前）変換のマッピングポート番号を選択すると、PAT は実際の送信元ポート番号を使用できます（使用可能な場合）。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含む（Include Reserved Ports）] オプションも選択します。バージョン 6.7 以降を実行している Firewall Threat Defense デバイスの場合、オプションを選択するかどうかにかかわらず、フラットなポート範囲が常に設定されます。これらのシステムには、**[予約済みポートを含む（Include Reserved Ports）]** オプションを選択しても、その設定が適用されます。
- [ブロック割り当て（Block Allocation）]：ポートのブロック割り当てを有効にする場合。キャリア グレードまたは大規模 PAT では、NATに 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、元のブロックにすべてのポートに対するアクティブな接続がホストにある場合は、追加のブロックが割り当てられます。ポートのブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当てはラウンド ロビンと互換性がありますが、拡張 PAT またはフラットなポート範囲のオプションと一緒に使用することはできません。また、インターフェイス PAT フォールバックも使用できません。

ステップ 9 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段として宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）を指定します。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 10 [保存（Save）] をクリックしてルールを追加します。

ステップ 11 NAT ページで [保存（Save）] をクリックして変更を保存します。

ポート ブロック割り当てによる PAT の設定

キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、元のブロックにすべてのポートに

対するアクティブな接続がホストにある場合は、追加のブロックが割り当てられます。ブロック内のポートを使用する最後の xlate が削除されると、ブロックは解放されます。

ポート ブロックを割り当てる主な理由は、ロギングの縮小です。ポート ブロックの割り当てが記録され、接続が記録されますが、ポートブロック内で作成された xlate は記録されません。一方、ログ分析はより困難になります。

ポートのブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。TCP、UDP、および ICMP 接続用の個別のブロックがあり、これらのブロックは重複する場合があります。そのため、アプリケーションに低いポート番号（1 ～ 1023）が必要な場合は、機能しない可能性があります。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内のホストに割り当てられたブロック内でマッピングされたポートを取得します。低いポート番号を使用するアプリケーションに対してブロック割り当てを使用しない個別の NAT ルールを作成できます。Twice NAT の場合は、ルールが確実にブロック割り当てルールの前に来るようにします。

始める前に

NAT ルールの使用上の注意：

- [ラウンドロビン割り当ての使用（Use Round Robin Allocation）] オプションは含めることができますが、PAT 一意性の拡張、フラットな範囲の使用、予約済みポートを含めること、またはインターフェイス PAT へのフォールスルーに関するオプションは含めることができません。その他の送信元/宛先のアドレスとポート情報も許可されます。
- 既存のルールを置き換える場合は、NAT を変更するすべてのケースと同様、置き換えるルールに関連する xlate をクリアする必要があります。これは、新しいルールを有効にするために必要です。それらを明示的にクリアするか、または単にタイムアウトになるまで待ちます。クラスタでの動作の場合、クラスタ全体で xlate をグローバルにクリアする必要があります。

（注） 通常の PAT ルールとブロック割り当て PAT ルールを切り替える場合、オブジェクト NAT では、まずルールを削除してから xlate をクリアする必要があります。その後、新しいオブジェクト NAT ルールを作成できます。そうしないと、**show asp drop** 出力に pat-port-block-state-mismatch ドロップが表示されます。

- 特定の PAT プールに対し、そのプールを使用するすべてのルールに対してブロック割り当てを指定する（または指定しない）必要があります。1 つのルールにブロックを割り当てることはできず、別のルールに割り当てることもできません。重複する PAT プールもまたロック割り当て設定を混在させることはできません。また、ポート変換ルールを含むスタティック NAT とプールを重複させることはできません。

手順

ステップ 1 （任意）グローバル PAT ポート ブロック割り当ての設定を行います。

ポートブロック割り当てを制御するグローバル設定がいくつかあります。これらのオプションのデフォルトを変更する場合は、FlexConfig オブジェクトを設定し、それを FlexConfig ポリシーに追加する必要があります。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfig オブジェクト（FlexConfig Object）]** を選択します。

b) ブロック割り当てサイズを設定します。これは各ブロックのポート数です。

xlate block-allocation size *value*

範囲は 32 ～ 4096 です。デフォルトは 512 です。デフォルト値に戻すには、no 形式を使用します。

デフォルトを使用しない場合は、選択したサイズが 64,512 に均等に分割していることを確認します（1024 ～ 65535 の範囲のポート数）。確認を怠ると、使用できないポートが混入します。たとえば、100 を指定すると、12 個の未使用ポートがあります。

c) ホストごとに割り当てることができる最大ブロック数を設定します。

xlate block-allocation maximum-per-host *number*

制限はプロトコルごとに設定されるので、制限「4」は、ホストごとの上限が 4 つの UDP ブロック、4 つの TCP ブロック、および 4 つの ICMP ブロックであることを意味します。指定できる値の範囲は 1 ～ 8 で、デフォルトは 4 です。デフォルト値に戻すには、no 形式を使用します。

d) （オプション）暫定 syslog の生成をイネーブルにします。

xlate block-allocation pba-interim-logging *seconds*

デフォルトでは、ポートブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ロギングをイネーブルにすると、指定した間隔で次のメッセージが生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポート ブロックをレポートします（プロトコル（ICMP、TCP、UDP）、送信元および宛先インターフェイス、IP アドレス、ポート ブロックを含む）。間隔は 21600 ～ 604800 秒（6 時間から 7 日間）を指定することができます。

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

例：

次に、ブロック割り当てサイズを 64（ホストごとの最大サイズは 8）に設定し、暫定ロギングを 6 時間おきに有効にする例を示します。

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) FlexConfig オブジェクトで、次のオプションを選択します。

- [展開（Deployment）] = [毎回（Everytime）]
- [タイプ（Type）] = [後ろに付加（Append）]

f) [保存（保存）] をクリックして FlexConfig オブジェクトを作成します。

g) **[デバイス（Devices）]** > **[FlexConfig]** を選択し、これらの設定を調整する必要があるデバイスに割り当てられている FlexConfig ポリシーを作成または編集します。

h) 使用可能なオブジェクトリスト内のオブジェクトを選択し、>をクリックしてそのオブジェクトを選択したオブジェクト リストに移動します。

i) [保存（Save）] をクリックします。

[設定のプレビュー（Preview Config）] をクリックしてターゲット デバイスのいずれかを選択し、xlate コマンドが正しく表示されていることを確認します。

ステップ 2 PAT プール ポートのブロック割り当てを使用する NAT ルールを追加します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Threat Defense の NAT ポリシーを追加または編集します。

b) NAT ルールを追加または編集し、少なくとも次のオプションを設定します。

- [タイプ（Type）] = [ダイナミック（Dynamic）]
- **[変換（Translation）]** > **[元の送信元（Original Source）]** で、送信元アドレスを定義するオブジェクトを選択します。
- [PATプール（PAT Pool）] で、次のオプションを設定します。
  - [PAT プールの有効化（Enable PAT Pool）] を選択します。
  - **[PAT]** > **[アドレス（Address）]** で、PAT プールを定義するネットワークオブジェクトを選択します。
  - [ブロック割り当て（Block Allocation）] オプションを選択します。

c) ルールと NAT ポリシーに変更を保存します。

スタティック NAT

ここでは、スタティック NAT の概要およびその実装方法について説明します。

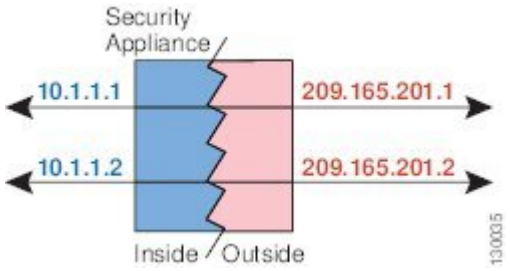
スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じなので、スタティック NAT では、双方向の接続（ホストへの接続とホストからの接続の両方）を開始できます（接続を許可するアクセス

ルールが存在する場合）。一方、ダイナミック NAT および PAT では、各ホストが後続の変換に対して異なるアドレスまたはポートを使用するので、双方向の接続は開始できません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブなので、実際のホストとリモート ホストの両方が接続を開始できます。

図 *274 :* スタティック *NAT*



（注） 必要に応じて、双方向の接続を無効化できます。

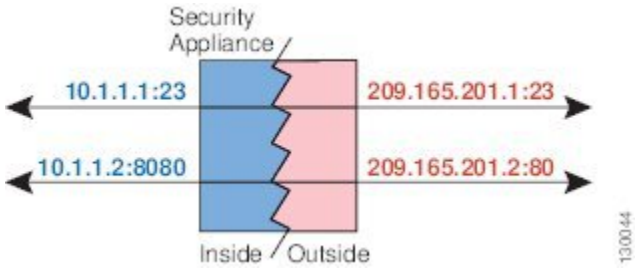
ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルとマッピング プロトコルおよびポートを指定できます。

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IPアドレスは別の値にマッピングされています。この変換は常にアクティブなので、変換されたホストとリモート ホストの両方が接続を開始できます。

図 *275 :* ポート変換を設定したスタティック *NAT* の一般的なシナリオ



ポート変換ルールを設定したスタティック NAT は、指定されたポートの宛先 IP アドレスのみにアクセスを制限します。NAT ルールの対象となっていない別のポートの宛先 IP アドレスにアクセスしようとすると、接続がブロックされます。さらに、手動 NAT の場合、NAT ルールの送信元 IP アドレスと一致しないトラフィックは、宛先ポートに関係なく、宛先 IP アドレスと一致するとドロップされます。そのため、宛先 IP アドレスに対して許可される他のすべてのトラフィックに関してルールを追加する必要があります。たとえば、ポートを指定しないで

IP アドレスのスタティック NAT ルールを設定し、それをポート変換ルールの後に配置することができます。

（注） セカンダリ チャネルのアプリケーション インスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、NAT が自動的にセカンダリ ポートを変換します。

次は、ポート変換を使用するスタティック NAT のその他の使用例です。

アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポート（FTP、HTTP、および SMTP など）でサービスを提供する、3 つの独立したサーバがある場合、外部ユーザに単一の IP アドレスを付与してこれらのサービスにアクセスできるようにすることができます。次に、アイデンティティ ポート変換を設定したスタティック NAT を設定して、単一の外部 IP アドレスを実際のサーバの正しい IP アドレスに、アクセスしようとしているポートに基づいてマッピングします。サーバは標準のポート（それぞれ21、80、および 25）を使用しているため、ポートを変更する必要はありません。

標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

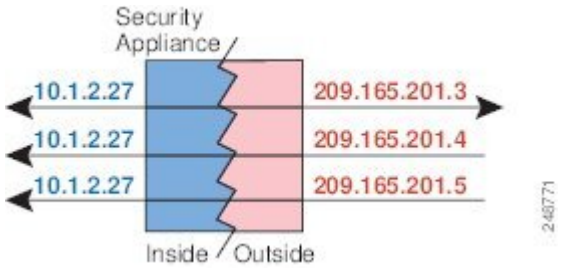
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

1 対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります（1 対多）。1 対多のスタティック NAT を設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピング アドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピング アドレスへのトラフィックを開始でき、1 つの実際のアドレスには変換されません。

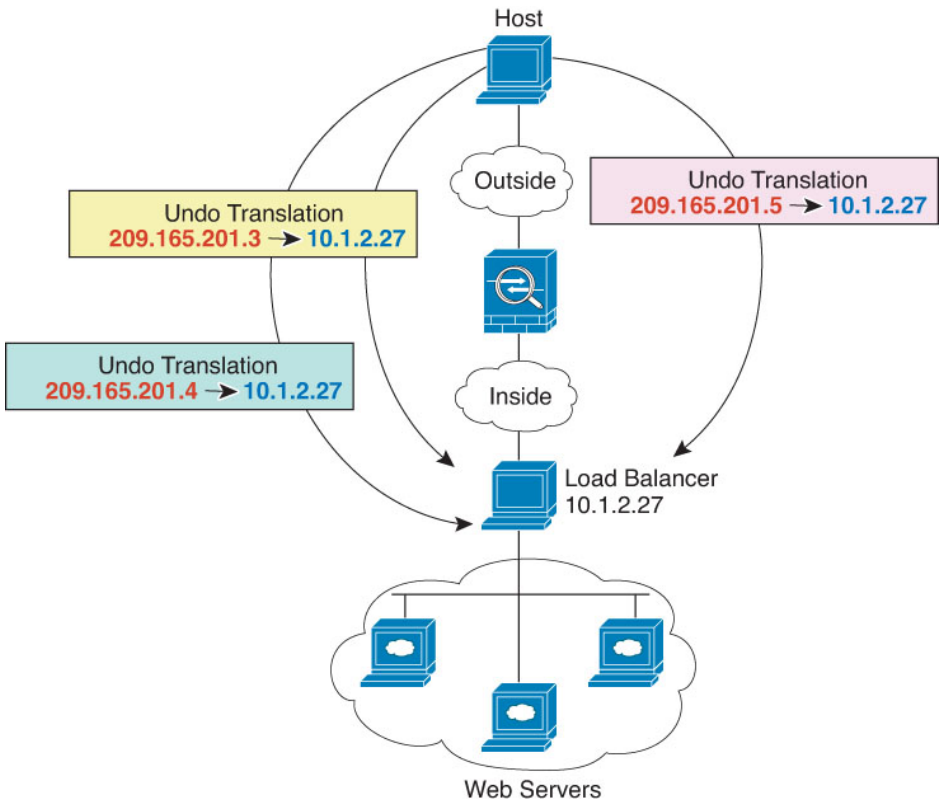
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 *276*：一対多のスタティック *NAT*



たとえば、10.1.2.27 にロード バランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 *277*：一対多のスタティック *NAT* の例



他のマッピング シナリオ（非推奨）

NAT には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多マッピングだけを使用することをお勧めします。その他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は、1 対多と同じです。しかし、コンフィギュレーションが複雑化して、実際のマッピングが一目では明らかでない場合があるため、必要とする実際の各アドレスに対

して1対多のコンフィギュレーションを作成することを推奨します。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピング アドレスに順番にマッピングされます（A は 1、B は 2、C は 3）。すべての実際のアドレスがマッピングされたら、次にマッピング アドレスは、最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（A は 4、B は 5、C は 6）。この結果、実際の各アドレスに対して複数のマッピング アドレスが存在することになります。1対多のコンフィギュレーションのように、最初のマッピングだけが双方向です。後続のマッピングでは、実際のホストへのトラフィックは開始できますが、実際のホストからのすべてのトラフィックは、送信元として最初にマッピングされたアドレスだけを使用します。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

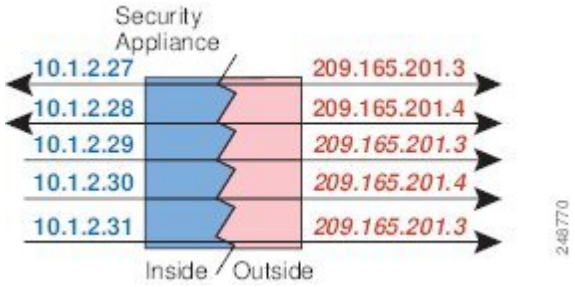
図 *278 :* 少対多のスタティック *NAT*

多対少または多対1コンフィギュレーションでは、マッピング アドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピング アドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングされたプールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックは開始できません。リターン トラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注） 多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合が起こるため（5 タプルが一意でない）、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 *279* : 多対少のスタティック *NAT*



このようにスタティック ルールを使用するのではなく、双方向の開始を必要とするトラフィックに 1 対 1 のルールを作成し、残りのアドレスにダイナミック ルールを作成することをお勧めします。

スタティック自動 NAT の設定

スタティック自動 NAT ルールを使用して、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールではポート変換を行うこともできます。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件を満たす必要があります：

- [元の送信元（Original Source）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲またはサブネットも可能です。
- [変換済み送信元（Translated Source）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイス アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットを含むネットワークオブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（✎） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）] : [自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [スタティック（Static）] を選択します。

ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）] :（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [変換（Translation）] で、次のオプションを設定します。

- [元の送信元（Original Source）] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）] : 次のいずれかになります。
  - アドレスの設定グループを使用するには、[アドレス（Address）] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）宛先インターフェイスのアドレスを使用するには、[宛先インターフェイスIP（Destination Interface IP）] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスのIPv6アドレスを使用するには、[詳細（Advanced）] で[IPv6]オプションを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。

- （オプション）。[元のポート（Original Port）]、[変換済みポート（Translated Port）]：TCP または UDP ポートを変換する必要がある場合は、[元のポート（Original Port）] でプロトコルを選択し、元のポート番号と変換済みポート番号を入力します。たとえば、必要に応じて TCP/80 を 8080 に変換できます。

ステップ 6 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、NAT を使用した DNS クエリと応答の書き換え（1033 ページ）を参照してください。 このオプションはポート変換を行う場合は使用できません。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。
- [ネット間マッピング（Net to Net Mapping）]：NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを使用する必要があります。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

スタティック手動 NAT の設定

スタティック手動 NAT ルールは、自動 NAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。スタティック NAT ルールを使用して、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールではポート変換を行うこともできます。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件も満たしている必要があります。

- [元の送信元（Original Source）]：ネットワークオブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元（Translated Source）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイス アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットを含むネットワークオブジェクトまたはグループを作成します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワークオブジェクトまたはグループを作成できます。ポート変換のみを適用する宛先スタティック インターフェイス NAT を設定する場合は、宛先マッピングアドレスのオブジェクトを追加せずに、インターフェイスをルールに指定できます。

送信元、宛先、またはその両方でポート変換を実行することもできます。オブジェクトマネージャで、元のポートと変換済みポートに使用できるポートオブジェクトがあることを確認します。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（ ） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

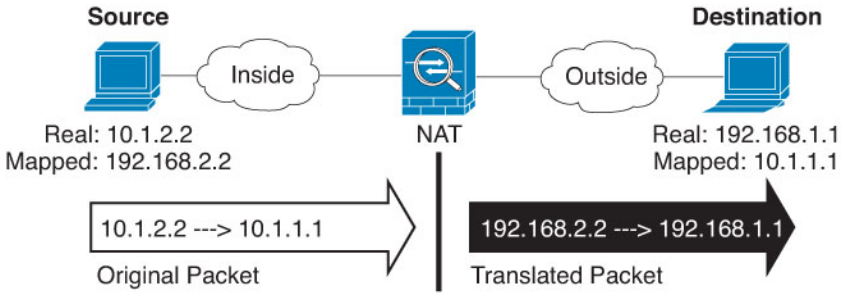
- [NAT ルール（NAT Rule）]：[手動 NAT ルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[スタティック（Static）]を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。
- [有効化（Enable）]：ルールをアクティブにするかどうかを指定します。ルールページで右クリック メニューを使用することにより、後からルールをアクティブ化または非アクティブ化できます。
- [挿入（Insert）]：ルールを追加する場所を指定します。You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 （[変換（Translation）] ページ上。）元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。

- [Original Destination][Address]：（オプション）。宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。空白のままにすると、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [送信元インターフェイスIP（Source Interface IP）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック イン

ターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、[アドレス（Address）]およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）宛先インターフェイスのアドレスを使用するには、[宛先インターフェイスIP（Destination Interface IP）] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスのIPv6アドレスを使用するには、[詳細（Advanced）]で[IPv6]オプションを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- [変換済み宛先（Translated Destination）]：（オプション）。変換後のパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループを指定します。[変換前の宛先（Original Destination）] にオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT（つまり、変換なし）を設定します。

ステップ 7 （任意）サービス変換の送信元または宛先サービスのポートを特定します。

ポート変換を適用するスタティック NAT を設定している場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 の間での変換が可能です。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）]、[変換済み送信元ポート（Translated Source Port）]：送信元アドレスのポート変換を定義します。
- **[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]**：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへのDNS応答の場合、レコー

ドは実際の値からマッピングされた値に書き換えられます。このオプションは特殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、NAT を使用した DNS クエリと応答の書き換え（1033 ページ）を参照してください。 このオプションはポート変換を行う場合は使用できません。

- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。
- [ネット間マッピング（Net to Net Mapping）]：NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを使用する必要があります。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [単一方向（Unidirectional）]：このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。

ステップ 9 [保存（Save）] をクリックしてルールを追加します。

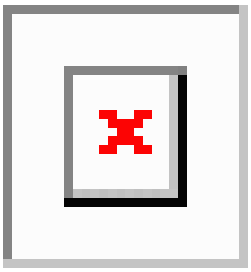
ステップ 10 NAT ページで [保存（Save）] をクリックして変更を保存します。

アイデンティティ NAT

IP アドレスを自身に変換する必要のある NAT コンフィギュレーションを設定できます。たとえば、1 つのネットワークを除いた、すべてのネットワークに NAT を適用するといった広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換することができます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 *280 :* アイデンティティ *NAT*



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ自動 NAT の設定

アドレスが変換されないようにするには、スタティック アイデンティティ自動 NAT ルールを使用します。つまり、アドレスをそのアドレス自体に変換するということです。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件を満たす必要があります：

- [元の送信元（Original Source）] : これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元（Translated Source）] : 元の送信元オブジェクトとコンテンツが全く同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用することもできます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（✎） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）] : [自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [スタティック（Static）] を選択します。

ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [変換（Translation）] で、次のオプションを設定します。

- [元の送信元（Original Source）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）]：元の送信元と同じオブジェクト。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。

アイデンティティ NAT には、[元のポート（Original Port）] および [変換済みポート（Translated Port）] オプションを設定しないでください。

ステップ 6 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6]：アイデンティティ NAT にこのオプションを設定しないでください。
- [ネット マッピングへのネット（Net to Net Mapping）]：アイデンティティ NAT にこのオプションを設定しないでください。
- [宛先インターフェイスでARPをプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [宛先インターフェイスのルートルックアップの実行（Perform Route Lookup for Destination Interface）]：元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

アイデンティティ手動 NAT の設定

スタティック アイデンティティ手動 NAT ルールは、自動 NAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。アドレスが変換されないようにするには、スタティック アイデンティティ NAT ルールを使用します。つまり、アドレスをそのアドレス自体に変換するということです。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下の要件も満たしている必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元（Translated Source）]：元の送信元と同じオブジェクトまたはグループ。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワークオブジェクトまたはグループを作成できます。ポート変換のみを適用する宛先スタティック インターフェイス NAT を設定する場合は、宛先マッピングアドレスのオブジェクトを追加せずに、インターフェイスをルールに指定できます。

送信元、宛先、またはその両方でポート変換を実行することもできます。オブジェクトマネージャで、元のポートと変換済みポートに使用できるポート オブジェクトがあることを確認します。アイデンティティ NAT では、同じオブジェクトを使用できます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [Add Rule] ボタンをクリックして、新しいルールを作成します。
- [編集（Edit）]（✎） をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[手動 NAT ルール（Manual NAT Rule）] を選択します。

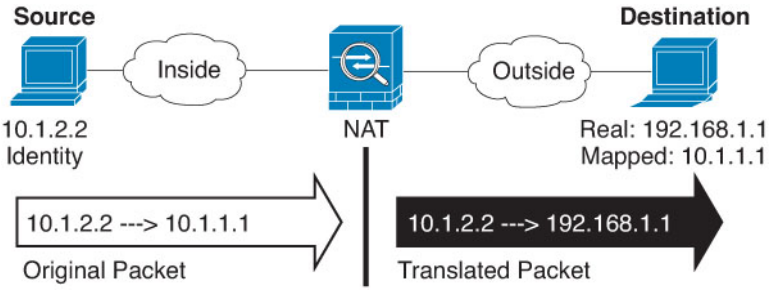
- [タイプ（Type）]：[スタティック（Static）]を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。
- [有効化（Enable）]：ルールをアクティブにするかどうかを指定します。ルールページで右クリック メニューを使用することにより、後からルールをアクティブ化または非アクティブ化できます。
- [挿入（Insert）]：ルールを追加する場所を指定します。You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

ステップ 4 [インターフェイスオブジェクト（Interface Objects）] で、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）] は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）を識別します。つまり、元のパケットで表されているパケット アドレスです。

元のパケットと変換後のパケットを比較する例として、以下の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストは変換します。



- [元の送信元（Original Source）]：変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先（Original Destination）]：（オプション）。宛先のアドレスを含むネットワーク オブジェクト、またはネットワークグループ。空白のままにすると、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [インターフェイス オブジェクト（Interface Object）] を選択し、送信元インターフェイスの元の宛先（[すべて（Any）]は選択不可）をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：元の送信元と同じオブジェクトまたはグループ。オプションで、内容がまったく同じ別のオブジェクトを選択できます。
- [変換済み宛先（Translated Destination）]：（オプション）。変換後のパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループを指定します。[変換前の宛先（Original Destination）] にオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT（つまり、変換なし）を設定します。

ステップ 7 （任意）サービス変換の送信元または宛先サービスのポートを特定します。

ポート変換を適用するスタティック NAT を設定している場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 の間での変換が可能です。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）]、[変換済み送信元ポート（Translated Source Port）]：送信元アドレスのポート変換を定義します。
- **[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]**：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細（Advanced）] で、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。
- [宛先インターフェイスでARPをプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [宛先インターフェイスのルートルックアップの実行（Perform Route Lookup for Destination Interface）]：元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

- [単一方向（Unidirectional）]：このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。

ステップ 9 [保存（Save）] をクリックしてルールを追加します。

ステップ 10 NAT ページで [保存（Save）] をクリックして変更を保存します。

Firewall Threat Defense の NAT ルールのプロパティ

ネットワークアドレス変換（NAT）ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常は、NAT ルールを使用してプライベートアドレスをパブリックにルーティングできるアドレスに変換します。1 つのアドレスを別のアドレスに変換するか、ポートアドレス変換（PAT）を使用して多数のアドレスを 1 つまたは少数のアドレスに変換し、ポート番号を使用して送信元アドレスを識別することができます。

NAT ルールの基本的なプロパティは、次のとおりです。プロパティは、指示されていることを除き、自動 NAT ルールと手動 NAT ルールで同じです。

NAT タイプ（NAT Type）

[手動 NAT ルール（Manual NAT Rule）] または [自動 NAT ルール（Auto NAT Rule）] のどちらを設定するのかを指定します。自動 NAT は、送信元アドレスのみを変換します。宛先アドレスに基づいた他の変換方法作成することはできません。自動 NAT のほうが設定するのが簡単なので、手動 NAT の機能を追加する必要がない限り、自動 NAT を使用してください。この 2 つの間の違いについて詳しくは、自動 NAT および 手動 NAT （906 ページ）を参照してください。

[タイプ（Type）]

変換ルールを [ダイナミック（Dynamic）] または [スタティック（Static）] で指定します。ダイナミック変換はマッピング アドレスをアドレスのプール（PAT 実装時にはアドレスとポートの組み合わせ）から自動的に選択します。マッピング アドレス/ポートを明確に定義する必要がある場合は、スタティック変換を使用します。

有効化（Enable）（手動 NAT のみ）

ルールをアクティブにするかどうかを指定します。ルールページで右クリック メニューを使用することにより、後からルールをアクティブ化または非アクティブ化できます。自動 NAT ルールを無効化することはできません。

挿入（Insert）（手動 NAT のみ）

ルールを追加する場所を指定します。You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

説明（任意、手動 NAT のみ）。

ルールの目的の説明。

以降のトピックで、NAT ルール プロパティのタブについて説明します。

インターフェイス オブジェクト：NAT のプロパティ

インターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）は、NAT ルールが適用されるインターフェイスを定義します。ルーテッド モードでは、送信元と宛先の両方にデフォルトの「任意（Any）」を使用すれば、割り当てられたすべてのデバイスのすべてのインターフェイスに適用できます。ただし、通常は特定の送信元と宛先インターフェイスを選択します。

注記

- 「任意」のインターフェイスの概念は、ブリッジグループ メンバー インターフェイスには適用されません。「任意の」インターフェイスを指定する場合、すべてのブリッジ グループ メンバー インターフェイスは除外されます。このため、NAT をブリッジ グループ メンバーに適用するには、メンバーインターフェイスを指定する必要があります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできず、メンバーインターフェイスにのみ NAT を設定できます。

  インターフェイス オブジェクトを選択すると、NAT ルールはデバイスのインターフェイスが選択されたすべてのオブジェクトに含まれているときにのみ設定されます。たとえば、送信元と宛先の両方のセキュリティ ゾーンを選択すると、特定のデバイスに対して 1 つ以上のインターフェイスが両方のゾーンに含まれている必要があります。

- 特定のデバイスにインターフェイス オブジェクト内の複数のインターフェイスが存在する場合は、インターフェイスごとに同一のルールが作成されます。これは、宛先変換を含む静的 NAT ルールで問題になる可能性があります。NAT ルールは最初に一致したルールに基づいて適用されるため、オブジェクトに設定された最初のインターフェイス用に作成されたルールのみがトラフィックと一致します。宛先変換を使用して静的 NAT を設定する場合は、NAT ポリシーに割り当てられたデバイスごとに最大 1 つのインターフェイスを含むインターフェイス オブジェクトを使用して、目的の結果が得られるようにします。

送信元インターフェイス オブジェクト、宛先インターフェイス オブジェクト

（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）。[送信元（Source）]は、デバイスへの着信トラフィックが経由する実際のインターフェイスを含むオブジェクトです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

自動 NAT の変換プロパティ

[変換（Translation）] オプションを使用して、送信元アドレスと変換済みマッピングアドレスを定義します。次のプロパティは、自動 NAT にのみ適用されます。

[元の送信元（Original Source）]（常に必須）。

変換しているアドレスを含むネットワーク オブジェクト。グループではなくネットワーク オブジェクトにする必要があり、ホスト、範囲、またはサブネットを含めることができます。

システム定義の any-ipv4 または any-ipv6 オブジェクトには自動 NAT ルールを作成できません。

[変換済み送信元（Translated Source）]（通常は必須）。

変換先のマッピング アドレス。ここでの選択は定義する変換ルールのタイプに依存します。

- [ダイナミック NAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。これはネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかです。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、[宛先インターフェイスIP（Destination Interface IP）] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] で [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
  - PAT プールを使用するには、[変換された送信元（Translated Source）] を空のままにしておきます。[PATプール（PAT Pool）] で PAT プールオブジェクトを選択します。
- [スタティック NAT（Static NAT）]：次のいずれかを実行します。
  - アドレスの設定グループを使用するには、[アドレス（Address）]およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含めることができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）宛先インターフェイスのアドレスを使用するには、[宛先インターフェイスIP（Destination Interface IP）] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスのIPv6アドレスを使用するには、

[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。

- [アイデンティティ NAT（Identity NAT）]：送信元と同じオブジェクト。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。

[変換前のポート（Original Port）]、[変換後のポート（Translated Port）]（スタティック NAT のみ）

TCP または UDP ポートを変換する必要がある場合、[元のポート（Original Port）] でプロトコルを選択し、元のポートおよび変換済みポートの番号を入力します。たとえば、必要に応じて TCP/80 を 8080 に変換できます。アイデンティティ NAT にこれらのオプションを設定しないでください。

手動 NAT の変換プロパティ

[変換（Translation）] オプションを使用して、送信元アドレスと変換済みマッピング アドレスを定義します。次のプロパティは手動 NAT にのみ適用されます。特に説明がない限り、すべてオプションです。

[元の送信元（Original Source）]（常に必須）。

変換するアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることが可能で、ホスト、範囲、またはサブネットを含めることができます。変換前のすべての送信元トラフィックを変換する場合、ルール内に [任意（Any）] を指定できます。

[変換済み送信元（Translated Source）]（通常は必須）。

変換先のマッピング アドレス。ここでの選択は定義する変換ルールのタイプに依存します。

- [ダイナミック NAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。これはネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかです。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、[宛先インターフェイス IP（Destination Interface IP）] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] で [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。

- 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
- PAT プールを使用するには、[変換された送信元（Translated Source）] を空のままにしておきます。[PATプール（PAT Pool）] で PAT プールオブジェクトを選択します。

- [スタティック NAT（Static NAT）]：次のいずれかを実行します。
  - アドレスの設定グループを使用するには、[アドレス（Address）]およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループはホスト、範囲、またはサブネットを含むことができます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）宛先インターフェイスのアドレスを使用するには、[宛先インターフェイスIP（Destination Interface IP）] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスのIPv6アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- [アイデンティティ NAT（Identity NAT）]：送信元と同じオブジェクト。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。

[元の宛先（Original Destination）]

宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。空白のままにすると、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティNATを使用できます。

[送信元インターフェイスIP（Source Interface IP）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

[変換済みの宛先（Translated Destination）]

変換後のパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループを指定します。[変換前の宛先（Original Destination）]にオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT（つまり、変換なし）を設定します。

変換後の宛先として完全修飾ドメイン名を指定するネットワークオブジェクトを使用できます。詳細については、FQDN 宛先のガイドライン （917 ページ）を参照してください。

[変換前の送信元ポート（Original Source Port）]、[変換後の送信元ポート（Translated Source Port）]、[変換前の宛先ポート（Original Destination Port）]、[変換後の宛先ポート（Translated Destination Port）]

変換前のパケットと変換後のパケットに対する送信元サービスと宛先サービスを定義するポート オブジェクト。ポートを変換する、もしくは、ポートを変換せずにルールをサービスに提供できるように同じオブジェクトを選択します。サービスを設定するときは、次のルールに注意してください。

- （ダイナミック NAT または PAT）。[変換前の送信元ポート（Original Source Port）] および [変換後の送信元ポート（Translated Source Port）] では変換できません。変換は宛先ポートでのみ実行できます。
- NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

PAT プールの NAT プロパティ

ダイナミック NAT を設定する際に、[PAT プール（PAT Pool）] タブのプロパティを使用して、ポート アドレス変換に使用するアドレスのプールを定義できます。

PAT プールの有効化（Enable PAT Pool）

PAT に使用するアドレスのプールを設定する場合は、このオプションを選択します。

PAT

PAT プールに使用するアドレスとして、以下のいずれかを指定します。

- [アドレス（Address）] : PAT プール アドレスを定義するオブジェクト。アドレスの範囲を含むネットワーク オブジェクト、またはホスト、範囲、あるいはその両方を含むネットワーク オブジェクト グループのいずれかです。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。
- [宛先インターフェイスIP（Destination Interface IP）] : PAT アドレスとして使用する宛先インターフェイスを指定します。このオプションを使用する場合、特定の [宛先インターフェイス オブジェクト（Destination Interface Object）] を選択する必要があります。[すべて（Any）] を宛先インターフェイスとして使用することはできません。これは、インターフェイス PAT を実装するもう 1 つの方法です。

ラウンドロビン（Round Robin）

アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレ

スが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。

拡張 PAT テーブル（Extended PAT Table）

拡張 PAT を使用します。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。インターフェイス PAT やインターフェイス PAT フォールバックとこのオプションを併用することはできません。

フラット ポート範囲（Flat Port Range）、予約済みポートを含める（Include Reserved Ports）

TCP/UDP ポートを割り当てる際に、ポート範囲（1024 ～ 65535）を単一のフラットな範囲として使用します。（6.7 より前）変換のマッピングポート番号を選択すると、PAT は実際の送信元ポート番号を使用できます（使用可能な場合）。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含む（Include Reserved Ports）] オプションも選択します。バージョン 6.7 以降を実行している Firewall Threat Defense デバイスの場合、オプションを選択するかどうかにかかわらず、フラットなポート範囲が常に設定されます。これらのシステムには、**[予約済みポートを含む（Include Reserved Ports）]** オプションを選択しても、その設定が適用されます。

ブロック割り当て

ポートのブロック割り当てを有効にする場合。キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、元のブロックにすべてのポートに対するアクティブな接続がホストにある場合は、追加のブロックが割り当てられます。ポートのブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当てはラウンド ロビンと互換性がありますが、拡張 PAT またはフラットなポート範囲のオプションと一緒に使用することはできません。また、インターフェイス PAT フォールバックも使用できません。

詳細 NAT プロパティ

NAT を設定する場合、**[詳細（Advanced）]** オプションで、専門サービスを提供するプロパティを設定できます。これらのプロパティはすべてオプションです。サービスが必要な場合にのみ設定します。

このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6

AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへのDNS応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、NAT を使用したDNS クエリと応答の書き換え（1033 ページ）を参照してください。このオプションは、スタティック NAT ルールでポート変換を行っているときは利用できません。

[インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT (Destination Interface)）]（ダイナミック NAT のみ）

他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段として宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）を指定します。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。変換されたアドレスとしてすでにインターフェイス PAT を設定している場合、このオプションを選択できません。PAT プールを構成する場合も、このオプションを選択することはできません。

IPv6

インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

[ネット間マッピング（Net to Net Mapping）]（スタティック NAT のみ）

NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを使用する必要があります。

宛先インターフェイスでプロキシ ARP なし（スタティック NAT のみ）

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP を無効にすることもできます。その場合、アップストリームルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

[宛先インターフェイスのルート ルックアップの実行（Perform Route Lookup for Destination Interface）]（静的アイデンティティ NAT のみ、ルーテッド モードのみ）

元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

[単方向（Unidirectional）]（手動 NAT のみ、スタティック NAT のみ）

このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。

IPv6 ネットワークの変換

トラフィックが IPv6 のみのネットワークと IPv4 のみのネットワークの間を通過するようにする必要がある場合、NAT を使用してアドレス タイプを変換する必要があります。2 つの IPv6 ネットワークの場合でも、外部ネットワークに対して内部アドレスを非表示にする必要がある場合があります。

IPv6 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46—IPv6 パケットから IPv4 パケットへの変換とその逆変換2 つのポリシー、IPv6 から IPv4 への変換、および IPv4 から IPv6 への変換を定義する必要があります。これは、1 つの 手動 NAT ルールで実行できますが、DNS サーバが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに 手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの 自動 NAT ルールを作成することがより適切なソリューションです。

（注） NAT46 はスタティック マッピングのみをサポートします。

- NAT66—IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

（注） NAT64 および NAT 46 は、標準のルーテッド インターフェイスのみで使用できます。NAT66 は、ルーテッドおよびブリッジ グループ メンバー インターフェイスの両方で使用できます。

NAT64/46：IPv6 から IPv4 へのアドレス変換

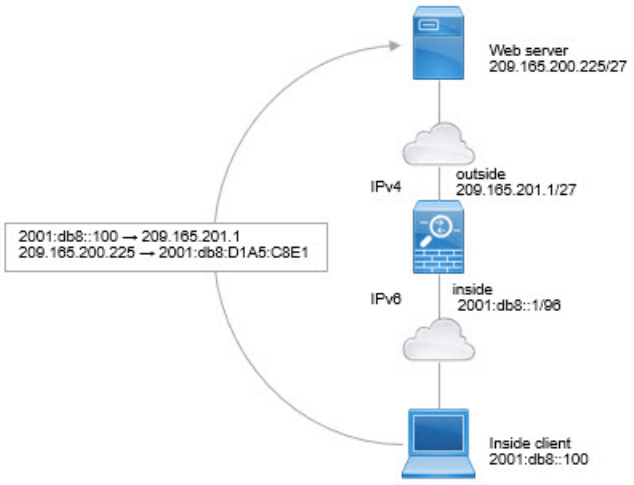
トラフィックが IPv6 ネットワークから IPv4 専用のネットワークへ通過する際には IPv6 アドレスを IPv4 に変換し、リターン トラフィックに対しては IPv4 から IPv6 に変換する必要があります。IPv6 アドレスをバインドする IPv4 アドレス プール（IPv4 内）と IPv4 アドレスをバインドする IPv6 アドレス プール（IPv6 内）という 2 つのアドレス プールを定義する必要があります。

- NAT64 ルール用の IPv4 アドレス プールは、一般に小さく、通常は IPv6 クライアント アドレスと 1 対 1 でマッピングするために十分なアドレスを持っていません。ダイナミック PAT は、ダイナミック NAT やスタティック NAT と比較して、多数の IPv6 クライアント アドレスに容易に適合します。
- NAT 46 ルール用の IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数以上にすることができます。よって、各 IPv4 アドレスを異なる IPv6 アドレスにマッピングできます。NAT46 はスタティック マッピングのみをサポートするため、ダイナミック PAT は使用できません。

送信元 IPv6 ネットワーク用と、宛先 IPv4 ネットワーク用の 2 つのポリシーを定義する必要があります。これは、1 つの 手動 NAT ルールで実行できますが、DNS サーバが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに 手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの 自動 NAT ルールを作成することがより適切なソリューションです。

NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット

次に、内部 IPv6 専用ネットワークがある場合に、インターネットに送信されるトラフィックを IPv4 に変換する簡単な例を示します。この例では DNS 変換が不要なため、1 つの 手動 NAT ルールで NAT64 と NAT46 の両方の変換を実行できる、と想定しています。



この例では、外部インターフェイスの IP アドレスとダイナミック PAT インターフェイスを使用して、内部 IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは 2001:db8::/96 ネットワークのアドレスに静的に変換され、内部ネットワークでの送信が許可されます。

手順

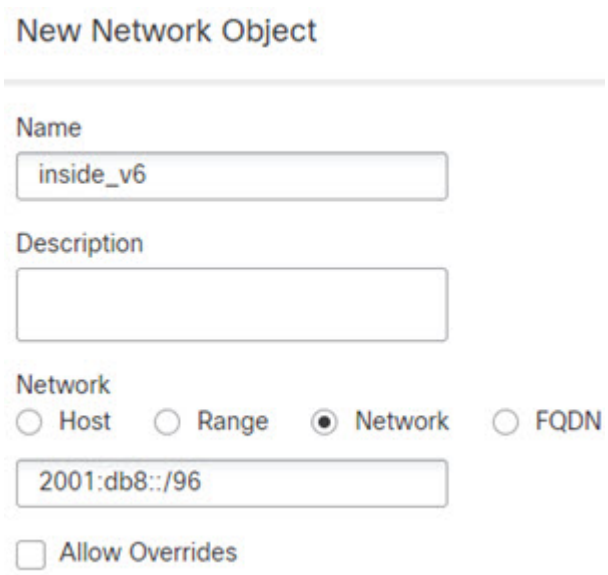
ステップ 1 内部 IPv6 ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前（inside_v6 など）を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。



d) [保存（Save）] をクリックします。

ステップ 2 IPv6 ネットワークを IPv4 に変換して再び戻すための手動 NAT ルールを作成します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

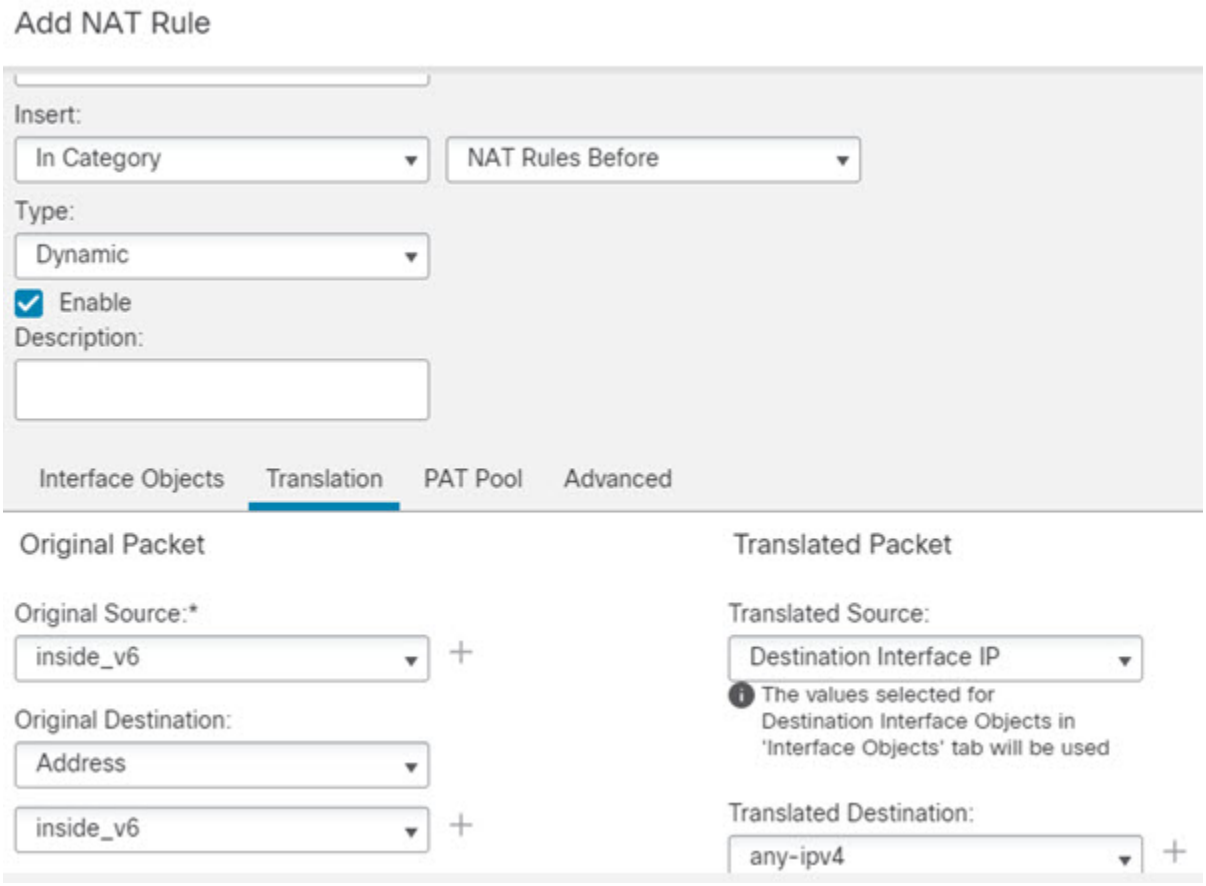
d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- [変換済みの送信元（Translated Source）] = 宛先インターフェイス IP（Destination Interface IP）。
- [元の宛先（Original Destination）]：inside_v6 ネットワーク オブジェクト。

• [変換済みの宛先（Translated Destination）] = any-ipv4 ネットワーク オブジェクト。



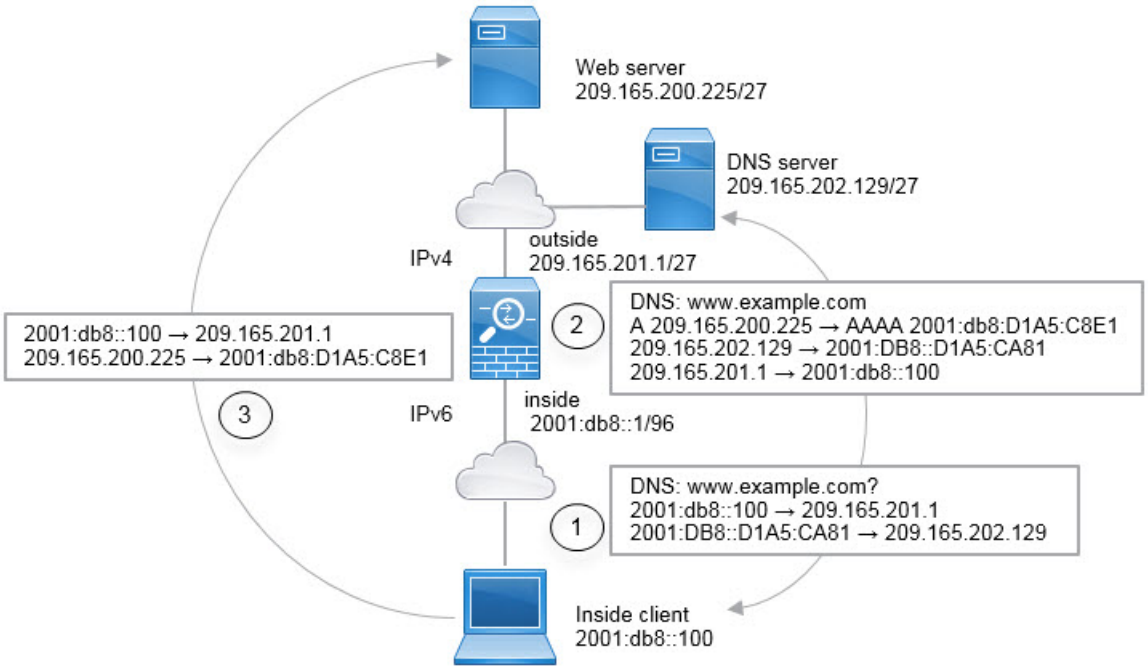
f) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。逆に、内部インターフェイスに入る外部ネットワークの IPv4 アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。

g) [NATルール（NAT rule）] ページで [保存（Save）] をクリックします。

NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク

内部の IPv6 専用ネットワークが存在するものの、内部ユーザが必要とする一部の IPv4 専用サービスがインターネット外部に存在する例を次に示します。



この例では、外部インターフェイスの IP アドレスとダイナミック PAT インターフェイスを使用して、内部 IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは 2001:db8::/96 ネットワークのアドレスに静的に変換され、内部ネットワークでの送信が許可されます。NAT46 ルールでの DNS の書き換えを有効にし、外部 DNS サーバからの応答を A（IPv4）から AAAA（IPv6）レコードに変換したり、アドレスを IPv4 から IPv6 に変換したりできます。

内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとする Web 要求の通常のシーケンスを次に示します。

1. クライアントのコンピュータは、2001:DB8::D1A5:CA81 で DNS サーバに DNS リクエストを送信します。NAT ルールは、DNS リクエストで送信元と宛先に以下の変換を実行します。
   - 2001:DB8::100 から 209.165.201.1 上の固有のポート（NAT64 インターフェイス PAT ルール）
   - 2001:DB8::D1A5:CA81 から 209.165.202.129（NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 と同じです）
2. DNS サーバが応答で、www.example.com が 209.165.200.225 であるという A レコードを示します。DNS の書き換えが有効になっている NAT46 ルールは、A レコードを IPv6 版の AAAA レコードに変換し、AAAA レコードの 209.165.200.225 を 2001:db8:D1A5:C8E1 に変換します。さらに、DNS 応答の発信元アドレスと宛先アドレスは変換されません。
   - 209.165.202.129 から 2001:DB8::D1A5:CA81
   - 209.165.201.1 から 2001:db8::100

3. これで、IPv6 クライアントには Web サーバの IP アドレスが含まれるようになり、2001:db8:D1A5:C8E1 で www.example.com への HTTP リクエストを行います（D1A5:C8E1 は IPv6 の 209.165.200.225 と同じです）。HTTP リクエストの発信元アドレスと送信先アドレスは次のように変換されます。
   - 2001:DB8::100 から 209.156.101.54 上の固有のポート（NAT64 インターフェイス PAT ルール）
   - 2001:db8:D1A5:C8E1 から 209.165.200.225（NAT46 ルール）

次の手順では、この例の指定方法について説明します。

始める前に

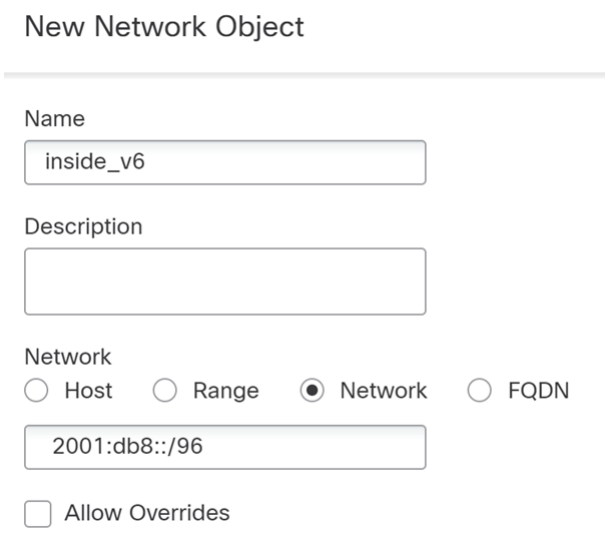
デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

ステップ 1 内部 IPv6 ネットワークと外部 IPv4 ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。
b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。
c) 内部 IPv6 ネットワークを定義します。

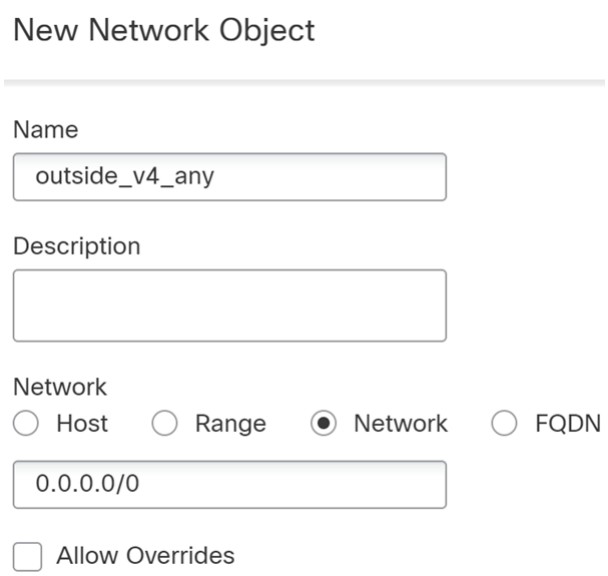
   ネットワーク オブジェクトに名前（inside_v6 など）を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、外部 IPv4 ネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、outside_v4_any）を付けて、ネットワークアドレス 0.0.0.0/0 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

ステップ 3 外部 IPv4 ネットワークのスタティック NAT46 ルールを設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

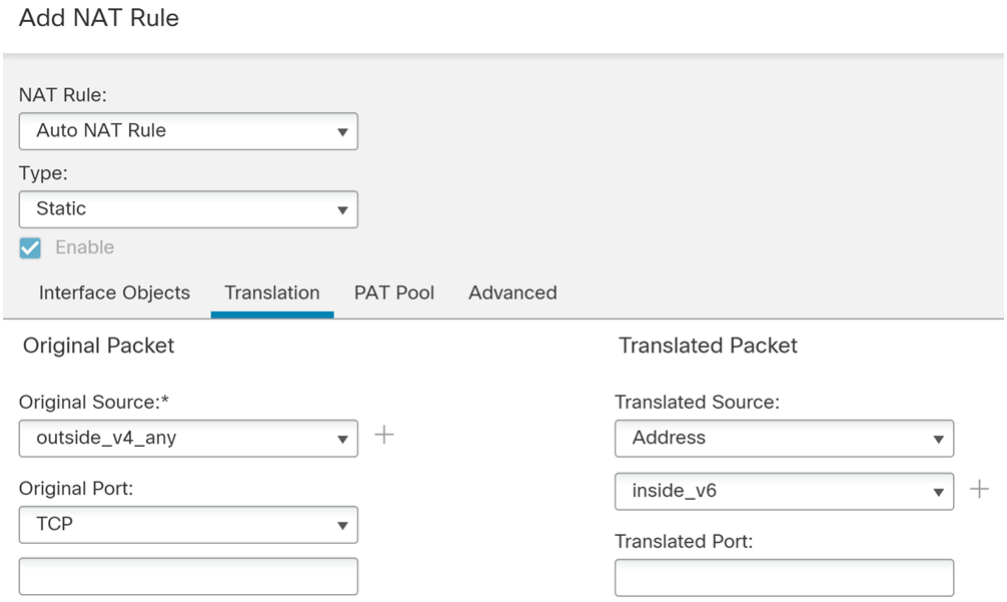
c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

d) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = outside_v4_any ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = inside_v6 ネットワークオブジェクト。

e) [詳細（Advanced）] で、[このルールと一致するDNS応答を変換（Translate DNS replies that match this rule）] を選択します。



f) [OK] をクリックします。

このルールを使用すると、内部インターフェイスに入る外部ネットワークのIPv4アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。さらに、DNS 応答は、A（IPv4）から AAAA（IPv6）レコードに変換され、アドレスは IPv4 から IPv6 に変換されます。

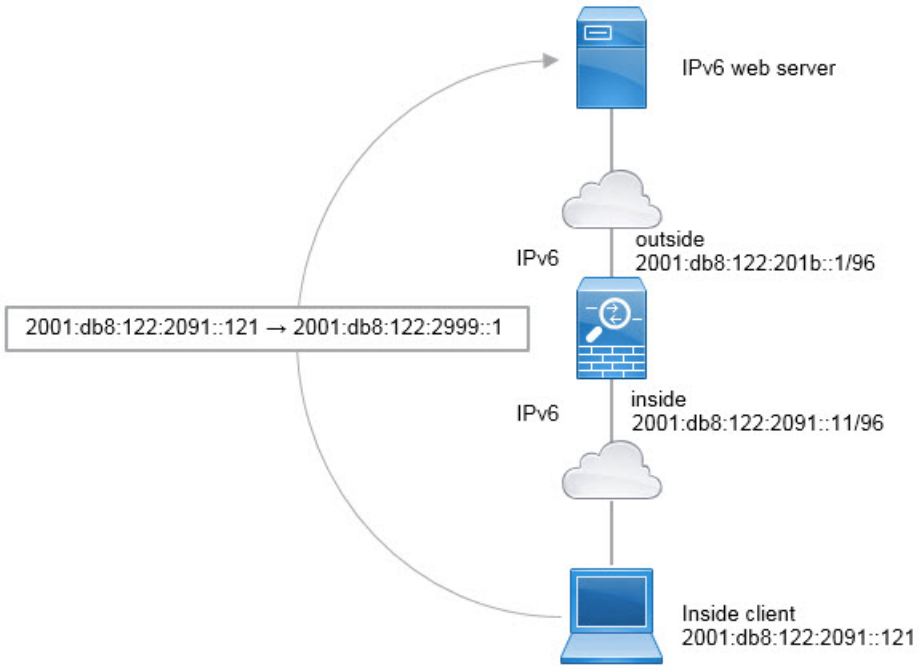
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークへと通過する場合、IPv6 アドレスを外部ネットワーク上の別の IPv6 アドレスに変換できます。スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

異なるアドレス タイプの間で変換されていないため、NAT66 変換用の 1 つのルールが必要です。これらのルールは、自動 NATを使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、手動 NAT のみを使用してスタティック NAT ルールを単方向にできます。

NAT66 の例：ネットワーク間のスタティック変換

自動NATを使用して、IPv6アドレスプール間のスタティック変換を設定できます。次の例は、2001:db8:122:2091::/96 ネットワークの内部アドレスを、2001:db8:122:2999::/96 ネットワークの外部アドレスへ変換する方法について説明しています。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

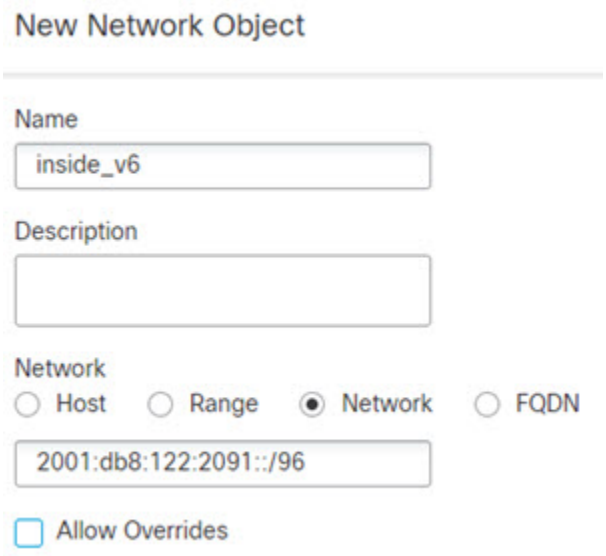
ステップ 1 内部 IPv6 ネットワークと外部 IPv6 NAT ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 内部 IPv6 ネットワークを定義します。

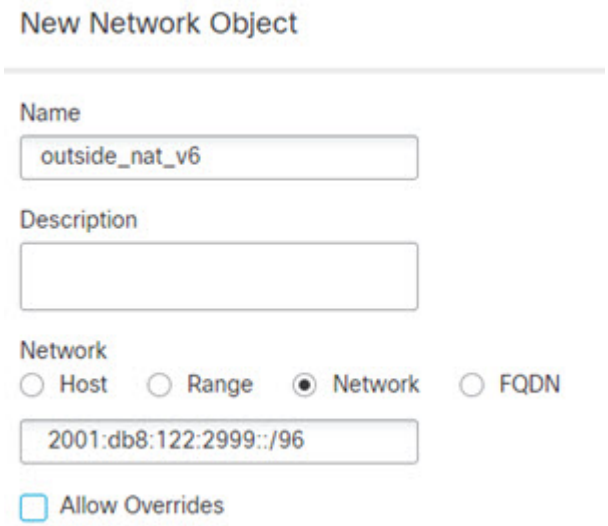
ネットワーク オブジェクトに名前（たとえば、inside_v6）を付けて、ネットワーク アドレス 2001:db8:122:2091::/96 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、外部 IPv6 NAT ネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、outside_nat_v6）を付けて、ネットワーク アドレス 2001:db8:122:2999::/96 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

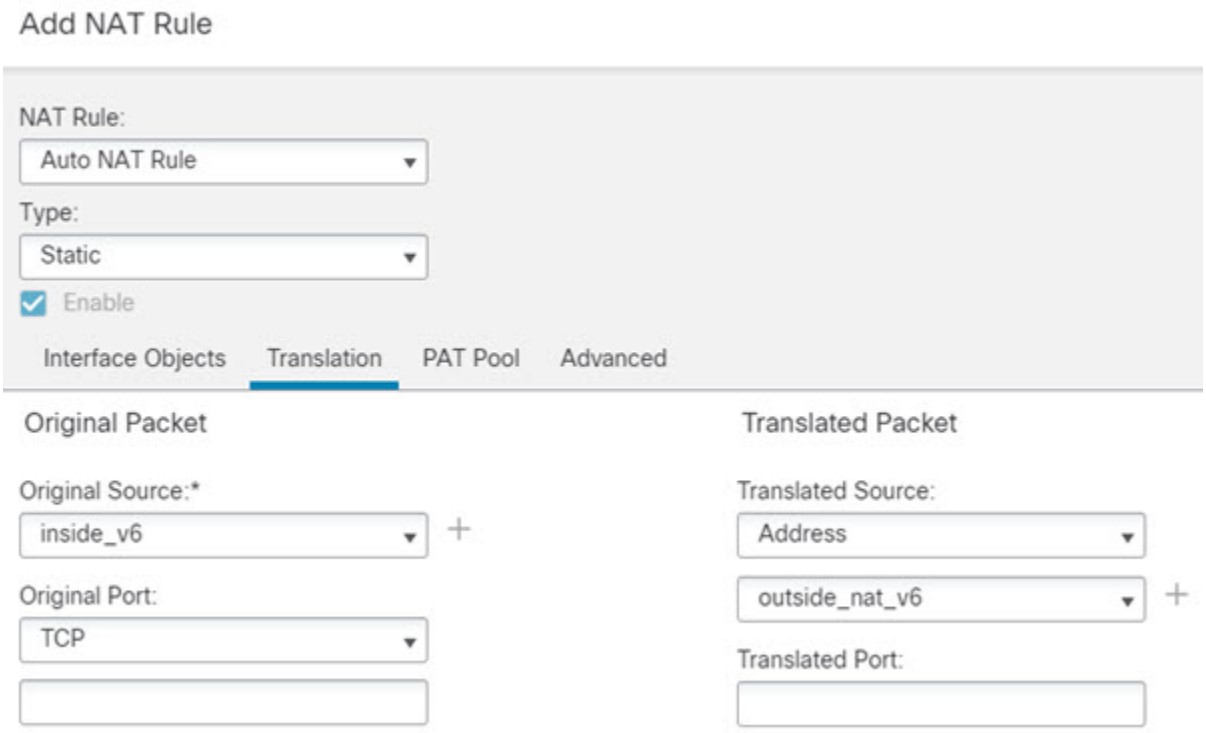
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）] > [アドレス（Address）]** = outside_nat_v6 ネットワークオブジェクト。



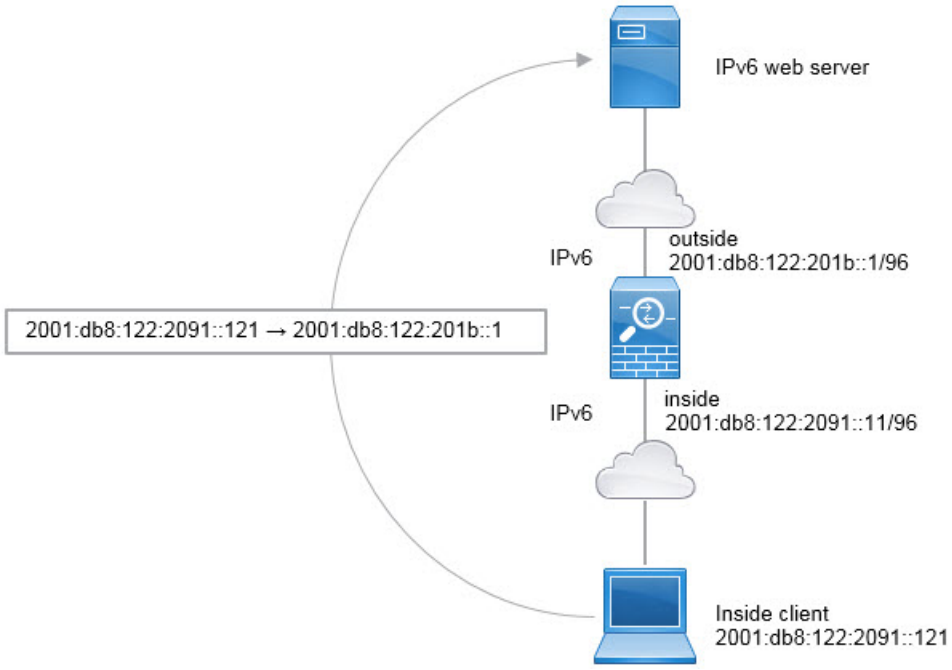
f) [OK] をクリックします。

このルールを使用すると、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに入るすべてのトラフィックは、2001:db8:122:2999::/96 ネットワークのアドレスへのスタティック NAT66 変換を受けます。

NAT66 の例：シンプル IPv6 インターフェイス PAT

NAT66 を実装する簡単な方法は、内部アドレスを外部インターフェイス IPv6 アドレスのさまざまなポートに動的に割り当てることです。

NAT66 に対してインターフェイス PAT ルールを設定する場合、そのインターフェイスで設定されたすべてのグローバル アドレスは PAT マッピングに使用されます。インターフェイスのリンクローカル アドレスまたはサイトローカル アドレスは PAT には使用されません。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

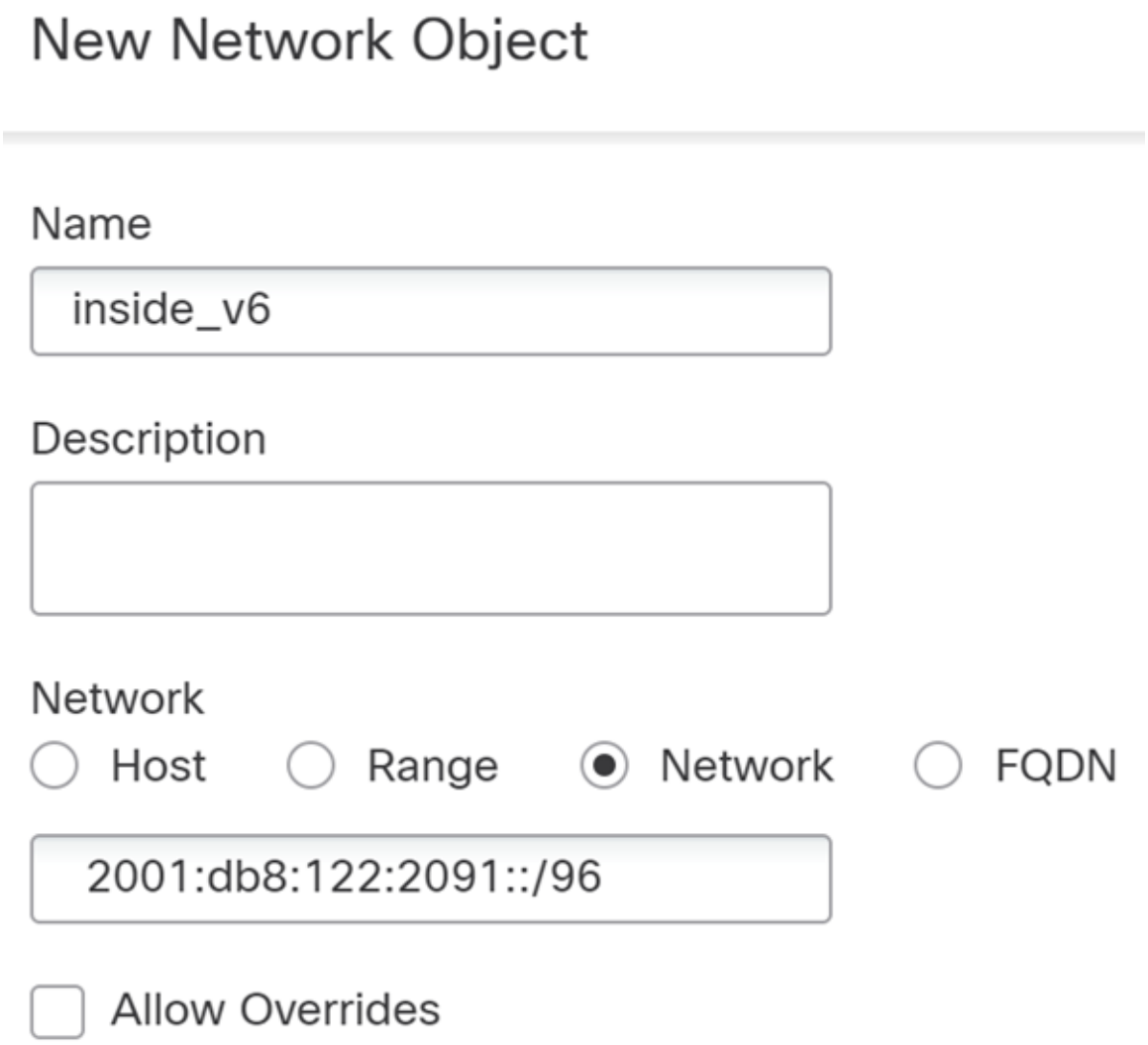
ステップ 1 内部 IPv6 ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、inside_v6）を付けて、ネットワーク アドレス 2001:db8:122:2091::/96 を入力します。



d) [保存（Save）] をクリックします。

ステップ 2 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

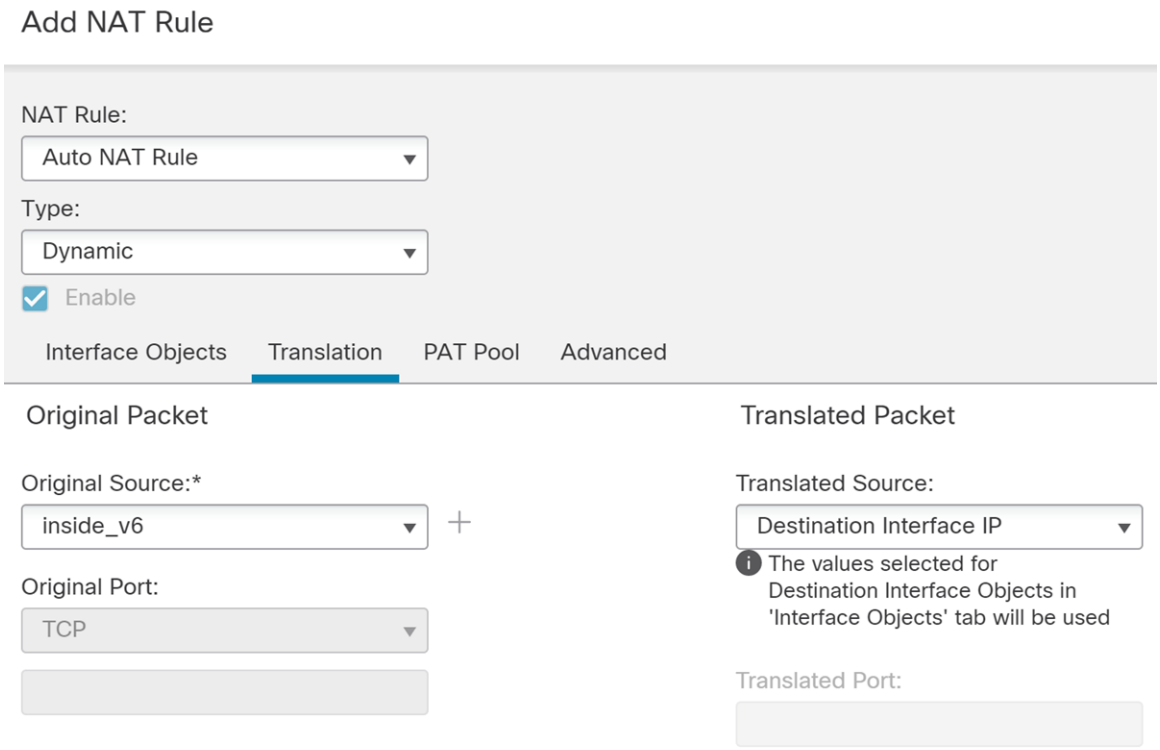
- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。

- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- [変換済みの送信元（Translated Source）] = 宛先インターフェイス IP（Destination Interface IP）。

f) [詳細（Advanced）] で、[IPv6] を選択します。これは、宛先インターフェイスの IPv6 が使用されることを意味します。



g) [OK] をクリックします。

このルールでは、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスへのトラフィックは、外部インターフェイス用に設定された IPv6 グローバル アドレスのいずれかへの NAT66 PAT 変換を取得します。

NAT のモニタリング

NAT 接続をモニタし、トラブルシューティングを行うには、デバイスの CLI にログインして、次のコマンドを使用します。

- **show nat** NAT ルールとルールごとのヒット数を表示します。NAT のその他の情報を表示する追加キーワードがあります。
- **show xlate** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換を消去することで、クライアントの次回の接続時に、システムは新しいルールに基づいてクライアントの新しい変換を作成します。

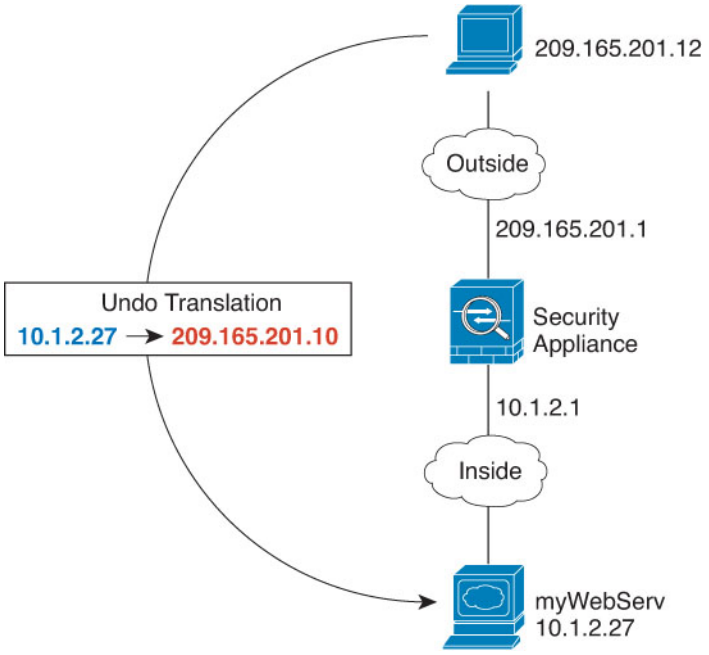
NAT の例

ここでは、Threat Defenceデバイス上で NAT を設定する例を紹介します。

内部 Web サーバへのアクセスの提供（スタティック自動 NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です

図 *281* : 内部 *Web* サーバーのスタティック *NAT*



始める前に

Webサーバーを保護するデバイスのインターフェイスが含まれているインターフェイ オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

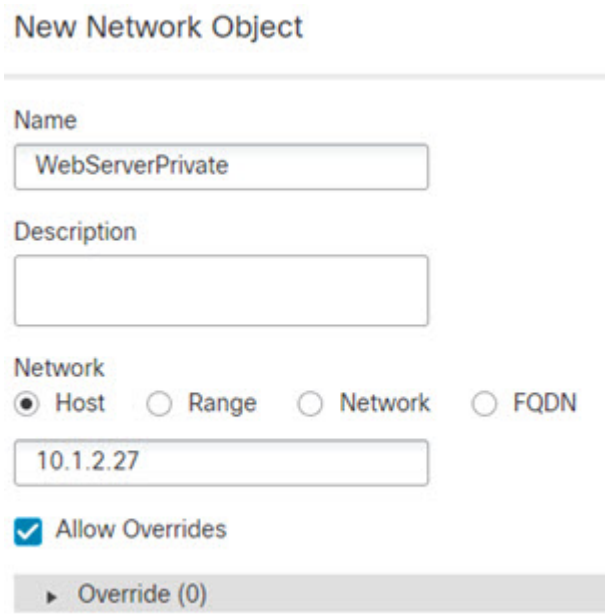
ステップ 1 サーバのプライベートおよびパブリック ホスト アドレスを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) Web サーバーのプライベート アドレスを定義します。

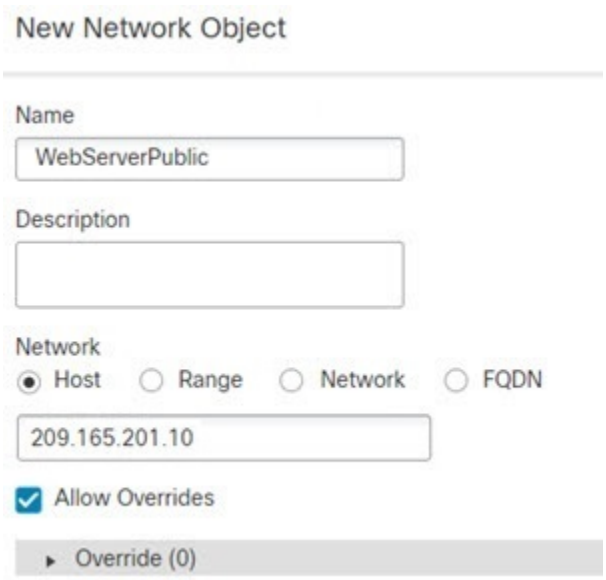
ネットワーク オブジェクトに名前（たとえば、WebServerPrivate）を付けて、実際のホスト IP アドレス 10.1.2.27 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、パブリックアドレスを定義します。

ネットワーク オブジェクトに名前（たとえば、WebServerPublic）を付けて、ホスト アドレス 209.165.201.10 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 オブジェクトのスタティック NAT を設定します。

a) **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

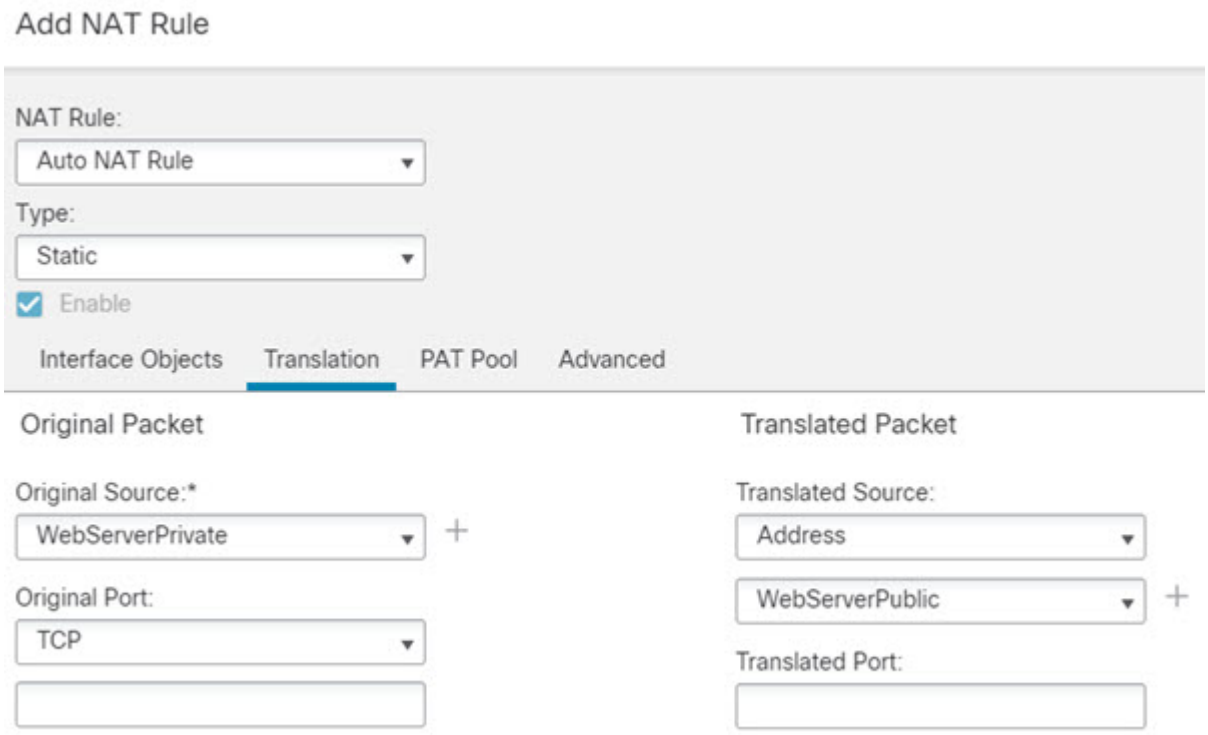
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = WebServerPrivate ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）] > [アドレス（Address）]** = WebServerPublic ネットワークオブジェクト。



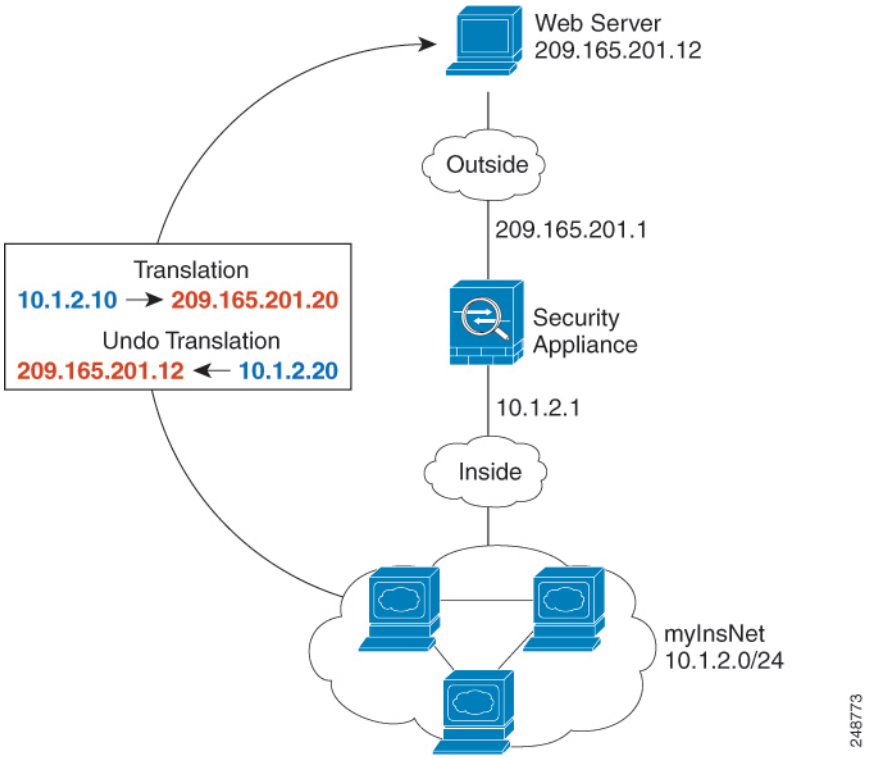
f) [保存（Save）] をクリックします。

ステップ 3 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

内部ホストのダイナミック自動 NAT および外部 Web サーバーのスタティック NAT

次の例では、プライベート ネットワーク上の内部ユーザーが外部にアクセスする場合、このユーザーにダイナミック NAT を設定します。また、内部ユーザーが外部 Web サーバーに接続する場合、この Web サーバーのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます

図 *282 :* 内部のダイナミック *NAT*、外部 *Web* サーバーのスタティック *NAT*



始める前に

Web サーバーを保護するデバイスのインターフェイスが含まれているインターフェイ オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

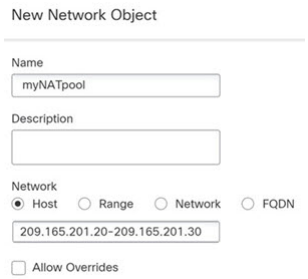
ステップ 1 内部アドレスを変換するダイナミック NAT プールのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) ダイナミック NAT プールを定義します。

ネットワーク オブジェクトに名前を付け（myNATpool など）、ネットワーク範囲 209.165.201.20 ～ 209.165.201.30 を入力します。

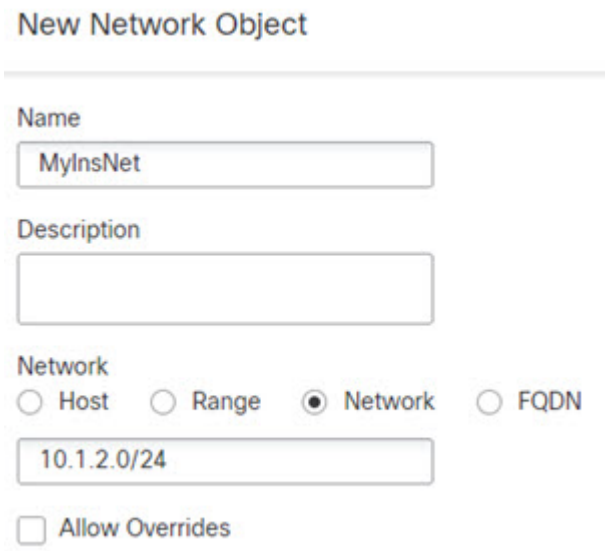


d) [保存（Save）] をクリックします。

ステップ 2 内部ネットワークのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（MyInsNet など）、ネットワーク アドレス 10.1.2.0/24 を入力します。

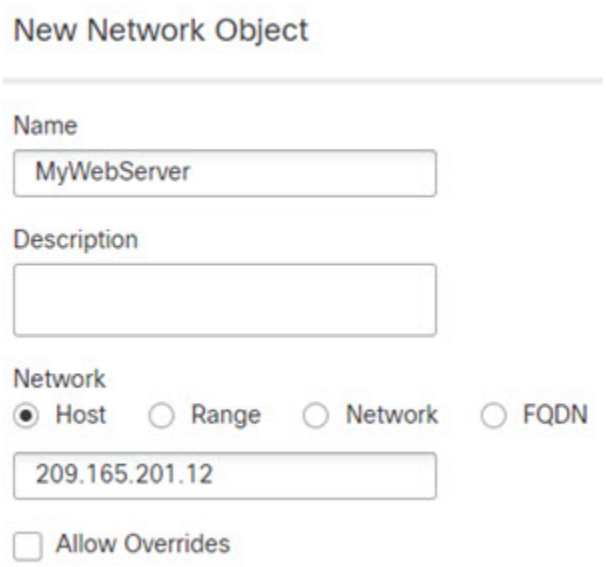


c) [保存（Save）] をクリックします。

ステップ 3 外部 Web サーバーのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（MyWebServer など）、ホスト アドレス 209.165.201.12 を入力します。

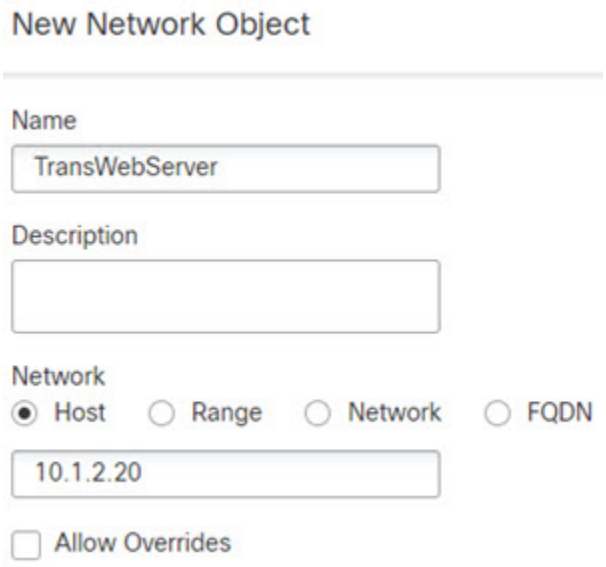


c) [保存（Save）] をクリックします。

ステップ 4 変換済み Web サーバー アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（TransWebServer など）、ホスト アドレス 10.1.2.20 を入力します。



c) [保存（Save）] をクリックします。

ステップ 5 ダイナミック NAT プール オブジェクトを使用して内部ネットワークのダイナミック NAT を設定します。

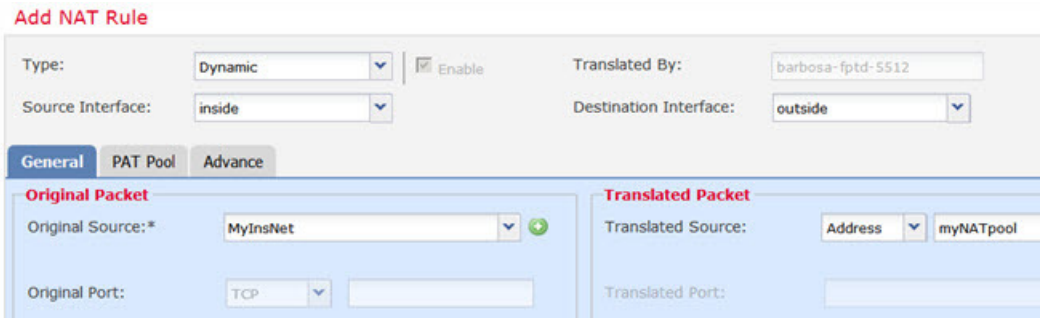
a) **[デバイス（Device）]** > **[デバイス管理（Device）]** を選択して、ルールを定義する Threat Defense デバイスを編集します。[NAT] を選択します。

複数のドメインを使用している場合、デバイスを含む同じリーフ ドメインに位置していることを確認します。

b) **[NAT ルールの追加（Add NAT Rule）]** > **[自動 NAT の追加（Add Auto NAT）]** をクリックします。

c) 次のプロパティを設定します。

- [種類（Type）]：Dynamic。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：outside。
- [元の発信元（Original Source）] = myInsNet ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = myNATpool ネットワークオブジェクト。



d) [保存（Save）] をクリックします。

ステップ 6 ダイナミック NAT プール オブジェクトを使用して内部ネットワークのダイナミック NAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

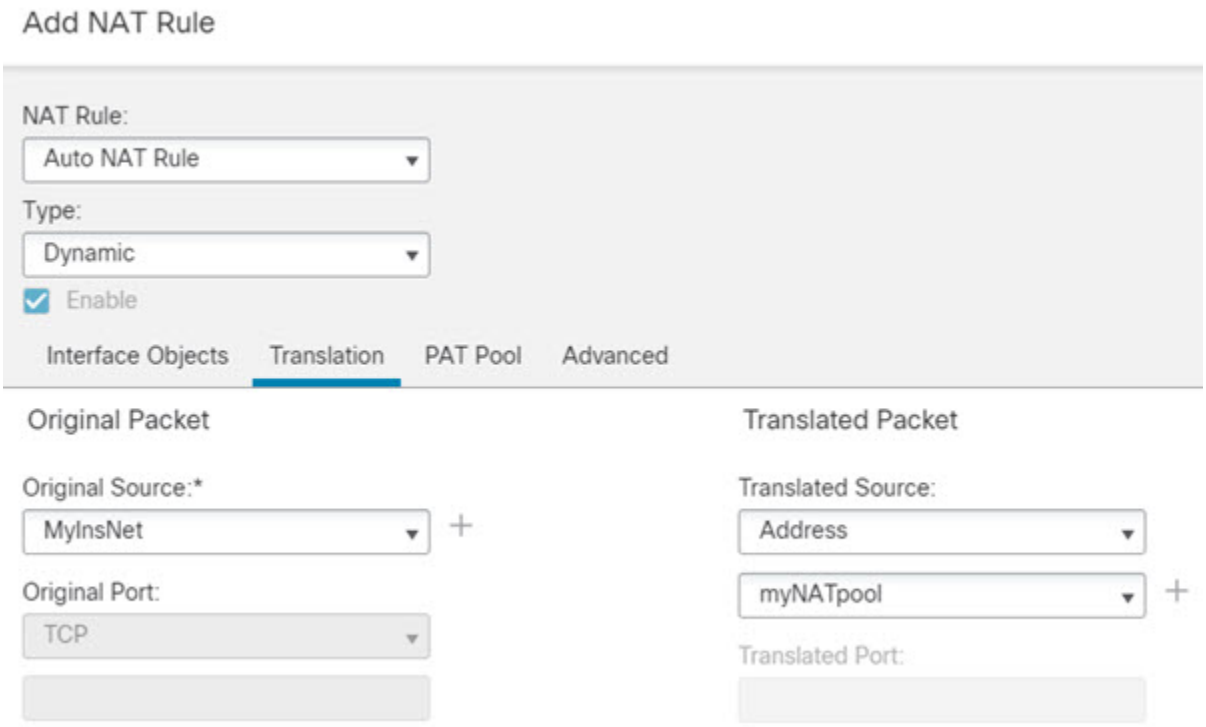
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = myInsNet ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = myNATpool ネットワークオブジェクト。



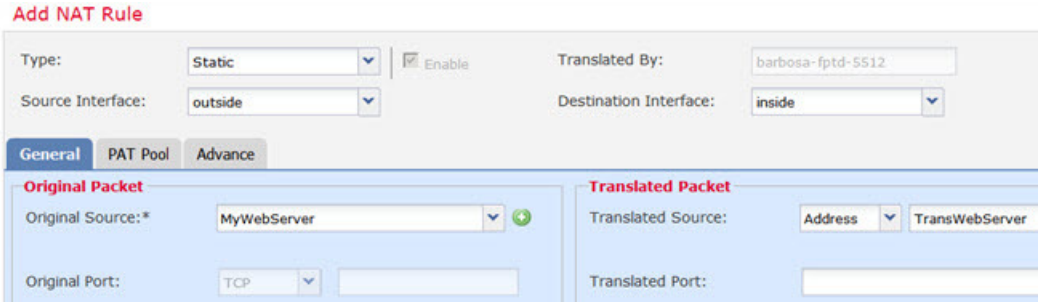
f) [保存（Save）] をクリックします。

ステップ 7 Web サーバーのスタティック NAT を設定します。

a) **[NAT ルールの追加（Add NAT Rule）]** > **[自動 NAT の追加（Add Auto NAT）]** をクリックします。

b) 次のプロパティを設定します。

- [種類（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：outside。
- [宛先インターフェイス（Destination Interface）]：inside。
- [元の発信元（Original Source）] = myWebServer ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = TransWebServer ネットワークオブジェクト。



c) [保存（Save）] をクリックします。

ステップ 8 Web サーバーのスタティック NAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

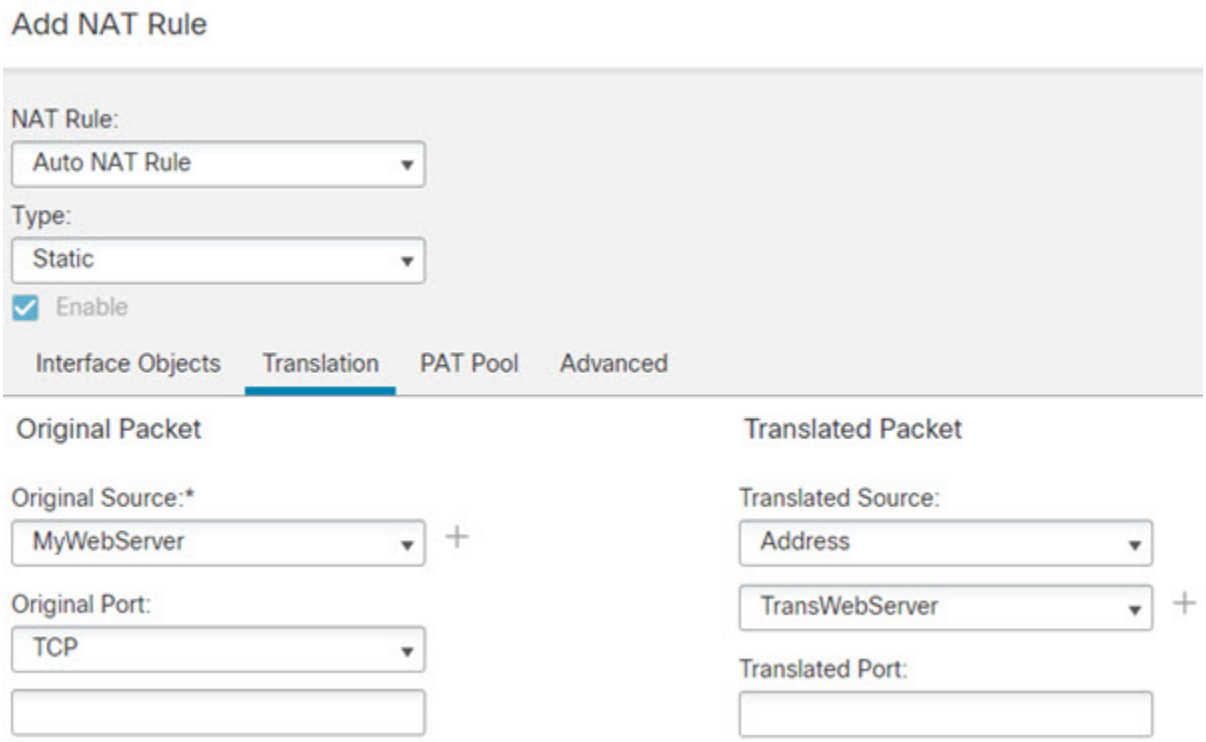
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

d) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = myWebServer ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = TransWebServer ネットワークオブジェクト。



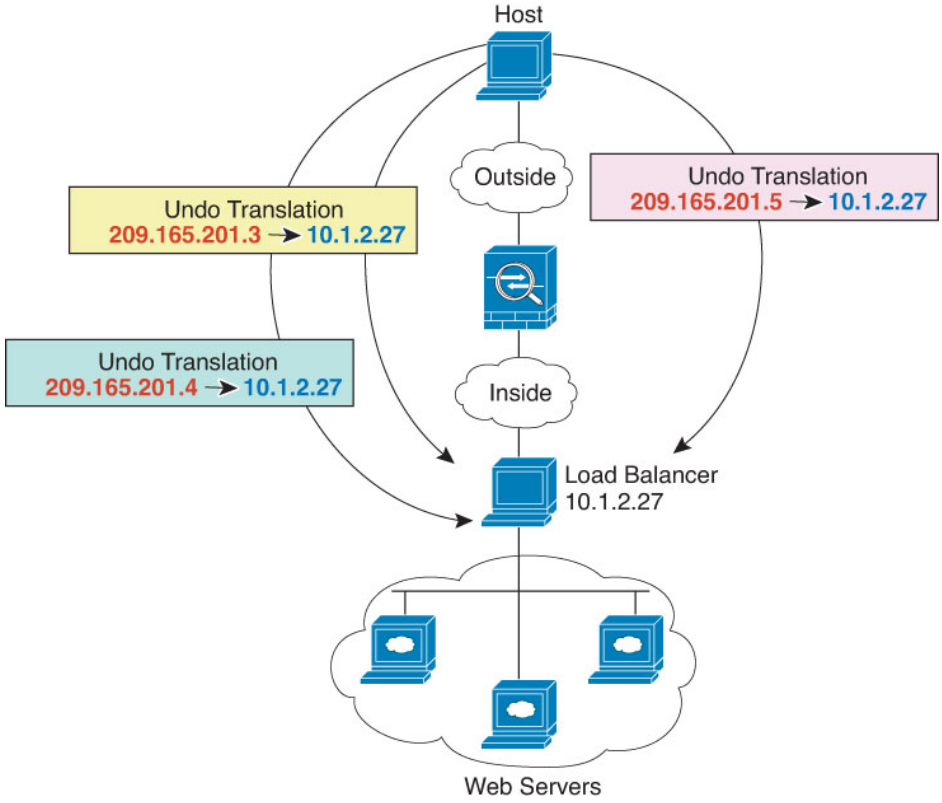
e) [保存（Save）] をクリックします。

ステップ 9 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

複数のマッピング アドレス（スタティック自動 NAT、1 対多）を持つ内部ロード バランサ

次の例では、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする際、1 つのロード バランサのアドレスには変換されません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 *283* : 内部ロード バランサのスタティック *NAT*（一対多）



始める前に

Web サーバーを保護するデバイスのインターフェイスが含まれているインターフェイ オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

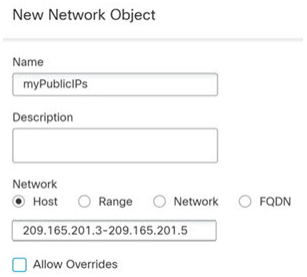
ステップ 1 ロードバランサをマッピングするアドレスに対し、ネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) アドレスを定義します。

ネットワーク オブジェクトに名前（たとえば、myPublicIPs）を付けて、ネットワーク範囲 209.165.201.3-209.165.201.5 を入力します。

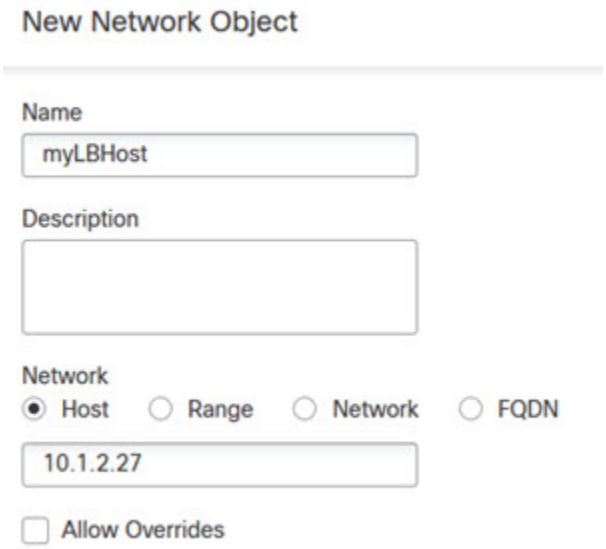


d) [保存（Save）] をクリックします。

ステップ 2 ロード バランサに対するネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前（たとえば、myLBHost）を付けて、ホスト アドレス 10.1.2.27 を入力します。



c) [保存（Save）] をクリックします。

ステップ 3 ロード バランサのスタティック NAT を設定します。

a) **[デバイス（Device）]** > **[デバイス管理（Device）]** を選択して、ルールを定義する Threat Defense デバイスを編集します。[NAT] を選択します。

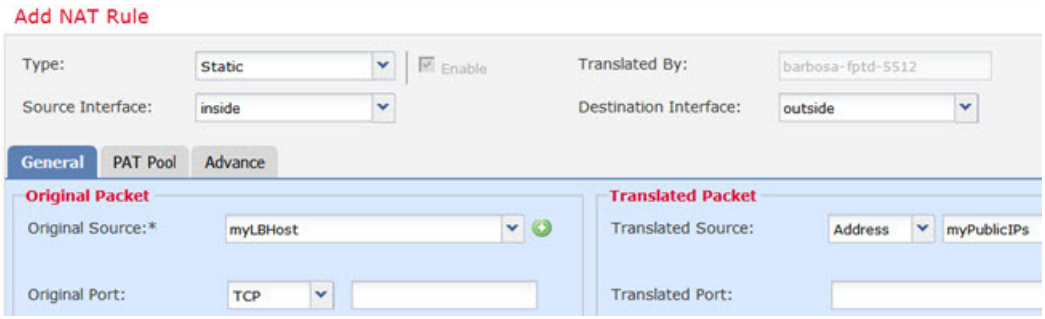
複数のドメインを使用している場合、デバイスを含む同じリーフ ドメインに位置していることを確認します。

b) **[NAT ルールの追加（Add NAT Rule）]** > **[自動 NAT の追加（Add Auto NAT）]** をクリックします。

c) 次のプロパティを設定します。

- [種類（Type）]：Static。

- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：outside。
- [元の送信元（Original Source）] = myLBHost ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]**= myPublicIPs ネットワークグループ。



d) [保存（Save）] をクリックします。

ステップ 4 ロード バランサのスタティック NAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

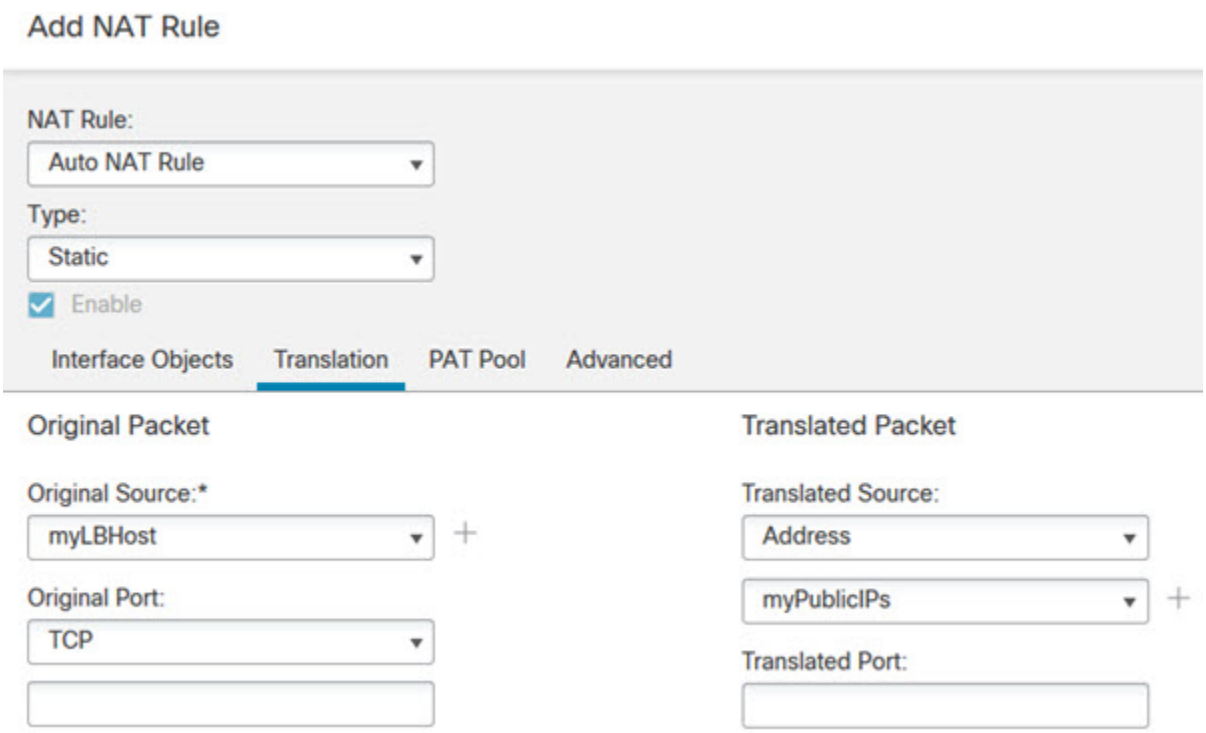
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = myLBHost ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]**= myPublicIPs ネットワークグループ。



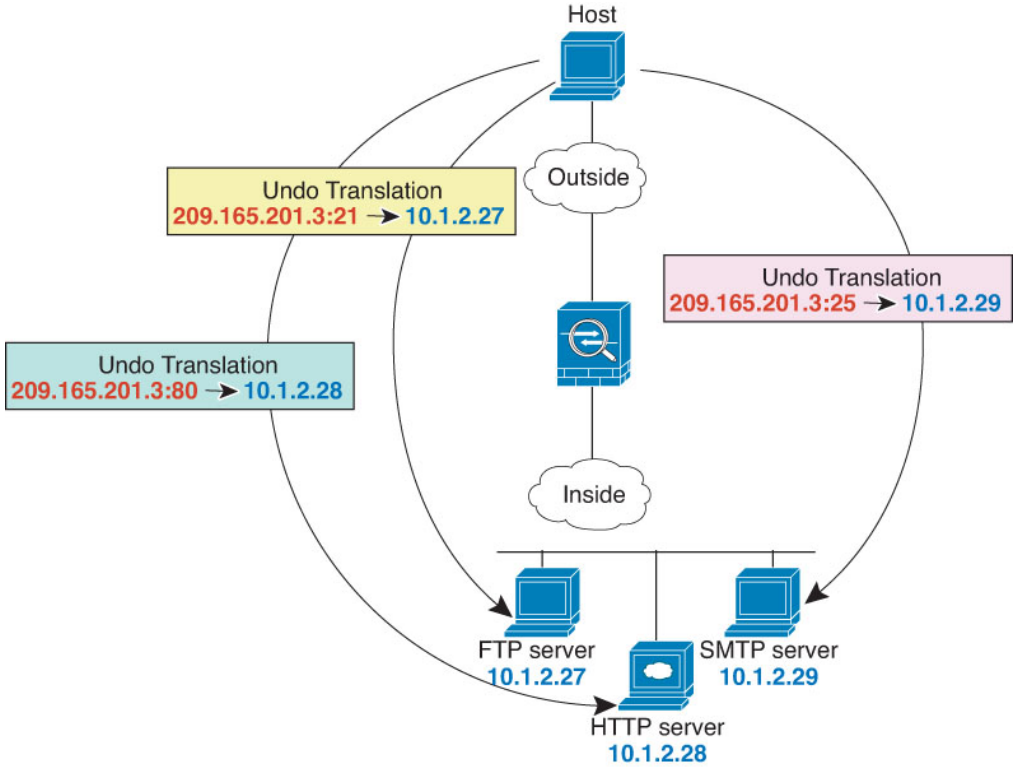
f) [保存（Save）] をクリックします。

ステップ 5 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック自動 NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザは単一のアドレスで FTP、HTTP、および SMTP にアクセスできるようになります。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。

図 *284 :* ポート変換を設定したスタティック *NAT*



始める前に

サーバーを保護するデバイスのインターフェイスが含まれるインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

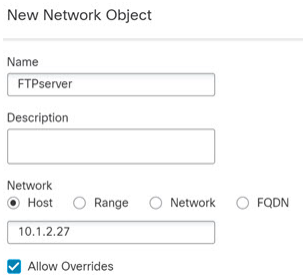
手順

ステップ 1 FTPサーバのネットワークオブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) ネットワーク オブジェクトに名前を付け（たとえば「FTPserver」）、FTP サーバーの実際の IP アドレス（10.1.2.27）を入力します。

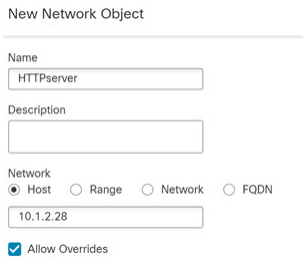


d) [保存（Save）] をクリックします。

ステップ 2 HTTP サーバーのネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば「HTTPserver」）、ホストアドレス（10.1.2.28）を入力します。

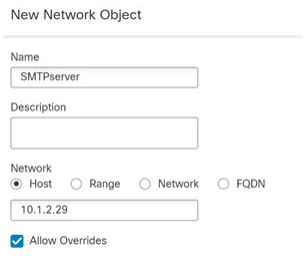


c) [保存（Save）] をクリックします。

ステップ 3 SMTP サーバーのネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば「SMTPserver」）、ホストアドレス（10.1.2.29）を入力します。

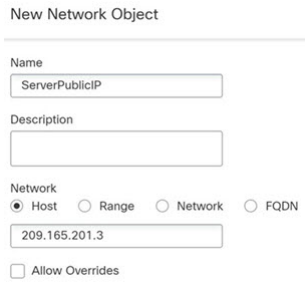


c) [保存（Save）] をクリックします。

ステップ 4 3 つのサーバーに使用されるパブリック IP アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば「ServerPublicIP」）、ホストアドレス（209.165.201.3）を入力します。



c) [保存（Save）] をクリックします。

ステップ 5 FTP サーバーのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

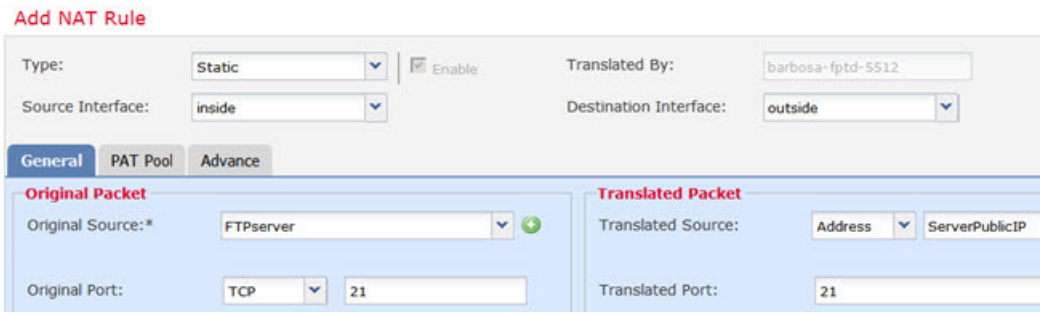
a) **[デバイス（Device）]** > **[デバイス管理（Device）]** を選択して、ルールを定義する Threat Defense デバイスを編集します。[NAT] を選択します。

複数のドメインを使用している場合、デバイスを含む同じリーフ ドメインに位置していることを確認します。

b) **[NAT ルールの追加（Add NAT Rule）]** > **[自動 NAT の追加（Add Auto NAT）]** をクリックします。

c) 次のプロパティを設定します。

- [種類（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：outside。
- [元の発信元（Original Source）] = FTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）]** > **[アドレス（Address）]** = ServerPublicIP ネットワークオブジェクト。
- **[元のポート（Original Port）]** > **[TCP]** = 21。
- **[変換済みポート（Translated Port）]** = 21。



d) [保存（Save）] をクリックします。

ステップ 6 FTP サーバーのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

a) **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

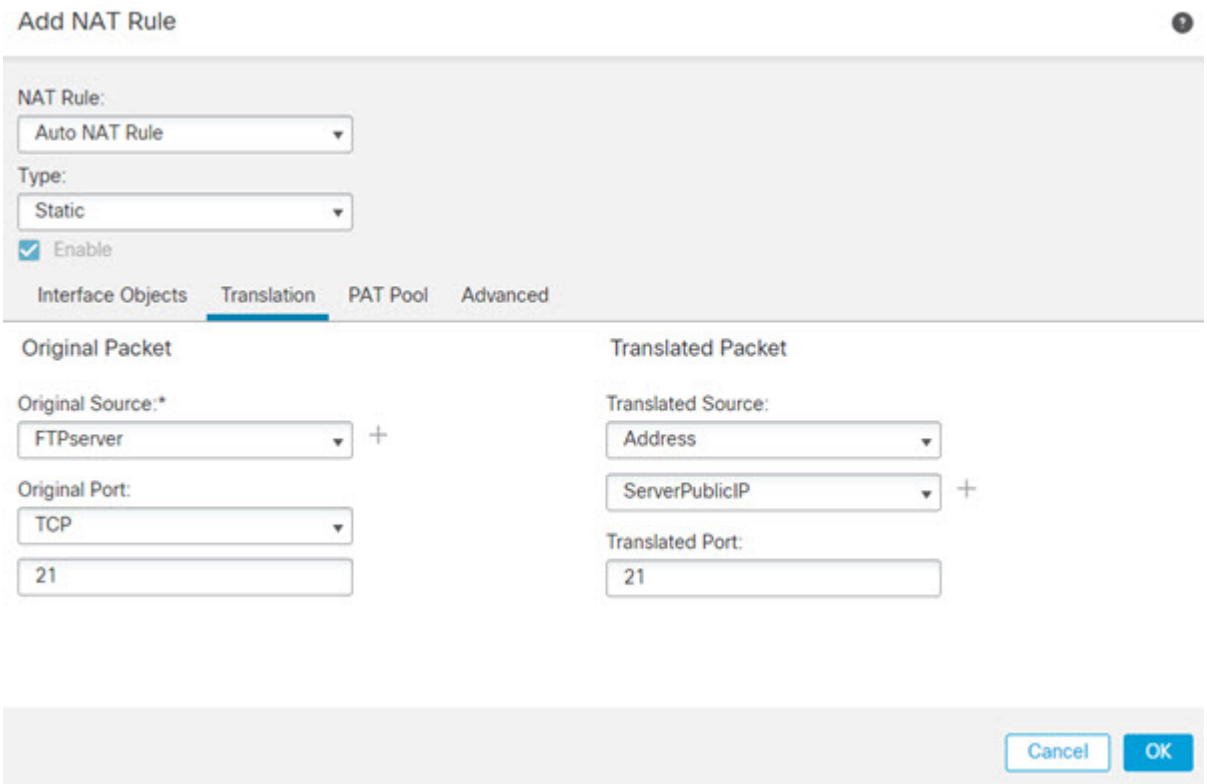
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = FTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）] > [アドレス（Address）]**= ServerPublicIP ネットワークオブジェクト。
- **[元のポート（Original Port）] > [TCP]** = 21。
- **[変換済みポート（Translated Port）]** = 21。



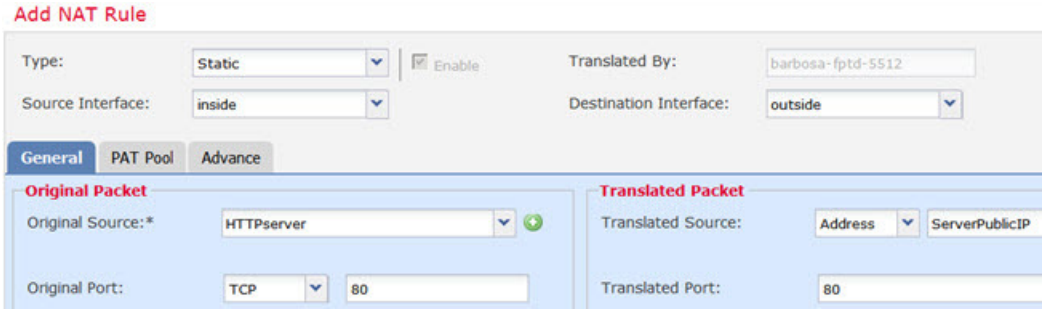
f) [保存（Save）] をクリックします。

ステップ 7 HTTP サーバーのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

a) **[NAT ルールの追加（Add NAT Rule）]** > **[自動 NAT の追加（Add Auto NAT）]** をクリックします。

b) 次のプロパティを設定します。

- [種類（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：outside。
- [元の発信元（Original Source）] = HTTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）]** > **[アドレス（Address）]**= ServerPublicIP ネットワークオブジェクト。
- **[元のポート（Original Port）]** > **[TCP]** = 80。
- **[変換済みポート（Translated Port）]** = 80。



c) [保存（Save）] をクリックします。

ステップ 8 HTTP サーバーのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

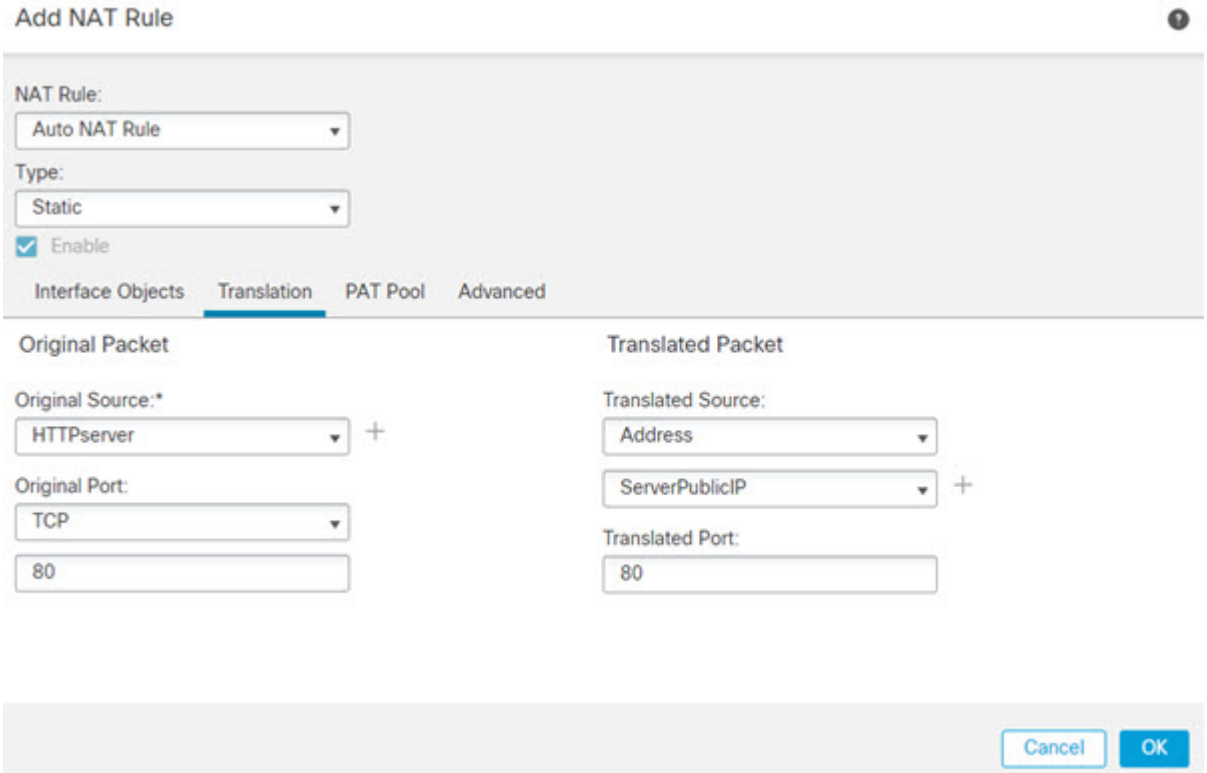
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

d) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = HTTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）]** > **[アドレス（Address）]** = ServerPublicIP ネットワークオブジェクト。
- **[元のポート（Original Port）]** > **[TCP]** = 80。
- **[変換済みポート（Translated Port）]** = 80。



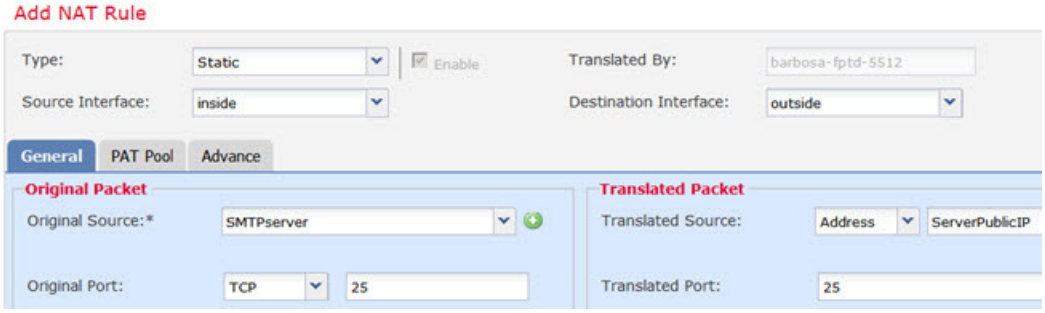
e) [保存（Save）] をクリックします。

ステップ 9 SMTP サーバーのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

a) **[NAT ルールの追加（Add NAT Rule）]** > **[自動 NAT の追加（Add Auto NAT）]** をクリックします。

b) 次のプロパティを設定します。

- [種類（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：outside。
- [元の発信元（Original Source）] = SMTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）]** > **[アドレス（Address）]**= ServerPublicIP ネットワークオブジェクト。
- **[元のポート（Original Port）]** > **[TCP]** = 25。
- **[変換済みポート（Translated Port）]** = 25。



c) [保存（Save）] をクリックします。

ステップ 10 SMTP サーバーのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

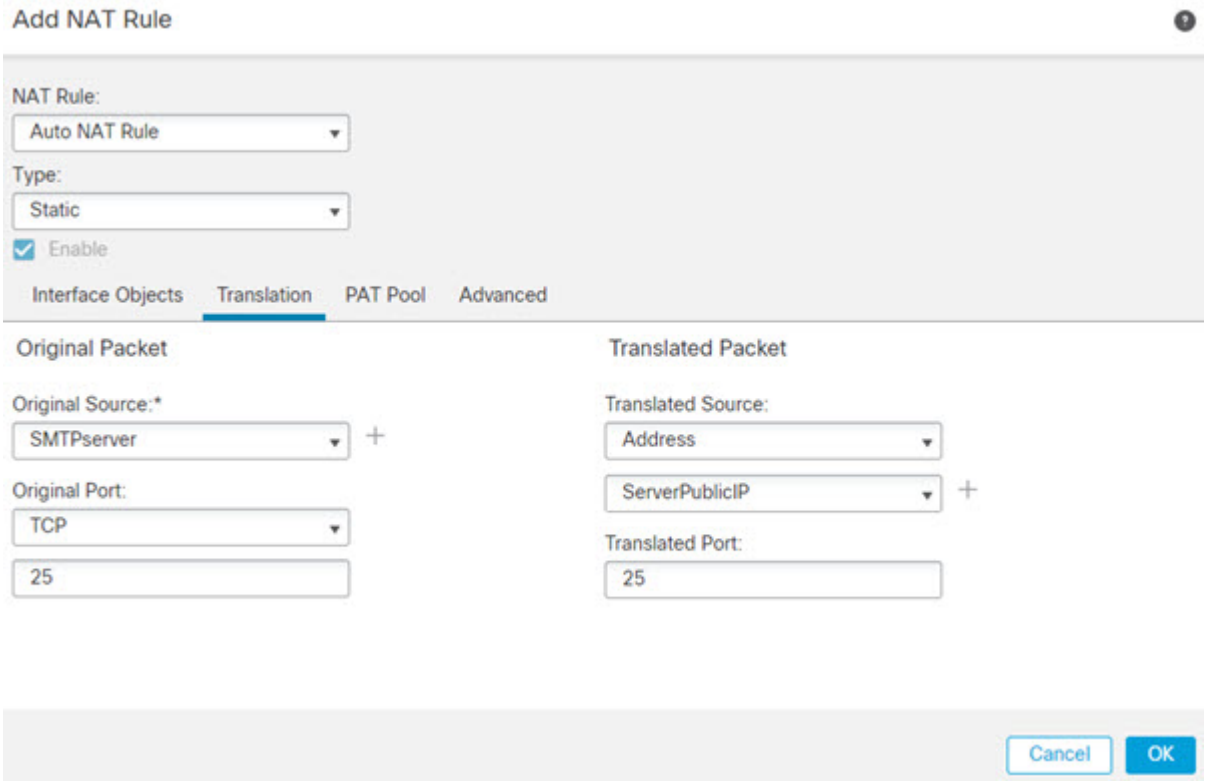
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

d) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = SMTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）]** > **[アドレス（Address）]** = ServerPublicIP ネットワークオブジェクト。
- **[元のポート（Original Port）]** > **[TCP]** = 25。
- **[変換済みポート（Translated Port）]** = 25。



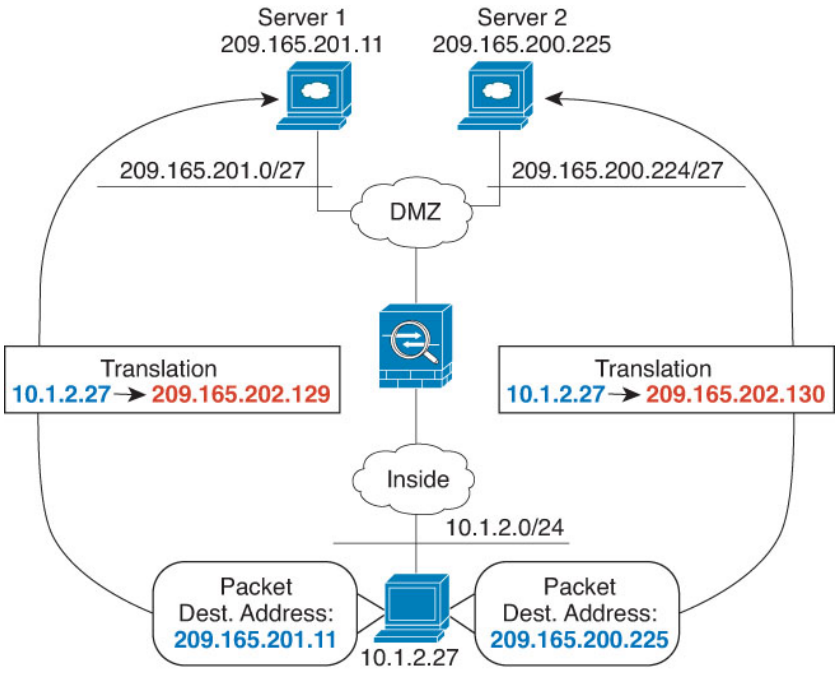
e) [保存（Save）] をクリックします。

ステップ 11 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

宛先に応じて異なる変換（ダイナミック手動 PAT）

次の図に、2 つの異なるサーバにアクセスする、10.1.2.0/24 ネットワーク上のホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 *285 :* 異なる宛先アドレスを使用する手動*NAT*



始める前に

サーバーを保護するデバイスのインターフェイスが含まれるインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは「**inside**」および「**dmz**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、[インターフェイス（Interface）] を選択します。

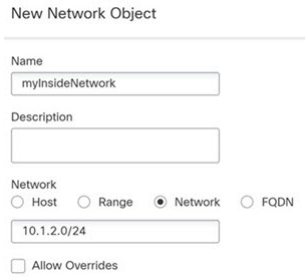
手順

ステップ 1 内部ネットワーク用のネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、実際のネットワーク アドレス 10.1.2.0/24 を入力します。



d) [保存（Save）] をクリックします。

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

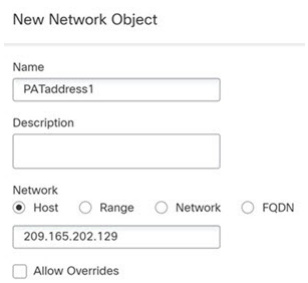
b) ネットワーク オブジェクトに名前を付け（DMZnetwork1 など）、ネットワーク アドレス 209.165.201.0/27 を入力します（255.255.255.224 のサブネット マスク）。

c) [保存（Save）] をクリックします。

ステップ 3 DMZ ネットワーク 1 の PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、ホスト アドレス 209.165.202.129 を入力します。

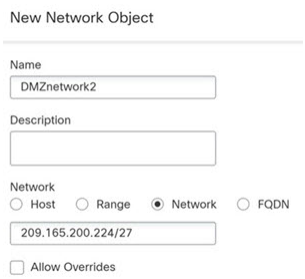


c) [保存（Save）] をクリックします。

ステップ 4 DMZ ネットワーク 2 のネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（DMZnetwork2 など）、ネットワーク アドレス 209.165.200.224/27 を入力します（255.255.255.224 のサブネット マスク）。



c) [保存（Save）] をクリックします。

ステップ 5 DMZ ネットワーク 2 の PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、ホスト アドレス 209.165.202.130 を入力します。

c) [保存（Save）] をクリックします。

ステップ 6 DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

a) **[デバイス（Device）]** > **[デバイス管理（Device）]** を選択して、ルールを定義する Threat Defense デバイスを編集します。[NAT] を選択します。

複数のドメインを使用している場合、デバイスを含む同じリーフ ドメインに位置していることを確認します。

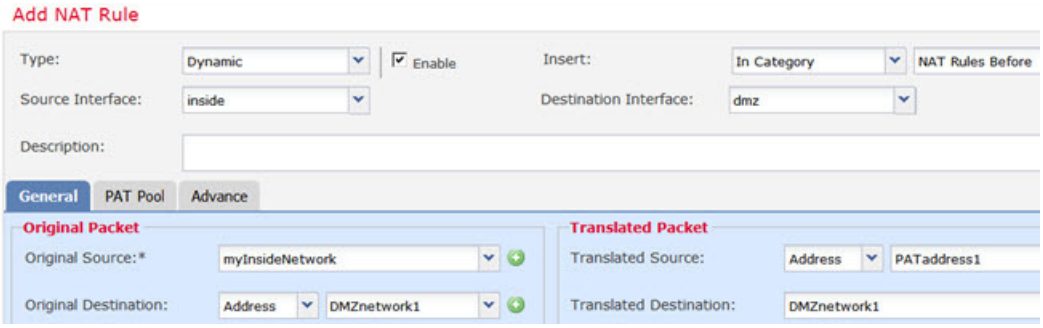
b) **[NAT ルールの追加（Add NAT Rule）]** > **[手動 NAT の追加（Add Manual NAT）]** をクリックします。

c) 次のプロパティを設定します。

- [種類（Type）]：Dynamic。
- [送信元インターフェイス（Source Interface）]：inside。

- [宛先インターフェイス（Destination Interface）]：dmz。
- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]**= PATaddress1 ネットワークオブジェクト。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = DMZnetwork1 ネットワークオブジェクト。
- [変換済みの宛先（Translated Destination）] = DMZnetwork1 ネットワーク オブジェクト。

（注）
宛先アドレスを変換する必要はないため、元の宛先アドレスと変換後の宛先アドレスに同じアドレスを指定することにより、アイデンティティ NAT を設定する必要があります。ポート フィールドはすべて空欄のままにしておきます。



d) [保存（Save）] をクリックします。

ステップ 7 DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

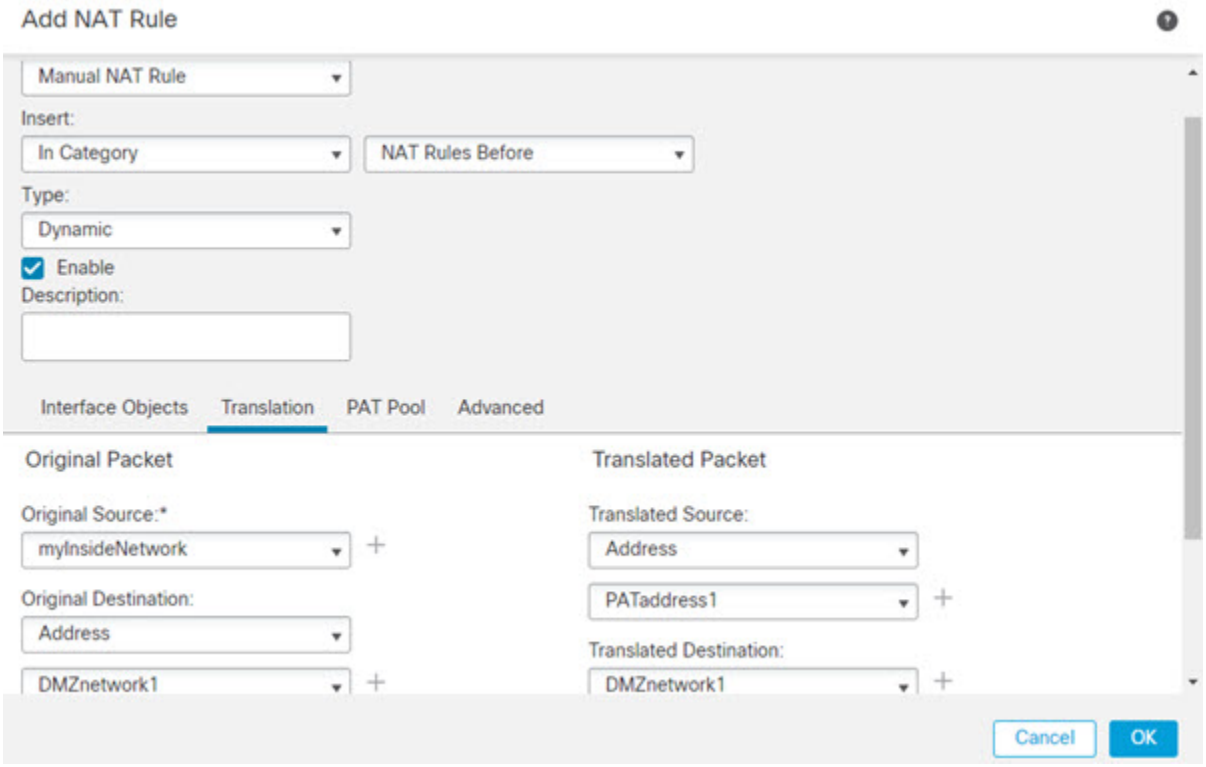
- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。

e) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。

- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]**= PATaddress1 ネットワークオブジェクト。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = DMZnetwork1 ネットワークオブジェクト。
- [変換済みの宛先（Translated Destination）] = DMZnetwork1 ネットワーク オブジェクト。

（注）
宛先アドレスを変換する必要はないため、元の宛先アドレスと変換後の宛先アドレスに同じアドレスを指定することにより、アイデンティティ NAT を設定する必要があります。ポート フィールドはすべて空欄のままにしておきます。



f) [保存（Save）] をクリックします。

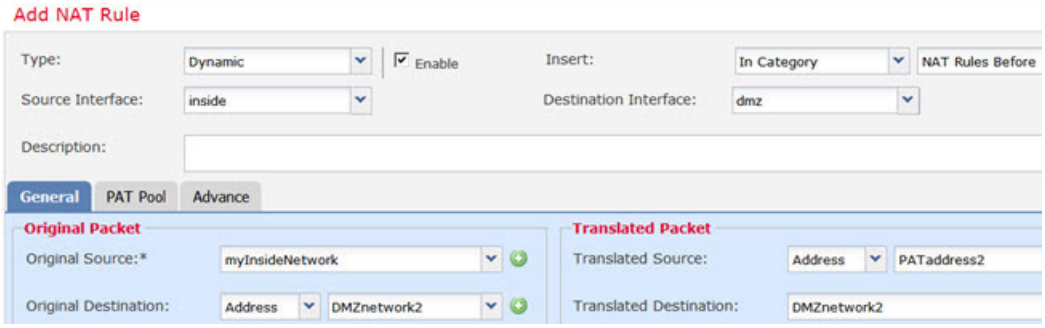
ステップ 8 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) **[NAT ルールの追加（Add NAT Rule）]** > **[手動 NAT の追加（Add Manual NAT）]** をクリックします。

b) 次のプロパティを設定します。

- [種類（Type）]：Dynamic。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：dmz。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]**= PATaddress2 ネットワークオブジェクト。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = DMZnetwork2 ネットワークオブジェクト。
- [変換済みの宛先（Translated Destination）] = DMZnetwork2 ネットワーク オブジェクト。



c) [保存（Save）] をクリックします。

ステップ 9 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

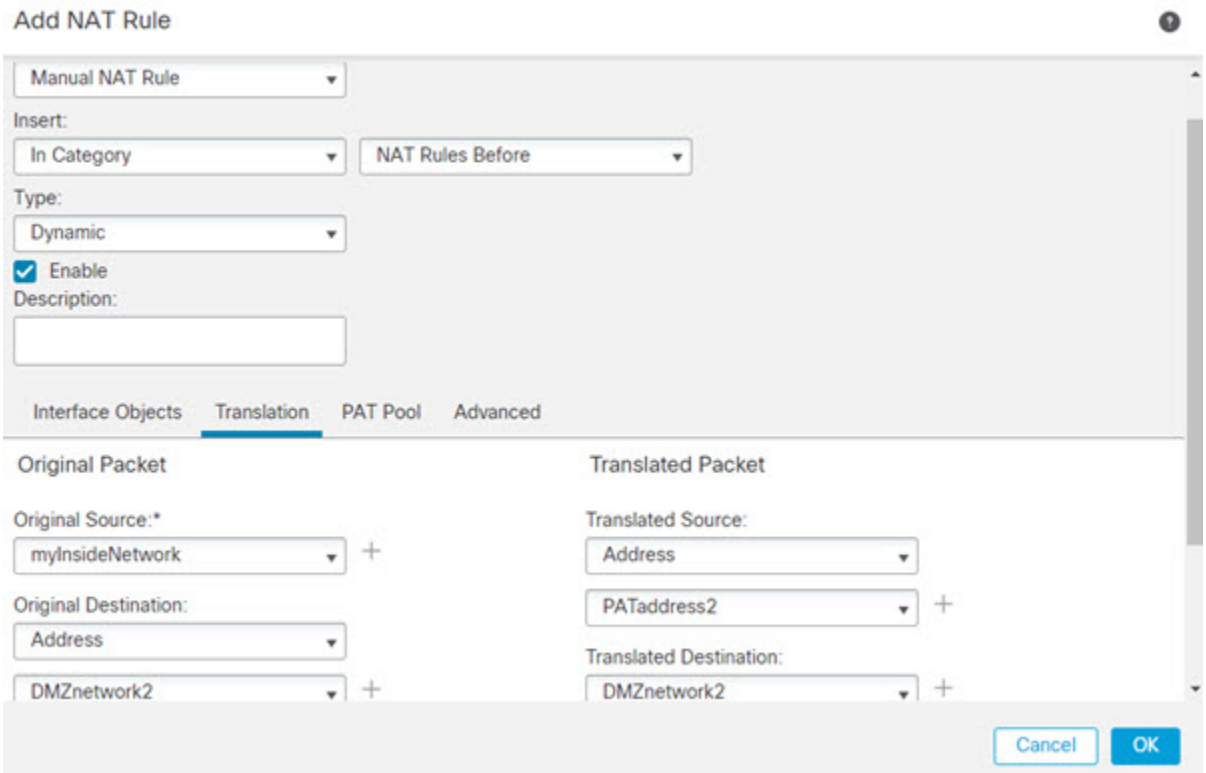
- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。

d) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]**= PATaddress2 ネットワークオブジェクト。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = DMZnetwork2 ネットワークオブジェクト。
- [変換済みの宛先（Translated Destination）] = DMZnetwork2 ネットワーク オブジェクト。



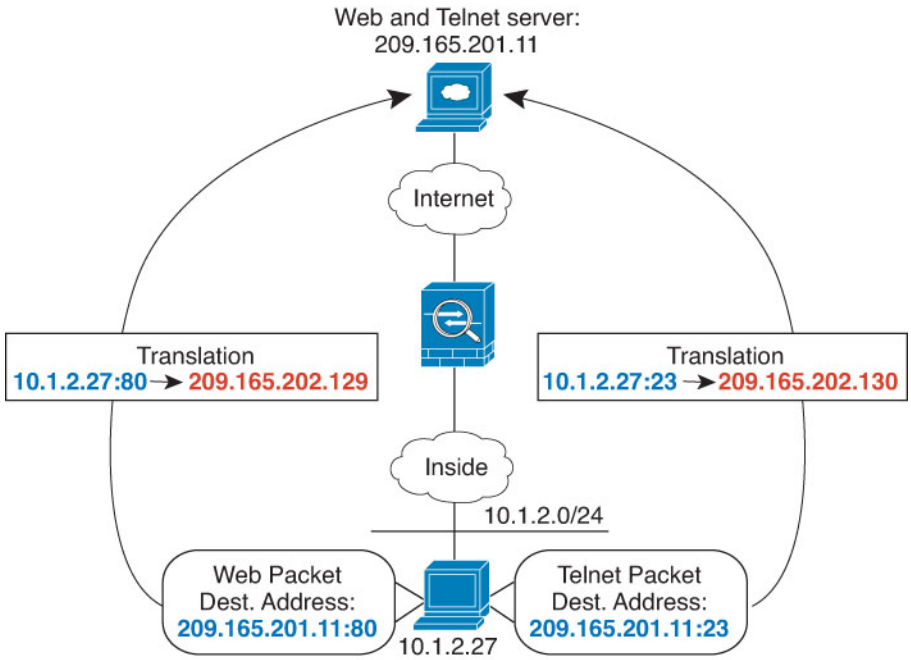
e) [保存（Save）] をクリックします。

ステップ 10 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:*port* に変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

図 *286 :* 異なる宛先ポートを使用する手動*NAT*



始める前に

サーバーを保護するデバイスのインターフェイスが含まれるインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは「**inside**」および「**dmz**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、[インターフェイス（Interface）] を選択します。

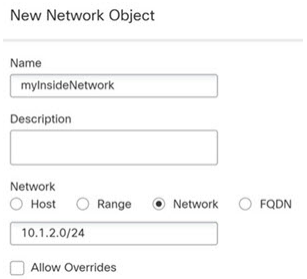
手順

ステップ 1 内部ネットワーク用のネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

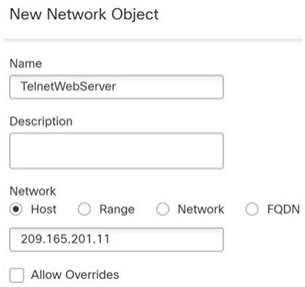


d) [保存（Save）] をクリックします。

ステップ 2 Telnet/Web サーバーのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（TelnetWebServer など）、ホスト アドレス 209.165.201.11 を入力します。

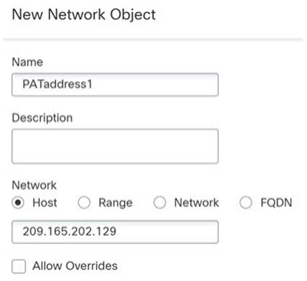


c) [保存（Save）] をクリックします。

ステップ 3 Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、ホスト アドレス 209.165.202.129 を入力します。



c) [保存（Save）] をクリックします。

ステップ 4 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、ホスト アドレス 209.165.202.130 を入力します。

c) [保存（Save）] をクリックします。

ステップ 5 Telnet アクセスのダイナミック手動 PAT を設定します。

a) **[デバイス（Device）] > [デバイス管理（Device）]** を選択して、ルールを定義する Threat Defense デバイスを編集します。[NAT] を選択します。

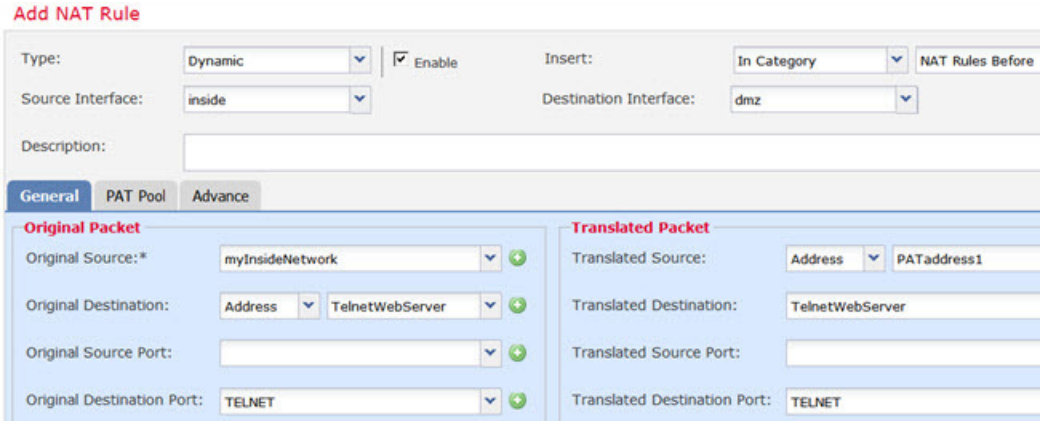
複数のドメインを使用している場合、デバイスを含む同じリーフ ドメインに位置していることを確認します。

b) **[NAT ルールの追加（Add NAT Rule）] > [手動 NAT の追加（Add Manual NAT）]** をクリックします。

c) 次のプロパティを設定します。

- [種類（Type）]：Dynamic。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：dmz。
- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）] > [アドレス（Address）]**= PATaddress1 ネットワークオブジェクト。
- **[元の宛先（Original Destination）] > [アドレス（Address）]** = TelnetWebServer ネットワークオブジェクト。
- [変換済みの宛先（Translated Destination）] = TelnetWebServer ネットワーク オブジェクト。
- [元の宛先ポート（Original Destination Port）] = TELNET ポート オブジェクト（システム定義）。
- [変換済みの宛先ポート（Translated Destination Port）] = TELNET ポート オブジェクト（システム定義）。

（注）
宛先アドレスまたはポートを変換しないため、元のアドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポートに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。



d) [保存（Save）] をクリックします。

ステップ 6 Telnet アクセスのダイナミック手動 PAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

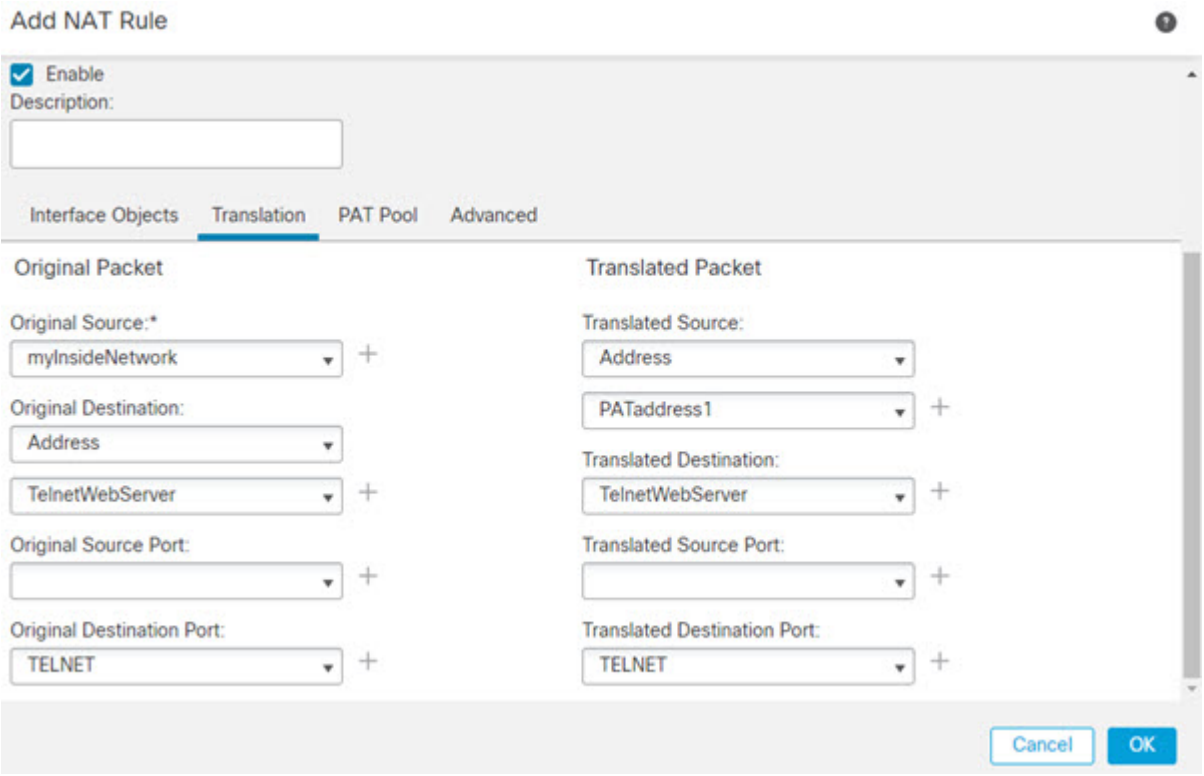
- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。

e) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]**= PATaddress1 ネットワークオブジェクト。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = TelnetWebServer ネットワークオブジェクト。
- [変換済みの宛先（Translated Destination）] = TelnetWebServer ネットワーク オブジェクト。
- [元の宛先ポート（Original Destination Port）] = TELNET ポート オブジェクト（システム定義）。
- [変換済みの宛先ポート（Translated Destination Port）] = TELNET ポート オブジェクト（システム定義）。

（注）

宛先アドレスまたはポートを変換しないため、元のアドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポートに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。



f) [保存（Save）] をクリックします。

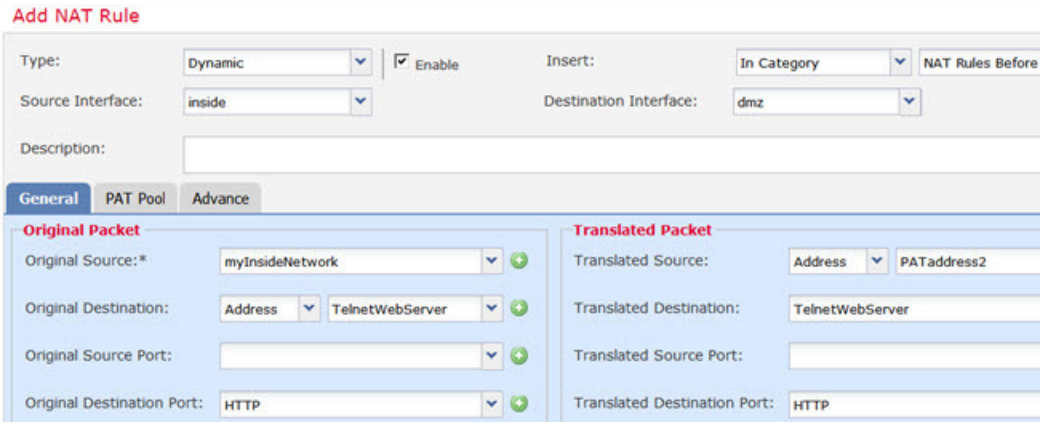
ステップ 7 Web アクセスのダイナミック手動 PAT を設定します。

a) **[NAT ルールの追加（Add NAT Rule）]** > **[手動 NAT の追加（Add Manual NAT）]** をクリックします。

b) 次のプロパティを設定します。

- [種類（Type）]：Dynamic。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス（Destination Interface）]：dmz。
- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]**= PATaddress2 ネットワークオブジェクト。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = TelnetWebServer ネットワークオブジェクト。

- [変換済みの宛先（Translated Destination）] = TelnetWebServer ネットワーク オブジェクト。
- [元の宛先ポート（Original Destination Port）] = HTTP ポート オブジェクト（システム定義）。
- [変換済みの宛先ポート（Translated Destination Port）] = HTTP ポート オブジェクト（システム定義）。



c) [保存（Save）] をクリックします。

ステップ 8 Web アクセスのダイナミック手動 PAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

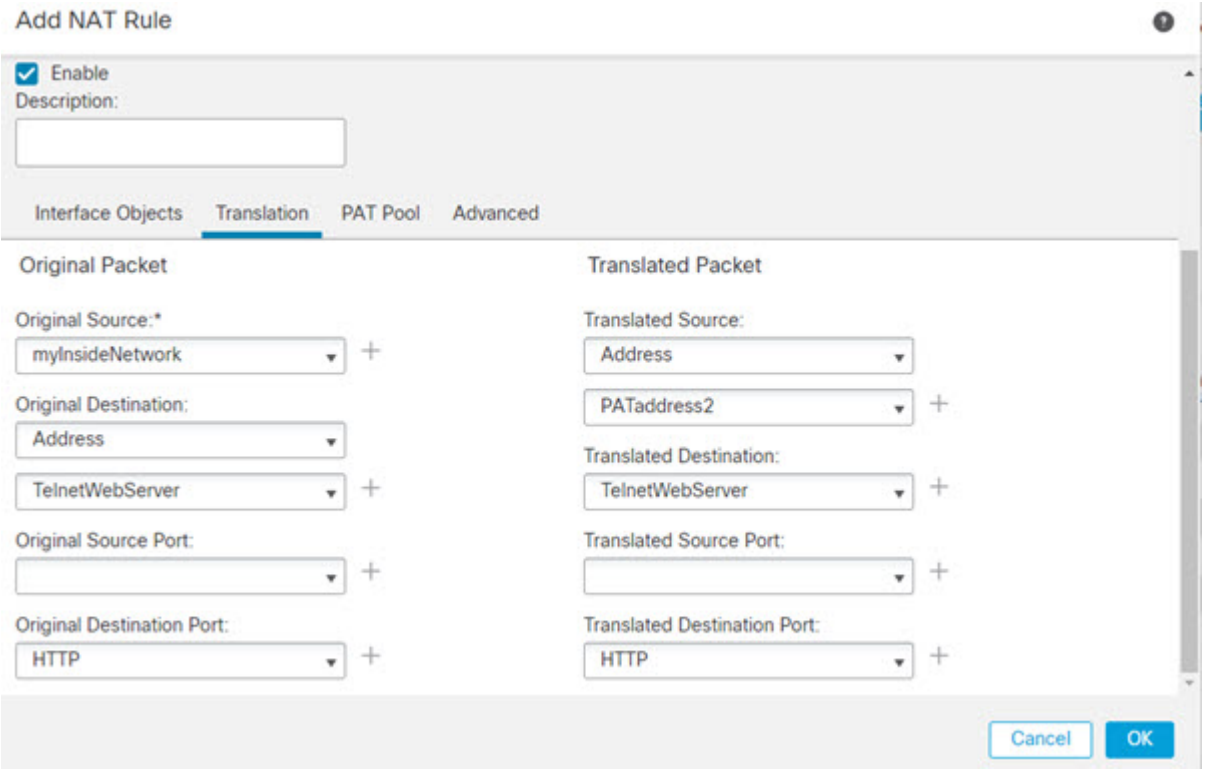
c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。

d) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）] > [アドレス（Address）]**= PATaddress2 ネットワークオブジェクト。
- **[元の宛先（Original Destination）] > [アドレス（Address）]** = TelnetWebServer ネットワークオブジェクト。
- [変換済みの宛先（Translated Destination）] = TelnetWebServer ネットワーク オブジェクト。

- [元の宛先ポート（Original Destination Port）] = HTTP ポート オブジェクト（システム定義）。
- [変換済みの宛先ポート（Translated Destination Port）] = HTTP ポート オブジェクト（システム定義）。



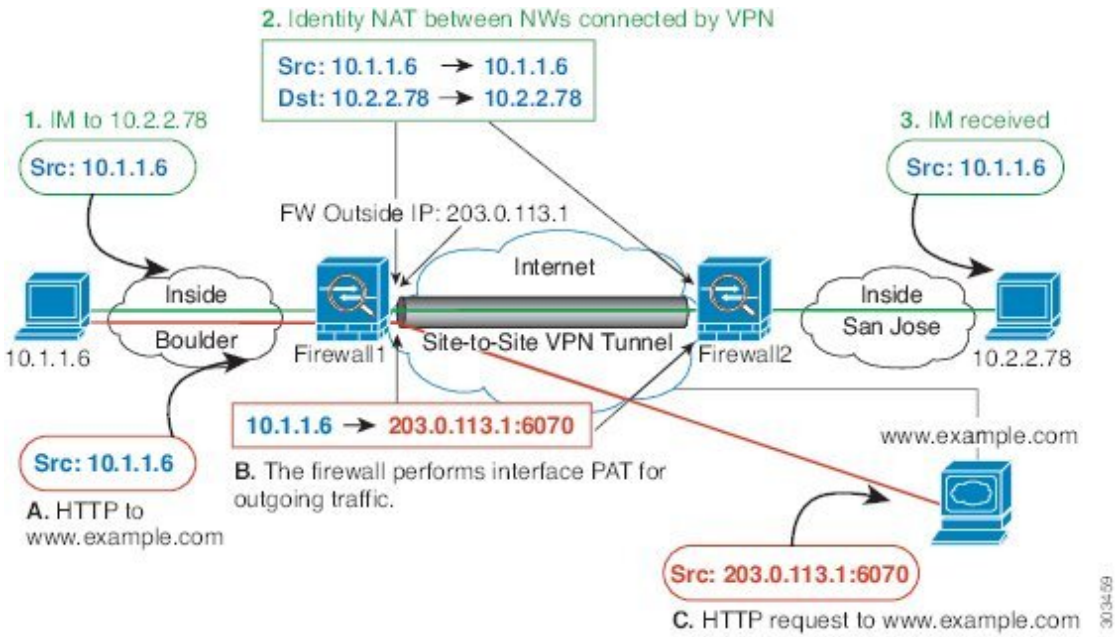
e) [保存（Save）] をクリックします。

ステップ 9 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

NAT およびサイトツーサイト VPN

次の図に、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに向かうトラフィック（たとえばボールダーの 10.1.1.6 から www.example.com へ）については、インターネット アクセス用に NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィック（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）については NAT を実行しません。したがって、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は、あるアドレスを同じアドレスに変換するだけです。

図 *287* : サイトツーサイト *VPN* のためのインターフェイス *PAT* およびアイデンティティ *NAT*



次の例は、Firewall1（ボールダー）の設定を示します。

始める前に

VPN 内のデバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは、Firewall1（ボールダー）インターフェイスに対応する **inside-boulder** および **outside-boulder** という名前のセキュリティ ゾーンであると仮定します。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interfaces）] を選択します。

手順

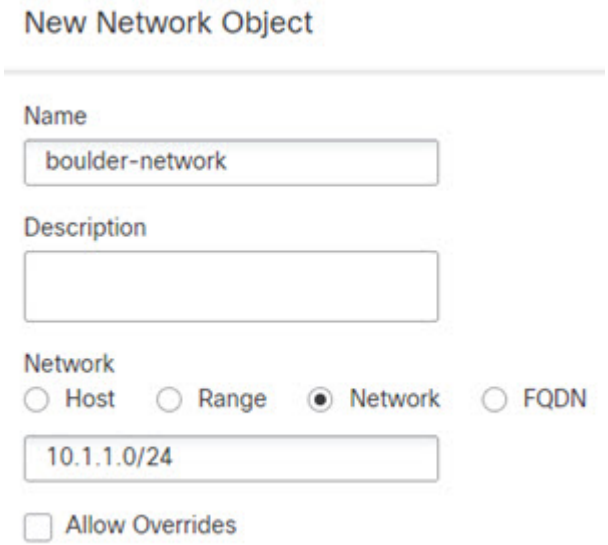
ステップ 1 さまざまなネットワークを定義するには、オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) ボールダー内部ネットワークを特定します。

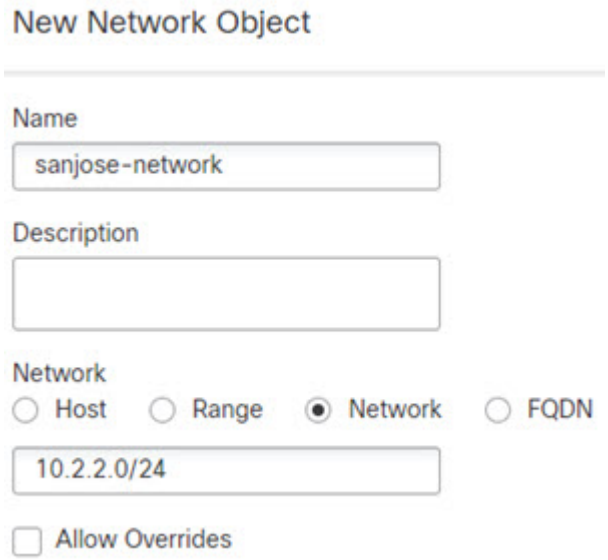
ネットワーク オブジェクトに名前（たとえば、boulder-network）を付けて、ネットワーク アドレス 10.1.1.0/24 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、内部サンノゼネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、sanjose-network）を付けて、ネットワークアドレス 10.2.2.0/24 を入力します。



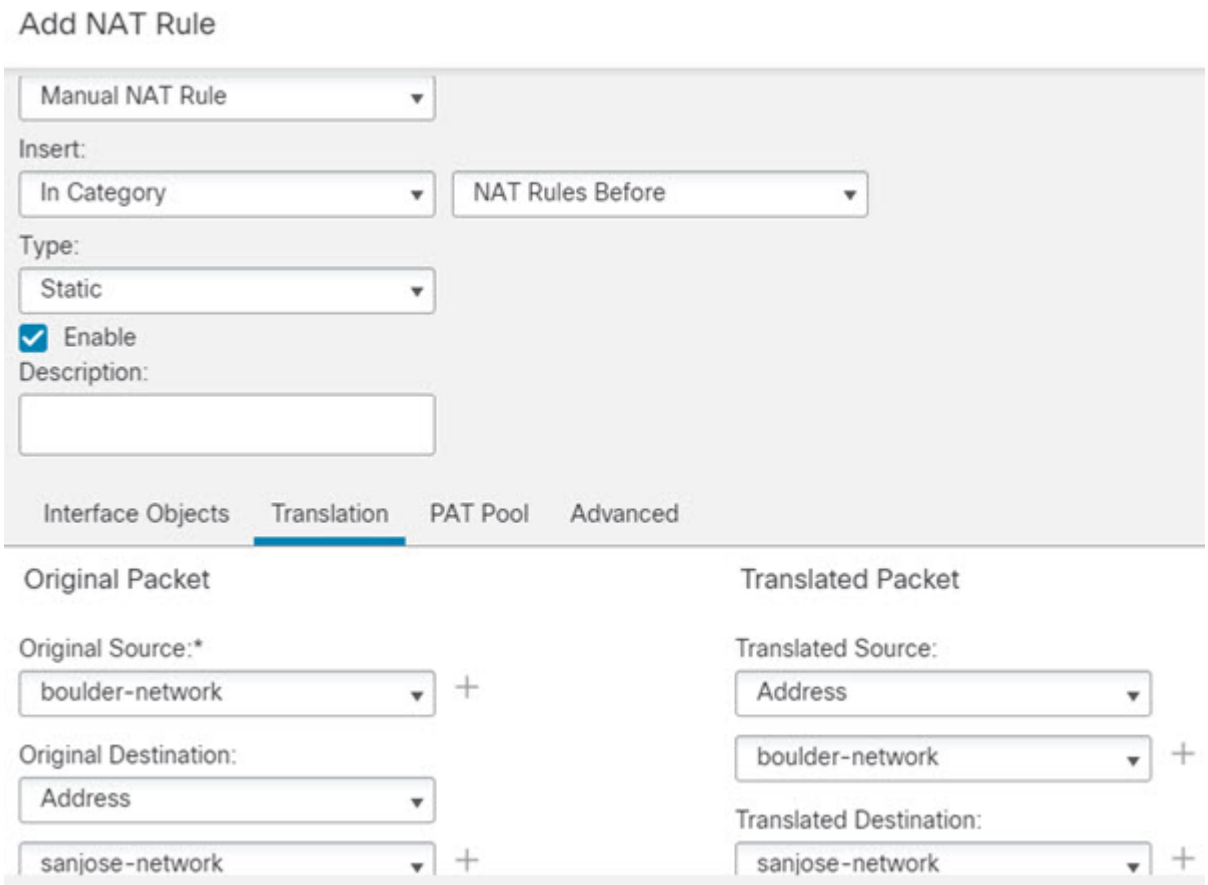
f) [保存（Save）] をクリックします。

ステップ 2 Firewall1（ボールダー）上で VPN 経由でサンノゼに向かう場合、ボールダー ネットワークの手動アイデンティティ NAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。
c) 次のプロパティを設定します。
   - [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
   - [タイプ（Type）] = Static。
d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。
   - [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside-boulder。
   - [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside-boulder。
e) [変換（Translation）] で、次の項目を設定します。
   - [元の送信元（Original Source）] = boulder-network オブジェクト。
   - **[変換済みの送信元（Translated Source）] > [アドレス（Address）]** = boulder-network オブジェクト。
   - **[元の宛先（Original Destination）] > [アドレス（Address）]** = sanjose-network オブジェクト。
   - [変換済みの宛先] = sanjose-network オブジェクト。

     （注）
     宛先アドレスを変換する必要はないため、元の宛先アドレスと変換後の宛先アドレスに同じアドレスを指定することにより、アイデンティティ NAT を設定する必要があります。ポート フィールドはすべて空欄のままにしておきます。このルールは、送信元と宛先の両方にアイデンティティ NAT を設定します。
f) [詳細（Advanced）] で [宛先インターフェイスでプロキシARPなし（Do not proxy ARP on Destination interface）] を選択します。



g) [保存（Save）] をクリックします。

ステップ 3 Firewall1（ボールダー）上で内部ボールダーネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

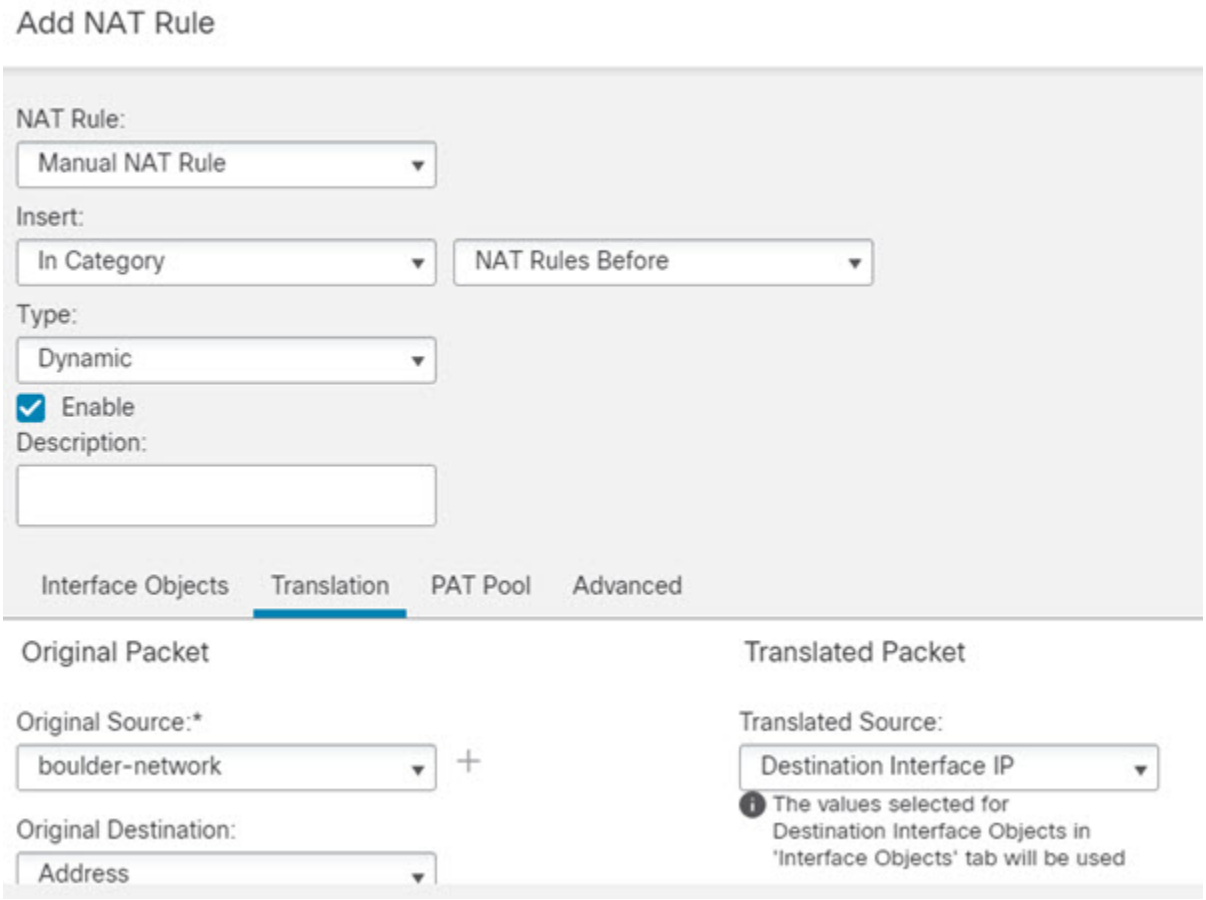
- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。
- [挿入ルール（Insert Rule）] = 最初のルールの後の任意の位置。このルールは任意の宛先アドレスに適用されるため、sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、sanjose-network ルールは永遠に一致することがありません。デフォルトでは、新しい手動 NAT ルールは [自動 NAT の前に NAT ルール（NAT Rules Before Auto NAT）] セクションの最後に配置されます。

c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside-boulder。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside-boulder。

d) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = boulder-network オブジェクト。
- [変換済みの送信元（Translated Source）]=宛先インターフェイス IP（Destination Interface IP）。このオプションでは、宛先インターフェイス オブジェクトに含まれているインターフェイスを使用して、インターフェイス PAT を設定します。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = 任意（空白のまま）。
- [変換済みの宛先（Translated Destination）] = 任意（空白のまま）。



e) [保存（Save）] をクリックします。

ステップ 4 Firewall2（San Jose）も管理している場合は、そのデバイスにも同様のルールを設定できます。

- 手動アイデンティティ NAT ルールの対象は、boulder-network を宛先とする sanjose-network です。Firewall2 内部/外部ネットワーク用に新しいインターフェイス オブジェクトを作成します。

- 手動ダイナミック インターフェイス PAT ルールの対象は、any を宛先とする sanjose-network です。

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するようにFirewall Threat Defense デバイスを設定することが必要になる場合があります。DNS 修正は、各変換ルールの設定時に設定できます。DNS 修正は、DNS Doctoring とも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリーと応答のアドレスをリライトします（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリーの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答の場合、レコードはマッピングされた値から実際の値に書き換えられます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。この機能は、NAT44、NAT66、 NAT46、および NAT64 と連動します。

以下に、NAT ルールで DNS の書き換えを設定する必要が生じる主な状況を示します。

- ルールが NAT64 または NAT46 で、DNS サーバが外部ネットワーク上に存在する。DNS A レコード（IPv4 ）と AAAA レコード（IPv6）間で変換するために DNS 書き換えが必要です。
- DNS サーバが外部に存在し、クライアントが内部に存在し、クライアントが使用する完全修飾ドメイン名の一部が、他の内部ホストに解決される。
- DNS サーバが内部に存在してプライベート IP アドレスで応答し、クライアントが外部に存在する。そして、クライアントが、内部でホストされているサーバを指す完全修飾ドメイン名にアクセスする。

DNS 書き換えに関する制限事項

DNS 書き換えに伴う制限事項を以下に示します。

- DNS 書き換えは PAT に適用できません。これは、個々の A または AAAA レコードに複数の PAT ルールを適用できるので、使用する PAT ルールが不明確になるためです。
- 手動NAT ルールを設定する場合、宛先アドレスおよび送信元アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- DNS クエリと応答を書き換えるには、NAT ルールに対して DNS NAT 書き換えを有効にした DNS アプリケーション インスペクションを有効にする必要があります。デフォルト

で、DNS NAT 書き換えを有効にした DNS インスペクションがグローバルに適用されるため、インスペクション設定を変更する必要はありません。

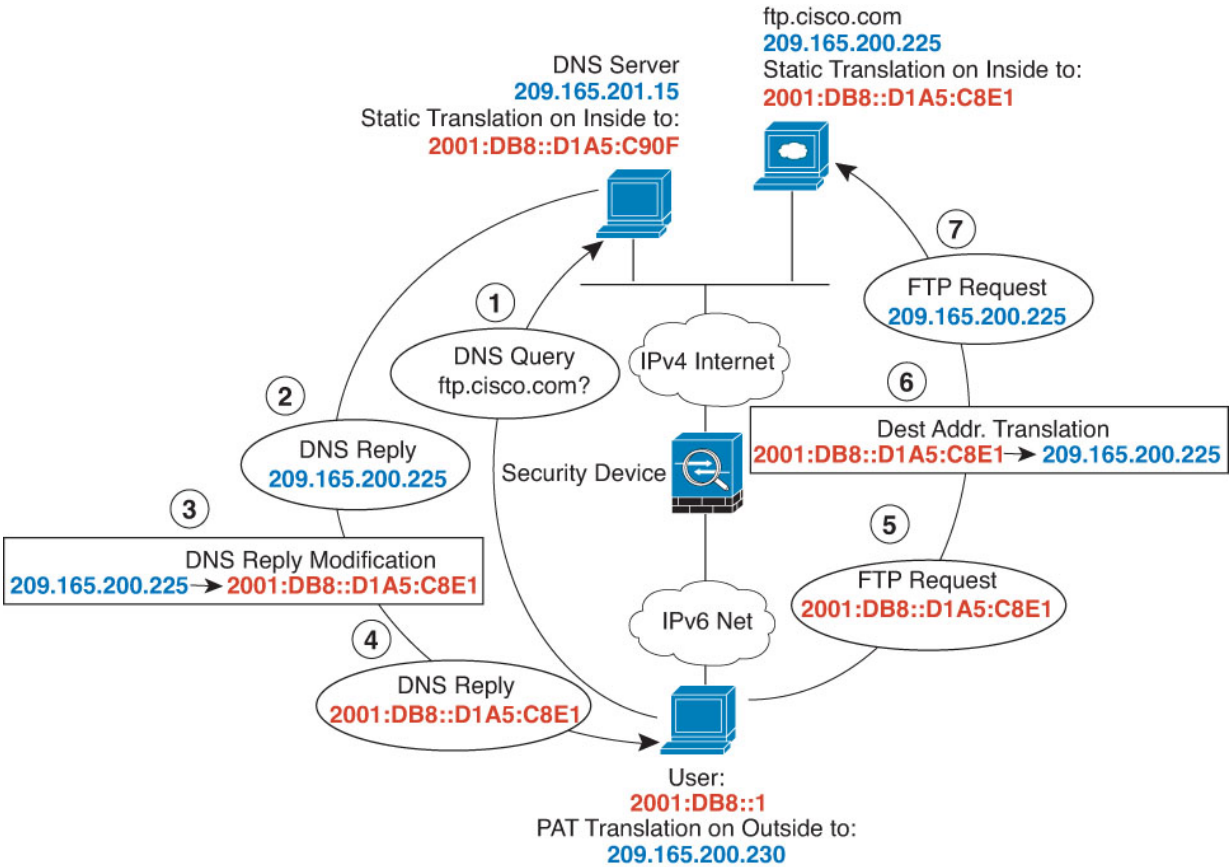
- 実際には、DNS 書き換えは NAT ルールではなく xlate エントリで実行されます。そのため、動的ルール用の xlate が存在しない場合は、書き換えを正しく実行できません。スタティック NAT では、同じ問題が発生しません。
- DNS 書き換えでは、DNS 動的更新メッセージ（opcode 5）が書き換えられません。

次のセクションでは、NAT ルール内の DNS 書き換えの例を示します。

DNS64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.200.225 を示します。

内部ユーザが ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1。D1A5:C8E1 は 209.165.200.225 と同等の IPv6 アドレス）を使用するようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

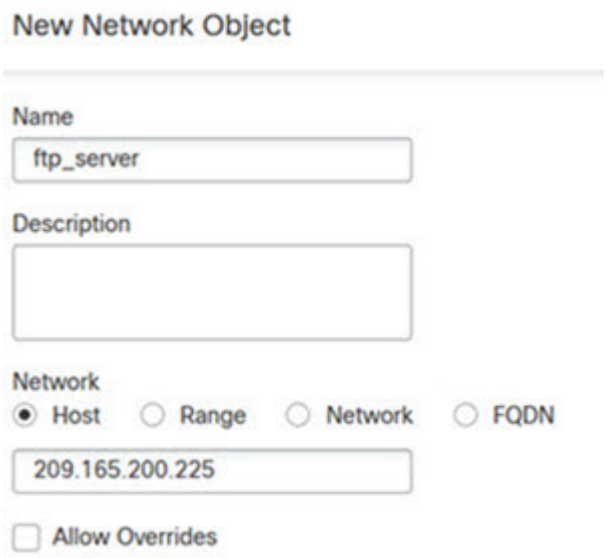
ステップ 1 FTP サーバー、DNS サーバー、内部ネットワーク、および PAT プールのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 実際の FTP サーバー アドレスを定義します。

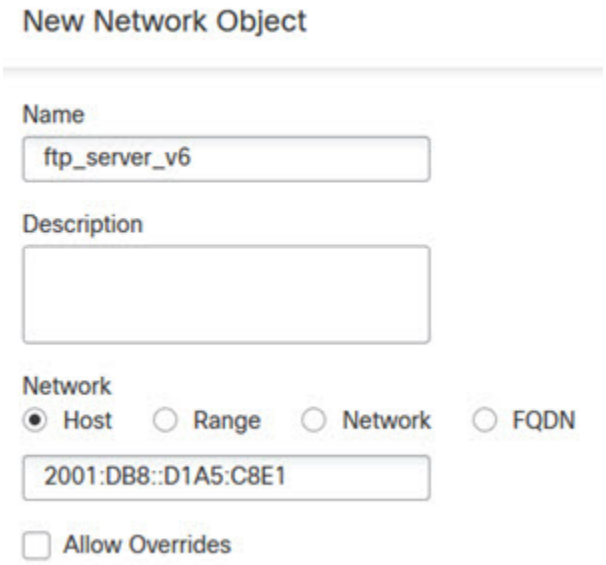
ネットワーク オブジェクトに名前を付け（ftp_server など）、ホスト アドレス 209.165.200.225 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、FTP サーバーの変換済み IPv6 アドレスを定義します。

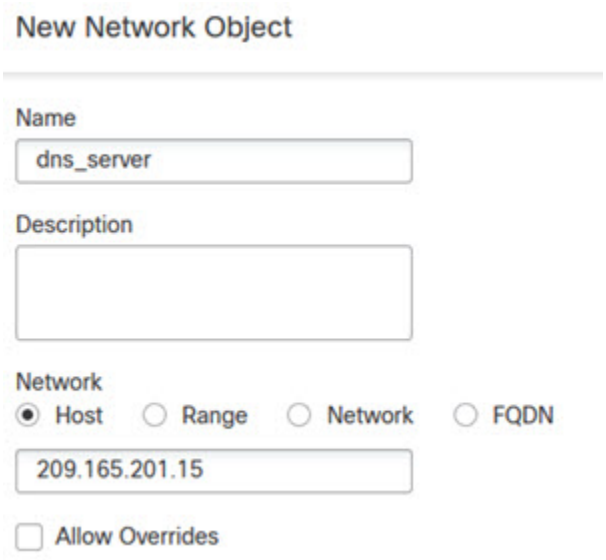
ネットワーク オブジェクトに名前を付け（ftp_server_v6 など）、ホスト アドレス 2001:DB8::D1A5:C8E1 を入力します。



f) [保存（Save）] をクリックします。

g) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、DNS サーバーの実際のアドレスを定義します。

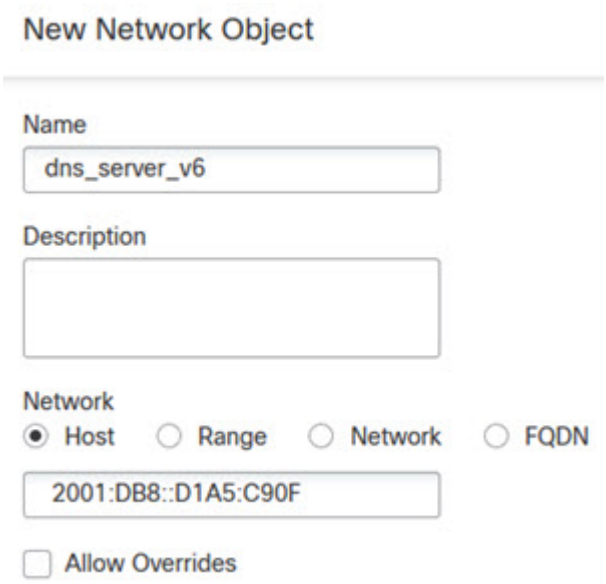
ネットワーク オブジェクトに名前を付け（dns_server など）、ホスト アドレス 209.165.201.15 を入力します。



h) [保存（Save）] をクリックします。

i) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、DNS サーバーの変換済み IPv6 アドレスを定義します。

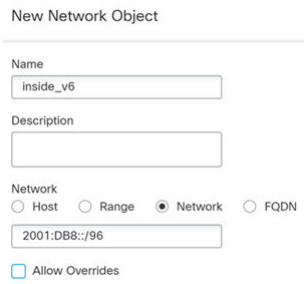
ネットワーク オブジェクトに名前を付け（dns_server_v6 など）、ホスト アドレス 2001:DB8::D1A5:C90F を入力します（ここで、D1A5:C90F は IPv6 の場合の 209.165.201.15 です）。



j) [保存（Save）] をクリックします。

k) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、内部 IPv6 ネットワークを定義します。

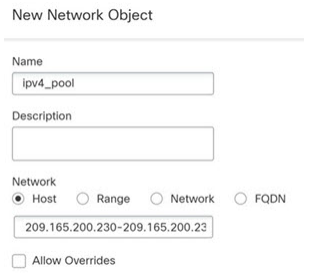
ネットワーク オブジェクトに名前（inside_v6 など）を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。



l) [保存（Save）] をクリックします。

m) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックし、内部 IPv6 ネットワークの IPv4 PAT プールを定義します。

ネットワーク オブジェクトに名前を付け（ipv4_pool など）、範囲 209.165.200.230 ～ 209.165.200.235 を入力します。



n) [保存（Save）] をクリックします。

ステップ 2 FTP サーバーのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

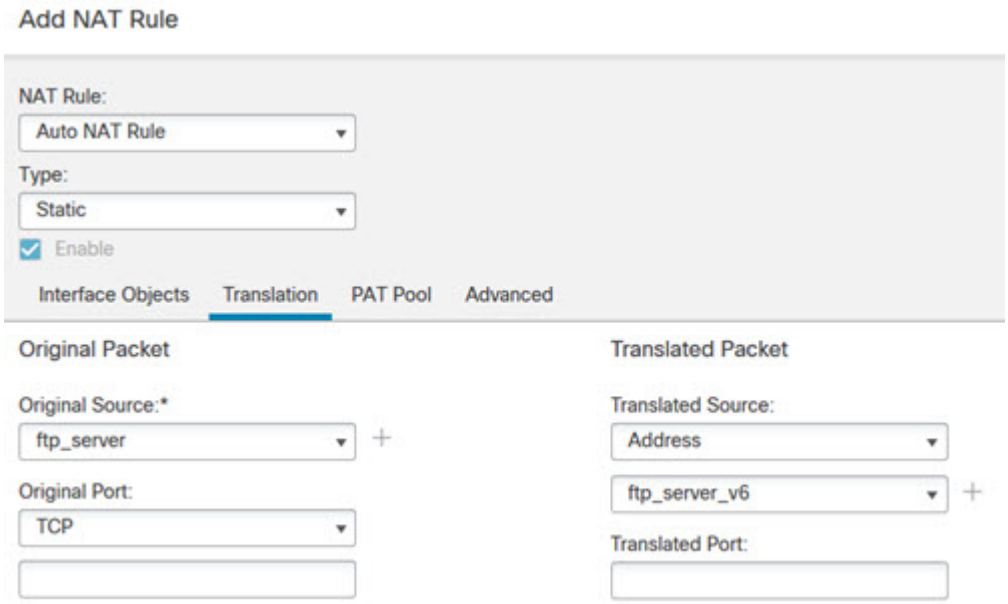
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = ftp_server ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]** = ftp_server_v6 ネットワークオブジェクト。



f) [詳細（Advanced）] で、以下のオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]。
- [ネット間マッピング（Net to Net Mapping）]。1 対 1 の NAT46 変換であるためです。

g) [OK] をクリックします。

ステップ 3 DNS サーバ用のスタティック NAT ルールを設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

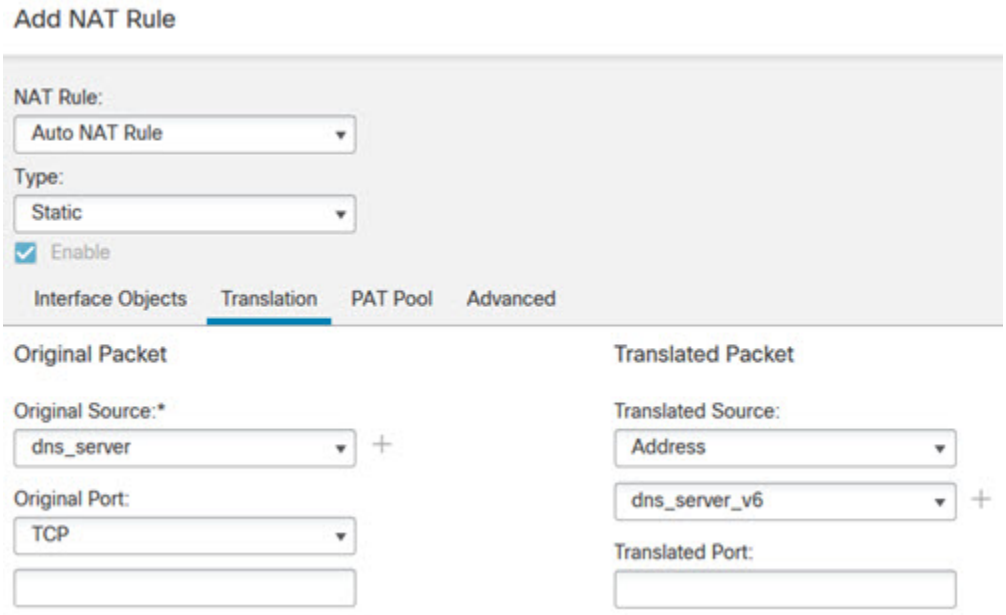
c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

d) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = dns_server ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]** = dns_server_v6 ネットワークオブジェクト。

e) これは 1 対 1 の NAT46 変換であるため、[詳細（Advanced）] で、[ネット間マッピング（Net to Net Mapping）] を選択します。



f) [OK] をクリックします。

ステップ 4 内部 IPv6 ネットワークに対し、PAT プール ルールを持つダイナミック NAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

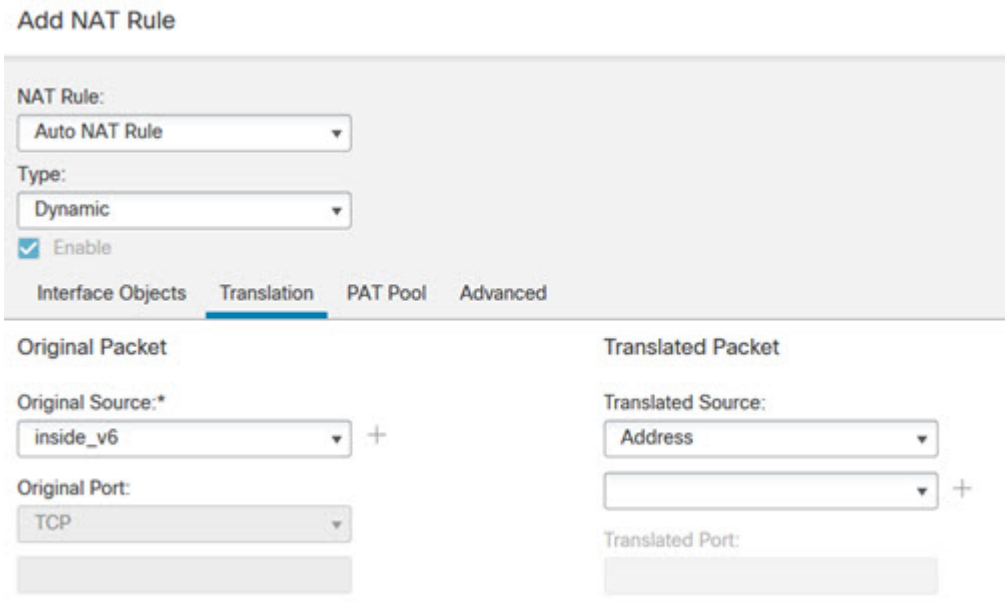
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

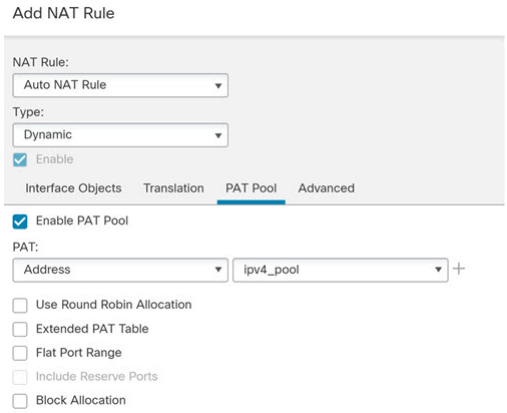
d) [変換（Translation）] で、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]** = このフィールドは空のままにします。



e) [PATプール（PAT Pool）] で、以下の設定を行います。

- [PAT プールの有効化（Enable PAT Pool）] = このオプションを選択します。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]** = ipv4_pool ネットワークオブジェクト。



f) **[OK]** をクリックします。

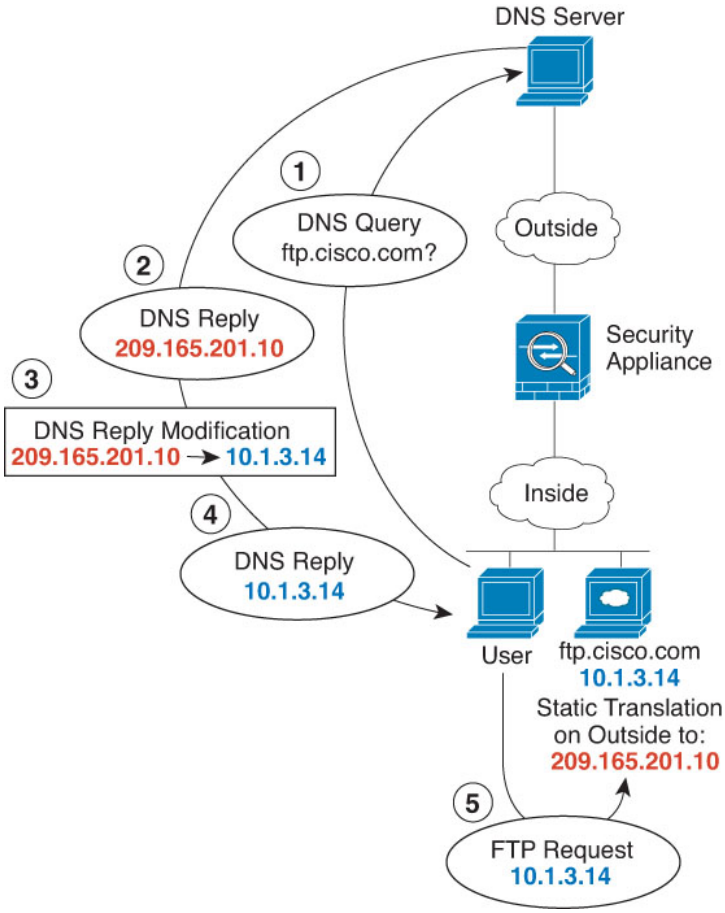
DNS 応答修正、外部の DNS サーバ

次の図に、外部インターフェイスからアクセス可能なDNSサーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）

を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、NAT を設定します。

この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト**

（**Objects**）] > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

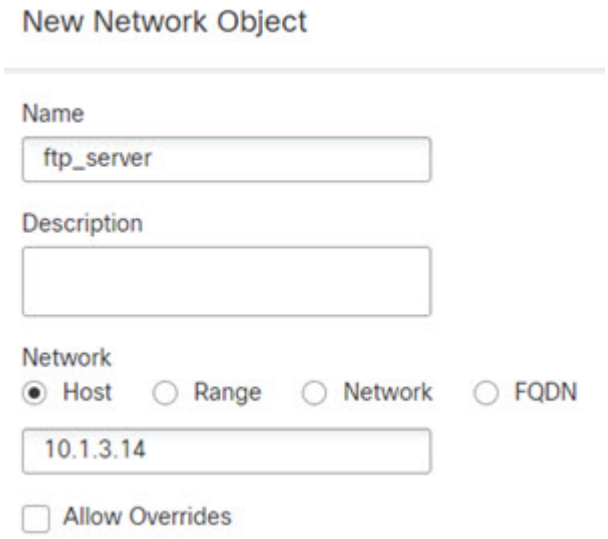
ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 実際の FTP サーバー アドレスを定義します。

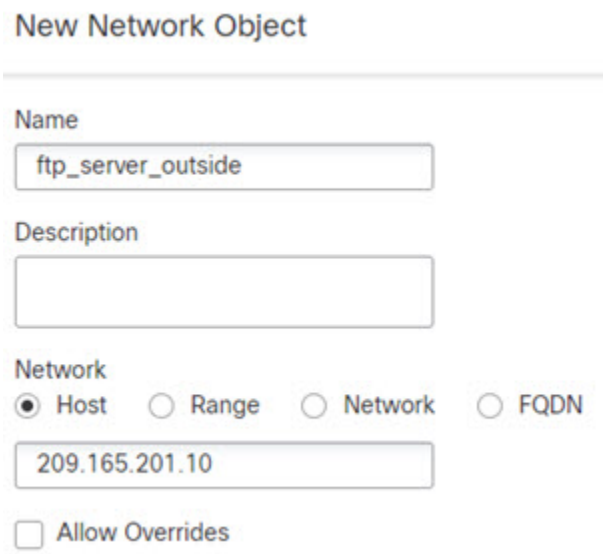
ネットワーク オブジェクトに名前を付け（ftp_server など）、ホスト アドレス 10.1.3.14 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、FTP サーバーの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け（ftp_server_outside など）、ホスト アドレス 209.165.201.10 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 FTP サーバーのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

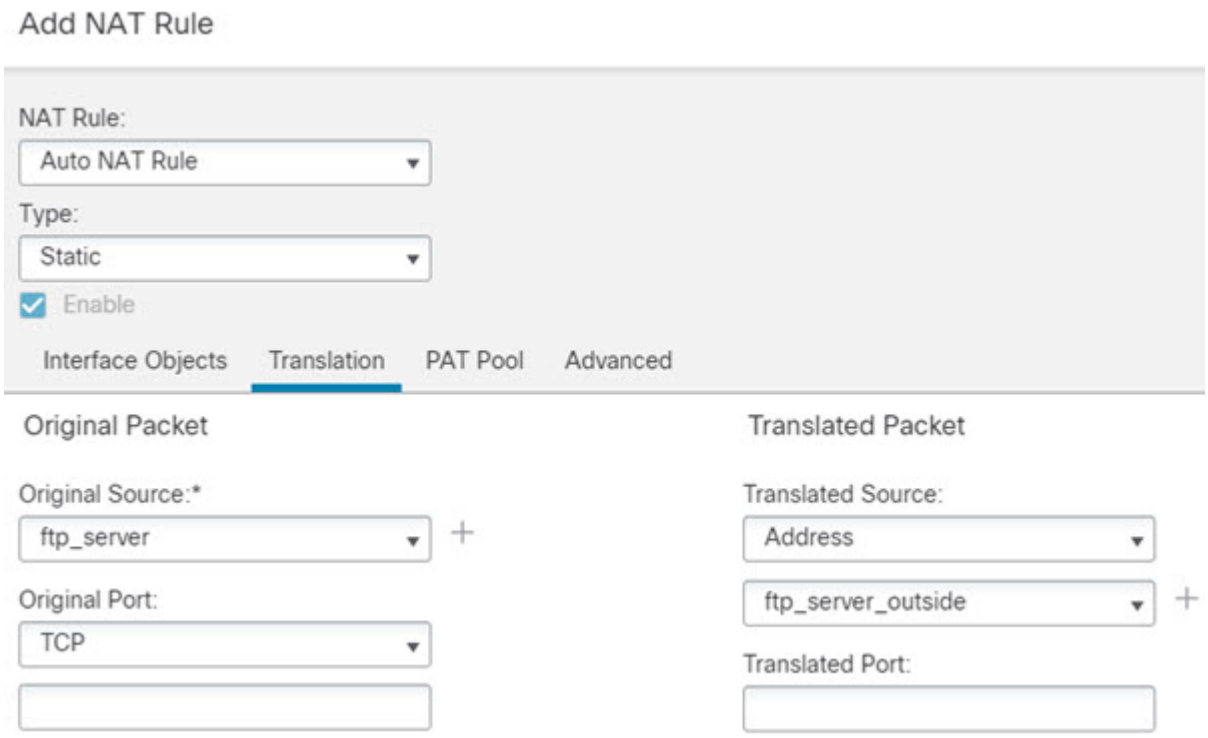
d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = ftp_server ネットワーク オブジェクト。
- **[変換済み送信元（Translated Source）] > [アドレス（Address）]** = ftp_server_outside ネットワークオブジェクト。

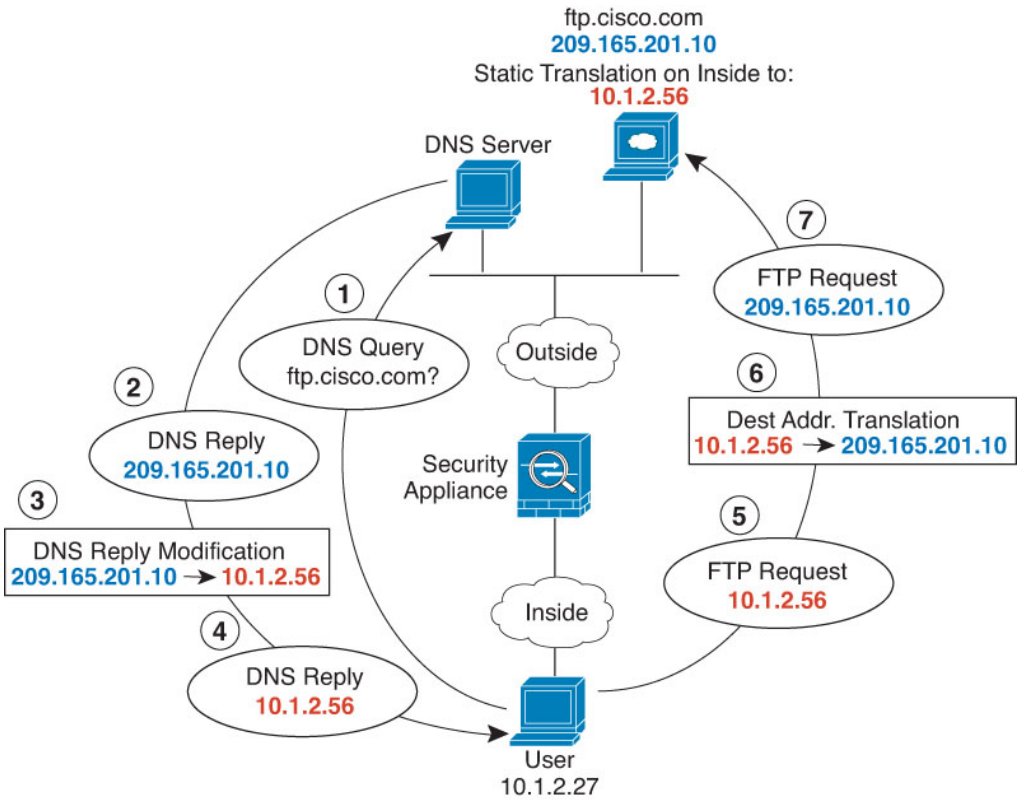
f) [詳細（Advanced）] で、[このルールと一致するDNS応答を変換（Translate DNS replies that match this rule）] を選択します。



g) **[OK]** をクリックします。

DNS 応答修正、ホスト ネットワーク上の DNS サーバ

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

手順

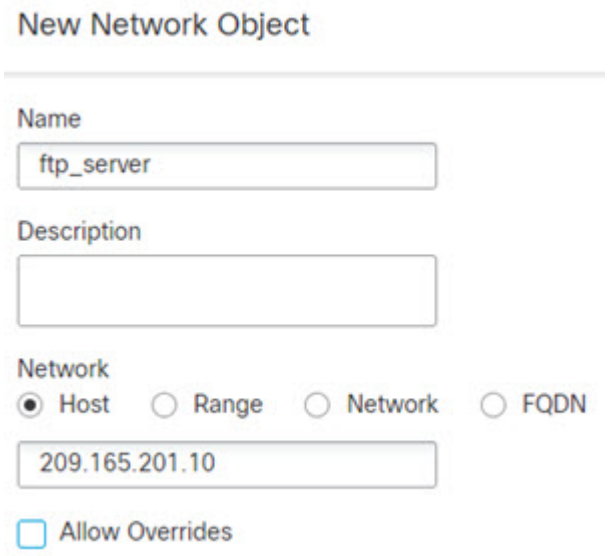
ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から [ネットワーク（Network）] を選択して、**[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 実際の FTP サーバー アドレスを定義します。

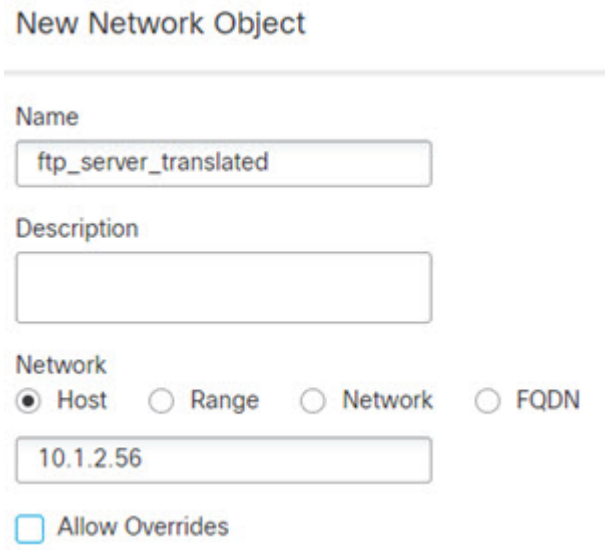
ネットワーク オブジェクトに名前を付け（ftp_server など）、ホスト アドレス 209.165.201.10 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、FTP サーバーの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け（ftp_server_translated など）、ホスト アドレス 10.1.2.56 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 FTP サーバーのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[デバイス（Devices）]** > **[NAT]** を選択し、Firewall Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

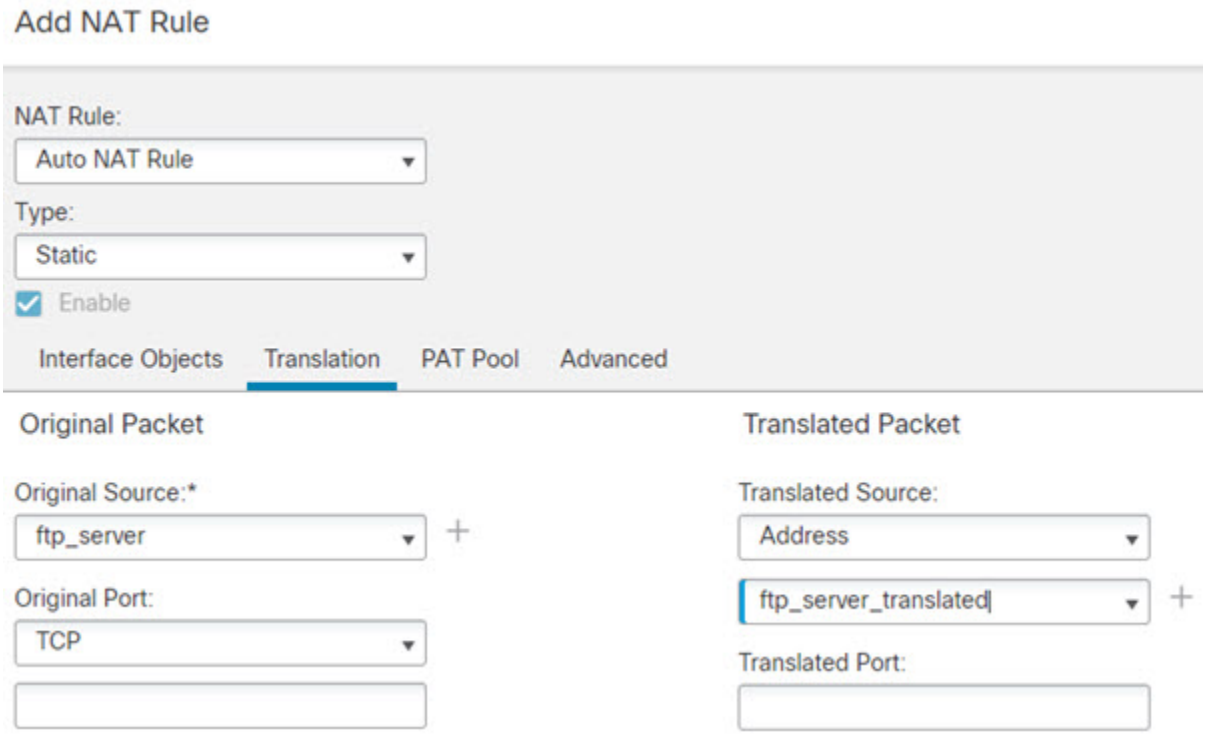
d) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

e) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = ftp_server ネットワーク オブジェクト。
- **[変換された送信元（Translated Source）]** > **[アドレス（Address）]** = ftp_server_translated ネットワークオブジェクト。

f) [詳細（Advanced）] で、[このルールと一致するDNS応答を変換（Translate DNS replies that match this rule）] を選択します。



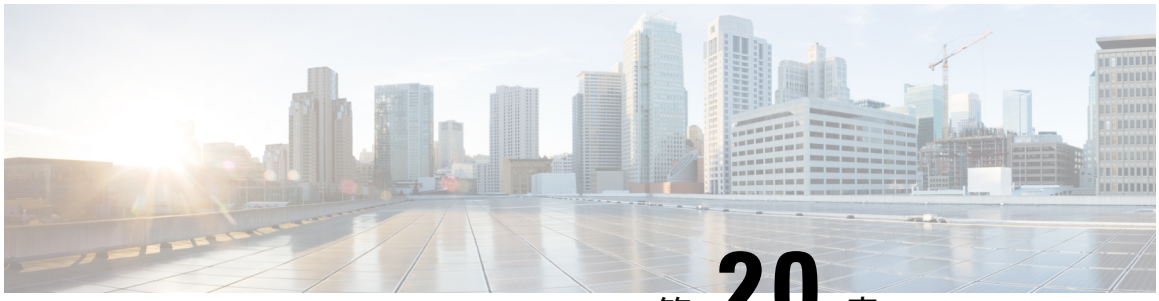
g) **[OK]** をクリックします。

Firewall Threat Defense NAT の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
一度に複数の NAT ルールの有効化、無効化、削除が可能。	7.2	任意（Any）	複数の NAT ルールを選択して、すべてを同時に有効化、無効化、または削除できます。有効化および無効化の対象は手動 NAT ルールのみです。削除はすべての NAT ルールが対象になります。
変換後の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの手動 NAT サポート。	7.1	任意（Any）	www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの [フラットなポート範囲（Flat Port Range）] オプションがデフォルトで有効になり、設定できなくなりました。	6.7	いずれか	PAT アドレスがクラスタのメンバーに配布される方法が変更されます。以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。制御ユニットは各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じ PAT アドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1023 ー 65535 を使用できるようになりました。以前は、[フラットなポート範囲（Flat Port Range）] オプションを PAT プールルールに含めることで、フラットな範囲をオプションで使用できました。[フラットなポート範囲（Flat Port Range）] オプションは無視され、PAT プールは常にフラットになります。必要に応じて [予約済みポートを含める（Include Reserved Ports）] オプションを選択して、PAT プールに 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（[ブロック割り当て（Block Allocation）] PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。
Firewall Threat Defense NAT ルールテーブルを検索およびフィルタリングする機能。	6.7	いずれか	Firewall Threat Defense NAT ポリシーでルールを検索して、IP アドレス、ポート、オブジェクト名などに基づいてルールを検索できるようになりました。検索結果には部分一致が含まれます。条件で検索すると、ルールテーブルがフィルタリングされ、一致するルールのみが表示されます。 Firewall Threat Defense NAT ポリシーを編集するときに、ルールテーブルの上に検索フィールドが追加されました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
キャリアグレードNATの拡張機能。	6.5	任意（Any）	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。 新規/変更された画面：[ブロック割り当て（Block Allocation）] オプションを Firewall Threat Defense の NAT ルールの [NAT PATプール（NAT PAT Pool）] タブに追加しました。
Firewall Threat Defense の NAT のネットワーク範囲のオブジェクトのサポート。	6.1.0	いずれか	Firewall Threat Defense NAT ルール内のネットワーク範囲のオブジェクトを必要に応じて使用できるようになりました。
Firewall Threat Defense のネットワークアドレス変換（NAT）。	6.0.1	いずれか	Firewall Threat Defense の NAT ポリシーが追加されました。 新規/変更された画面：Threat Defense が NAT ポリシーのタイプとして **[デバイス（Devices）]** > **[NAT]** ページに追加されました。



第 20 章

Cisco ISA 3000 のアラーム

Cisco ISA 3000 デバイスのアラーム システムを設定して、望ましくない状況になったときに警告することができます。

- アラームについて （1053 ページ）
- アラームのデフォルト設定 （1056 ページ）
- アラームの要件と前提条件 （1056 ページ）
- ISA 3000 のアラームの設定 （1057 ページ）
- アラームのモニタリング （1066 ページ）
- アラームの履歴 （1067 ページ）

アラームについて

さまざまな条件でアラームを発行するように ISA 3000 を設定できます。いずれかの条件が設定と一致しない場合、アラームがトリガーされます。これにより、LED、Syslog メッセージ、SNMP トラップによって、またアラーム出力インターフェイスに接続された外部デバイスを通じて、アラートがレポートされます。デフォルトでは、トリガーされたアラームにより Syslog メッセージだけが発行されます。

次のものをモニタするようにアラーム システムを設定できます。

- 電源装置
- プライマリおよびセカンダリ温度センサー
- アラーム入力インターフェイス

ISA 3000 には内部センサーに加えて 2 つのアラーム入力インターフェイスと 1 つのアラーム出力インターフェイスがあります。アラーム入力インターフェイスにはドアセンサーなどの外部センサーを接続できます。アラーム出力インターフェイスにはブザーやライトなどの外部アラーム デバイスを接続できます。

アラーム出力インターフェイスはリレーメカニズムです。アラーム状態に応じて、リレーは通電または非通電のいずれかの状態になります。リレーが通電状態になると、インターフェイスに接続されているデバイスがアクティブになります。リレーが非通電状態になると、接続され

ているデバイスが非アクティブ状態になります。アラームがトリガーされるかぎり、リレーは通電状態のままになります。

外部センサーとアラーム リレーの接続については、『Cisco ISA 3000 Industrial Security Appliance Hardware Installation Guide』を参照してください。

アラーム入力インターフェイス

アラーム入力インターフェイス（または接点）は外部センサー（ドアが開いているかどうかを検出するセンサーなど）に接続できます。

各アラーム入力インターフェイスには対応する LED があります。これらの LED は各アラーム入力のアラーム ステータスを示します。アラーム入力ごとにトリガーとシビラティ（重大度）を設定できます。LEDに加えて、出力リレーのトリガー（外部アラームをアクティブにするため）、Syslogメッセージの送信、およびSNMP トラップの送信を行うように接点を設定できます。

次の表に、アラーム入力のアラーム状態に応じたLEDのステータスを示します。また、アラーム入力に対する出力リレー、Syslogメッセージ、およびSNMP トラップの応答を有効にしている場合のそれらの動作も示します。

アラーム ステータス	LED	出力リレー	Syslog	SNMP トラップ
アラームが設定されていない	オフ	—	—	—
アラームがトリガーされていない	緑色で点灯	—	—	—
アラームがアクティブになっている	マイナー アラーム：赤色で点灯 メジャー アラーム：赤色で点滅	リレーが通電状態になる	Syslog が生成される	SNMP トラップが送信される
アラームが終了した	緑色で点灯	リレーが非通電状態になる	Syslog が生成される	—

アラーム出力インターフェイス

アラーム出力インターフェイスにはブザーやライトなどの外部アラームを接続できます。

アラーム出力インターフェイスはリレーとして機能します。また、このインターフェイスには、入力インターフェイスに接続された外部センサーや、デュアル電源センサー、温度センサーなどの内部センサーのアラーム ステータスを示す、対応するLEDがあります。出力リレーをアクティブにする必要があるアラームがある場合は、それを設定します。

次の表に、アラーム状態に応じた LED と出力リレーのステータスを示します。また、アラームに対する Syslog メッセージおよび SNMP トラップの応答を有効にしている場合のそれらの動作も示します。

アラーム ステータス	LED	出力リレー	Syslog	SNMP トラップ
アラームが設定されていない	オフ	—	—	—
アラームがトリガーされていない	緑色で点灯	—	—	—
アラームがアクティブになっている	赤色で点灯	リレーが通電状態になる	Syslog が生成される	SNMP トラップが送信される
アラームが終了した	緑色で点灯	リレーが非通電状態になる	Syslog が生成される	—

Syslog アラーム

デフォルトでは、アラームがトリガーされるとシステムは syslog メッセージを送信します。メッセージを送信しない場合は、syslog メッセージングを無効にすることができます。

syslog アラームを機能させるには、診断ロギングも有効にする必要があります。**[デバイス（Device）] > [プラットフォーム設定（Platform Settings）]**を選択し、デバイスに割り当てられる FTD プラットフォーム設定ポリシーを追加または編集して、[Syslog] ページで宛先と設定を構成します。syslog サーバー、コンソールロギング、または内部バッファロギングなどを設定できます。

診断ロギングの宛先を有効にしなければ、アラームシステムはどこにも syslog メッセージを送信しません。

SNMP アラーム

必要に応じて、SNMP トラップを SNMP サーバに送信するようにアラームを設定できます。SNMP トラップ アラームが機能するには、SNMP を設定する必要があります。

[デバイス（Device）] > [プラットフォーム設定（Platform Settings）] を選択して、デバイスに割り当てられている FTD プラットフォーム設定ポリシーを追加または編集し、[SNMP] ページで SNMP を有効にして設定を指定します。

アラームのデフォルト設定

次の表に、アラーム入力インターフェイス（コンタクト）、冗長電源、および温度のデフォルト設定を示します。

	アラーム	トリガー	シビラティ（重大度）	SNMP トラップ	出力リレー	Syslog メッセージ
アラーム コンタクト 1	[有効（Enabled）]	クローズ状態	マイナー	無効	無効	有効
アラーム コンタクト 2	[有効（Enabled）]	クローズ状態	マイナー	無効	無効	有効
冗長電源（有効な場合）	[有効（Enabled）]	—	—	無効	無効	有効
温度	プライマリ温度アラームで有効（高温/低温のデフォルトしきい値はそれぞれ 92°C および -40°C）。 セカンダリ アラームでは無効。	—	—	プライマリ温度アラームで有効	プライマリ温度アラームで有効	プライマリ温度アラームで有効

アラームの要件と前提条件

モデルのサポート

ISA 3000 上の Threat Defense 。

サポートされるドメイン

任意

ユーザの役割

管理者

ISA 3000 のアラームの設定

ISA 3000 のアラームを設定するには FlexConfig を使用します。ここでは、さまざまなタイプのアラームの設定方法について説明します。

アラーム入力コンタクトの設定

アラーム入力コンタクト（インターフェイス）を外部センサーに接続する場合、センサーからの入力に基づいてアラームを発行するようコンタクトを設定できます。実際には、デフォルトで、コンタクトはクローズ状態つまりコンタクトを流れる電流が停止すると syslog メッセージを送信するようになっています。デフォルトでは要件が満たされない場合にのみ、コンタクトを設定する必要があります。

アラーム コンタクトには 1 および 2 の番号が付いているため、正しく設定するためにどのように物理ピンを接続するのかを理解する必要があります。コンタクトを個別に設定します。

手順

ステップ 1 FlexConfig オブジェクトを作成して、アラーム入力コンタクトを設定します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から**[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]**を選択します。

c) [FlexConfigオブジェクトの追加（Add FlexConfig Object）] をクリックし、次のプロパティを設定して、[保存（Save）] をクリックします。

- [名前（Name）]：オブジェクト名。例：Configure_Alarm_Contacts。
- [展開（Deployment）]：[毎回（Everytime）] を選択します。この設定をすべての展開に送信し、設定されたままにする必要があります。
- [タイプ（Type）]：デフォルトの [後に付加（Append）] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
- [オブジェクト本文（Object body）]：オブジェクト本文に、アラームコンタクトの設定に必要なコマンドを入力します。次の手順では、コマンドについて説明します。

d) アラームコンタクトの説明を設定します。

alarm contact {**1** | **2**} **description** *string*

たとえば、コンタクト 1 の説明を「Door Open」に設定するには、次のように入力します。

```
alarm contact 1 description Door Open
```

e) アラームコンタクトの重大度を設定します。

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

1 つのコンタクトを設定する代わりに、**any** を指定してすべてのコンタクトの重大度を変更できます。重大度によって、コンタクトに関連付けられている LED の動作が制御されます。

- **major**：LED が赤色で点滅します。
- **minor**：LED が赤色で点灯します。これがデフォルトです。
- **none**：LED が消灯します。

たとえば、コンタクト 1 のシビラティ（重大度）をメジャーに設定するには、次のように入力します。

```
alarm contact 1 severity major
```

f) アラームコンタクトのトリガーを設定します。

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

1 つのコンタクトを設定する代わりに、**any** を指定してすべてのコンタクトのトリガーを変更できます。トリガーは、アラート信号を発する電気条件を決定します。

- **open**：コンタクトの通常状態はクローズです。つまり、コンタクトに電流が流れています。コンタクトがオープンになる、つまり電流が停止するとアラートがトリガーされます。
- **closed**：コンタクトの通常状態はオープンです。つまり、コンタクトに電流は流れていません。コンタクトがクローズになる、つまり電流がコンタクトを流れ始めるとアラートがトリガーされます。これはデフォルトです。

たとえば、ドア センサーをアラーム入力コンタクト 1 に接続して、通常状態ではアラーム コンタクトに電流は流れていない（オープン）とします。ドアが開くとコンタクトはクローズになり、アラーム コンタクトに電流が流れます。アラーム トリガーをクローズに設定しているため、電流が流れ始めたらアラームはオフになります。

```
alarm contact 1 trigger closed
```

g) アラームコンタクトがトリガーされるときに実行するアクションを設定します。

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー（relay）]：アラーム出力リレーに通電します。これにより、ブザーやフラッシュ ライトになどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog]：syslog メッセージを送信します。このオプションは、デフォルトで有効です。
- [通知（notifies）]：SNMP トラップを送信します。

たとえば、アラーム入力コンタクト 1 のすべてのアクションを有効にするには、次のように入力します。

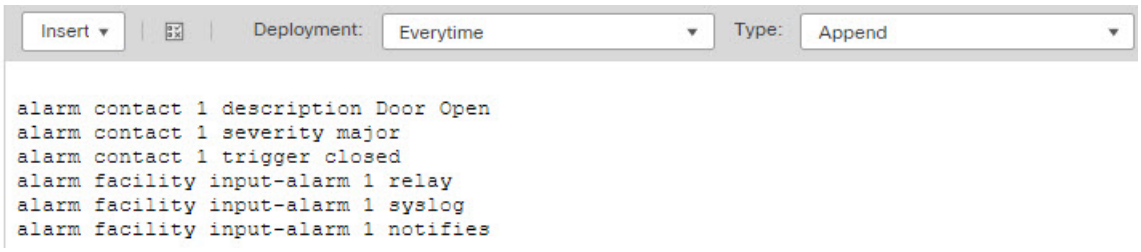
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

h) オブジェクト本文に必要なコマンドが含まれていることを確認します。

たとえば、この手順で示したすべてのコマンド例がテンプレートに含まれている場合、オブジェクト本文には次のコマンドが含まれます。

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

オブジェクト本文は、次のようになります。



i) [保存（Save）] をクリックします。

ステップ 2 FlexConfig ポリシーを作成し、デバイスに割り当てます。

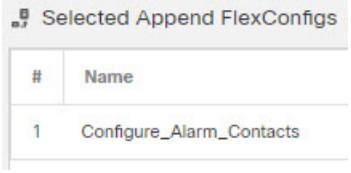
a) **[デバイス（Devices）]** > **[FlexConfig]** を選択します。

b) [新しいポリシー（New Policy）] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

c) 目次の [ユーザー定義（User Defined）] フォルダ内にあるアラームコンタクト FlexConfig オブジェクトを選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加FlexConfig（Selected Append FlexConfigs）] リストに追加されます。



d) **[保存（Save）]** をクリックします。

e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存（Save）] の下にある **[ポリシー割り当て（Policy Assignment）]** リンクをクリックし、ここで割り当てを行います。

f) [設定のプレビュー（Preview Config）] をクリックし、[プレビュー（Preview）] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。FlexConfig オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。アラームコンタクトコマンドについては、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

ステップ 3 変更を展開します。

FlexConfig ポリシーをデバイスに割り当てたため、展開に関する警告が常に表示されます。これは FlexConfig の使用方法に関する注意です。[続行（Proceed）] をクリックし、展開を続行します。

展開が完了したら、展開の履歴を確認し、展開のトランスクリプトを表示できます。これは展開に失敗した場合に特に役立ちます。「展開された構成の確認 （2725 ページ）」を参照してください。

電源装置アラームの設定

ISA 3000 には、電源装置が 2 台搭載されています。デフォルトでは、システムはシングル電源モードで稼働しています。ただし、デュアルモードでシステムを稼働するよう設定できます。その場合、プライマリ電源が故障すると 2 つ目の電源が自動的に電力を供給します。デュアルモードを有効にすると、電源アラームが自動的に有効になって syslog アラートが送信されますが、アラートを無効にしたり、SNMP トラップまたはアラーム ハードウェア リレーを有効にすることもできます。

次の手順では、デュアルモードを有効にする方法と電源アラームを設定する方法について説明します。

手順

ステップ 1 電源アラームを設定する FlexConfig オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から**[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]**を選択します。

c) [FlexConfigオブジェクトの追加（Add FlexConfig Object）] をクリックし、次のプロパティを設定して、[保存（Save）] をクリックします。

- [名前（Name）]：オブジェクト名。例：Power_Supply_Alarms。
- [展開（Deployment）]：[毎回（Everytime）] を選択します。この設定をすべての展開に送信し、設定されたままにする必要があります。
- [タイプ（Type）]：デフォルトの [後に付加（Append）] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
- [オブジェクト本文（Object body）]：オブジェクト本文に、電源アラームの設定に必要なコマンドを入力します。次の手順では、コマンドについて説明します。

d) デュアル電源モードを有効にします。

power-supply dual

次に例を示します。

```
power-supply dual
```

e) 電源アラームがトリガーされたときに実行するアクションを設定します。

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー（relay）]：アラーム出力リレーに通電します。これにより、ブザーやフラッシュ ライトになどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog]：syslog メッセージを送信します。このオプションは、デフォルトで有効です。
- [通知（notifies）]：SNMP トラップを送信します。
- [無効（disable）]：電源アラームを無効にします。電源アラームに設定されたその他のアクションは動作しなくなります。

たとえば、電源アラームのすべてのアクションを有効にするには、次のように入力します。

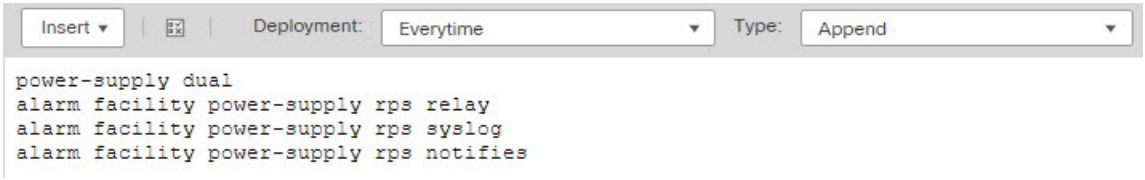
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

f) オブジェクト本文に必要なコマンドが含まれていることを確認します。

たとえば、この手順で示したすべてのコマンド例がテンプレートに含まれている場合、オブジェクト本文には次のコマンドが含まれます。

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

オブジェクト本文は、次のようになります。



g) [保存（Save）] をクリックします。

ステップ 2 FlexConfig ポリシーを作成し、デバイスに割り当てます。

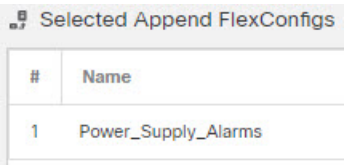
a) **[デバイス（Devices）]** > **[FlexConfig]** を選択します。

b) [新しいポリシー（New Policy）] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

c) 目次の [ユーザー定義（User Defined）] フォルダ内にある FlexConfig オブジェクトの電源アラームを選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加FlexConfig（Selected Append FlexConfigs）] リストに追加されます。



d) **[保存（Save）]** をクリックします。

e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存（Save）] の下にある **[ポリシー割り当て（Policy Assignment）]** リンクをクリックし、ここで割り当てを行います。

f) [設定のプレビュー（Preview Config）] をクリックし、[プレビュー（Preview）] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。FlexConfig オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。電源アラームコマンドの場合、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
```

```
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

ステップ 3 変更を展開します。

FlexConfig ポリシーをデバイスに割り当てたため、展開に関する警告が常に表示されます。これはFlexConfigの使用方法に関する注意です。[続行（Proceed）]をクリックし、展開を続行します。

展開が完了したら、展開の履歴を確認し、展開のトランスクリプトを表示できます。これは展開に失敗した場合に特に役立ちます。「展開された構成の確認（2725ページ）」を参照してください。

温度アラームの設定

デバイスの CPU カードの温度に基づいてアラームを設定できます。

プライマリ温度範囲とセカンダリ温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラーム アクション（出力リレー、syslog、および SNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40°C ～ 92°C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35°C ～ 85°C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温のいずれかを設定すると、プライマリ設定にデフォルト以外の値を設定していたとしても、対応するプライマリ設定はこの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

手順

ステップ 1 温度アラームを設定する FlexConfig オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) 目次から**[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]**を選択します。

c) [FlexConfigオブジェクトの追加（Add FlexConfig Object）] をクリックし、次のプロパティを設定して、[保存（Save）] をクリックします。

- [名前（Name）]：オブジェクト名。「Configure_Temperature_Alarms」などです。
- [展開（Deployment）]：[毎回（Everytime）] を選択します。この設定をすべての展開に送信し、設定されたままにする必要があります。

- [タイプ（Type）]：デフォルトの [後に付加（Append）] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
- [オブジェクト本文（Object body）]：オブジェクト本文に、温度アラームの設定に必要なコマンドを入力します。次の手順では、コマンドについて説明します。

d) 許容温度範囲を設定します。

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

温度は摂氏で示されます。プライマリ アラームの許容範囲は -40 ～ 92 で、これがデフォルト範囲でもあります。セカンダリ アラームの許容範囲は、-35 ～ 85 です。低い値は、高い値より小さくする必要があります。

たとえば、セカンダリ アラームの許容範囲内で、より制限された温度範囲の -20 ～ 80 を設定するには、次のようにセカンダリ アラームを設定します。

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

e) 温度アラームがトリガーされたときに実行するアクションを設定します。

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー（relay）]：アラーム出力リレーに通電します。これにより、ブザーやフラッシュ ライトになどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog]：syslog メッセージを送信します。
- [通知（notifies）]：SNMP トラップを送信します。

たとえば、セカンダリ温度アラームのすべてのアクションを有効にするには、次のように入力します。

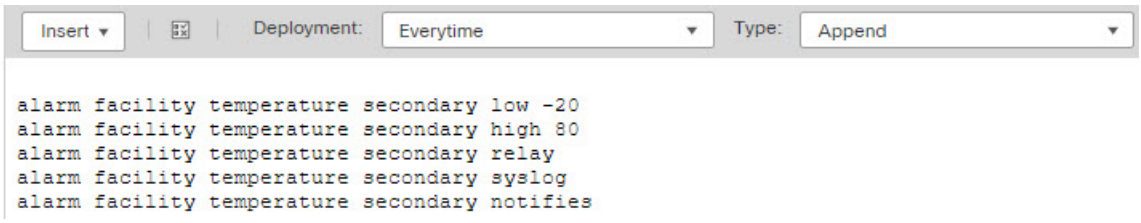
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

f) オブジェクト本文に必要なコマンドが含まれていることを確認します。

たとえば、この手順で示したすべてのコマンド例がテンプレートに含まれている場合、オブジェクト本文には次のコマンドが含まれます。

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

オブジェクト本文は、次のようになります。



g) [保存（Save）] をクリックします。

ステップ 2 FlexConfig ポリシーを作成し、デバイスに割り当てます。

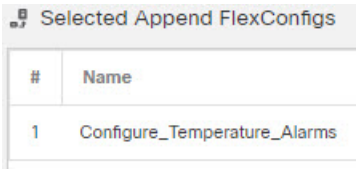
a) **[デバイス（Devices）] > [FlexConfig]** を選択します。

b) [新しいポリシー（New Policy）] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

c) 目次の [ユーザー定義（User Defined）] フォルダ内にある温度アラーム FlexConfig オブジェクトを選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加FlexConfig（Selected Append FlexConfigs）] リストに追加されます。



d) **[保存（Save）]** をクリックします。

e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存（Save）] の下にある **[ポリシー割り当て（Policy Assignment）]** リンクをクリックし、ここで割り当てを行います。

f) [設定のプレビュー（Preview Config）] をクリックし、[プレビュー（Preview）] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。FlexConfig オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。温度アラームコマンドについては、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

ステップ 3 変更を展開します。

FlexConfig ポリシーをデバイスに割り当てたため、展開に関する警告が常に表示されます。これは FlexConfig の使用方法に関する注意です。[続行（Proceed）] をクリックし、展開を続行します。

展開が完了したら、展開の履歴を確認し、展開のトランスクリプトを表示できます。これは展開に失敗した場合に特に役立ちます。「展開された構成の確認 （2725 ページ）」を参照してください。

アラームのモニタリング

ここでは、アラームのモニタおよび管理方法について説明します。

アラーム ステータスのモニタリング

CLI で次のコマンドを使用してアラームをモニタすることができます。

- **show alarm settings**

  使用可能な各アラームの現在の設定が表示されます。

- **show environment alarm-contact**

  入力アラーム コンタクトの物理ステータスに関する情報が表示されます。

- **show facility-alarm relay**

  出力リレーをトリガーしたアラームに関する情報が表示されます。

- **show facility-alarm status**[**info** |**major** |**minor**]

  トリガーされたすべてのアラームに関する情報が表示されます。**major** ステータスまたは **minor** ステータスでフィルタリングすることで表示の絞り込みができます。**info** キーワードを使用すると、キーワードを使用しない場合と同じ出力になります。

アラームに関する Syslog メッセージのモニタリング

設定するアラームのタイプに応じて、次の Syslog メッセージが表示される場合があります。

デュアル電源アラーム

- %FTD-1-735005：Power Supply Unit Redundancy OK
- %FTD-1-735006：Power Supply Unit Redundancy Lost

温度アラーム

これらのアラームでは、*Celsius* は、デバイス上で検出された温度（摂氏単位）に置き換えられます。

- %FTD-6-806001：Primary alarm CPU temperature is High *Celsius*
- %FTD-6-806002：Primary alarm for CPU high temperature is cleared
- %FTD-6-806003：Primary alarm CPU temperature is Low *Celsius*
- %FTD-6-806004：Primary alarm for CPU Low temperature is cleared
- %FTD-6-806005：Secondary alarm CPU temperature is High *Celsius*
- %FTD-6-806006：Secondary alarm for CPU high temperature is cleared
- %FTD-6-806007：Secondary alarm CPU temperature is Low *Celsius*
- %FTD-6-806008：Secondary alarm for CPU Low temperature is cleared

アラーム入力コンタクトアラーム

これらのアラームでは、「*description*」は、設定したコンタクトの説明です。

- %FTD-6-806009：Alarm asserted for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806010：Alarm cleared for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806011：Alarm asserted for ALARM_IN_2 *alarm_2_description*
- %FTD-6-806012: Alarm cleared for ALARM_IN_2 *alarm_2_description*

外部アラームをオフにする

アラーム出力にアタッチされる外部アラームを使用していて、アラームがトリガーされる場合、**clear facility-alarm output** コマンドを使用してデバイス CLI から外部アラームをオフにできます。このコマンドは、出力ピンの電源を切り、出力 LED もオフにします。

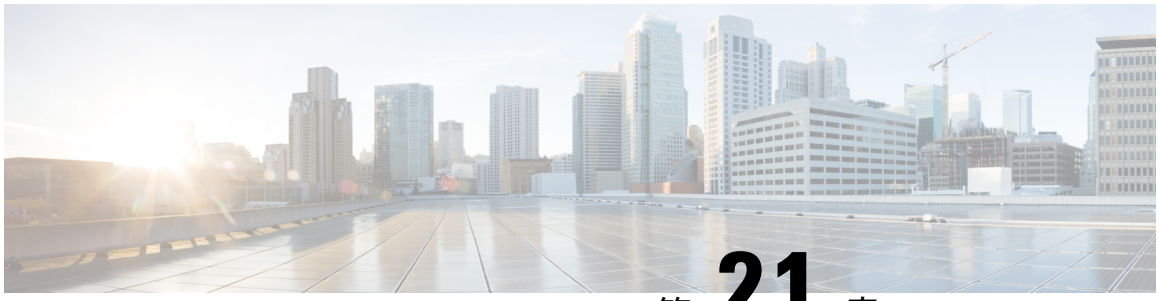
アラームの履歴

特長	最小 Firewall Management Center	最小 Firewall Threat Defense	説明
Cisco ISA 3000 シリーズのアラーム	6.7	いずれか	Cisco ISA 3000 シリーズのアラームの設定は、FlexConfig を使用して検証されました。デュアル電源アラームを除き、FlexConfig をサポートする古いリリースのアラームを設定できます。 サポートされているプラットフォーム：ISA 3000 の Secure Firewall Threat Defense。

第 IV 部

ルーティング

- スタティック ルートとデフォルト ルート （1071 ページ）
- 仮想ルータ （1091 ページ）
- ECMP （1153 ページ）
- 双方向フォワーディング検出ルーティング （1163 ページ）
- Open Shortest Path First（OSPF） （1169 ページ）
- EIGRP （1205 ページ）
- BGP （1219 ページ）
- RIP （1243 ページ）
- マルチキャスト （1251 ページ）
- ポリシーベースルーティング （1275 ページ）



第 21 章

スタティック ルートとデフォルト ルート

この章では、Firewall Threat Defense でスタティック ルートとデフォルト ルートを設定する方法について説明します。

- スタティック ルートとデフォルト ルートについて （1071 ページ）
- スタティックルートの要件と前提条件 （1074 ページ）
- スタティック ルートとデフォルト ルートのガイドライン （1075 ページ）
- スタティック ルートの追加 （1075 ページ）
- ルーティングのリファレンス （1077 ページ）

スタティック ルートとデフォルト ルートについて

接続されていないホストやネットワークにトラフィックをルーティングするには、スタティックルーティングまたはダイナミックルーティングを使用して、ホストまたはネットワークへのルートを定義する必要があります。通常は、少なくとも 1 つのスタティック ルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルト ルート（通常、ネクスト ホップ ルータ）を設定する必要があります。

デフォルトルート

最も単純なオプションは、すべてのトラフィックをアップストリームルータに送信するようにデフォルトスタティックルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、Firewall Threat Defense デバイスが送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0（IPv4）または ::/0（IPv6）が指定されたスタティック ルートのことです。

デフォルト ルートを常に定義する必要があります。

Firewall Threat Defense はデータトラフィックと管理トラフィックに個別のルーティングテーブルを使用するため、必要に応じて、データトラフィック用のデフォルトルートと管理トラフィック用の別のデフォルトルートを設定できます。デバイス間トラフィックでは、タイプに応じてデフォルトで管理専用またはデータルーティングテーブルが使用されます(管理トラフィック

用ルーティングテーブル（1087ページ）を参照)。ただし、ルートが見つからない場合は、他のルーティングテーブルにフォールバックします。デフォルトルートは常にトラフィックに一致するため、他のルーティングテーブルへのフォールバックが妨げられます。この場合、インターフェイスがデフォルトのルーティングテーブルになければ、出力トラフィックに使用するインターフェイスを指定する必要があります。診断インターフェイスは、管理専用テーブルに含まれています。特別な管理インターフェイスは、個別のLinuxルーティングテーブルを使用し、独自のデフォルトルートを持ちます。**configure network**コマンドを参照してください。

スタティック ルート

次の場合は、スタティックルートを使用します。

- ネットワークでサポートされていないルータ検出プロトコルが使用されている。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- デフォルトルートでは十分でない場合がある。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルトルートは、Firewall Threat Defense デバイスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。
- 仮想ルータは、スタティックルートを使用してルートリークを作成します。ルートリークは、仮想ルータのインターフェイスから別の仮想ルータ内の別のインターフェイスへのトラフィックフローを可能にします。詳細については、「仮想ルータの相互接続（1094ページ）」を参照してください。

不要なトラフィックをドロップするための null0 インターフェイスへのルート

アクセスルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセス ルールを補完するソリューションです。null0 ルートを使用して不要なトラフィックや望ましくないトラフィックを転送することで、トラフィックをドロップできます。

スタティック null0 ルートには、推奨パフォーマンス プロファイルが割り当てられます。また、スタティック null0 ルートを使用して、ルーティング ループを回避することもできます。BGP では、リモート トリガ型ブラック ホール ルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブ ディスタンスによってプライオリティが決まります。スタティック ルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。
- 宛先かつアドミニストレーティブ ディスタンスが同じスタティック ルートが複数存在する場合は、Equal-Cost Multipath（ECMP）ルーティング （1088 ページ）を参照してください。
- [トンネル化（Tunneled）] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルト ルートをすべてオーバーライドします。

トランスペアレント ファイアウォール モードおよびブリッジ グループのルート

ブリッジ グループ メンバー インターフェイスを通じて直接には接続されていないネットワークに向かう Firewall Threat Defense デバイス で発信されるトラフィックの場合、Firewall Threat Defense デバイス がどのブリッジ グループ メンバー インターフェイスからトラフィックを送信するかを認識するように、デフォルト ルートまたはスタティック ルートを設定する必要があります。Firewall Threat Defense デバイス で発信されるトラフィックには、syslog サーバーまたは SNMP サーバーへの通信が含まれることもあります。1 つのデフォルト ルートで到達できないサーバーがある場合、スタティック ルートを設定する必要があります。トランスペアレント モードの場合、ゲートウェイ インターフェイスに BVI を指定できません。メンバー インターフェイスのみが使用できます。ルーテッド モードのブリッジ グループの場合、スタティック ルートに BVI を指定する必要があります。メンバー インターフェイスを指定することはできません。詳細については、MAC アドレスとルート ルックアップ （205 ページ）を参照してください。

スタティック ルート トラッキング

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、Firewall Threat Defense デバイス 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。

Firewall Threat Defense デバイス では、Firewall Threat Defense デバイス が ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象スタティック ルートを関連付けることでスタティック ルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象がICMPエコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクストホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- Firewall Threat Defense デバイス が通信を行う必要のある対象ネットワーク上のサーバー（syslog サーバーなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト

（注） 夜間にシャットダウンする PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルト ルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけを有効化することができます。

スタティックルートの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

スタティック ルートとデフォルト ルートのガイドライン

ファイアウォール モードとブリッジ グループ

- トランスペアレント モードでは、スタティック ルートはブリッジ グループ メンバー インターフェイスをゲートウェイとして使用する必要があります。BVI を指定することはできません。
- ルーテッドモードでは、BVI をゲートウェイとして指定する必要があります。メンバーインターフェイスは指定できません。
- スタティック ルート トラッキングは、ブリッジ グループ メンバー インターフェイスまたは BVI ではサポートされません。

サポートされるネットワークアドレス

- IPv6 では、スタティック ルート トラッキングはサポートされません。
- Firewall Threat Defense はクラス E ルーティングをサポートしていないため、クラス E ネットワークはスタティックルートでルーティングできません。

クラスタリング

- クラスタリングでは、スタティック ルート トラッキングはコントロールノードでのみサポートされます。

ネットワーク オブジェクト グループ

スタティックルートの設定時は、ネットワークオブジェクトの範囲や IP アドレス範囲を持つネットワーク オブジェクト グループは使用できません。

ASP および RIB ルートエントリ

デバイスにインストールされているすべてのルートとその距離は、ASP ルーティングテーブルにキャプチャされます。これは、すべての静的および動的ルーティングプロトコルに共通です。最適な距離のルートのみが RIB テーブルにキャプチャされます。

スタティック ルートの追加

スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。少なくともデフォルト ルートを定義する必要があります。デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。

冗長マネージャ アクセス データ インターフェイスのルートを設定するには、冗長マネージャ アクセス用データインターフェイスの設定 （66 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （必要に応じて）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、スタティック ルートを設定する仮想ルータを選択します。

ステップ 4 [スタティックルート（Static Route）] を選択します。

ステップ 5 [ルートを追加（Add Routes）] をクリックします。

ステップ 6 追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] をクリックします。

ステップ 7 このスタティック ルートを適用する [インターフェイス（Interface）] を選択します。

トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を選択します。ブリッジ グループによるルーティング モードの場合、BVI 名として、いずれかのブリッジグループ メンバーインターフェイスを選択できます。不要なトラフィックを「ブラック ホール化」するには、**Null0** インターフェイスを選択します。

仮想ルーティングを使用するデバイスの場合は、別の仮想ルータに属するインターフェイスを選択できます。このようなスタティックルートは、この仮想ルータから他の仮想ルータにトラフィックをリークする場合に作成できます。詳細については、「仮想ルータの相互接続 （1094 ページ）」を参照してください。

ステップ 8 [利用可能なネットワーク（Available Network）] リストで、宛先ネットワークを選択します。

デフォルト ルートを定義するには、アドレス 0.0.0.0/0 のオブジェクトを作成し、ここでそれを選択します。

（注）
IP アドレス範囲を持つネットワーク オブジェクト グループを作成および選択できますが、Firewall Management Center ではスタティックルートでの範囲の使用はサポートされていません。

ステップ 9 [ゲートウェイ（Gateway）] または [IPv6 ゲートウェイ（IPv6 Gateway）] フィールドで、このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホスト オブジェクトを指定できます。

仮想ルータのスタティックルート構成を使用してルートをリークする場合は、ネクストホップのゲートウェイを指定しないでください。

ステップ 10 [メトリック（Metric）] フィールドに、宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。

メトリックは、特定のホストが存在するネットワークへのホップ数（ホップ カウント）に基づくルートの「コスト」を示す測定値です。ホップ カウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。メトリックは、複数のルーティング プロトコル間でルートを比較するために使用

されます。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 11 （任意）デフォルト ルートの場合は、[トンネル型（Tunneled）] チェックボックスをオンにして、VPN トラフィック用に別個のデフォルト ルートを定義します。

VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。[トンネル型（tunneled）] オプションを使用してデフォルト ルートを作成すると、デバイスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。設定できるデフォルトのトンネル ゲートウェイは、デバイスごとに 1 つのみです。トンネル トラフィックの ECMP はサポートされません。

ステップ 12 （IPv4 スタティック ルートのみ）ルートの可用性をモニタするには、モニタリング ポリシーを定義する SLA（サービス レベル契約）モニタ オブジェクトの名前を [ルート トラッキング（Route Tracking）] フィールドで入力または選択します。

SLA モニタ （1399 ページ）を参照してください。

ステップ 13 [OK] をクリックします。

ルーティングのリファレンス

ここでは、Firewall Threat Defense 内でのルーティング動作の基本概念について説明します。

パスの決定

ルーティング プロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティング アルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティング アルゴリズムは、ルート情報が格納されるルーティング テーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティング アルゴリズムにより、さまざまな情報がルーティング テーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できるこ

とがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティング テーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティング テーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデートを他のすべてのルータから分析することで、ルータはネットワーク トポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう 1 つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワーク トポロジの全体像の構築に使用できます。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。Firewall Threat Defense デバイス では、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティック ルーティング アルゴリズムは、実はネットワーク管理者が確立したテーブル マップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラストリゾートルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして

機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティング プロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパス アルゴリズムとは異なり、これらのマルチパス アルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパスアルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティングアルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラット ルーティング システムでは、ルータは他のすべてのルータのピアになります。階層型ルーティング システムでは、一部のルータが実質的なルーティング バックボーンを形成します。バックボーン以外のルータからのパケットはバックボーン ルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーン ルータから、1 つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティング システムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティング バックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織を模倣しているため、そのトラフィック パターンを適切にサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティングアルゴリズムを簡素化できます。また、使用しているルーティングアルゴリズムに応じて、ルーティングアップデートトラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステートアルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティング テーブルの一部だけを送信します。リンクステート アルゴリズムでは、各ルータはネットワークの全体像をそのルーティング テーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティングテーブル全体または一部を送信するように要求されます。つまり、リンクステートアルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステート アルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ルーティングでサポートされるインターネット プロトコル

Firewall Threat Defense デバイス は、ルーティングに対してさまざまなインターネット プロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol（EIGRP）

  EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First（OSPF）

  OSPF は、インターネット プロトコル（IP）ネットワーク向けに、インターネット技術特別調査委員会（IETF）の Interior Gateway Protocol（IGP）作業部会によって開発されたルーティング プロトコルです。OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- Routing Information Protocol（RIP）

  RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル プロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol（IGP）です。つまり、1 つの自律システム内部でルーティングを実行します。

- ボーダー ゲートウェイ プロトコル（BGP）

  BGP は自律システム間のルーティング プロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。カスタマーはISPに接続し、ISPはBGPを使用してカスタマーおよび ISPルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービスプロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

ルーティングテーブル

Firewall Threat Defense はデータ トラフィック（デバイスを介して）および管理トラフィック（デバイスから）に別々のルーティングテーブルを使用します。ここでは、ルーティングテーブルの仕組みについて説明します。管理ルーティング テーブルの詳細については、管理トラフィック用ルーティングテーブル （1087 ページ）も参照してください。

ルーティング テーブルへの入力方法

Firewall Threat Defense ルーティングテーブルには、静的に定義されたルート、直接接続されているルート、およびダイナミック ルーティング プロトコルで検出されたルートを入力できます。Firewall Threat Defense デバイスは、ルーティングテーブルに含まれるスタティックルート

と接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

  たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- Firewall Threat Defense デバイスが、（RIP などの）1 つのルーティングプロトコルから同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティングテーブルに入力されます。

  メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックスの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

- Firewall Threat Defense デバイスが、ある宛先へのルーティングプロトコルが複数あることを検知すると、ルートのアドミニストレーティブディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティングテーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティング プロトコルによって検出されるルート、またはルーティング プロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2 つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブディスタンスが同じ場合、デフォルトのアドミニストレーティブディスタンスが小さい方のルートがルーティングテーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、Firewall Threat Defense デバイスが最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティングプロトコルによって生成された同じ宛先への2つのルートのいずれが最適パスであるかは、必ずしも判別できません。

各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。次の表に、Firewall Threat Defense デバイスでサポートされているルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス値を示します。

表 *64*：サポートされるルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス

ルートの送信元	デフォルトのアドミニストレーティブディスタンス
接続されているインターフェイス	0
VPN ルート	1
スタティック ルート	1
EIGRP集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカルBGP	200
不明	255

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、Firewall Threat Defense デバイスが OSPF ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 110）と RIP ルーティング プロセス（デフォルトのアドミニストレーティブディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティング プロセスの方が優先度が高いため、Firewall Threat Defense デバイスは OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティング テーブルに追加します。

VPN アドバタイズされたルート（V-Route/RRI）は、デフォルトのアドミニストレーティブ ディスタンス 1 のスタティックルートと同等です。ただし、ネットワークマスク 255.255.255.255 の場合と同じように優先度が高くなります。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、Firewall Threat Defense デバイスは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブ ディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された Firewall Threat Defense デバイス のルーティング テーブルにだけ影響します。ア

ドミニストレーティブ ディスタンスがルーティング アップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。ルーティング プロセスは、ルーティング プロセスで検出されたか、またはルーティング プロセスに再配布されたルートだけをアドバタイズします。たとえば、RIPルーティングプロセスは、のルーティング テーブルで OSPF ルーティング プロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミック ルーロとフローティング スタティック ルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップ ルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティング スタティック ルートを作成できます。フローティングスタティックルートとは、単に、Firewall Threat Defense デバイスで動作しているダイナミックルーティングプロトコルよりも大きなアドミニストレーティブディスタンスが設定されているスタティックルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先がルーティングテーブル内の複数のエントリと一致した場合は、パケットが、ネットワーク プレフィックス長がより長いルートに関連付けられたインターフェイスから転送されます。

たとえば、192.168.32.1宛てのパケットが、ルーティングテーブルの次のルートでインターフェイスに到着するとします。

- 192.168.32.0/24 ゲートウェイ 10.1.1.2
- 192.168.32.0/19 ゲートウェイ 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワーク内にあるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。もうひとつのルートにもあてはまりますが、192.168.32.0/24 の方が長いプレフィックスを持つためです（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先される。

（注） 既存の接続は、新しい同様の接続がルートの変更により異なる動作になる場合でも、引き続き確立されたインターフェイスを使用します。

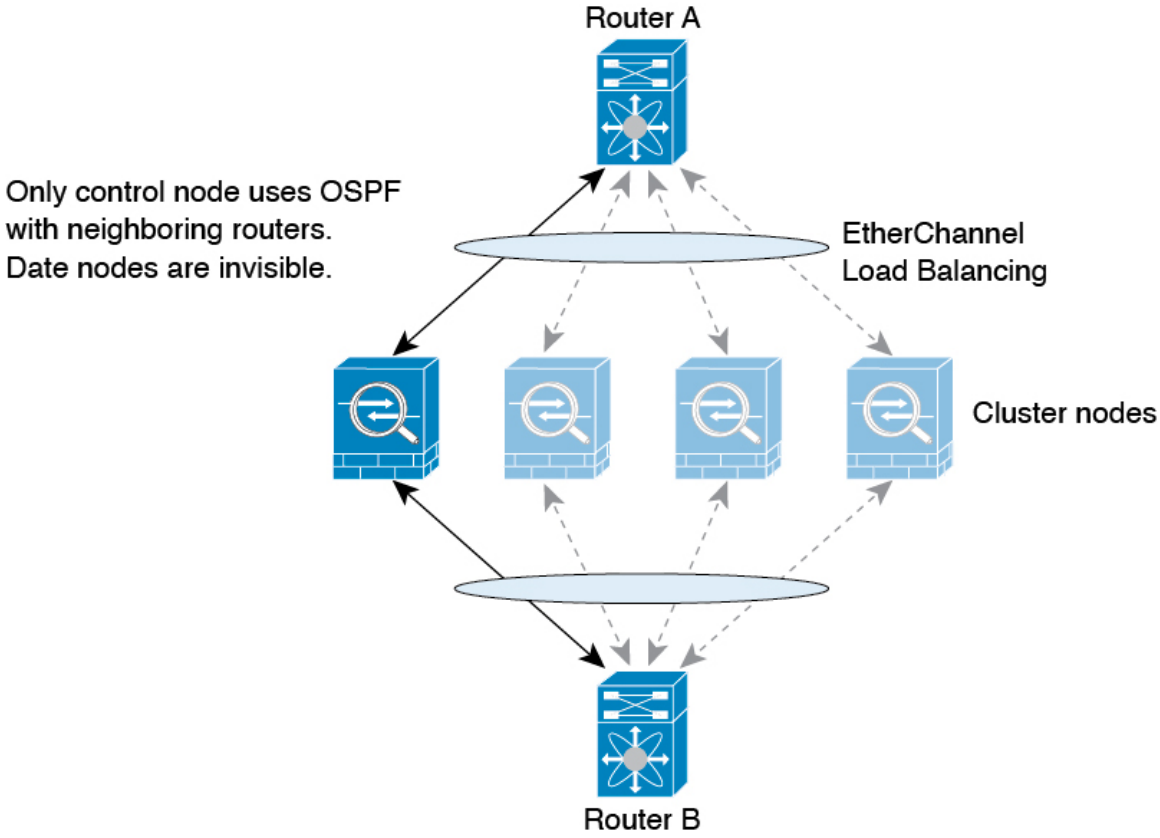
ダイナミック ルーティングおよび 高可用性

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 高可用性 ペアでアクティブになると、ルートは 高可用性 バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

クラスタリングでのダイナミック ルーティング

ルーティングプロセスは制御ノード上だけで実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 *288* : スパンド *EtherChannel* モードでのダイナミック ルーティング



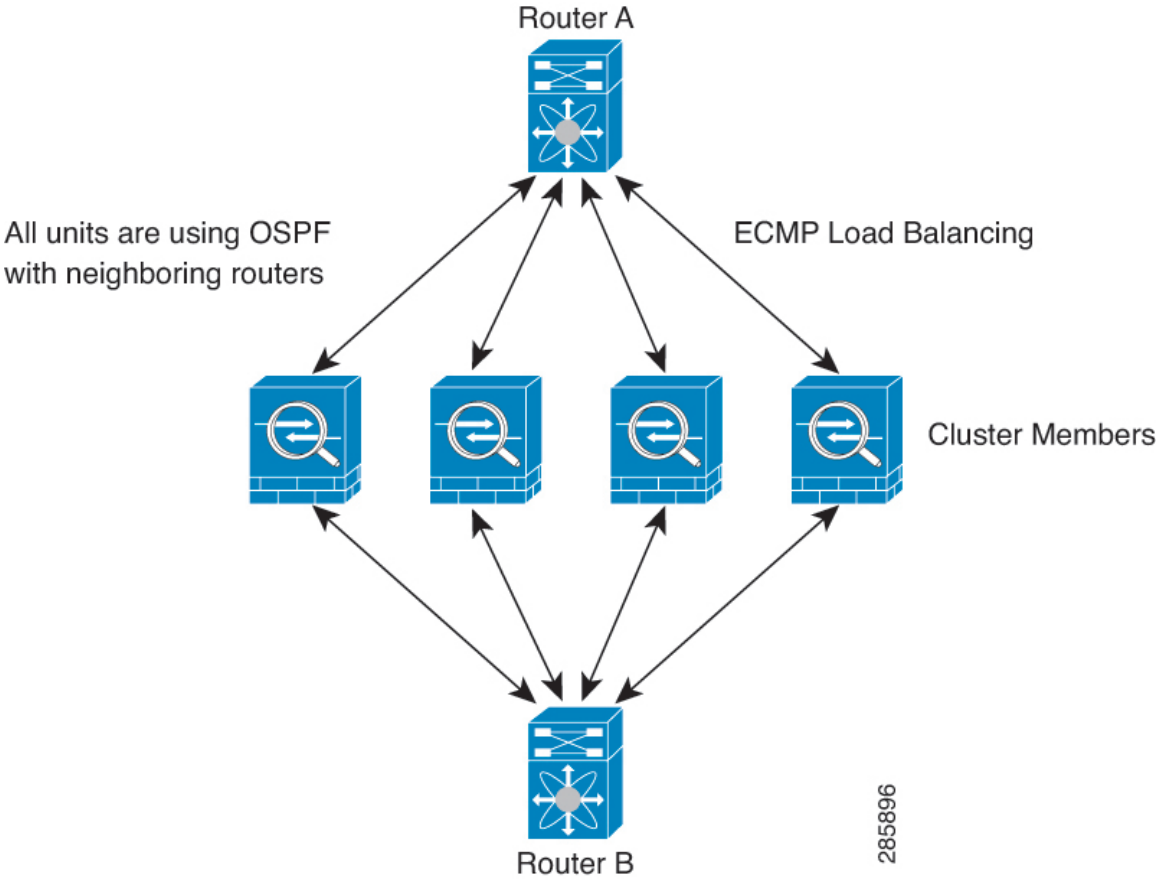
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバールータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *289 :* 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィック ゾーンにこれらすべてのノード インターフェイスをまとめます。ECMP ゾーンの作成 （1155 ページ）を参照してください。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ対策として、多くの場合、（デバイスからの）管理トラフィックをデータトラフィックから分離する必要があります。この分離を実現するために、Firewall Threat Defense は管理専用トラフィックとデータトラフィックに個別のルーティングテーブルを使用します。個別のルーティングテーブルを使用することで、データと管理用に別のデフォルトルートを作成できます。

各ルーティングテーブルのトラフィックのタイプ

デバイス間トラフィックでは、常にデータルーティングテーブルが使用されます。

デバイス発信トラフィックでは、タイプに応じて、デフォルトで管理専用ルーティングテーブルまたはデータルーティングテーブルが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

- 管理専用テーブルのデバイス発信トラフィックには、AAA サーバー通信が含まれます。
- データテーブルのデバイス発信トラフィックには、DNS サーバルックアップと DDNS が含まれます。例外として、DNS の診断インターフェイスのみを指定した場合、Firewall Threat Defense は管理専用テーブルのみを使用します。

管理専用ルーティングテーブルに含まれるインターフェイス

管理専用インターフェイスには、すべてのDiagnostic x/x インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。

（注） 管理論理インターフェイスは、Firewall Threat Defense ルートルックアップの一部ではない独自の Linux ルーティングテーブルを使用します。管理インターフェイスで発信されるトラフィックには、Firewall Management Center 通信、ライセンス通信、およびデータベース更新が含まれます。一方、診断論理インターフェイスは、このセクションで説明されている管理専用ルーティングテーブルを使用します。

他のルーティングテーブルへのフォールバック

デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デフォルト以外のルーティングテーブルの使用

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。Firewall Threat Defense デバイスは、指定されたインターフェイスのルートのみをチェックします。たとえば、あるデータインターフェイスでRADIUS サーバーと通信する必要がある場合は、RADIUS 設定でそのインターフェイスを指定します。他方、管理専用ルーティングテーブルにデフォルトルートがある場合は、デフォルトルートに一致し、データルーティングテーブルにフォールバックすることは決してありません。

ダイナミック ルーティング

管理専用ルーティングテーブルは、データ インターフェイス ルーティング テーブルから分離したダイナミックルーティングをサポートします。ダイナミック ルーティング プロセスは管理専用インターフェイスまたはデータインターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。

Equal-Cost Multipath（ECMP）ルーティング

Firewall Threat Defense デバイスは、等コスト マルチパス（ECMP）ルーティングをサポートしています。

インターフェイスごとに最大8つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは10.1.1.2、10.1.1.3、および10.1.1.4間の外部インターフェイスでロードバランシングされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

トラフィック ゾーンを使用した複数のインターフェイス間の ECMP

インターフェイスのグループを含むようにトラフィックゾーンを設定する場合、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストの静的または動的ルートを設定できます。たとえば、次のようにゾーン内の3つのインターフェイ間に複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、等コストルートを自動的に設定できます。Firewall Threat Defense デバイス は、より堅牢なロード バランシング メカニズムを使用して、インターフェイス間のトラフィックのロードバランシングを行います。

ルートが紛失した場合、 デバイスはフローをシームレスに別のルートに移動させます。

ルート マップについて

ルート マップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティング プロセスに再配布するときに使用します。また、OSPF ルーティング プロセスにデフォルト ルートを生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個別のステートメントの順序シーケンスです。ACL またはルート マップの評価は、事前に定義された順序でのリストのスキャンと、一致する各ステートメントの基準の評価で構成されています。リストのスキャンは、ステートメントの一致が初めて見つかり、そのステートメントの一致に関連付けられたアクションが実行されると中断します。
- これらは汎用的なメカニズムです。基準照合と一致解釈は、適用方法とこれらを使用する機能によって決定します。同じルートマップであっても異なる機能に適用されると、解釈が異なる場合があります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルート マップはルート タイプが内部であるかどうかを確認できます。
- 設計規則により、各 ACL は暗黙の deny ステートメントで終了します。照合中にルート マップの終わりに達した場合、そのルート マップの特定の適用によって結果が異なります。再配布に適用されるルート マップの動作は ACL と同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny ステートメントが含まれている場合と同様に、ルート再配布が拒否されます。

permit 句と deny 句

ルート マップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるので、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL の permit + ルート マップの permit：ルートは再配布されます。
- ACL の permit + ルート マップの deny：ルートは再配布されません。
- ACL の deny + ルート マップの permit または deny：ルート マップの句は一致せず、次のルート マップ句が評価されます。

match 句と set 句の値

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲット プロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句

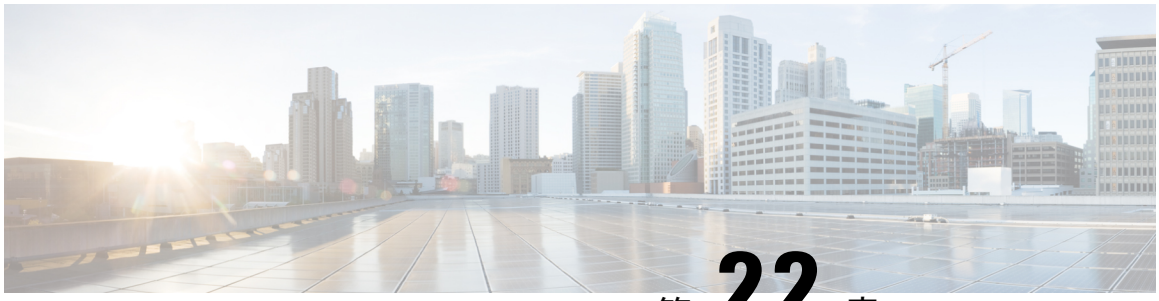
でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。
- ルート マップの permit 句に set エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。

（注） ルート マップの deny 句では set エントリを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

match エントリまたは set エントリがないルート マップ句はアクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。



第 22 章

仮想ルータ

この章では、仮想ルータおよびSecure Firewall Threat Defense内での仮想ルーティングの仕組みに関する基本概念について説明します。

- 仮想ルータと Virtual Route Forwarding（VRF）について （1091 ページ）
- デバイス モデルごとの仮想ルータの最大数 （1098 ページ）
- 仮想ルータの要件と前提条件 （1099 ページ）
- 仮想ルータに関する注意事項と制限事項 （1100 ページ）
- Firewall Management Center Web インターフェイスの変更：[ルーティング（Routing）] ページ （1102 ページ）
- 仮想ルータの管理 （1103 ページ）
- 仮想ルータの作成 （1103 ページ）
- 仮想ルータのモニタリング （1107 ページ）
- 仮想ルータの設定例 （1108 ページ）
- 仮想ルータの履歴 （1150 ページ）

仮想ルータと Virtual Route Forwarding（VRF）について

複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できます。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。

これにより、共通のネットワーク機器のセットを使用して、2 件以上のお客様にサポートを提供できます。また、たとえば開発ネットワークを汎用企業ネットワークから分離することによって、仮想ルータを使用して、独自のネットワーク要素をより明確に分離することもできます。

仮想ルータは、Virtual Routing and Forwarding の「軽量」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。

仮想ルータを作成するときに、インターフェイスをルータに割り当てます。特定のインターフェイスを 1 つのみの仮想ルータに割り当てることができます。次に、スタティックルートを定義し、各仮想ルータに OSPF や BGP などのルーティングプロトコルを設定します。また、ネットワーク全体で個別のルーティングプロセスを設定し、すべての参加デバイス上のルー

ティングテーブルが、仮想ルータごとの同じルーティングプロセスとテーブルを使用するようにします。仮想ルータを使用して、同じ物理ネットワーク上に論理的に分離されたネットワークを作成し、各仮想ルータを通過するトラフィックのプライバシーを確保します。

ルーティングテーブルは個別にあるため、仮想ルータ全体で同じ、または重複するアドレス空間を使用できます。たとえば、2 つの別個の物理インターフェイスでサポートされている 2 つの別個の仮想ルータ用に、192.168.1.0/24 アドレス空間を使用できます。

仮想ルータごとに個別の管理およびデータのルーティングテーブルがあることに注意してください。たとえば、管理専用インターフェイスを仮想ルータに割り当てると、そのインターフェイスのルーティング テーブルは、仮想ルータに割り当てられたデータ インターフェイスとは別のものになります。

仮想ルータの適用

仮想ルータにより、共有リソース上のネットワークを分離したり、共通セキュリティポリシーを使用してネットワークを分離したりすることができます。そのため、仮想ルータは、次のことを実現するために役立ちます。

- 顧客または部門ごとの専用ルーティングテーブルによって顧客のトラフィックを分離する。
- 異なる部門またはネットワークで共通セキュリティポリシーを管理する。
- 異なる部門またはネットワークでインターネットアクセスを共有する。

グローバルおよびユーザー定義の仮想ルータ

グローバル仮想ルータ

仮想ルーティング機能を備えたデバイスの場合、デフォルトでグローバル仮想ルータが作成され、ネットワーク内のすべてのインターフェイスがグローバル仮想ルータに割り当てられます。ルーテッドインターフェイスは、ユーザー定義の仮想ルータまたはグローバル仮想ルータのいずれかに属することができます。仮想ルータ機能を備えたバージョンに Firewall Threat Defense をアップグレードすると、既存のすべてのルーティング構成がグローバル仮想ルータの一部になります。

ユーザー定義の仮想ルータ

ユーザー定義の仮想ルータは、ユーザーが定義するルータです。1 つのデバイス上に複数の仮想ルータを作成できます。ただし、1 つのインターフェイスは常に 1 つのユーザー定義の仮想ルータにのみ割り当てることができます。一部のデバイス機能はユーザー定義の仮想ルータでサポートされていますが、一部の機能はグローバル仮想ルータでのみサポートされています。ユーザー定義の仮想ルータは、ルートベースのサイト間VPN（スタティック VTI）をサポートしています。

サポートされている機能とモニタリングポリシー

次の機能は、グローバル仮想ルータでのみ設定できます。

- OSPFv3
- RIP
- EIGRP
- IS-IS
- マルチキャストルーティング
- Policy Based Routing（PBR）

ISIS、およびPBRは、Firewall Management CenterのFlexConfigを介してサポートされます（定義済みのFlexConfigオブジェクト（2701ページ）を参照）。これらの機能に対しては、グローバル仮想ルータのインターフェイスのみを設定します。

DHCPサーバーの自動設定では、インターフェイスから学習したWINS/DNSサーバーが使用されます。このインターフェイスに指定できるのは、グローバル仮想ルータインターフェイスだけできます。

次の機能は、ユーザー定義の仮想ルータごとに個別に設定できます。

- スタティックルートとルートのSLAモニター
- OSPFv2
- BGPv4/v6
- Integrated Routing and Bridging（IRB）
- SNMP

次の機能は、リモートシステムに対してクエリまたは通信を行うときにシステムによって使用されます（ボックス内のトラフィック）。これらの機能は、グローバル仮想ルータのインターフェイスのみを使用します。つまり、この機能のインターフェイスを設定する場合、そのインターフェイスはグローバル仮想ルータに属している必要があります。一般的なルールとして、管理目的で外部サーバーに到達するためにルートを検索する必要があるシステムでは、グローバル仮想ルータでルートルックアップが実行されます。

- アクセス制御ルールで使用される完全修飾名を解決する場合、または**ping**コマンドの名前解決に使用されるDNSサーバー。DNSサーバのインターフェイスとして**any**を指定すると、システムはグローバル仮想ルータのインターフェイスだけを考慮します。
- AAAサーバまたはアイデンティティレルム（VPNで使用する場合）。VPNは、グローバル仮想ルータのインターフェイスでのみ設定できるため、VPNに使用される外部AAAサーバー（Active Directoryなど）は、グローバル仮想ルータのインターフェイスを介して到達可能である必要があります。
- SYSLOGサーバ。

仮想ルーター対応ポリシーの設定

仮想ルータを作成する場合、その仮想ルータのルーティングテーブルは、グローバル仮想ルータまたは他の仮想ルータから自動的に分離されます。ただし、セキュリティポリシーは自動的に仮想ルータ対応にはなりません。

たとえば、「任意の」送信元または宛先のセキュリティゾーンに適用されるアクセス制御ルールを作成する場合、ルールはすべての仮想ルータのすべてのインターフェイスに適用されます。実はこれがまさに必要な機能かもしれません。たとえば、すべてのお客様が、同じリストの好ましくない URL カテゴリへのアクセスをブロックしたい場合があります。

ただし、いずれかの仮想ルータにのみポリシーを適用する必要がある場合は、その1つの仮想ルータからのインターフェイスのみを含むセキュリティゾーンを作成する必要があります。その後、セキュリティポリシーの送信元と宛先の条件に、仮想ルータが制約されたセキュリティゾーンを使用します。

メンバーシップが1つの仮想ルータに割り当てられたインターフェイスに制限されたセキュリティゾーンを使用することにより、次のポリシーで仮想ルータ対応ルールを作成できます。

- アクセス コントロール ポリシー
- 侵入およびファイルポリシー。
- SSL 復号ポリシー。
- アイデンティティ ポリシーと、ユーザから IP アドレスへのマッピング。仮想ルータで重複するアドレス空間を使用する場合は、仮想ルータごとに個別のレルムを作成し、アイデンティティ ポリシー ルールでそれらを正しく適用してください。

仮想ルータで重複するアドレス空間を使用する場合は、適切なポリシーが適用されるようにセキュリティゾーンを使用する必要があります。たとえば、2 つの個別の仮想ルータで 192.168.1.0/24 アドレス空間を使用する場合、192.168.1.0/24 ネットワークを指定するだけのアクセスコントロールルールは、両方の仮想ルータのトラフィックに適用されます。これが求める結果ではない場合は、1つの仮想ルータのみに対して送信元/宛先セキュリティゾーンも指定することで、ルールの適用を制限できます。

仮想ルータの相互接続

スタティックおよびダイナミックルートリーク

仮想ルータ間でトラフィックをルーティングするようにデバイスを設定できます。このルートリークのプロセスは、スタティックルートを設定して手動で実行することも、BGPの設定を介して動的に実行することもできます。

スタティックルートリーク

仮想ルータ間でトラフィックをルーティングするようにスタティックルートを設定できます。

たとえば、グローバル仮想ルータに外部インターフェイスがある場合、外部インターフェイスにトラフィックを送信するために、他の各仮想ルータでスタティック デフォルト ルートを設定できます。その後、特定の仮想ルータ内でルーティングできないトラフィックは、その後のルーティングのためにグローバルルータに送信されます。

仮想ルータ間のスタティックルートは、別の仮想ルータにトラフィックをリークしているため、ルートリークと呼ばれます。ルートをリークしている場合（VR2 への VR1 ルートなど）、VR2 から VR1 のみへの接続を開始できます。トラフィックが VR1 から VR2 に流れるようにするには、逆ルートを設定する必要があります。別の仮想ルータのインターフェイスへのスタティックルートを作成する場合は、ゲートウェイアドレスを指定する必要はありません。単純に宛先インターフェイスを選択します。

仮想ルータ間ルートの場合、システムは送信元の仮想ルータ内で宛先インターフェイスルックアップを行います。次に、宛先の仮想ルータでネクストホップの MAC アドレスを検索します。したがって、宛先の仮想ルータには、宛先アドレスに対して選択されたインターフェイスのダイナミック（学習済み）ルートまたはスタティックルートのいずれかが設定されている必要があります。

異なる仮想ルータで送信元インターフェイスと宛先インターフェイスを使用する NAT ルールを設定すると、仮想ルータ間でトラフィックをルーティングすることもできます。ルートルックアップを実行するために NAT のオプションを選択しない場合、宛先の変換が発生するたびに、NAT 変換アドレスを使用して宛先インターフェイスからトラフィックが送信されます。ただし、宛先の仮想ルータには、ネクストホップルックアップが成功するように、変換後の宛先 IP アドレスのルートが設定されている必要があります。

NAT ルールは、ある仮想ルータから別の仮想ルータへのトラフィックをリークしますが、正しいルーティングを確保するため、変換されたトラフィック用に仮想ルータ間のスタティックルートリークを設定することを推奨します。ルートリークがないと、ルールが適合すると予想されるトラフィックにルールが適合しないことがあり、変換が適用されないおそれがあります。

仮想ルーティングは、ルートリークのカスケーディングまたはチェーンをサポートしません。たとえば、Firewall Threat Defense に VR1、VR2、および VR3 仮想ルータがあるとします。VR3 は、ネットワーク 10.1.1.0/24 に直接接続されています。ここで、VR2 のインターフェイス経由でネットワーク 10.1.1.0/24 の VR1 におけるルートリークを設定し、VR3 経由で 10.1.1.0/24 の VR2 におけるルートリークを定義するとします。このルートリークのチェーンは、VR1 から VR2 へのトラフィックのホップを許可せず、VR3 を終了します。ルートリークの場合、ルートルックアップでは、まず入力側の仮想ルータのルーティングテーブルで出力インターフェイスが決定され、仮想ルータのルーティングテーブルの出力でネクストホップルックアップが確認されます。両方のルックアップで、出力インターフェイスが一致している必要があります。この例では、出力インターフェイスが同じものにならないため、トラフィックは通過しません。

宛先ネットワークがアップストリーム（発信）VR の直接接続されたサブネットでない場合は、静的な VRF 間ルートを注意して使用してください。たとえば、VR1 と VR2 の 2 つの VR があるとします。VR1 は、BGP または任意の動的ルーティングプロトコルを介して外部のピアからデフォルトルートを取得する発信トラフィックを処理し、VR2 は、VR1 をネクストホップとして使用する静的な VRF 間のデフォルトルートで構成された着信トラフィックを処理しま

す。VR1 がピアからのデフォルトルートを失っても VR2 はそのアップストリーム（発信）VR がデフォルトルートを失ったことを検出できず、トラフィックは引き続き VR1 に送信され、最終的に通知なしでドロップされます。このシナリオでは、BGP を介した動的なルートリークを使用して VR2 を構成することをお勧めします。

BGP を使用したダイナミックルートリーク

ルートターゲット拡張コミュニティを使用して送信元仮想ルータ（VR1 など）から送信元 BGP テーブルにルートをエクスポートし、同じルートターゲット拡張コミュニティを送信元 BGP テーブルから宛先 BGP テーブルにインポートすることで、仮想ルータ間ルートリークを実装できます。これは、その後、宛先仮想ルータ（VR2 など）によって使用されます。ルートのフィルタリングにルートマップを使用できます。グローバル仮想ルータのルートは、ユーザ定義の仮想ルータにリークすることも、その逆も可能です。BGP 仮想ルータ間ルートリークは、IPv4 と IPv6 の両方のプレフィックスをサポートします。

BGP ルートリークの設定の詳細については、BGP ルートのインポート/エクスポート設定の設定 （1239 ページ）を参照してください。

BGP ルートリークのガイドライン

- 再帰に必要なすべてのルートがインポートされ、入力仮想ルータのルーティングテーブルに存在することを確認します。
- ECMP は仮想ルータごとにサポートされます。したがって、異なる仮想ルータ間で ECMP を設定しないでください。異なる仮想ルータからインポートされた重複するプレフィックスは、ECMP を形成できません。つまり、2つの異なる仮想ルータから他の仮想ルータ（グローバル仮想ルータまたはユーザ定義の仮想ルータ）に重複するアドレスを持つルートをインポートしようとすると、1 つのルート（BGP ベストパスアルゴリズムに従って、アドバタイズされた最初のルート）がそれぞれの仮想ルーティングテーブルにインポートされます。たとえば、VR1 に接続されたネットワーク 10.10.0.0/24 が BGP を介して最初にグローバル仮想ルータにアドバタイズされ、その後、VR2 に接続された同じアドレス 10.10.0.0/24 を持つ別のネットワークも BGP を介してグローバル仮想ルータにアドバタイズされた場合、 VR1 ネットワークルートのみがグローバル仮想ルーティングテーブルにインポートされます。
- ユーザ定義の仮想ルータでは OSPFv3 はサポートされません。したがって、OSPFv3 ユーザ定義の仮想ルータをグローバル仮想ルータにリークするように BGPv6 を設定しないでください。ただし、再配布によって OSPFv3 グローバル仮想ルータのルートをユーザ定義の仮想ルータにリークするように BGPv6 を設定できます。
- ルートをリークしなくて済むように、VTI インターフェイスと保護されている内部インターフェイス（VTI でサポートされている場合はループバック インターフェイス）を同じ仮想ルータの一部にしておくことをお勧めします。

IP アドレスのオーバーラップ

仮想ルータは、独立したルーティングテーブルの複数のインスタンスを作成するため、同じ（重複する）IP アドレスを競合することなく使用できます。Firewall Threat Defense により、同じネットワークを 2 つ以上の仮想ルータの一部にすることができます。これには、インターフェイスまたは仮想ルータレベルで適用される複数のポリシーが含まれます。

いくつかの例外を除いて、ルーティング機能とほとんどの NGFW および IPS 機能は、重複する IP アドレスの影響を受けません。以下では、重複する IP アドレスによる制限がある機能と、それらに対処するための提案または推奨事項について説明します。

重複する IP アドレスによる制限

複数の仮想ルータで重複する IP アドレスを使用する場合、ポリシーを適切に適用するには、一部の機能のポリシーまたはルールを変更する必要があります。そのような機能では、既存のセキュリティゾーンを分割するか、必要に応じて新しいインターフェイスグループを使用して、より限定されたインターフェイスを使用する必要があります。

次の機能は、重複する IP アドレスで適切に動作させるために変更を加えてください。

- ネットワークマップ：ネットワーク検出ポリシーを変更して、一部の重複する IP セグメントを除外し、マッピングされる IP アドレスが重複しないようにします。
- アイデンティティポリシー：アイデンティティ フィード ソースは仮想ルータ間で区別できません。この制限に対処するには、重複するアドレス空間または仮想ルータを異なるレルムにマッピングします。

次の機能については、特定のインターフェイスにルールを適用して、重複する IP セグメントに異なるポリシーが適用されるようにする必要があります。

- アクセスポリシー
- プレフィルタポリシー
- QoS/レート制限
- SSL ポリシー

重複した IP アドレスがあるとサポートされない機能

- AC ポリシーの ISE SGT ベースのルール：Cisco Identity Services Engine（ISE）からダウンロードした IP アドレスマッピングへのスタティック セキュリティ グループ タグ（SGT）は仮想ルータに対応していません。仮想ルータごとに異なる SGT マッピングを作成する必要がある場合は、仮想ルータごとに個別の ISE システムをセットアップします。これは、各仮想ルータで同じ IP アドレスを同じ SGT 番号にマッピングする場合には必要ありません。
- 仮想ルータ間での重複する DHCP サーバープールはサポートされていません。
- イベントと分析：Firewall Management Center 分析の多くは、同じ IP アドレスが 2 つの異なるエンドホストに属している場合に区別できないネットワークマップおよび ID マッピ

ングに依存しています。そのため、それらの分析は、同じデバイスであっても異なる仮想ルータに重複する IP セグメントが存在する場合、正確なものになりません。

ユーザー定義の仮想ルータでの SNMP の設定

管理インターフェイスおよびグローバル仮想ルータのデータインターフェイスでの SNMP のサポートに加えて、Secure Firewall Threat Defense ではユーザー定義の仮想ルータで SNMP ホストを設定できるようになりました。

ユーザー定義の仮想ルータでの SNMP ホストの設定には、次のプロセスが含まれます。

1. デバイスインターフェイスを設定します。
2. インターフェイスで仮想ルータを設定します。
3. 仮想ルータインターフェイスで SNMP ホストを設定します。

（注） SNMP は仮想ルータに対応していません。したがって、ユーザー定義の仮想ルータで SNMP サーバーを設定するときは、ネットワークアドレスが重複する IP アドレスでないことを確認してください。

4. 設定を Secure Firewall Threat Defense に展開します。展開が成功すると、SNMP ポーリングとトラップが仮想ルータインターフェイスを介してネットワーク管理ステーションに送信されます。

デバイス モデルごとの仮想ルータの最大数

作成できる仮想ルータの最大数は、デバイスモデルによって異なります。次の表に、上限を示します。**show vrf counters** コマンドを入力して、システムでダブルチェックできます。これにより、グローバル仮想ルータを含まない、そのプラットフォームにユーザが定義した仮想ルータの最大数が表示されます。次の表の数字には、ユーザ ルータとグローバル ルータが含まれています。Firepower 4100/9300 の場合、これらの数字はネイティブモードに適用されます。

Firepower 4100/9300 などのマルチインスタンス機能をサポートするプラットフォームでは、仮想ルータの最大数をデバイス上のコア数で割ってから、インスタンスに割り当てられたコア数を乗じて最も近い整数に丸めることにより、コンテナインスタンスごとの仮想ルータの最大数を決定します。たとえば、プラットフォームが最大 100 の仮想ルータをサポートする環境で、70 のコアが存在する場合、各コアは最大 1.43（切り上げた数）の仮想ルータをサポートします。したがって、6 つのコアが割り当てられたインスタンスは、8.58 の仮想ルータをサポートします（この数は 8 に切り下げる）。10 のコアが割り当てられたインスタンスは、14.3 の仮想ルータをサポートします（この数は 14 に切り下げる）。

デバイス モデル	最大仮想ルータ数
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Cisco Secure Firewall 3105	10
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Firepower 9300 appliance、すべてのモデル	100
Firewall Threat Defense Virtual、すべてのプラットフォーム	30
ISA 3000	10

関連トピック

コンテナ インスタンスの要件と前提条件 （244 ページ）

仮想ルータの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

セキュリティ承認者

仮想ルータに関する注意事項と制限事項

ファイアウォール モードのガイドライン

仮想ルータは、ルーテッド ファイアウォール モードでのみサポートされます。

インターフェイスのガイドライン

- インターフェイスは 1 つの仮想ルータにのみ割り当てることができます。
- 仮想ルータには、任意の数のインターフェイスを割り当てることができます。
- ユーザー定義の仮想ルータには、論理名と VTI を持つルーテッドインターフェイスのみを割り当てることができます。
- 仮想ルータインターフェイスを非ルーテッドモードに変更する場合は、仮想ルータからインターフェイスを削除してから、そのモードを変更します。
- グローバル仮想ルータまたは別のユーザー定義の仮想ルータから、インターフェイスを仮想ルータに割り当てることができます。
- 次のインターフェイスは、ユーザー定義の仮想ルータに割り当てることはできません。
  - 診断インターフェイス。
  - EtherChannel のメンバー。
  - 冗長インターフェイスのメンバー。
  - BVI のメンバー。
- VTI はルートベースの VPN です。したがって、トンネルが確立されたら、暗号化に VTI を使用するトラフィックはルーティングを通して制御される必要があります。スタティックルーティング、および BGP、OSPFv2/v3、または EIGRP を使用したダイナミックルーティングがサポートされています。
- ポリシーベースのサイト間 VPN またはリモートアクセス VPN では、ユーザー定義の仮想ルータに属するインターフェイスを使用できません。

- 移行中のインターフェイスを使用している、またはその仮想ルータが削除されたルートが送信元または宛先の仮想ルータテーブルに存在する場合は、インターフェイスを移行または仮想ルータを削除する前に、そのルートを削除してください。
- 仮想ルータごとに個別のルーティングテーブルが維持されるため、インターフェイスが 1 つの仮想ルータから別の仮想ルータ（グローバルかユーザー定義かを問わず）に移行されると、インターフェイスで設定されたIPアドレスは一時的に削除されます。インターフェイス上の既存の接続はすべて終了します。このように、仮想ルータ間でインターフェイスを移行すると、ネットワークトラフィックに大きな影響を与えます。インターフェイスを移行する前に予防措置を講じてください。

グローバル仮想ルータのガイドライン

- 名前が付けられていて、他の仮想ルータの一部ではないインターフェイスは、グローバル仮想ルータの一部です。
- グローバル仮想ルータからルーテッドインターフェイスを削除することはできません。
- グローバル仮想ルータを変更することはできません。
- 一般に、インターフェイスを設定した後、登録を解除して同じまたは別の Firewall Management Center に登録し直すと、インターフェイス設定がデバイスからインポートされます。仮想ルータのサポートには制限があります。つまり、グローバル仮想ルータインターフェイスの IP アドレスのみが保持されます。

クラスタリングのガイドライン

- コントロールユニットのリンクがそのインターフェイスの障害のために失敗すると、ユニットはそのインターフェイスのリークされたすべてのルートをグローバルルーティングテーブルから削除し、非アクティブな接続ルートとスタティックルートをクラスタの他のユニットに伝搬します。これにより、リークされたルートが他のユニットのルーティングテーブルから削除されます。これらの削除は、別のユニットが新しいコントロールユニットになる前に実行され、約500 msかかります。別のユニットが新しいコントロールユニットになると、これらのルートが学習され、BGP コンバージェンスを介してルーティングテーブルに追加されます。したがって、コンバージェンスの時間になるまで（約1分間）、リークされたルートはルーティングイベントの発生のために利用できません。
- クラスタでコントロールロールの変更が発生すると、BGPを介して学習されたリークされたルートが最適な ECMP パスで更新されます。ただし、最適でない ECMP パスは、BGP 再コンバージェンスタイマー（210 秒）が経過しないと、クラスタのルーティングテーブルから削除されません。したがって、BGP 再コンバージェンスタイマーの期限切れるまで、古い最適ではない ECMP パスがルーティングイベントの優先ルートとして存続します。

その他のガイドライン

- 仮想ルータのBGPを設定するときに、同じ仮想ルータ内の異なるプロトコルに属するルートを再配布できます。たとえば、OSPF VR2ルートはBGP VR1にインポートできません。OSPF VR2 を BGP VR2 に再配布し、その後 BGP VR2 と BGP VR1 の間でルートリークを設定するのみ可能です。
- ルートマップ内のルートをフィルタリングするために IPv6 ACL を使用することはできません。プレフィックスリストのみがサポートされています。
- セキュリティ インテリジェンス ポリシー：セキュリティ インテリジェンス ポリシーは、仮想ルータに対応していません。IP アドレス、URL、または DNS 名をブロックリストに追加すると、すべての仮想ルータに対してブロックされます。この制限は、セキュリティゾーンを持つインターフェイスに適用されます。
- NAT ルール：NAT ルールにインターフェイスを混在させないでください。仮想ルーティングでは、指定された送信元インターフェイスと宛先インターフェイスオブジェクト（インターフェイスグループまたはセキュリティゾーン）に異なる仮想ルータに属するインターフェイスがある場合、NAT ルールにより、ある仮想ルータから別の仮想ルータにトラフィックが転送されます。NATは、着信インターフェイスのみに対して仮想ルータテーブルでルートルックアップを行います。必要に応じて、宛先インターフェイスに対して送信元仮想ルータでスタティックルートを定義します。インターフェイスを [任意（any）] のままにした場合は、仮想ルータのメンバーシップに関係なく、すべてのインターフェイスにルールが適用されます。
- DHCP リレー：DHCP リレーでは仮想ルータの相互接続はサポートされていません。たとえば、VR1 インターフェイスで DHCP リレークライアントが有効になっていて、VR2 インターフェイスで DHCP リレーサーバーが有効になっている場合、DHCP 要求は VR2 インターフェイスの外部に転送されません。
- 削除された仮想ルータの再作成：10秒以内に削除された仮想ルータを再作成すると、仮想ルータの削除が進行中であることを示すエラーメッセージが表示されます。削除された仮想ルータを引き続き再作成する場合は、新しい仮想ルータに別の名前を使用します。

Firewall Management Center Web インターフェイスの変更：[ルーティング（Routing）] ページ

Firewall Threat Defense 6.6 より前のデバイスと一部のデバイスモデルは、仮想ルーティング機能でサポートされていません。Firewall Management Center Web インターフェイスには、サポート対象外デバイスなどの Firewall Management Center 6.5 以前のバージョンと同じ [ルーティング（Routing）] ページが表示されます。仮想ルーティングでサポートされているデバイスとプラットフォームについては、「サポートされているデバイスモデル」を参照してください。

サポートされているデバイスの [ルーティング（Routing）] ページで仮想ルータを設定できます。

1. **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** に移動し、仮想ルータ対応デバイスを編集します。
2. [ルーティング（Routing）] をクリックして、 [仮想ルータ（Virtual Routers）] ページを開きます。

仮想ルーティングを使用しているデバイスの場合、[ルーティング（Routing）]ページの左側のペインに次の項目が表示されます。

- [仮想ルータの管理（Manage Virtual Routers）]：仮想ルータを作成および管理できます。
- 仮想ルーティングプロトコルのリスト：仮想ルータに設定できるルーティングプロトコルがリストされます。
- [一般設定（General Settings）]：すべての仮想ルータに適用できる BGP の一般設定を設定できます。他の BGP 設定を定義するには、[BGPの有効化（Enable BGP）]チェックボックスをオンにします。仮想ルータの他の BGP 設定を設定するには、仮想ルーティングプロトコルで BGP に移動します。

仮想ルータの管理

[仮想ルータ（Virtual Routers）] ペインで [仮想ルータの管理（Manage Virtual Routers）] をクリックすると、[仮想ルータの管理（Manage Virtual Routers）]ページが表示されます。このページには、デバイス上の既存の仮想ルータと関連するインターフェイスが表示されます。このページでは、デバイスに **[仮想ルータの追加（Add Virtual Router）]**（＋） できます。また、ユーザー定義の仮想ルータを [編集（Edit）]（✎） または [削除（Delete）]（🗑） できます。グローバル仮想ルータは編集も削除もできません。グローバル仮想ルータの詳細のみ **表示**（🔍） できます。

仮想ルータの作成

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [Routing] をクリックします。

ステップ 3 [Manage Virtual Routers] をクリックします。

ステップ 4 **[仮想ルータの追加（Add Virtual Router）]**（＋） をクリックします。

ステップ 5 [Add Virtual Router] ボックスに、仮想ルータの名前と説明を入力します。

（注）

10秒以内に削除された仮想ルータを作成している場合は、仮想ルータの削除が進行中であることを示すエラーメッセージが表示されます。削除された仮想ルータを引き続き作成する場合は、新しい仮想ルータに別の名前を使用します。

ステップ 6 [OK] をクリックします。

[ルーティング（Routing）]ページが表示され、新しく作成された[仮想ルータ（Virtual Router）]ページが表示されます。

次のタスク

- 仮想ルータを設定します。

仮想ルータの設定

インターフェイスをユーザ定義の仮想ルータに割り当てて、デバイスのルーティングポリシーを設定できます。グローバル仮想ルータのインターフェイスは手動で追加または削除できませんが、デバイスインターフェイスのルーティングポリシーは設定できます。

始める前に

- ユーザ定義の仮想ルータのルーティングポリシーを設定するには、ルータを追加します。仮想ルータの作成 （1103 ページ）を参照してください。
- 仮想ルーティング対応ではないデバイスのすべてのルーティング設定は、グローバル仮想ルータでも使用できます。設定の詳細については、「Routing Settings」を参照してください。
- ユーザ定義の仮想ルータでは、限定されたルーティングプロトコルのみがサポートされます。

手順

ステップ 1 **[デバイス（Devices）]>[デバイス管理（Device Management）]**ページで、仮想ルータでサポートされているデバイスを編集します。[ルーティング（Routing）] に移動します。[ルーティング（Routing）] ページの変更の詳細については、Firewall Management Center Web インターフェイスの変更：[ルーティング（Routing）] ページ （1102 ページ）を参照してください。

ステップ 2 ドロップダウンリストから、目的の仮想ルータを選択します。

ステップ 3 [仮想ルータのプロパティ（Virtual Router Properties）] ページで、説明を変更できます。

ステップ 4 インターフェイスを追加するには、[Available Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックします。

次の点を忘れないでください。

- 論理名を持つインターフェイスのみが [Available Interfaces] ボックスの下にリストされます。インターフェイスを編集し、[インターフェイス（Interfaces）] で論理名を指定できます。設定を有効にするには、必ず変更を保存してください。
- グローバル仮想ルータのインターフェイスのみを割り当てに使用できます。[使用可能なインターフェイス（Available Interfaces）] ボックスには、他のユーザ定義仮想ルータに割り当てられていないインターフェイスのみが表示されます。仮想ルータには物理インターフェイス、サブインターフェイス、冗長インターフェイス、ブリッジグループ、VTI、およびEtherChannelを割り当てられますが、それらのメンバーインターフェイスは割り当てられません。メンバーインターフェイスに名前を付けることはできないため、仮想ルーティングでは使用できません。

  診断インターフェイスは、グローバル仮想ルータにのみ割り当てることができます。

ステップ5 設定を保存するには、[Save] をクリックします。

ステップ6 仮想ルータのルーティングポリシーを設定するには、それぞれの名前をクリックして、対応する設定ページを開きます。

- [OSPF]：ユーザ定義の仮想ルータではOSPFv2のみがサポートされます。仮想ルータ対応ではないインターフェイスに関しては、OSPFv2のその他すべての設定を適用できます。ただし、[インターフェイス（Interface）] では、設定している仮想ルータのインターフェイスのみ選択できます。グローバル仮想ルータのOSPFv3およびOSPFv2ルーティングポリシーを定義できます。OSPF設定の詳細については、Open Shortest Path First（OSPF）（1169 ページ）を参照してください。
- [RIP]：グローバル仮想ルータに対してのみRIPルーティングポリシーを設定できます。RIP設定の詳細については、RIP （1243 ページ）を参照してください。
- [BGP]：このページには、[設定（Settings）] で設定したBGPの一般設定が表示されます。
  - このページでは、ルータIDの設定を除き、BGPの一般設定は変更できません。[設定（Settings）] ページで定義されているルータIDの設定は、このページで編集することによりオーバーライドできます。
  - その他のBGP IPv4またはIPv6設定を設定するには、[BGP] ページの [一般設定（General Settings）] で [BGP] オプションを有効にする必要があります。
  - IPv4とIPv6の両方のアドレスファミリのBGP設定は、グローバルルータとユーザ定義の仮想ルータでサポートされます。

  BGPの設定の詳細については、BGP （1219 ページ）を参照してください。
- [スタティックルート（Static Route）]：この設定を使用して、特定の宛先ネットワークに関するトラフィックの送信先を定義します。この設定を使用して、仮想ルータ間のスタティックルートも作成できます。ユーザ定義またはグローバル仮想ルータのインターフェイスを使用して、接続されたルートまたはスタティックルートのリークを作成できます。FMCは、別の仮想ルータに属し、ルートリークに使用できることを示すためにインターフェイスにプレフィックスを付けます。ルートリークを成功させるには、ネクストホップゲートウェイを指定しないでください。

スタティックルートテーブルの [仮想ルータからのリーク（Leaked from Virtual Router）] 列に、インターフェイスがルートリークに使用される仮想ルータが表示されます。ルートリークではない場合、この列には「該当なし」と表示されます。

スタティックルートが属している仮想ルータに関係なく、スタティックルートが属する同じ仮想ルータのインターフェイスとともに、Null0 インターフェイスがリストされます。

スタティックルートの設定の詳細については、スタティック ルートとデフォルト ルート（1071 ページ）を参照してください。

- [マルチキャスト（Multicast）]：グローバル仮想ルータにのみマルチキャスト ルーティング ポリシーを設定できます。マルチキャスト設定の詳細については、マルチキャスト（1251 ページ）を参照してください。

ステップ 7 設定を保存するには、[Save] をクリックします。

次のタスク

- 仮想ルータを変更します。
- 仮想ルータを削除します。

仮想ルータの変更

仮想ルータの説明やその他のルーティングポリシーを変更できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [Routing] をクリックします。

ステップ 3 [Manage Virtual Routers] をクリックします。

すべての仮想ルータと、割り当てられたインターフェイスが [Virtual Routers] ページに表示されます。

ステップ 4 仮想ルータを変更するには、目的の仮想ルータに対して [編集（Edit）]（✎）をクリックします。

（注）
グローバル仮想ルータの一般設定は変更できません。したがって、グローバルルータの編集はできません。代わりに、設定を表示する **表示**（🔍）が用意されています。

ステップ 5 変更を保存するには、[Save] をクリックします。

次のタスク

- 仮想ルータを削除します。

仮想ルータの削除

始める前に

- グローバル仮想ルータを削除することはできません。したがって、グローバル仮想ルータには削除オプションは使用できません。
- 一度に複数の仮想ルータを削除できます。
- 削除された仮想ルータのすべてのルーティングポリシーも削除されます。
- 削除された仮想ルータのインターフェイスはすべて、グローバル仮想ルータに移動します。
- IP の重複、ルートの競合など、インターフェイスの移動に関する制限がある場合、競合を解決した後にのみルータを削除できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [Routing] をクリックします。

ステップ 3 [Manage Virtual Routers] をクリックします。

すべての仮想ルータと、マッピングされたインターフェイスが [Virtual Routers] ページに表示されます。

ステップ 4 仮想ルータを削除するには、目的の仮想ルータに対して [削除（Delete）]（🗑）をクリックします。

ステップ 5 複数のルータを削除するには、Ctrl キーを押しながら、削除する仮想ルータをクリックします。右クリックして、[削除（Delete）] をクリックします。

ステップ 6 変更を保存するには、[Save] をクリックします。

仮想ルータのモニタリング

仮想ルータをモニターし、トラブルシューティングを行うには、デバイスの CLI にログインして、次のコマンドを使用します。

- **show vrf**：仮想ルータとその関連インターフェイスの詳細情報が表示されます。

- **show route vrf** <*vrf_name*>：仮想ルータのルーティング詳細情報が表示されます。
- **show run router bgp all**：すべての仮想ルータの BGP ルーティング詳細情報が表示されます。
- **show run router bgp vrf** <*vrf_name*>：仮想ルータの BGP ルーティング詳細情報が表示されます。

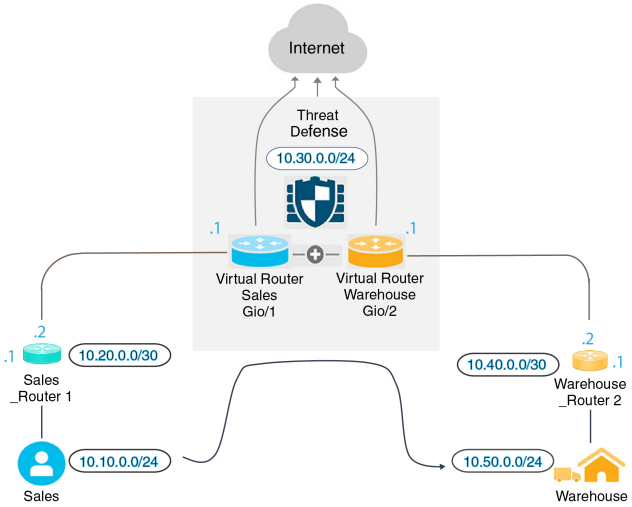
仮想ルータの設定例

仮想ルータを介して遠隔サーバにルーティングする方法

仮想ルーティングでは、複数の仮想ルータを作成して、インターフェイスグループごとに個別のルーティングテーブルを用意することにより、ネットワークの分離を実現できます。場合によっては、個別の仮想ルータを介してのみ到達可能なサーバにアクセスする必要が生じることがあります。この例では、仮想ルータを相互接続して、複数のホップで隔てられているホストに到達する手順について説明します。

たとえば、衣料品会社の販売部門のメンバーが、工場単位の保管倉庫部門で保管されている在庫を検索するとします。仮想ルーティング環境では、宛先（保管倉庫部門）が販売部門から複数ホップ離れている仮想ルータ間でルートをリークする必要があります。この操作は、マルチホップルートリークを追加することで実行されます。この場合、販売部門の仮想ルータ（送信元）で、保管倉庫の仮想ルータ（宛先）のインターフェイスへのスタティックルートを設定する必要があります。宛先ネットワークが複数ホップ離れているため、宛先ネットワーク（10.50.0.0/24）へのルートを使用して、保管倉庫の仮想ルータを設定する必要もあります。

図 *290 : 2*つの仮想ルータの相互接続：例



始める前に

この例では、10.20.0.1/30 インターフェイスから 10.50.0.5/24 へトラフィックをルーティングするように Sales_Router1 がすでに設定されていることを前提としています。

手順

ステップ 1 販売部門の仮想ルータに割り当てられるデバイスの内部インターフェイス（Gi0/1）を設定します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** を選択します。

b) Gi0/1 インターフェイスを編集します。

- [名前（Name）]：この例では、VR-Sales です。
- [有効（Enabled）] チェックボックスをオンにします。
- [IPv4] で、[IPタイプ（IP Type）] として [静的IPを使用する（Use Static IP）] を選択します。
- [IPアドレス（IP Address）]：「10.30.0.1/24」と入力します。

c) [OK] をクリックします。

d) [保存（Save）] をクリックします。

ステップ 2 保管倉庫部門の仮想ルータに割り当てられるデバイスの内部インターフェイス（Gi0/2）を設定します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** を選択します。

b) Gi0/2 インターフェイスを編集します。

- [名前（Name）]：この例では、VR-Warehouse です。
- [有効（Enabled）] チェックボックスをオンにします。
- [IPv4] で、[IPタイプ（IP Type）] として [静的IPを使用する（Use Static IP）] を選択します。
- [IPアドレス（IP Address）]：空白のままにします。ユーザ定義の仮想ルータをまだ作成していないため、システムは、同じ IP アドレス（10.30.0.1/24）を使用してインターフェイスを設定することをユーザに許可しません。

c) [OK] をクリックします。

d) [保存（Save）] をクリックします。

ステップ 3 販売部門および保管倉庫部門の仮想ルータを作成し、それぞれのインターフェイスを割り当てます。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。
b) **[ルーティング（Routing）]** > **[仮想ルータの管理（Manage Virtual Routers）]**を選択します。
c) [仮想ルータの追加（Add Virtual Router）] をクリックして、販売部門の仮想ルータを作成します。
d) [仮想ルータの追加（Add Virtual Router）] をクリックして、保管倉庫部門の仮想ルータを作成します。
e) 仮想ルータのドロップダウンから [販売部門（Sales）] を選択し、[仮想ルータのプロパティ（Virtual Router Properties）]] で、[選択したインターフェイス（Selected Interface）] として [VR-Sales] を追加して保存します。
f) 仮想ルータのドロップダウンから [保管倉庫部門（Warehouse）] を選択し、[仮想ルータのプロパティ（Virtual Router Properties）]] で、[選択したインターフェイス（Selected Interface）] として [VR-Warehouse] を追加して保存します。

ステップ 4 VR-Warehouse インターフェイスの設定を再確認します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** を選択します。
b) [VR-Warehouse] インターフェイスに対する [編集（Edit）] をクリックします。[IPアドレス（IP Address）] に「10.30.0.1/24」と入力します。インターフェイスが 2 つの異なる仮想ルータに個別に割り当てられたため、VR-Sales に同じ IP アドレスを設定できるようになりました。
c) [OK] をクリックします。
d) [保存（Save）] をクリックします。

ステップ 5 保管倉庫部門のサーバ（10.50.0.0/24）のネットワークオブジェクトと、保管倉庫部門のゲートウェイ（10.40.0.2/30）のネットワークオブジェクトを作成します。

a) **[オブジェクト（Object）]** > **[オブジェクト管理（Object Management）]**を選択します。
b) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]**の順に選択します。
   - [名前（Name）] : この例では、Warehouse-Server です。
   - [ネットワーク（Network）] : [ネットワーク（Network）] をクリックして「10.50.0.0/24」と入力します。
c) [保存（Save）] をクリックします。
d) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]**の順に選択します。
   - [名前（Name）] : この例では、Warehouse-Gateway です。
   - [ネットワーク（Network）] : [ホスト（Host）] をクリックして「10.40.0.2」と入力します。
e) [保存（Save）] をクリックします。

ステップ 6 VR-Warehouse インターフェイスをポイントする、販売部門でのルートリークを定義します。

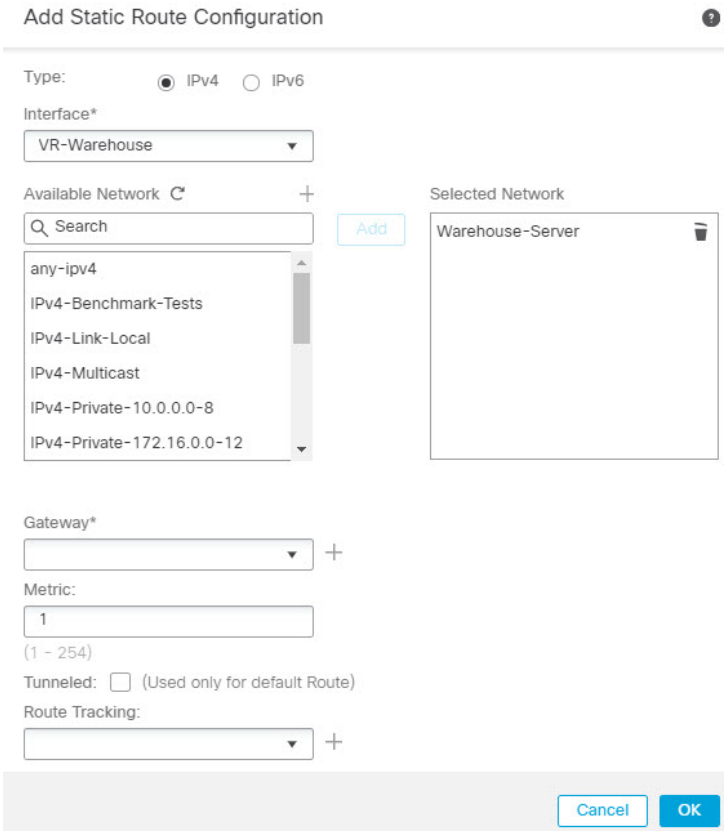
a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) [ルーティング（Routing）] を選択します。

c) ドロップダウンから販売部門の仮想ルータを選択して、[スタティックルート（Static Route）] をクリックします。

d) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：[VR-Warehouse] を選択します。
- [ネットワーク（Network）]： Warehouse-Server オブジェクトを選択します。
- [ゲートウェイ（Gateway）]：空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。



e) [OK] をクリックします。

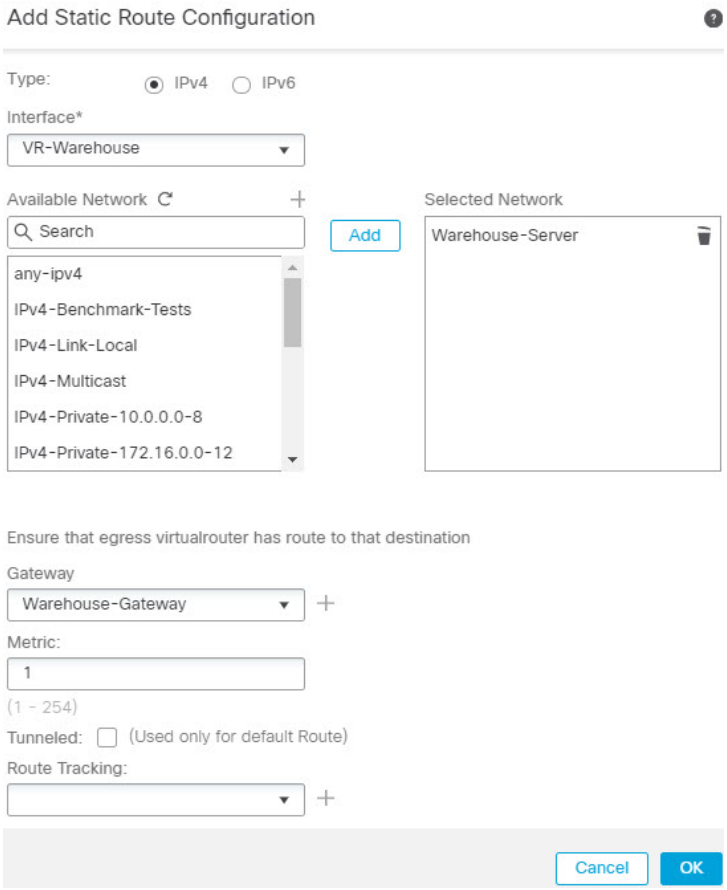
f) [保存（Save）] をクリックします。

ステップ 7 保管倉庫部門の仮想ルータで、Warehouse Router 2 ゲートウェイをポイントするルートを定義します。

a) ドロップダウンから保管倉庫部門の仮想ルータを選択して、[スタティックルート（Static Route）] をクリックします。

b) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）] : [VR-Warehouse] を選択します。
- [ネットワーク（Network）] : Warehouse-Server オブジェクトを選択します。
- [ゲートウェイ（Gateway）] : Warehouse-Gateway オブジェクトを選択します。



c) [OK] をクリックします。

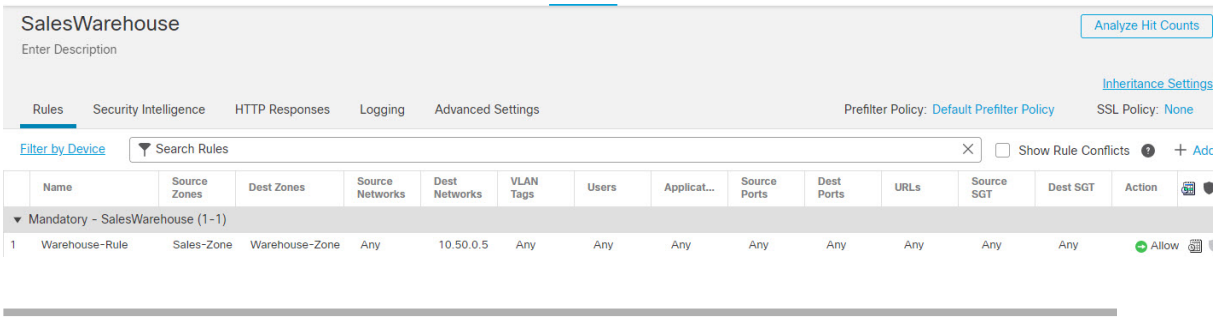
d) [保存（Save）] をクリックします。

ステップ 8 保管倉庫部門のサーバへのアクセスを許可するアクセスコントロールルールを設定します。アクセスコントロールルールを作成するには、セキュリティゾーンを作成する必要があります。**[オブジェクト（Object）] > [オブジェクト管理（Object Management）] > [インターフェイス（Interface）]**を使用します。**[追加（Add）] > [セキュリティゾーン（Security Zone）]**を選択して、VR-Sales および VR-Warehouse のセキュリティゾーンを作成します。Warehouse-Server のネットワークオブジェクト用に、Warehouse-Server インターフェイスグループを作成します（**[追加（Add）] > [インターフェイスグループ（Interface Group）]**を選択）。

ステップ 9 **[ポリシー（Policies）] > [アクセス制御（Access Control）]**を選択してアクセスコントロールルールを設定し、販売部門の仮想ルータの送信元インターフェイスから、宛先 Warehouse-Server

ネットワークオブジェクトの保管倉庫部門用仮想ルータに含まれる宛先インターフェイスへのトラフィックを許可します。

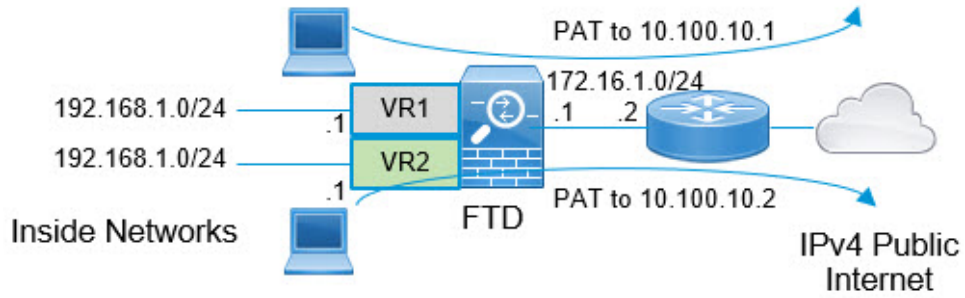
たとえば、Sales のインターフェイスが Sales-Zone セキュリティゾーンにあり、Warehouse のインターフェイスが Warehouse-Zone セキュリティゾーンにある場合、アクセス制御ルールは次のようになります。



重複するアドレス空間を使用してインターネットアクセスを提供する方法

仮想ルータを使用する場合、別のルータに存在するインターフェイスに対して同じネットワークアドレスを設定できます。ただし、個別の仮想ルータでルーティングされる IP アドレスは同じであるため、個別の NAT/PAT プールを持つ各インターフェイスに NAT/PAT ルールを適用して、リターントラフィックが正しい宛先に送信されるようにします。この例では、仮想ルータと NAT/PAT ルールを設定して、重複するアドレス空間を管理する手順を示します。

たとえば、Firewall Threat Defense のインターフェイス vr1-inside および vr2-inside は、IP アドレス 192.168.1.1/24 を使用するように定義して、192.168.1.0/24 ネットワーク内の各セグメント上のエンドポイントを管理できます。たとえば、同じアドレス空間を使用する 2 つの仮想ルータからのインターネットアクセスを許可するには、NAT ルールを各仮想ルータ内のインターフェイスに個別に適用する必要があります。個別の NAT または PAT プールを使用するのが理想的です。PAT を使用して、VR1 の送信元アドレスを 10.100.10.1 に変換し、VR2 の送信元アドレスを 10.100.10.2 に変換できます。次の図は、インターネット側の外部インターフェイスがグローバルルータの一部である場合の設定を示しています。送信元インターフェイス（vr1-inside および vr2-inside）を明示的に選択して NAT/PAT ルールを定義する必要があります。送信元インターフェイスとして「any」を使用すると、同じ IP アドレスが 2 つの異なるインターフェイスに存在する可能性があるため、システムが正しい送信元を識別できなくなります。



（注） 重複するアドレス空間を使用しない仮想ルータ内に一部のインターフェイスがある場合でも、送信元インターフェイスを指定して NAT ルールを定義することでトラブルシューティングが容易になり、インターネットにバインドされた仮想ルータからのトラフィックを確実に分離できます。

手順

ステップ 1 VR1 のデバイスの内部インターフェイスを設定します。

a) **[Devices]** > **[Device Management]** > **[Interfaces]** の順に選択します。

b) VR1 に割り当てるインターフェイスを編集します。

- [名前（Name）]：この例では、vr1-inside。
- [有効（Enabled）] チェックボックスをオンにします。
- [IPv4] で、[IPタイプ（IP Type）] として [静的IPを使用する（Use Static IP）] を選択します。
- [IPアドレス（IP Address）]：192.168.1.1/24 を入力します。

c) [OK] をクリックします。

d) [保存（Save）] をクリックします。

ステップ 2 VR2 のデバイスの内部インターフェイスを設定します。

a) **[Devices]** > **[Device Management]** > **[Interfaces]** の順に選択します。

b) VR2 に割り当てるインターフェイスを編集します。

- [名前（Name）]：この例では、vr2-inside。
- [有効（Enabled）] チェックボックスをオンにします。
- [IPv4] で、[IPタイプ（IP Type）] として [静的IPを使用する（Use Static IP）] を選択します。
- [IPアドレス（IP Address）]：空白のままにします。ユーザー定義の仮想ルータをまだ作成していないため、ユーザーは同じ IP アドレスを使用してインターフェイスを設定できません。

c) [OK] をクリックします。

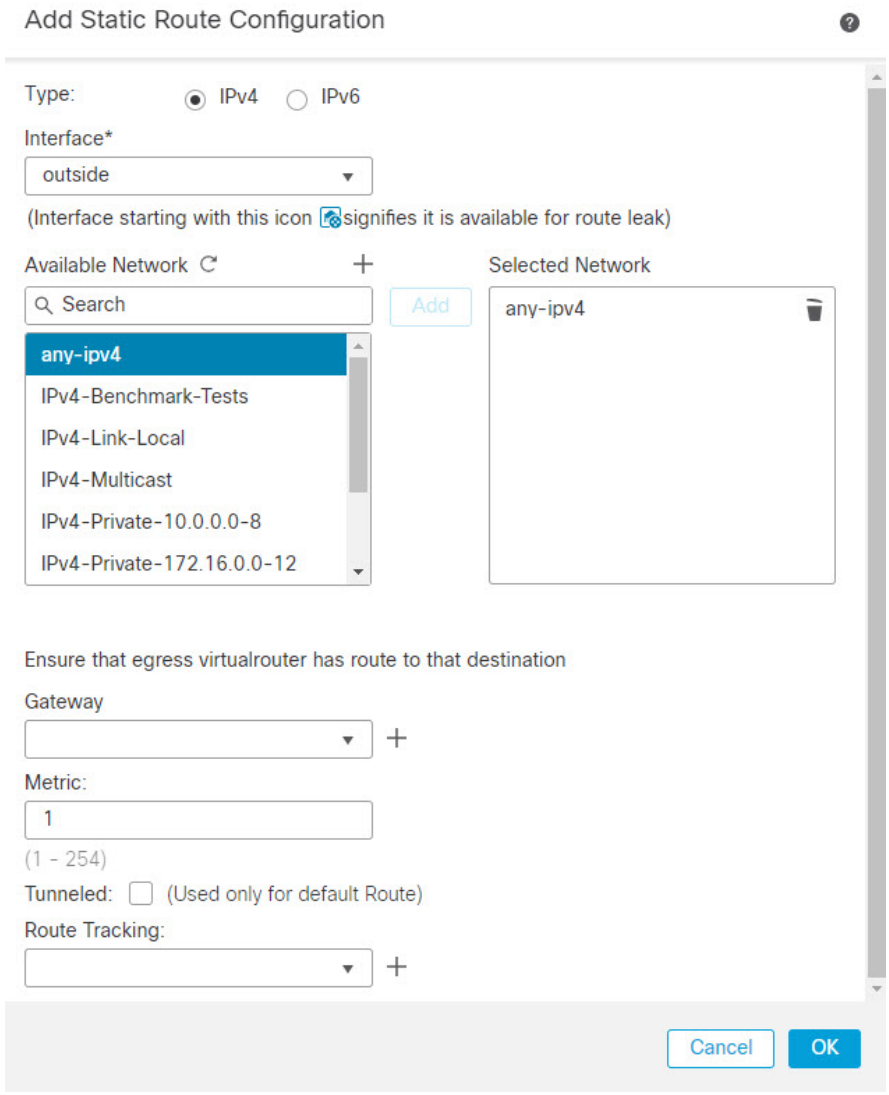
d) [保存（Save）] をクリックします。

ステップ 3 VR1 および外部インターフェイスへの静的デフォルトルートリークを設定します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) **[ルーティング（Routing）]** > **[仮想ルータの管理（Manage Virtual Routers）]** の順に選択します。[仮想ルータの追加（Add Virtual Router）] をクリックして、VR1 を作成します。
c) VR1 の場合、[仮想ルータのプロパティ（Virtual Router Properties）] で、vr1-inside を割り当てて保存します。
d) [Static Route] をクリックします。
e) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：グローバルルータの外部インターフェイスを選択します。
- [ネットワーク（Network）]：any-ipv4 オブジェクトを選択します。このネットワークは、VR1 内でルーティングできないすべてのトラフィックのデフォルトルートになります。
- [Gateway]：空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを指定しません。



f) [OK] をクリックします。

g) [保存（Save）] をクリックします。

ステップ 4 VR2 および外部インターフェイスへの静的デフォルトルートリークを設定します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

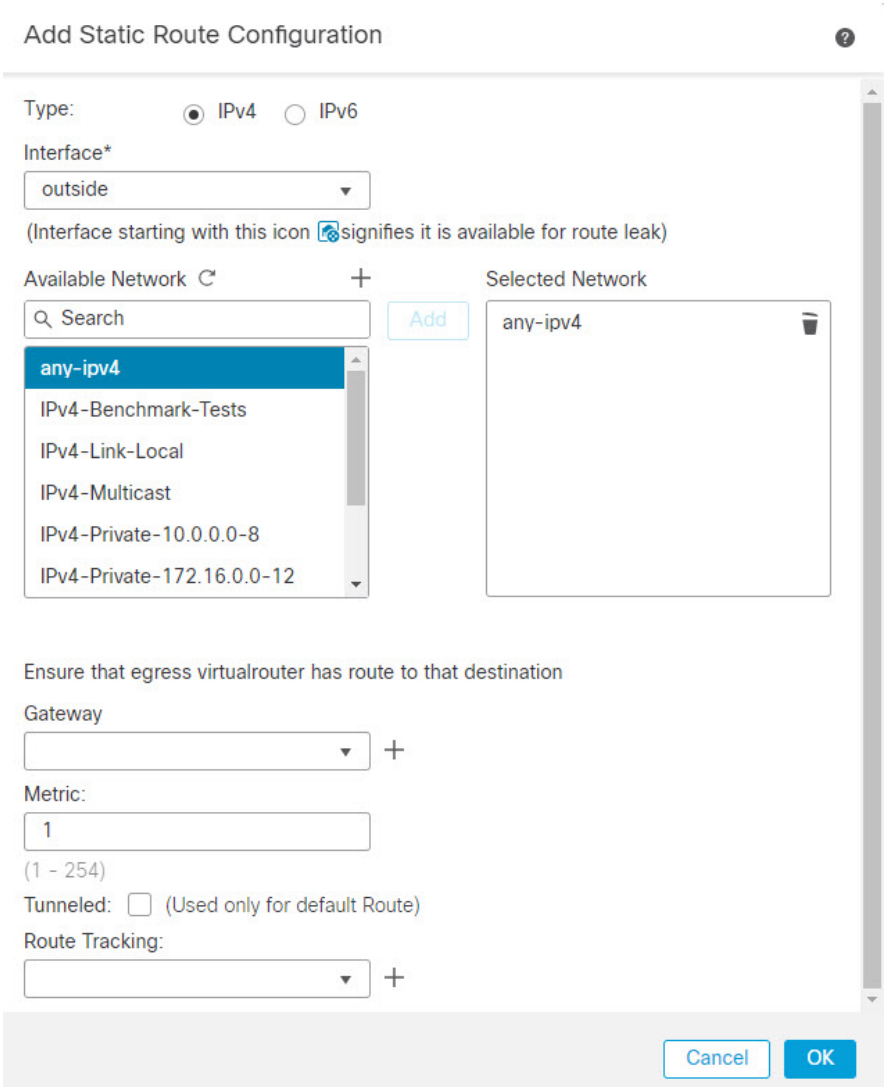
b) **[ルーティング（Routing）] > [仮想ルータの管理（Manage Virtual Routers）]** の順に選択します。[仮想ルータの追加（Add Virtual Router）] をクリックして、VR2 を作成します。

c) VR2 の場合、[仮想ルータのプロパティ（Virtual Router Properties）] で、vr2-inside を割り当てて保存します。

d) [Static Route] をクリックします。

e) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：グローバルルータの外部インターフェイスを選択します。
- [ネットワーク（Network）]：any-ipv4 オブジェクトを選択します。このネットワークは、VR2 内でルーティングできないすべてのトラフィックのデフォルトルートになります。
- [Gateway]：空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイを選択しません。



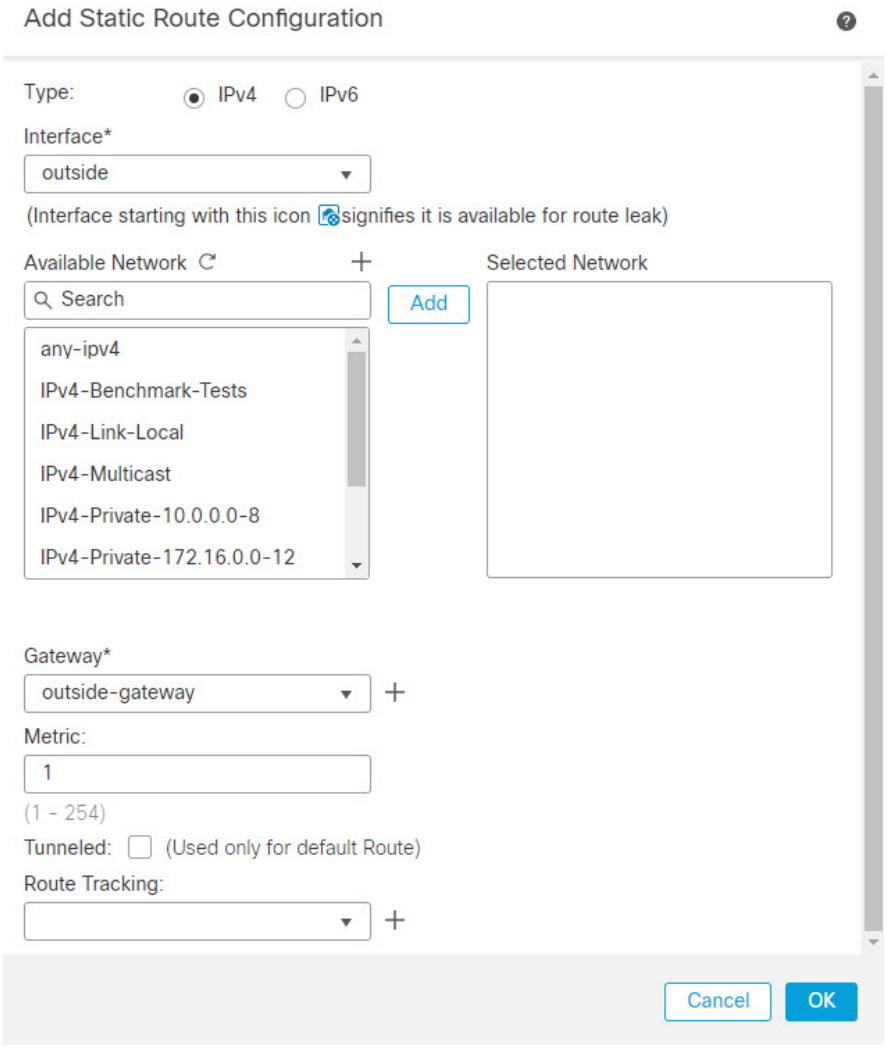
f) [OK] をクリックします。

g) [保存（Save）] をクリックします。

ステップ 5 グローバルルータの外部インターフェイスで IPv4 スタティック デフォルトルート、つまり 172.16.1.2 を設定します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。
b) **[ルーティング（Routing）]**を選択し、グローバルルータのプロパティを編集します。
c) [Static Route] をクリックします。
d) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：グローバルルータの外部インターフェイスを選択します。
- [ネットワーク（Network）]：any-ipv4 オブジェクトを選択します。これは、任意の IPv4 トラフィックのデフォルトルートになります。
- [ゲートウェイ（Gateway）]：作成されている場合は、ドロップダウンからホスト名を選択します。オブジェクトがまだ作成されていない場合は、[追加（Add）] をクリックして、外部インターフェイス（この例では 172.16.1.2）のネットワークリンクの反対側にあるゲートウェイの IP アドレスに対してホストオブジェクトを定義します。オブジェクトを作成したら、[ゲートウェイ（Gateway）] フィールドで選択します。



e) [OK] をクリックします。

f) [保存（Save）] をクリックします。

ステップ 6 vr2-inside インターフェイスの設定を再確認します。

a) **[Devices]** > **[Device Management]** > **[Interfaces]** の順に選択します。

b) vr2-inside インターフェイスに対して [編集（Edit）] をクリックします。IP アドレスを 192.168.1.1/24 として指定します。インターフェイスが 2 つの異なる仮想ルータに個別に割り当てられたため、vr2-inside に同じ IP アドレスを設定できるようになりました。

c) [OK] をクリックします。

d) [保存（Save）] をクリックします。

ステップ 7 VR1 の内部から外部へのトラフィックの 10.100.10.1 への PAT を実行する NAT ルールを作成します。

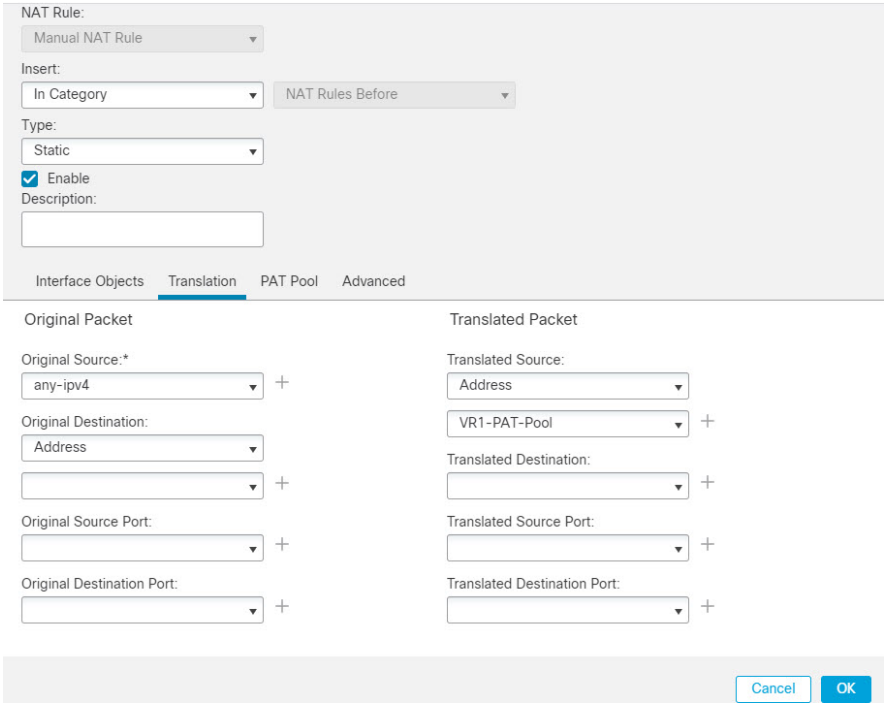
a) **[デバイス（Devices）]** > **[NAT]** の順に選択します。

b) **[新しいポリシー（New Policy）]** > **[Threat Defense NAT]**をクリックします。

c) NAT ポリシー名として InsideOutsideNATRule を入力し、Firewall Threat Defense デバイスを選択します。[保存（Save）] をクリックします。

d) [InsideOutsideNATRule] ページで、[ルールの追加（Add Rule）] をクリックして、以下を定義します。

- [NATルール（NAT Rule）] : [手動NATルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）] : [ダイナミック（Dynamic）] を選択します。
- [挿入（Insert）] : ダイナミック NAT ルールが存在する場合は [前述（Above）] を選択します。
- [Enabled] をクリックします。
- [インターフェイスオブジェクト（Interface Objects）] で、vr1-interface オブジェクトを選択し、[ソースに追加（Add to Source）] をクリックします（オブジェクトがない場合は、**[オブジェクト（Object）]**>**[オブジェクト管理（Object Management）]**>**[インターフェイス（Interface）]**でオブジェクトを作成します）。次に、[宛先に追加（Add to Destination）] で [外部（Outside）] を選択します。
- [変換（Translation）] の [元の送信元（Original Source）] で、[any-ipv4] を選択します。[変換済み送信元（Translated Source）] で、[追加（Add）] をクリックし、10.100.10.1 を指定してホストオブジェクト VR1-PAT-Pool を定義します。次の図に示されているように、VR1-PAT-Pool を選択します。



e) [OK] をクリックします。

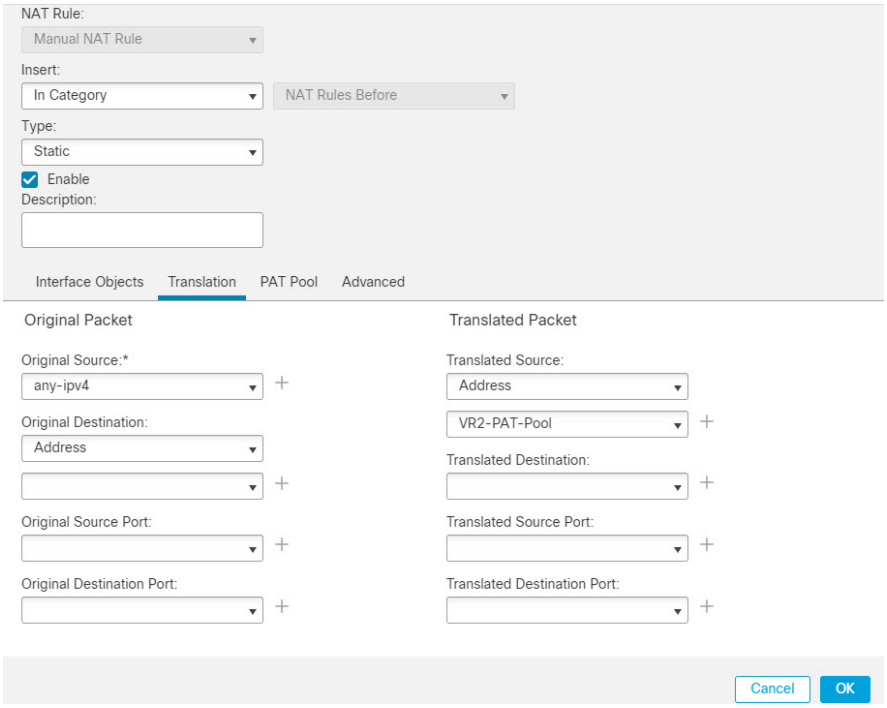
f) [保存（Save）] をクリックします。

ステップ 8 VR2 の内部から外部へのトラフィックの 10.100.10.2 への PAT を実行する NAT ルールを追加します。

a) **[デバイス（Devices）]** > **[NAT]** の順に選択します。

b) InsideOutsideNATRule を編集して、VR2 NAT ルールを定義します。

- [NATルール（NAT Rule）]：[手動NATルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。
- [挿入（Insert）]：ダイナミック NAT ルールが存在する場合は [前述（Above）] を選択します。
- [Enabled] をクリックします。
- [インターフェイスオブジェクト（Interface Objects）] で、vr2-interface オブジェクトを選択し、[ソースに追加（Add to Source）] をクリックします（オブジェクトがない場合は、**[オブジェクト（Object）]**>**[オブジェクト管理（Object Management）]**>**[インターフェイス（Interface）]**でオブジェクトを作成します）。次に、[宛先に追加（Add to Destination）] で [外部（Outside）] を選択します。
- [変換（Translation）] の [元の送信元（Original Source）] で、[any-ipv4] を選択します。[変換済み送信元（Translated Source）] で、[追加（Add）] をクリックし、10.100.10.2 を指定してホストオブジェクト VR2-PAT-Pool を定義します。次の図に示されているように、VR2-PAT-Pool を選択します。



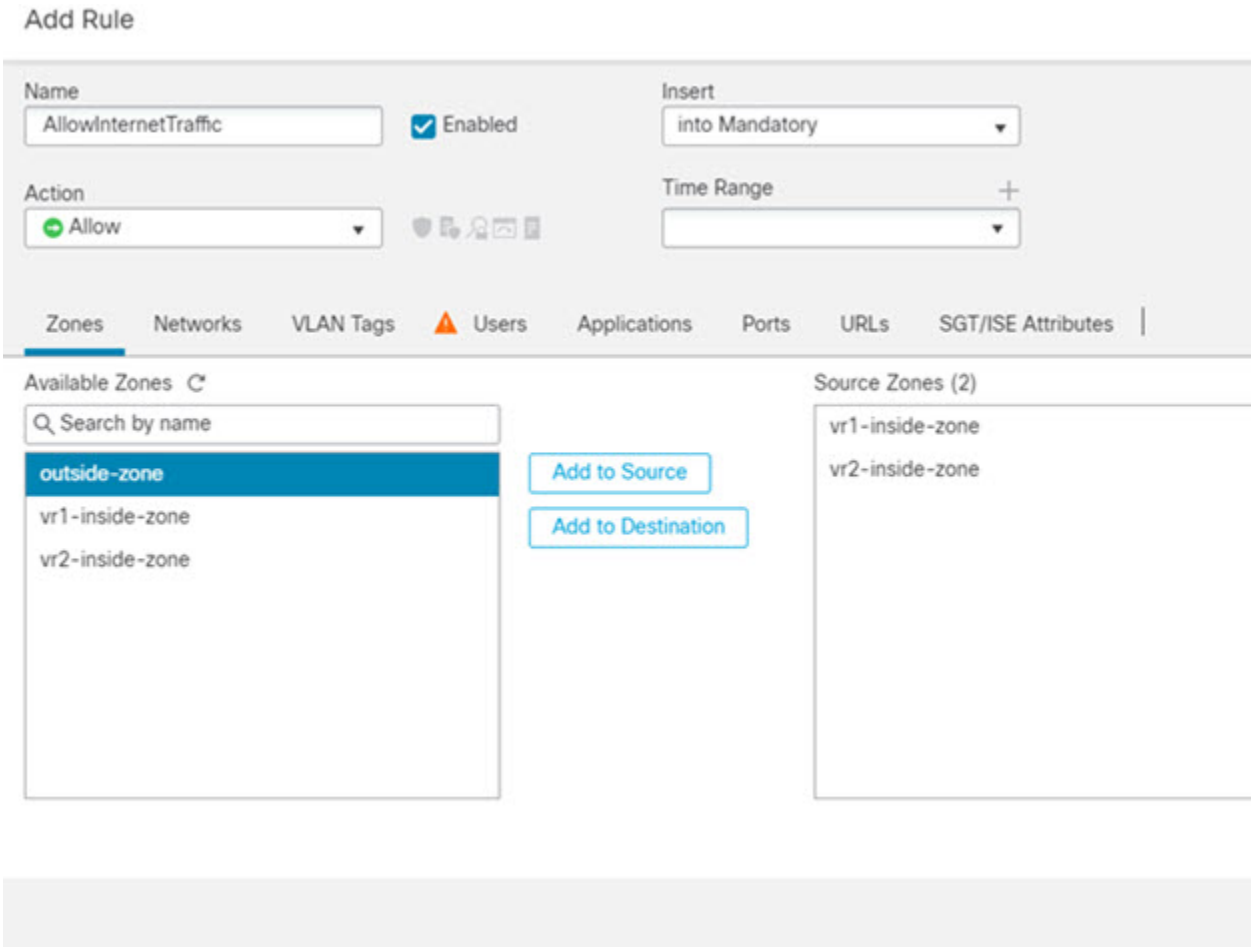
c) [OK] をクリックします。

d) [保存（Save）] をクリックします。

ステップ 9 vr1-inside および vr2-inside インターフェイスから外部インターフェイスへのトラフィックを許可するアクセス コントロール ポリシーを設定するには、セキュリティゾーンを作成する必要があります。**[Object]** > **[Object Management]** > **[Interface]** を使用します。**[追加（Add）]** > **[セキュリティゾーン（Security Zone）]**を選択し、vr1-inside、vr2-inside、および外部インターフェイスのセキュリティゾーンを作成します。

ステップ 10 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択し、vr1-inside-zone および vr2- inside-zone から outside_zone へのトラフィックを許可するアクセス制御ルールを設定します。

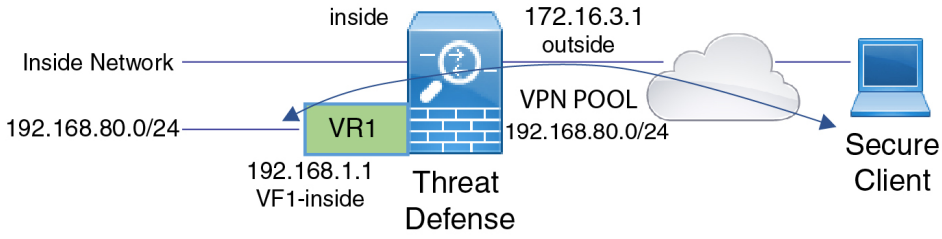
インターフェイスの名前が付けられたゾーンを作成したとすると、すべてのトラフィックがインターネットに流れることを許可する基本ルールは、次のようになります。このアクセス コントロール ポリシーに他のパラメータを適用できます。



仮想ルーティングで内部ネットワークへの RA VPN アクセスを許可する方法

仮想ルーティング対応デバイスでは、RA VPN は、グローバル仮想ルータインターフェイスでのみサポートされます。この例では、セキュアクライアント ユーザーがユーザー定義の仮想ルータネットワークに接続できるようにする手順を示します。

次の例では、RA VPN（セキュアクライアント）ユーザーが、172.16.3.1 の Firewall Threat Defense の外部インターフェイスに接続します。このユーザーには192.168.80.0/24 のプールに含まれる IP アドレスが割り当てられます。ユーザーは、グローバル仮想ルータのみの内部ネットワークにアクセスできます。ユーザー定義の仮想ルータ VR1 のネットワーク（つまり、192.168.1.0/24）を介したトラフィックフローを許可するには、グローバルと VR1 でスタティックルートを設定してルートをリークします。



始める前に

この例では、すでに RA VPN を設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

ステップ 1 グローバル仮想ルータからユーザー定義の VR1 へのルートリークを設定します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

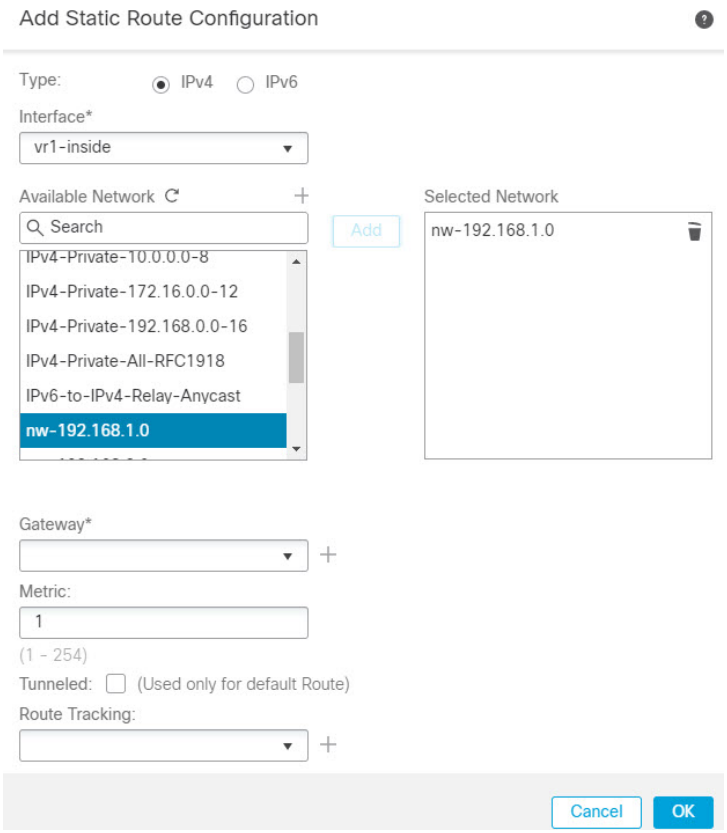
b) [ルーティング（Routing）] をクリックします。デフォルトでは、グローバル ルーティング プロパティのページが表示されます。

c) [Static Route] をクリックします。

d) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：VR1 内部インターフェイスを選択します。
- [ネットワーク（Network）]：VR1 仮想ルータ ネットワーク オブジェクトを選択します。[オブジェクトの追加（Add Object）] オプションを使用してオブジェクトを作成できます。

- [Gateway]：空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。



ルートリークにより、VPN プール内の IP アドレスが割り当てられた セキュアクライアントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできるようになります。

e) [OK] をクリックします。

ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

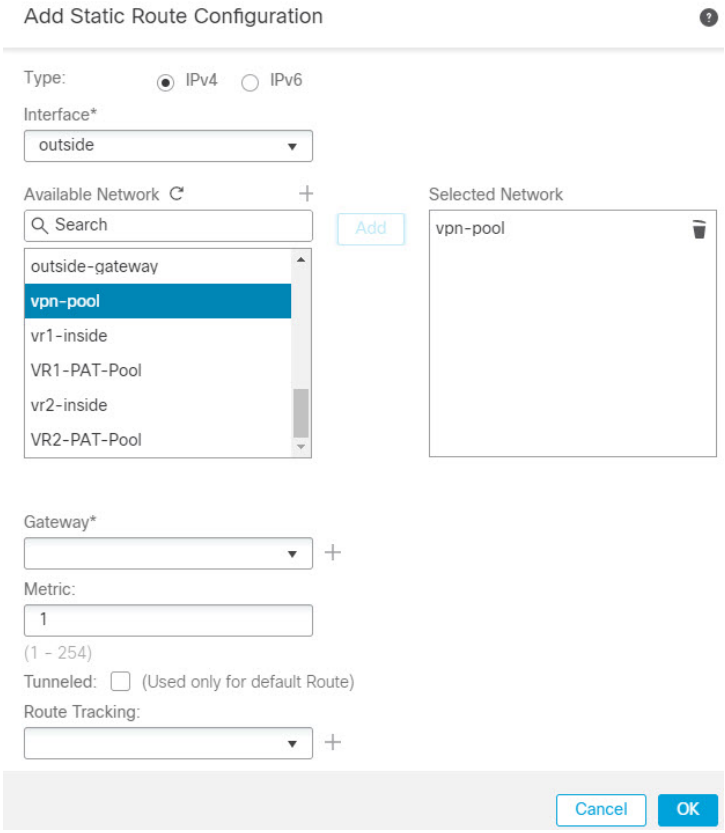
a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) [ルーティング（Routing）] をクリックし、ドロップダウンから [VR1] を選択します。

c) [Static Route] をクリックします。

d) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：グローバルルータの外部インターフェイスを選択します。
- [ネットワーク（Network）]：グローバル仮想ルータ ネットワーク オブジェクトを選択します。
- [Gateway]：空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。



設定されたスタティックルートにより、192.168.1.0/24 ネットワーク（VR1）上のエンドポイントは、VPN プール内の IP アドレスが割り当てられた セキュアクライアントへの接続を開始できます。

e) [OK] をクリックします。

次のタスク

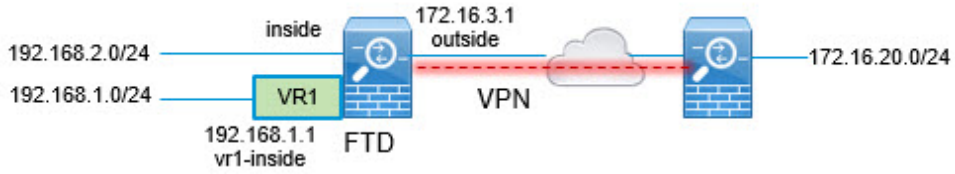
RA VPNアドレスプールとユーザー定義の仮想ルータのIPアドレスが重複している場合には、IP アドレスに対してスタティック NAT ルールを使用し、適切なルーティングを有効にする必要があります。または、重複しないように RA VPN アドレスプールを変更することもできます。

サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

仮想ルーティング対応デバイスでは、サイト間 VPN はグローバル仮想ルータインターフェイスでのみサポートされます。ユーザー定義の仮想ルータに属するインターフェイスでは設定できません。この例では、サイト間 VPN を介して、ユーザー定義の仮想ルータ内でホストされ

ているネットワークとの間の接続を保護する手順を示します。また、ユーザー定義の仮想ルーティングネットワークが含まれるように、サイト間 VPN 接続を更新する必要もあります。

ブランチ オフィス ネットワークと本社ネットワークの間にサイト間 VPN が設定されているシナリオを考えてみましょう。ブランチオフィスの Firewall Threat Defense に仮想ルータがあります。この例では、サイト間 VPN は 172.16.3.1 のブランチオフィスの外部インターフェイスで定義されます。この VPN には、内部インターフェイスがグローバル仮想ルータの一部でもあるため、追加の設定なしで内部ネットワーク 192.168.2.0/24 が含まれます。ただし、VR1 仮想ルータの一部である 192.168.1.0/24 ネットワークにサイト間 VPN サービスを提供するには、グローバルおよび VR1 でスタティックルートを設定して、VR1 ネットワークをサイト間 VPN 設定に追加して、ルートをリークする必要があります。



始める前に

この例では、すでに 192.168.2.0/24 ローカルネットワークと 172.16.20.0/24 外部ネットワークの間にサイト間 VPN を設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

ステップ 1 グローバル仮想ルータからユーザー定義の VR1 へのルートリークを設定します。

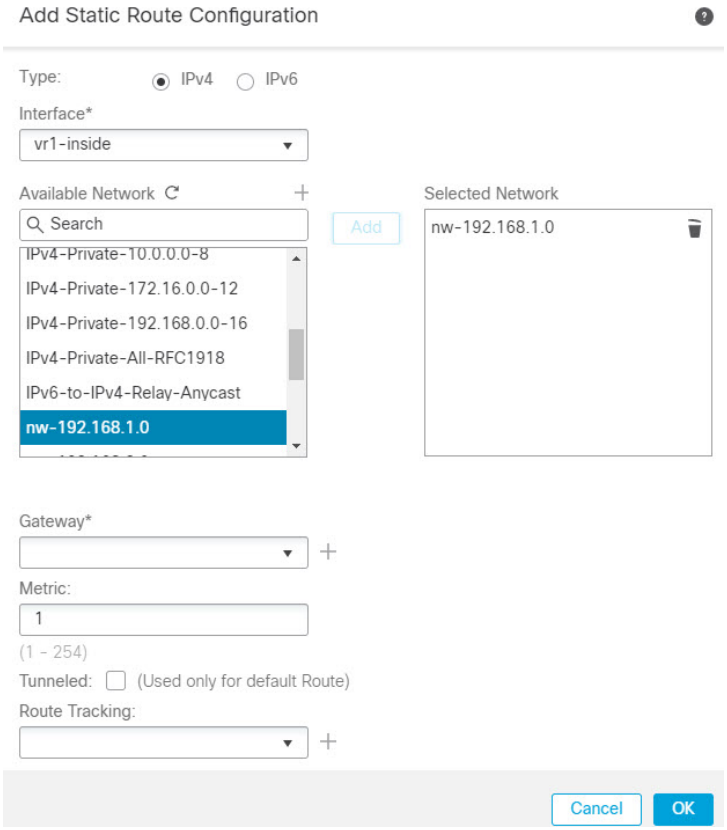
a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) [ルーティング（Routing）] をクリックします。デフォルトでは、グローバル ルーティング プロパティのページが表示されます。

c) [Static Route] をクリックします。

d) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：VR1 内部インターフェイスを選択します。
- [ネットワーク（Network）]：VR1 仮想ルータ ネットワーク オブジェクトを選択します。[オブジェクトの追加（Add Object）] オプションを使用してオブジェクトを作成できます。
- [ゲートウェイ（Gateway）]：空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。



ルートリークにより、サイト間 VPN の外部（リモート）エンドによって保護されたエンドポイントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできます。

e) [OK] をクリックします。

ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

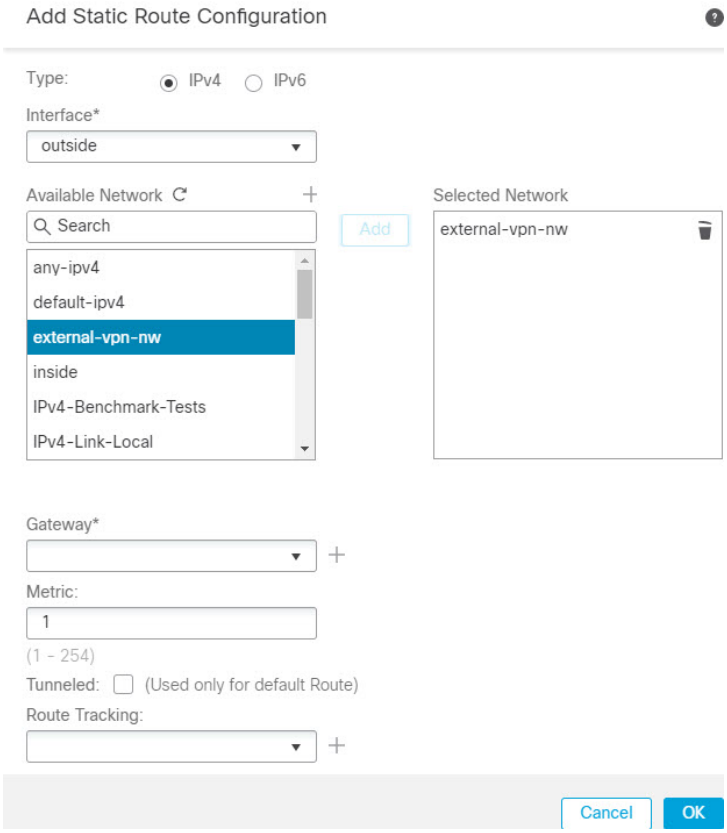
a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) [ルーティング（Routing）] をクリックし、ドロップダウンから [VR1] を選択します。

c) [Static Route] をクリックします。

d) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：グローバルルータの外部インターフェイスを選択します。
- [ネットワーク（Network）]：グローバル仮想ルータ ネットワーク オブジェクトを選択します。
- [ゲートウェイ（Gateway）]：空白のままにします。別の仮想ルータにルートをリークする場合には、ゲートウェイを選択しません。



このスタティックルートにより、192.168.1.0/24 ネットワーク（VR1）上のエンドポイントは、サイト間 VPN トンネルを通過する接続を開始できます。この例では、リモートエンドポイントが 172.16.20.0/24 ネットワークを保護しています。

e) [OK] をクリックします。

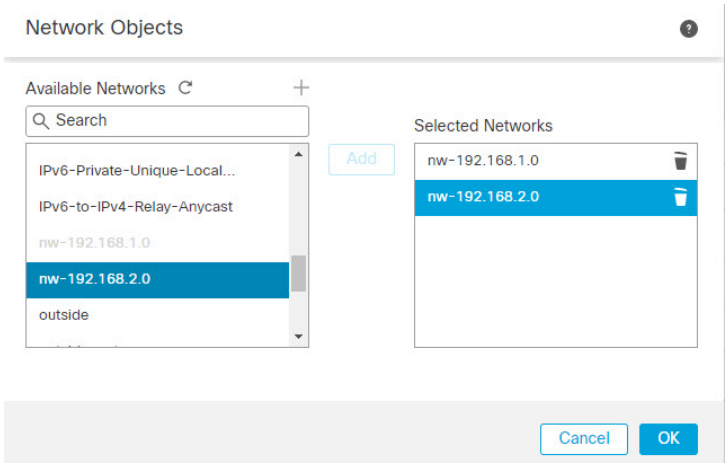
ステップ 3 192.168.1.0/24 ネットワークをサイト間 VPN 接続プロファイルに追加します。

a) **[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site To Site）]**を選択し、VPN トポロジを編集します。

b) [エンドポイント（Endpoints）] で、ノード A エンドポイントを編集します。

c) [エンドポイントの編集（Edit Endpoint）] の [保護されたネットワーク（Protected Networks）] フィールドで、[新しいネットワークオブジェクトの追加（Add New Network Object）] をクリックします。

d) 192.168.1.0 ネットワークで VR1 ネットワークオブジェクトを追加します。

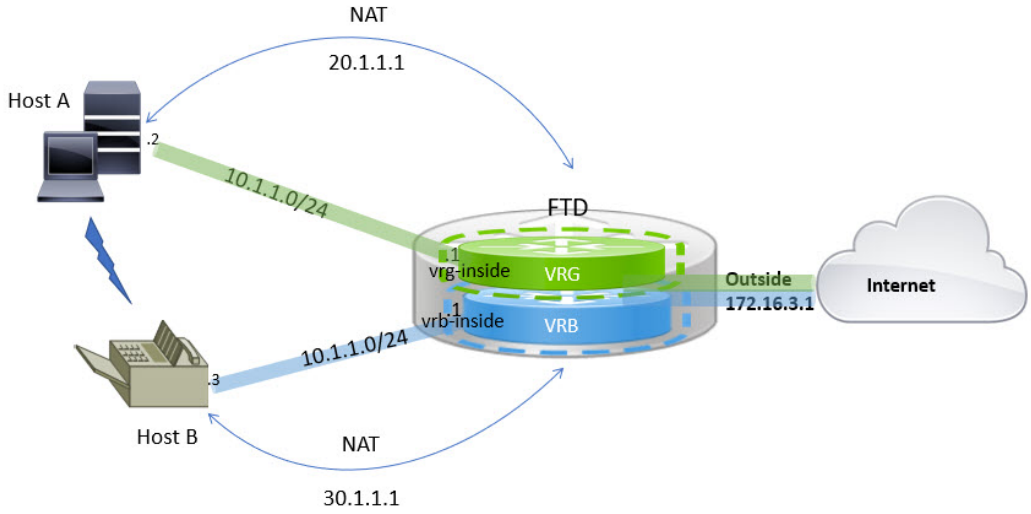


e) [OK] をクリックして設定を保存します。

仮想ルーティングにおいて 2 つの重複するネットワークホスト間でトラフィックをルーティングする方法

同じネットワークアドレスを持つ仮想ルータ上にホストを構成できます。ホストの通信には、Twice NAT を設定できます。この例では、重複するネットワークホストを管理するための NAT ルールの設定手順を示します。

次の例では、2 つのホスト（ホスト A とホスト B）が異なる仮想ルータ（VRG（インターフェイス vrg-inside）、VRB（インターフェイス vrb-inside））にそれぞれ属しており、サブネット（10.1.1.0/24）は同じです。両方のホストが通信するために、VRG-Host インターフェイス オブジェクトがマップされた NAT アドレス（20.1.1.1）を使用し、VRB-Host インターフェイス オブジェクトがマップされた NAT アドレス（30.1.1.1）を使用する NAT ポリシーを作成します。結果として、ホスト A は 30.1.1.1 を使用してホスト B と通信します。ホスト B は 20.1.1.1 を使用してホスト A に到達します。



始める前に

この例では、すでに以下の設定が実施されていることを前提としています。

- vrg-inside および vrb-inside インターフェイスは、仮想ルータ（VRG および VRB）にそれぞれ関連付けられており、どちらのインターフェイスも同じサブネットアドレス（10.1.1.0/24 など）を使用して設定されています。
- インターフェイスゾーン VRG-Inf、VRB-Inf は、それぞれ vrg-inside および vrb-inside インターフェイスを指定して作成されています。
- デフォルトゲートウェイとして vrg-inside を使用する VRG のホスト A。デフォルトゲートウェイとして vrb-inside を使用する VRB のホスト B。

手順

ステップ 1 ホスト A からホスト B へのトラフィックを処理する NAT ルールを作成します。**[デバイス（Devices）] > [NAT]**を選択します。

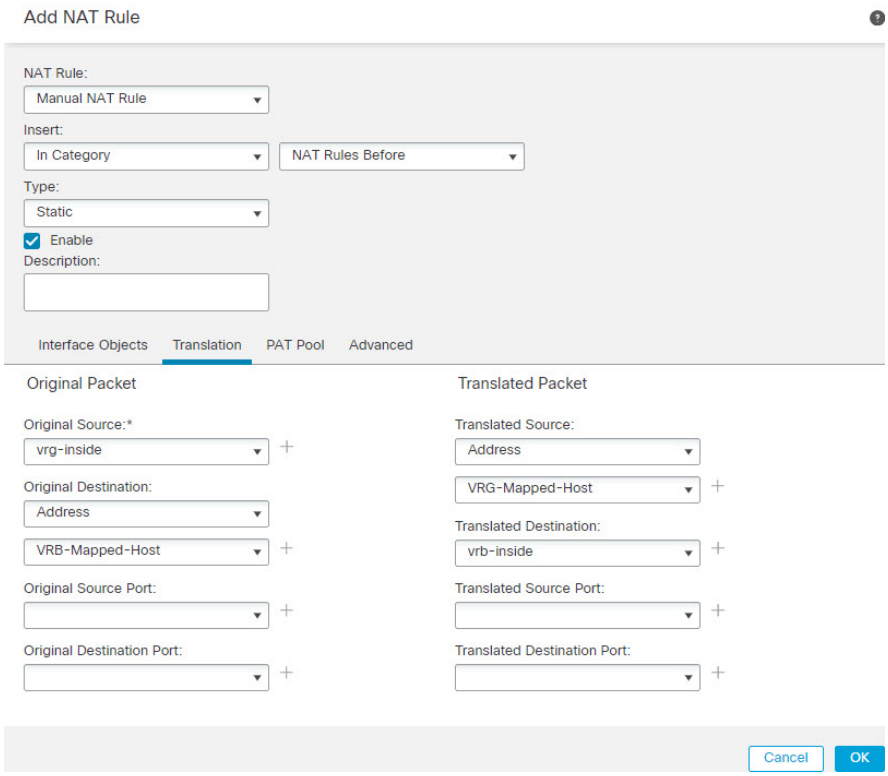
ステップ 2 **[新しいポリシー（New Policy）] > [Threat Defense NAT]** をクリックします。

ステップ 3 NAT ポリシー名を入力し、Firewall Threat Defense デバイスを選択します。[保存（Save）] をクリックします。

ステップ 4 [NAT] ページで、[ルールの追加（Add Rule）] をクリックして、以下の項目を定義します。

- [NATルール（NAT Rule）]：[手動NATルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[静的（Static）] を選択します。
- [挿入（Insert）]：NAT ルールが存在する場合は [前述（Above）] を選択します。
- [Enabled] をクリックします。

- [インターフェイス オブジェクト（Interface Objects）] で、VRB-Inf オブジェクトを選択し、[ソースに追加（Add to Source）] をクリックします（オブジェクトがない場合は、**[オブジェクト（Object）]** > **[オブジェクト管理（Object Management）]** > **[インターフェイス（Interface）]** でオブジェクトを作成します）。次に、VRB-Inf オブジェクトを選択して [宛先に追加（Add to Destination）] をクリックします。
- [変換（Translation）] で、以下を選択します。
  - [元の送信元（Original Source）] で vrg-inside を選択します。
  - [元の宛先（Original Destination）] で [追加（Add）] をクリックし、30.1.1.1 を指定してオブジェクト VRB-Mapped-Host を定義します。VRB-Mapped-Host を選択します。
  - [変換済み送信元（Translated Source）] で [追加（Add）] をクリックし、20.1.1.1 を指定してオブジェクト VRG-Mapped-Host を定義します。VRG-Mapped-Host を選択します。
  - [変換済みの宛先（Translated Destination）] で、次の図に示されているように vrb-inside を選択します。



Firewall Threat Defense デバイスで **show nat detail** コマンドを実行すると、次のような出力が表示されます。

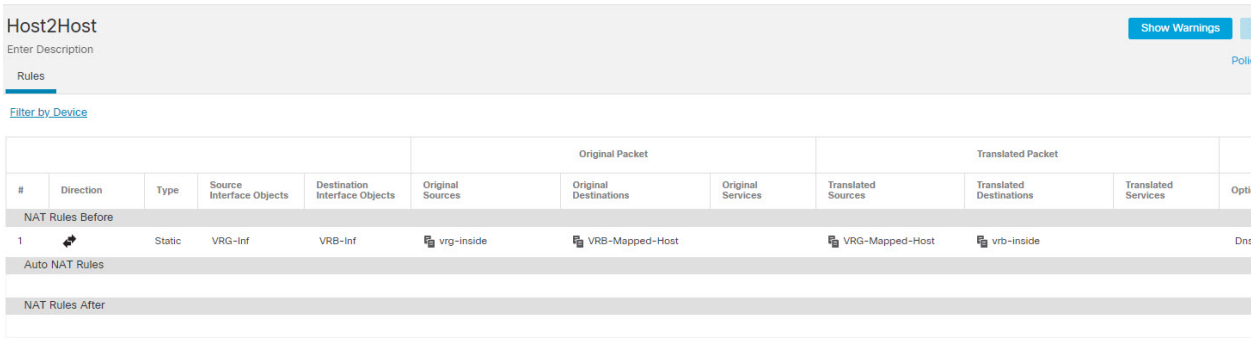
```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static
VRB-MAPPED-HOST vrb-inside
translate_hits = 0, untranslate_hits = 0
```

```
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

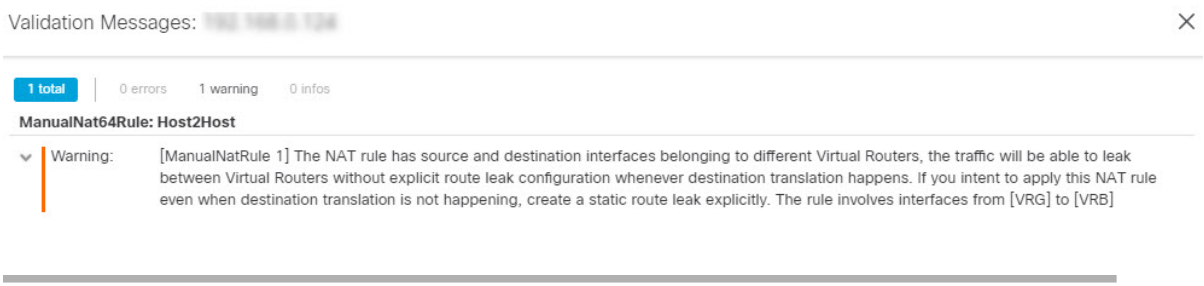
ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

NAT ルールは次のようになります。



構成を展開すると、警告メッセージが表示されます。

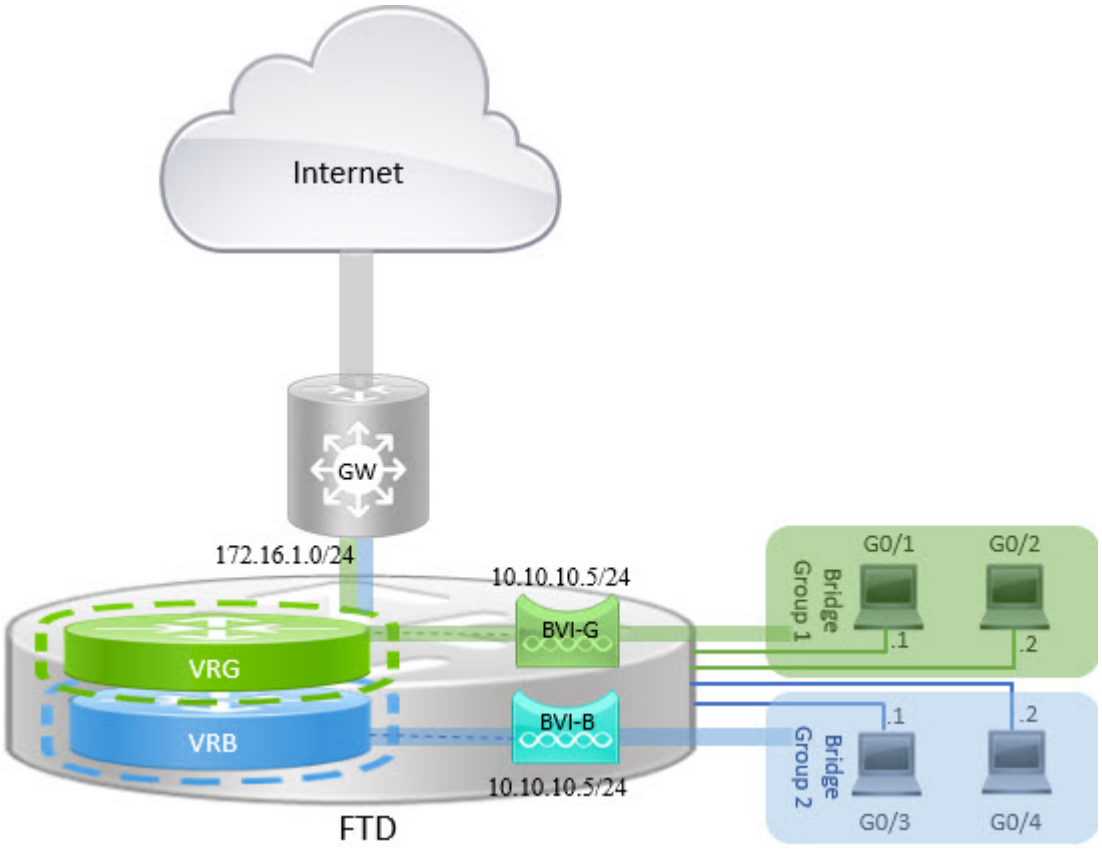


BVI インターフェイスを使用したルーテッド ファイアウォール モードでの重複セグメントの管理方法

複数の重複ネットワーク間に単一の Firewall Threat Defense を透過的に展開したり、同じネットワークのホスト間にファイアウォールを展開することができます。この展開を実現するには、仮想ルータごとに BVI を設定します。ここでは、仮想ルータで BVI を設定する手順について説明します。

BVI は、通常のルーテッドインターフェイスのように動作する、ルータ内の仮想インターフェイスです。これはブリッジングをサポートしませんが、ルータ内のルーテッドインターフェイスに相当するブリッジグループを表します。これらのブリッジドインターフェイスで着信または発信するすべてのパケットは、BVI インターフェイスをパススルーします。BVI のインターフェイス番号は、仮想インターフェイスが代表するブリッジ グループの番号です。

次の例では、BVI-G が VRG で設定されており、Bridge Group 1 がインターフェイス G0/1 および G0/2 のルーテッドインターフェイスです。同様に、BVI-B が VRB で設定されており、Bridge Group 2 がインターフェイス G0/3 および G0/4 のルーテッドインターフェイスです。両方の BVI が同じ IP サブネットアドレス（10.10.10.5/24）を持っていると考えてください。仮想ルータにより、ネットワークは共有リソース上で分離されます。



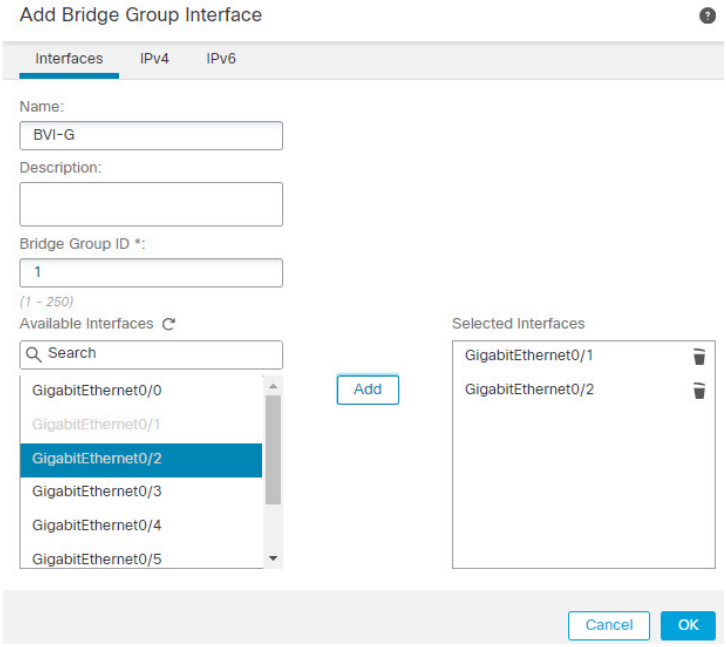
手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。必要なデバイスを編集します。

ステップ 2 [インターフェイス（Interfaces）] で、**[インターフェイスの追加（Add Interfaces）]** > **[ブリッジ グループ インターフェイス（Bridge Group Interface）]** を選択します。

a) BVI-G の次の詳細情報を入力します。

- [名前（Name）]：この例では、「BVI-G」。
- [ブリッジグループID（Bridge Group ID）]：この例では、「1」。
- [利用可能なインターフェイス（Available Interface）]：インターフェイスを選択します。
- [IPv4] で、[IP Type] として [Use Static IP] を選択します。
- [IPアドレス（IP Address）]：「10.10.10.5/24」と入力します。

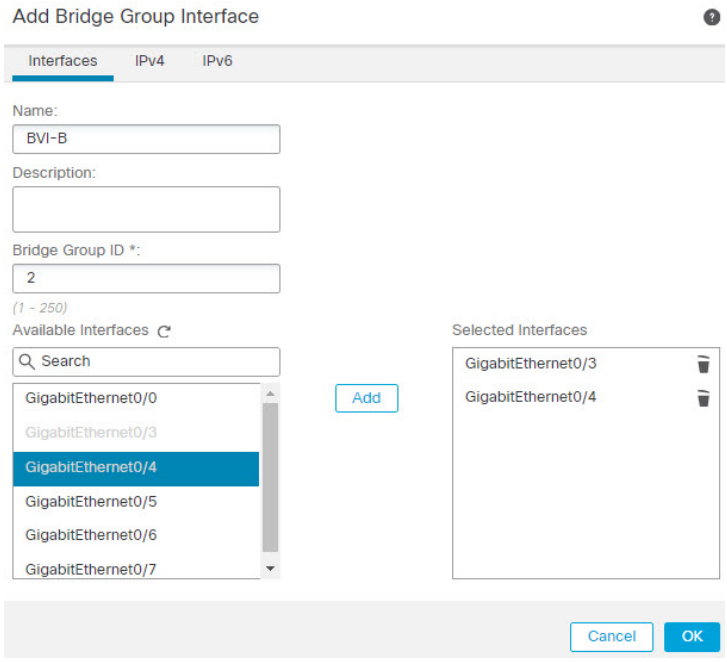


b) [OK] をクリックします。

c) [保存（Save）] をクリックします。

a) BVI-B の次の詳細情報を入力します。

- [名前（Name）]：この例では、「BVI-B」。
- [ブリッジグループID（Bridge Group ID）]：この例では、「2」。
- [利用可能なインターフェイス（Available Interface）]：サブインターフェイスを選択します。
- [IPv4] で、[IP Type] として [Use Static IP] を選択します。
- [IPアドレス（IP Address）]：2 つのインターフェイスが重複する IP アドレスを持つことをシステムが許可しないため、このフィールドは空のままにします。仮想ルータで IP アドレスを調整した後に、ブリッジグループに再度アクセスし、同じ IP アドレスを指定することができます。



b) [OK] をクリックします。

c) [保存（Save）] をクリックします。

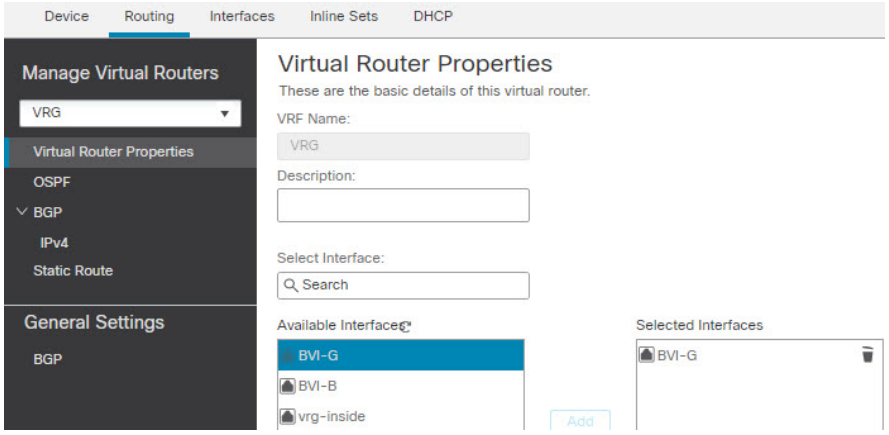
ステップ 3 仮想ルータ（VRG）を作成し、そのネットワークとして BVI-G を選択します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

b) デバイスを編集し、**[ルーティング（Routing）] > [仮想ルータの管理（Manage Virtual Routers）]** を選択します。

c) [仮想ルータの追加（Add Virtual Router）] をクリックします。仮想ルータの名前を入力し、[OK] をクリックします。

d) [仮想ルーティングのプロパティ（Virtual Routing Properties）] で、[BVI-G] を選択し、[追加（Add）] をクリックします。



e) [保存（Save）] をクリックします。

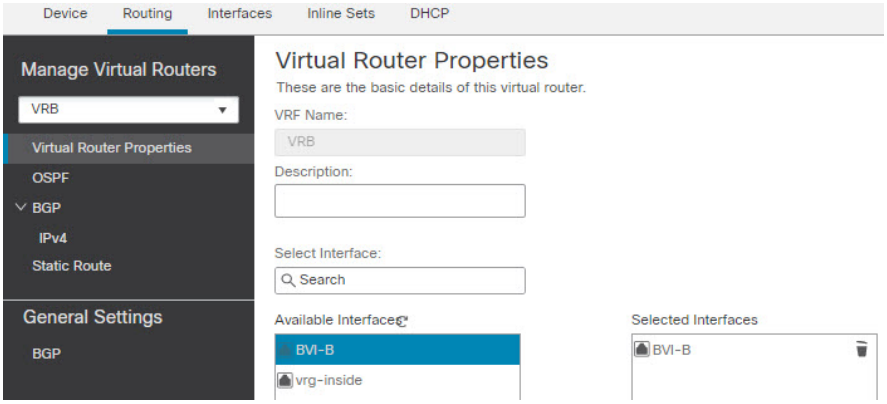
ステップ 4 仮想ルータ（VRB）を作成し、そのネットワークとして BVI-B を選択します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

b) デバイスを編集し、**[ルーティング（Routing）]** > **[仮想ルータの管理（Manage Virtual Routers）]** を選択します。

c) [仮想ルータの追加（Add Virtual Router）] をクリックします。仮想ルータの名前を入力し、[OK] をクリックします。

d) [仮想ルーティングのプロパティ（Virtual Routing Properties）] で、[BVI-B] を選択し、[追加（Add）] をクリックします。



e) [保存（Save）] をクリックします。

ステップ 5 BVI-B の設定に再度アクセスします。

a) **[Devices]** > **[Device Management]** > **[Interfaces]** の順に選択します。

b) BVI-B インターフェイスに対して [編集（Edit）] をクリックします。IP アドレスを「10.10.10.5/24」と指定します。インターフェイスが 2 つの異なる仮想ルータに個別に割り当てられたため、BVI-G に同じ IP アドレスを設定できるようになりました。

c) [OK] をクリックします。

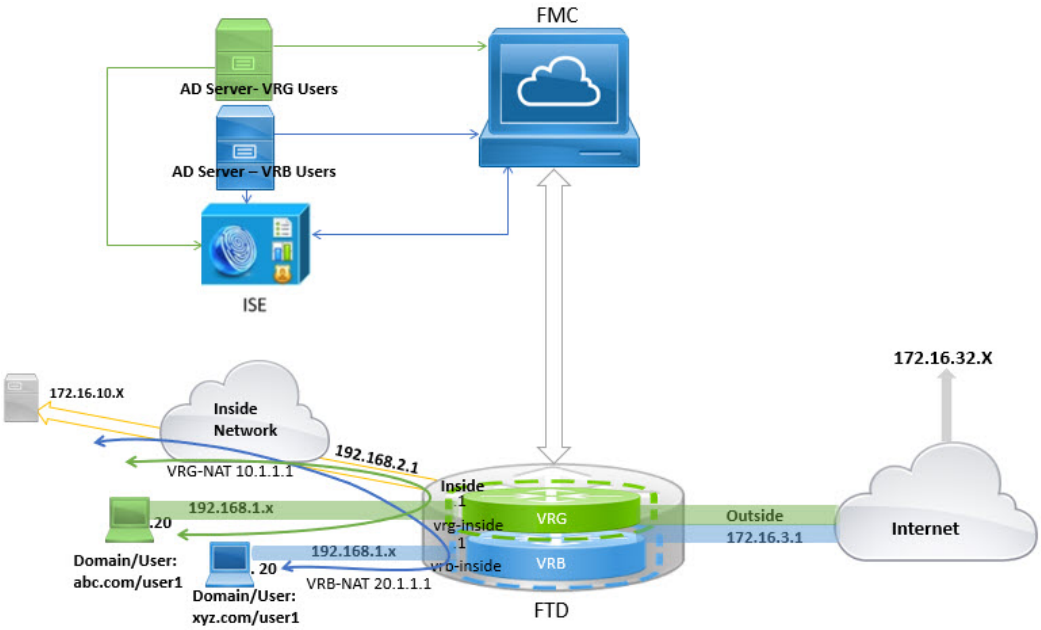
d) [保存（Save）] をクリックします。

BVI 間通信を有効にする場合は、外部ルータをデフォルトゲートウェイとして使用します。この例のような重複 BVI のシナリオでは、Twice NAT 外部ルータをゲートウェイとして使用して、BVI 間トラフィックを確立します。ブリッジ グループのメンバーの NAT を設定するときは、メンバー インターフェイスを指定します。ブリッジ グループ インターフェイス（BVI）自体に NAT を設定することはできません。ブリッジ グループ メンバーのインターフェイス間で NAT を実行するときには、実際のおよびマッピングされたアドレスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。

重複するネットワークを使用したユーザー認証の設定方法

仮想ルーティングでは、IP が重複し、ユーザーが重複する複数の仮想ルータを構成できます。この例では、VRG と VRB は、IP（192.168.1.1/24）が重複している仮想ルータです。2 つの異なるドメインのユーザーは、重複するネットワーク IP（192.168.1.20）にも存在します。VRG

およびVRBユーザーが共有サーバー172.16.10.Xにアクセスする場合、ルートはグローバル仮想ルータにリークされます。送信元NATを使用して、重複するIPを処理します。VRGおよびVRBユーザーからのアクセスを制御するには、Firewall Management Centerでユーザー認証を設定する必要があります。Firewall Management Centerでは、レルム、Active Directory、アイデンティティソース、アイデンティティルールとポリシーを使用して、ユーザーIDが認証されます。Firewall Threat Defenseにはユーザーの認証に関する直接的な役割がないため、ユーザーアクセスはアクセスコントロールポリシーを通じてのみ管理されます。重複するユーザーからのトラフィックを制御するには、IDポリシーとルールを使用してアクセスコントロールポリシーを作成します。



始める前に

この例では、次のことを前提としています。

- VRGおよびVRBユーザー用の2つのADサーバーがある。
- ISEに2つのADサーバーが追加されている。

手順

ステップ1 VRGのデバイスの内部インターフェイスを設定します。

a) **[Devices]** > **[Device Management]** > **[Interfaces]** の順に選択します。

b) VRGに割り当てるインターフェイスを編集します。

- [名前（Name）]：この例では、VRG-inside。
- [有効（Enabled）]チェックボックスをオンにします。

- [IPv4] で、[IPタイプ（IP Type）] として [静的IPを使用する（Use Static IP）] を選択します。
- [IPアドレス（IP Address）]：192.168.1.1/24 を入力します。

c) [OK] をクリックします。
d) [保存（Save）] をクリックします。

ステップ 2 VRB のデバイスの内部インターフェイスを設定します。

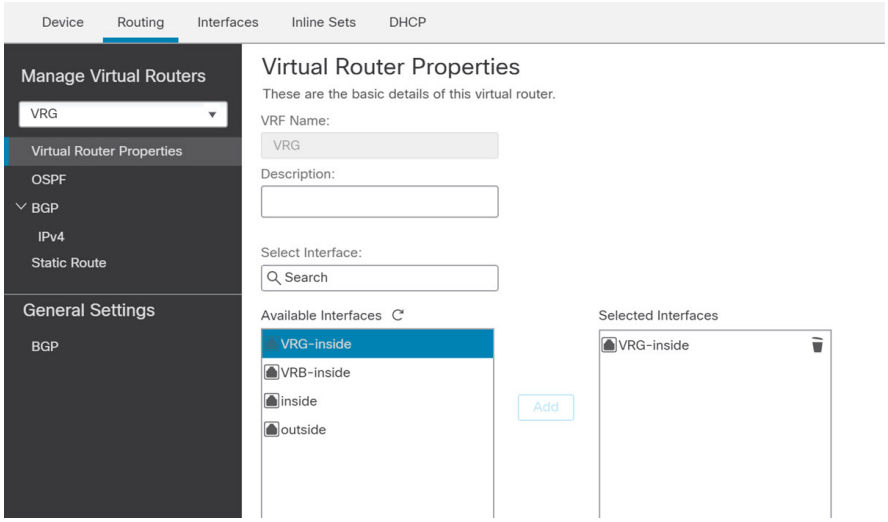
a) **[Devices]** > **[Device Management]** > **[Interfaces]** の順に選択します。
b) VRB に割り当てるインターフェイスを編集します。

- [名前（Name）]：この例では、VRB-inside。
- [有効（Enabled）] チェックボックスをオンにします。
- [IPv4] で、[IPタイプ（IP Type）] として [静的IPを使用する（Use Static IP）] を選択します。
- [IPアドレス（IP Address）]：空白のままにします。ユーザー定義の仮想ルータをまだ作成していないため、ユーザーは同じ IP アドレスを使用してインターフェイスを設定できません。

c) [OK] をクリックします。
d) [保存（Save）] をクリックします。

ステップ 3 VRG ユーザーが共通サーバー 172.16.10.1 にアクセスするためのグローバルルータの内部インターフェイスに対する VRG および静的デフォルトルートリークを設定します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。
b) **[ルーティング（Routing）]** > **[仮想ルータの管理（Manage Virtual Routers）]** の順に選択します。[仮想ルータの追加（Add Virtual Router）] をクリックして、VRG を作成します。
c) VRG の場合、[仮想ルータのプロパティ（Virtual Router Properties）] で、VRG-inside を割り当てて保存します。



d) [Static Route] をクリックします。

e) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：グローバルルータの内部インターフェイスを選択します。
- [ネットワーク（Network）]：any-ipv4 オブジェクトを選択します。
- [Gateway]：空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイを選択しません。

f) [OK] をクリックします。

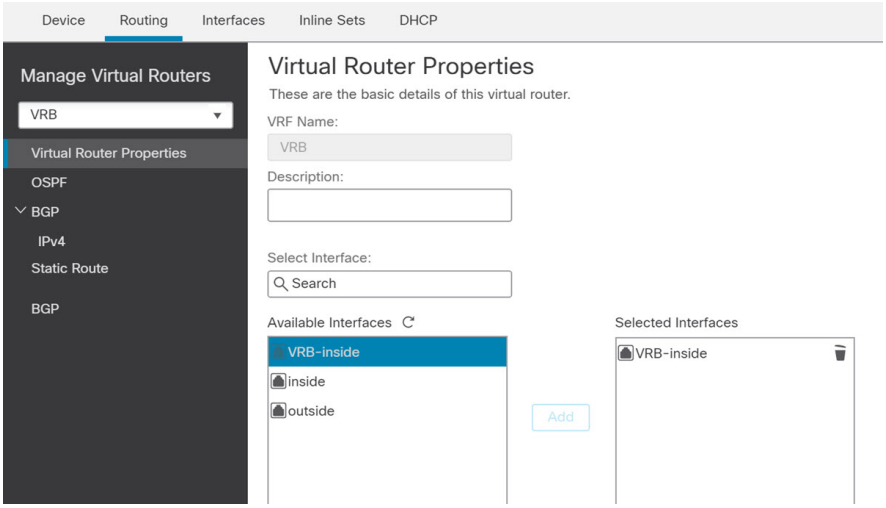
g) [保存（Save）] をクリックします。

ステップ 4 VRB ユーザーが共有サーバー 172.16.10.x にアクセスするためのグローバルルータの内部インターフェイスに対する VRB および静的デフォルトルートリークを設定します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) **[ルーティング（Routing）] > [仮想ルータの管理（Manage Virtual Routers）]** の順に選択します。[仮想ルータの追加（Add Virtual Router）] をクリックして、VRB を作成します。

c) VRB の場合、[仮想ルータのプロパティ（Virtual Router Properties）] で、VRB-inside を割り当てて保存します。



d) [Static Route] をクリックします。

e) [ルートを追加（Add Route）] をクリックします。[スタティックルート設定の追加（Add Static Route Configuration）] で、次の項目を指定します。

- [インターフェイス（Interface）]：グローバルルータの内部インターフェイスを選択します。
- [ネットワーク（Network）]：any-ipv4 オブジェクトを選択します。
- [Gateway]：空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイを選択しません。

f) [OK] をクリックします。

g) [保存（Save）] をクリックします。

ステップ 5 VRB-inside インターフェイスの設定を再確認します。

a) **[Devices]** > **[Device Management]** > **[Interfaces]** の順に選択します。

b) VRB-inside インターフェイスに対して [編集（Edit）] をクリックします。IP アドレスを 192.168.1.1/24 として指定します。インターフェイスが 2 つの異なる仮想ルータに個別に割り当てられたため、VR-inside に同じ IP アドレスを設定できるようになりました。

c) [OK] をクリックします。

d) [保存（Save）] をクリックします。

ステップ 6 ソースオブジェクト VRG および VRB の NAT ルールを追加します。**[デバイス（Devices）]** > **[NAT]**をクリックします。

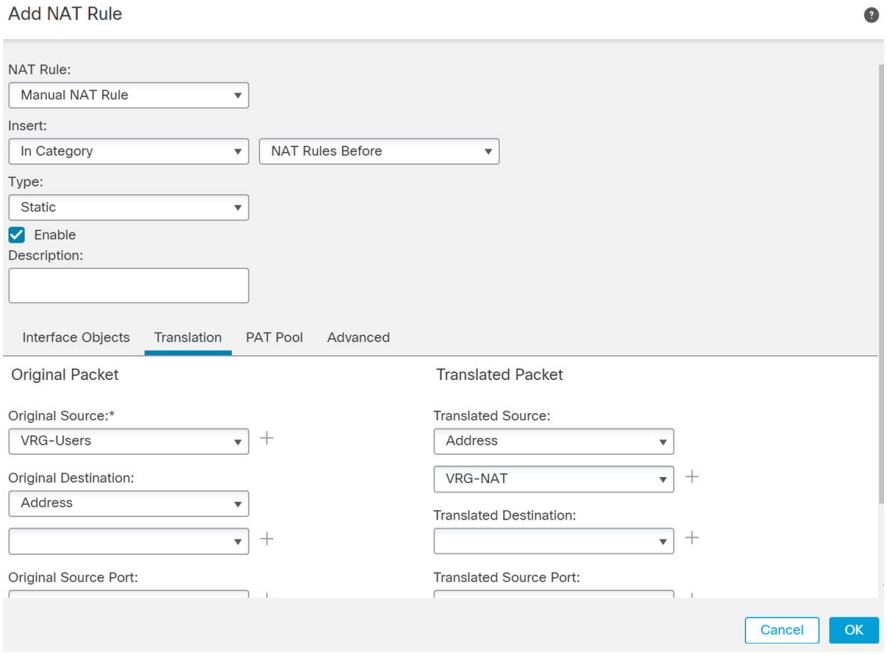
ステップ 7 **[新しいポリシー（New Policy）]** > **[Threat Defense NAT]** をクリックします。

ステップ 8 NAT ポリシー名を入力し、Firewall Threat Defense デバイスを選択します。[保存（Save）] をクリックします。

ステップ 9 [NAT] ページで、[ルールの追加（Add Rule）] をクリックし、VRG の次の送信元 NAT を定義します。

- [NATルール（NAT Rule）]：[手動NATルール（Manual NAT Rule）] を選択します。

- [タイプ（Type）]：[静的（Static）] を選択します。
- [挿入（Insert）]：NAT ルールが存在する場合は [前述（Above）] を選択します。
- [Enabled] をクリックします。
- [インターフェイス オブジェクト（Interface Objects）] で、VRG-Inside オブジェクトを選択し、[ソースに追加（Add to Source）] をクリックします（オブジェクトがない場合は、**[オブジェクト（Object）]** > **[オブジェクト管理（Object Management）]** > **[インターフェイス（Interface）]** でオブジェクトを作成します）。次に、Global-Inside オブジェクトを選択して [宛先に追加（Add to Destination）] をクリックします。
- [変換（Translation）] で、以下を選択します。
  - [元の送信元（Original Source）] で VRG-Users を選択します。
  - [変換済み送信元（Translated Source）] で、[追加（Add）] をクリックし、10.1.1.1 を指定してオブジェクト VRG-NAT を定義します。次の図に示されているように、VRG-NAT を選択します。

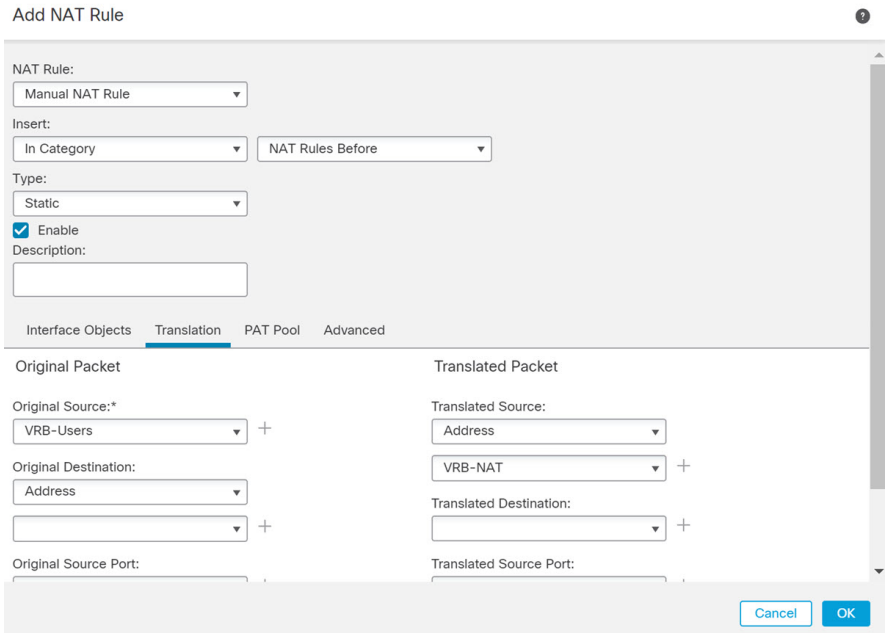


ステップ 10 [OK] をクリックします。

ステップ 11 [NAT] ページで、[ルールの追加（Add Rule）] をクリックし、VRB の次の送信元 NAT を定義します。

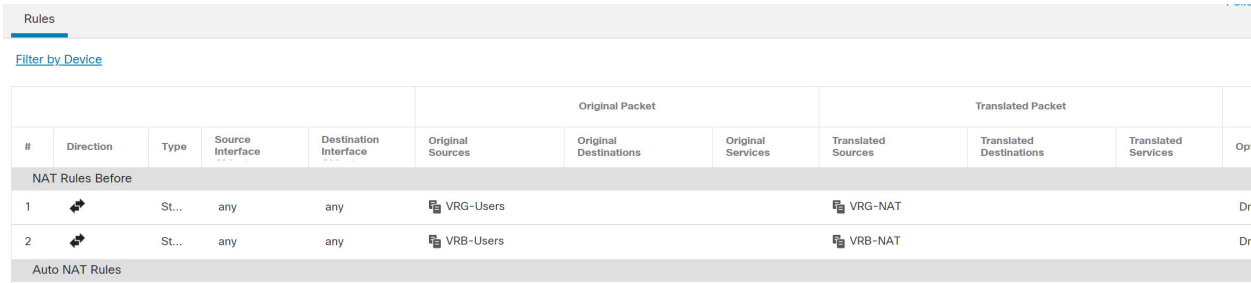
- [NATルール（NAT Rule）]：[手動NATルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[静的（Static）] を選択します。
- [挿入（Insert）]：NAT ルールが存在する場合は [前述（Above）] を選択します。
- [Enabled] をクリックします。

- [インターフェイス オブジェクト（Interface Objects）] で、VRB-Inside オブジェクトを選択し、[ソースに追加（Add to Source）] をクリックします（オブジェクトがない場合は、**[オブジェクト（Object）] > [オブジェクト管理（Object Management）] > [インターフェイス（Interface）]**でオブジェクトを作成します）。次に、Global-Inside オブジェクトを選択して [宛先に追加（Add to Destination）] をクリックします。
- [変換（Translation）] で、以下を選択します。
  - [元の送信元（Original Source）] で VRG-Users を選択します。
  - [変換済み送信元（Translated Source）] で、[追加（Add）] をクリックし、20.1.1.1 を指定してオブジェクト VRB-NAT を定義します。次の図に示されているように、VRB-NAT を選択します。



ステップ 12 **[保存（Save）]** をクリックします。

NAT ルールは次のようになります。



ステップ 13 Firewall Management Center に 2 つの一意の AD サーバー（VRG および VRB ユーザーごとに 1 つ）を追加します（**[システム（System）] > [統合（Integration）] > [レルム（Realms）]** を選択します）。

ステップ 14 [新しいレルム（New Realm）] をクリックして、フィールドに入力します。各フィールドの詳細については、レルム フィールド （2464 ページ）を参照してください。

ステップ 15 VRG および VRB ユーザーからのアクセスを制御するには、2 つの Active Directory を定義します。[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド （2468 ページ）を参照LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452 ページ）を参照してください。

ステップ 16 Firewall Management Center に ISE を追加します（**[システム（System）]** > **[統合（Integration）]** > **[アイデンティティ ソース（Identity Sources）]** を選択）。

ステップ 17 [Identity Services Engine] をクリックして、フィールドに入力します。各フィールドの詳細については、レルムを使用したユーザー制御用 ISE/ISE-PIC の設定方法 （2505 ページ）を参照してください。

ステップ 18 ID ポリシーとルールを作成し、VRG および VRB からの重複するユーザーのアクセスを制御するためのアクセス コントロール ポリシーを定義します。

BGP を使用して仮想ルータを相互接続する方法

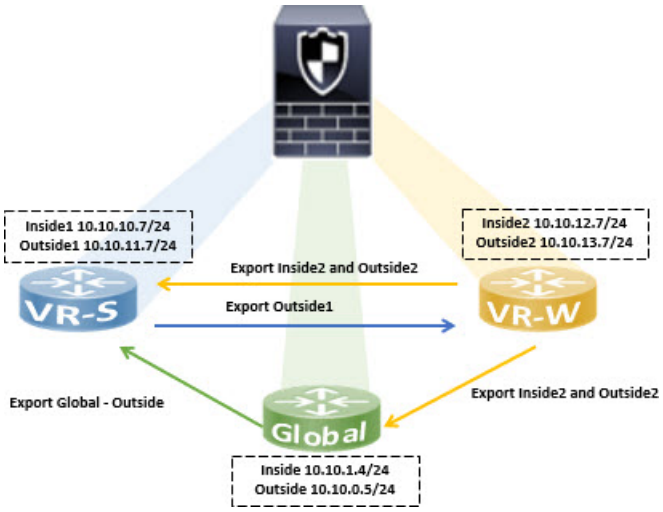
デバイスで BGP 設定を構成して、仮想ルータ（グローバルおよびユーザー定義の仮想ルータ）間のルートをリークできるようになりました。送信元仮想ルータのルートターゲットは BGP テーブルにエクスポートされ、次に宛先の仮想ルータにインポートされます。ルートマップは、グローバル仮想ルートをユーザー定義の仮想ルータと共有するために使用することも、その逆も可能です。BGP テーブルへのルートのインポートまたはエクスポートはすべて、グローバル仮想ルートを含む、ユーザー定義の仮想ルータで構成されることに注意してください。

工場のファイアウォールデバイスが次の仮想ルータとインターフェイスで構成されているとします。

- グローバル仮想ルータは Inside（10.10.1.4/24）および Outside（10.10.0.5/24）で構成されます。
- VR-S（営業）仮想ルータは Inside1（10.10.10.7/24）および Outside1（10.10.11.7/24）で構成されます。
- VR-W（倉庫）仮想ルータは Inside2（10.10.12.7/24）および Outside2（10.10.13.7/24）で構成されます。

倉庫（VR-W）のルートを営業（VR-S）とグローバルを使用してリークし、VR-S の外部インターフェイスルートを VR-W にリークするとします。同様に、グローバルルータの外部インターフェイスルートを営業（VR-S）にリークする必要があります。この例では、ルータの相互接続を実現するための BGP 構成手順を示しています。

図 *291 : BGP* を使用した仮想ルータの相互接続



始める前に

- 仮想ルータの作成：VR-S および VR-W。
- BGP を有効にし、各仮想ルータで接続されたルートの再配布用に BGP を構成します。

手順

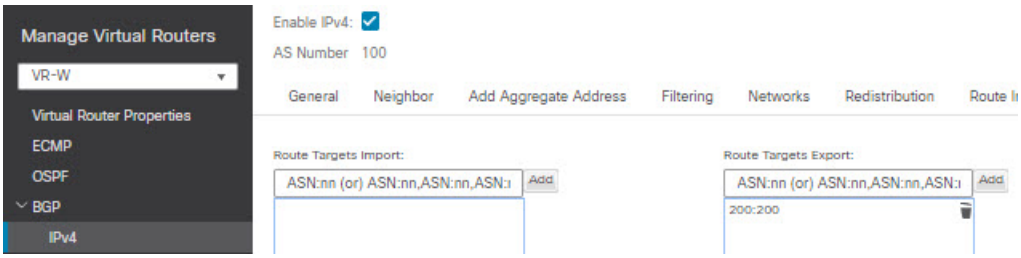
ステップ 1 ルートターゲットでタグ付けされたルートを VR-S にエクスポートするように VR-W を構成します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択し、 デバイスを編集して [ルーティング（Routing）] タブをクリックします。

b) 仮想ルータのドロップダウンから、VR-W を選択します。

c) **[BGP] > [IPv4] > [ルートのインポート/エクスポート（Route Import/Export）]**をクリックします。

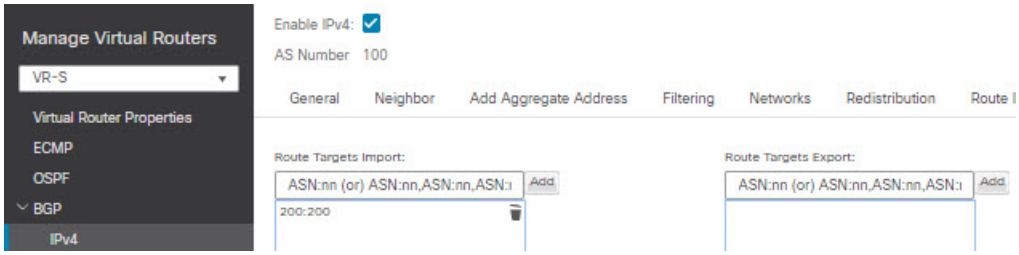
d) VR-W ルートを VR-S にリークするには、ルートにルートターゲットのタグを付けます。これにより、VR-W ルートは、ルートターゲットとマークされた BGP テーブルにエクスポートされます。[ルートターゲットのエクスポート（Route Targets Export）] フィールドに、*200:200* などの値を入力します。[追加（Add）] をクリックします。



e) 仮想ルータのドロップダウンから、VR-S を選択します。

f) **[BGP]** > **[IPv4]** > **[ルートのインポート/エクスポート（Route Import/Export）]**をクリックします。

g) VR-W からリークされたルートを受け取るには、ルートターゲットのインポートを構成して、（ピアまたは再配布された）BGP テーブルから、ルートターゲットとマークされた VR-W ルートをインポートします。[ルートターゲットのインポート（Route Targets Import）] フィールドに、VR-W に設定したのと同じルートターゲット値（*200:200*）を入力します。[Add] をクリックします。



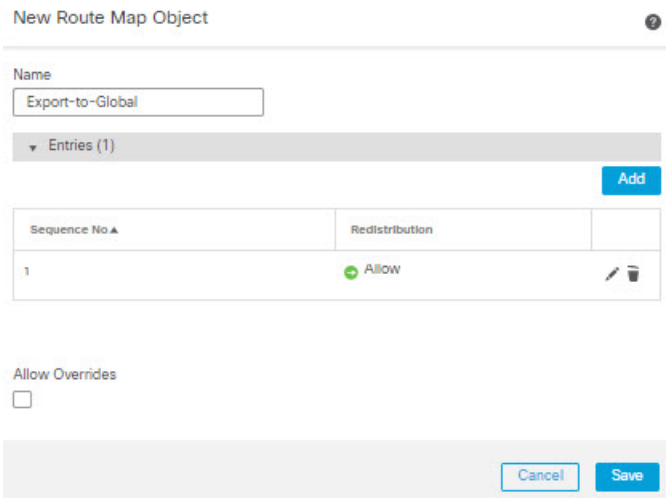
（注）
VR-W からリークされるルートを条件付きにする場合は、ルートマップオブジェクトで一致基準を指定し、[ユーザー仮想ルータのエクスポートルートマップ（User Virtual Router Export Route Map）] でそれを選択できます。同様に、BGP テーブルから VR-S にインポートするルートを条件付きにする場合は、[ユーザー仮想ルータのインポートルートマップ（User Virtual Router Import Route Map）] を使用できます。この手順については、ステップ 3 で説明します。

ステップ 2 ルートをグローバル仮想ルータにエクスポートするように VR-W を構成します。

a) VR-W ルートをグローバルルーティングテーブルにエクスポートできるようにするルートマップを作成する必要があります。**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]** > **[ルートマップ（Route Map）]**を選択します。

b) [ルートマップの追加（Add Route Map）] をクリックし、*Export-to-Global* などの名前を付けて、[追加（Add）] をクリックします。

c) [シーケンス番号（Sequence Number）]（1 など）を指定し、[再配布（Redistribution）] ドロップダウンリストから [許可（Allow）] を選択します。

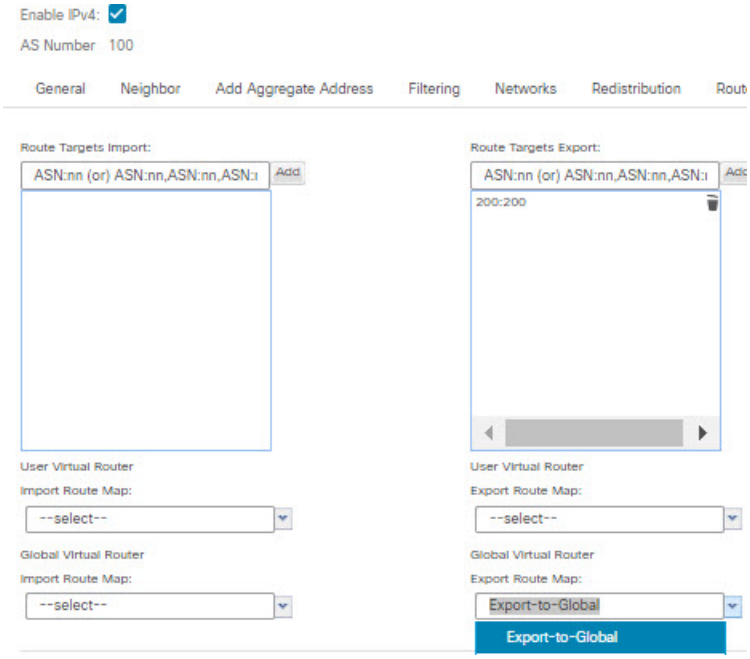


d) [保存（Save）] をクリックします。

この例では、すべての VR-W ルートがグローバル ルーティング テーブルにリークされます。したがって、ルートマップには一致基準が設定されません。

e) デバイスの [ルーティング（Routing）] タブに移動し、VR-W を選択します。**[BGP]** > **[IPv4]** > **[ルートのインポート/エクスポート（Route Import/Export）]** をクリックします。

f) [グローバル仮想ルータのエクスポートルートマップ（Global Virtual Router Export Route Map）] ドロップダウンリストから、[Export-to-Global] を選択します。



ステップ 3 VR-S の Outside1 ルートのみを VR-W にリークするには：

a) 仮想ルータのドロップダウンから、VR-S を選択します。

b) **[BGP]** > **[IPv4]** > **[ルートのインポート/エクスポート（Route Import/Export）]**をクリックします。

c) VR-S ルートを VR-W にリークするには、ルートにルートターゲットのタグを付けます。これにより、VR-S ルートは、ルートターゲットとマークされた BGP テーブルにエクスポートされます。[ルートターゲットのエクスポート（Route Targets Export）] フィールドに、*100:100* などの値を入力します。[Add] をクリックします。

d) 仮想ルータのドロップダウンから [VR-W] を選択し、**[BGP]** > **[IPv4]** > **[ルートのインポート/エクスポート（Route Import/Export）]**を選択します。

e) VR-S からリークされたルートを受け取るには、ルートターゲットのインポートを構成して、（ピアまたは再配布された）BGP テーブルから、ルートターゲットとマークされた VR-S ルートをインポートします。[ルートターゲットのエクスポート（Route Targets Export）] フィールドに、VR-S のルートターゲットの値（*100:100*）を入力します。[Add] をクリックします。

f) ここで、VR-S の Outside1 ルートのみが VR-W にリークされることを条件付ける必要があります。**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[プレフィックスリスト（Prefix List）]** > **[IPv4プレフィックスリスト（IPv4 Prefix List）]** を選択します。

g) [IPv4プレフィックスリストの追加（Add IPv4 Prefix List）] をクリックし、*VRS-Outside1-Only* などの名前を付けて、[追加（Add）] をクリックします。

h) [シーケンス番号（Sequence Number）]（1 など）を指定し、[再配布（Redistribution）] ドロップダウンリストから [許可（Allow）] を選択します。

i) VR-S Outside1 インターフェイスの IP アドレス（最初の 2 オクテット）を入力します。

j) [保存（Save）] をクリックします。

k) プレフィックスリストを含む match 句を使用してルートマップを作成します。[ルートマップ（Route Map）] をクリックします。[ルートマップの追加（Add Route Map）] をクリックし、*Import-from-VRS* などの名前を付けて、[追加（Add）] をクリックします。

l) [シーケンス番号（Sequence Number）]（1 など）を指定し、[再配布（Redistribution）] ドロップダウンリストから [許可（Allow）] を選択します。

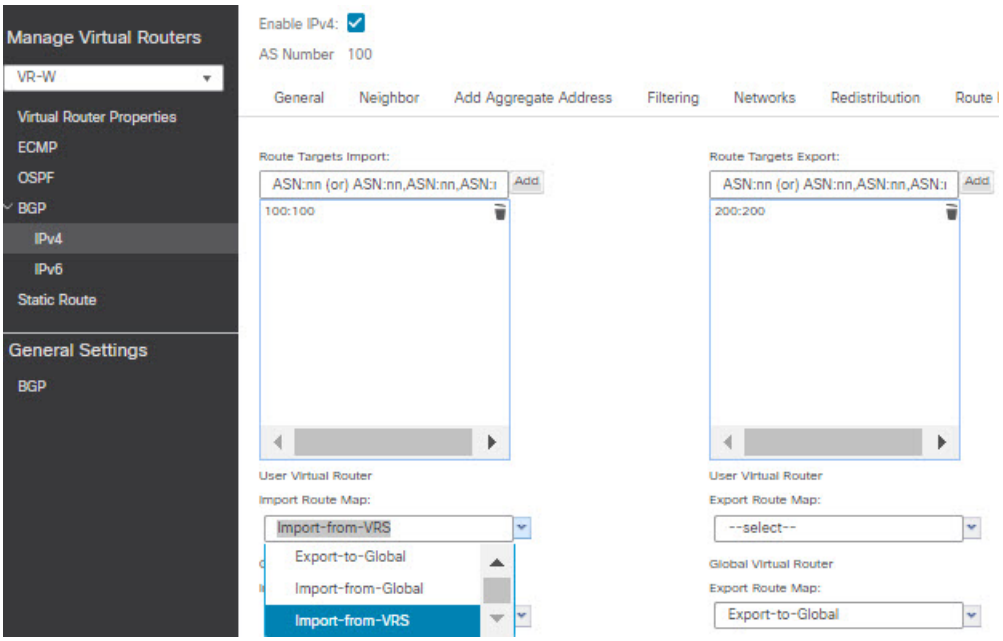
m) [match 句（Match Clause）] タブで [IPv4] をクリックします。[アドレス（Address）] タブで、[プレフィックスリスト（Prefix List）] をクリックします。

n) [利用可能なIPv4プレフィックスリスト（Available IPv4 Prefix List）] で、[VRS-Outside1-Only] を選択し、[追加（Add）] をクリックします。

o) [保存（Save）] をクリックします。

p) デバイスの [ルーティング（Routing）] タブに移動し、VR-W を選択します。**[BGP]** > **[IPv4]** > **[ルートのインポート/エクスポート（Route Import/Export）]**をクリックします。

q) [グローバル仮想ルータのインポートルートマップ（Global Virtual Router Import Route Map）] ドロップダウンリストから、[Import-from-VRS] を選択します。



ステップ 4 グローバル仮想ルータの Outside ルートをインポートするように VR-S を構成します。

（注）
グローバル仮想ルータとの間でルートをリークするには、送信元または宛先のユーザー定義仮想ルータをそれぞれ構成する必要があります。したがって、この例では、VR-S は、グローバル仮想ルータの Outside インターフェイスからルートをインポートする宛先ルータとなります。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [プレフィックスリスト（]Prefix List）] > [IPv4プレフィックスリスト（IPv4 Prefix List）]** を選択します。

b) [IPv4プレフィックスリストの追加（Add IPv4 Prefix List）] をクリックし、*Global-Outside-Only* などの名前を付けて、[追加（Add）] をクリックします。

c) [シーケンス番号（Sequence Number）]（1 など）を指定し、[再配布（Redistribution）] ドロップダウンリストから [許可（Allow）] を選択します。

d) グローバル Outside インターフェイスの IP アドレス（最初の 2 オクテット）を入力します。

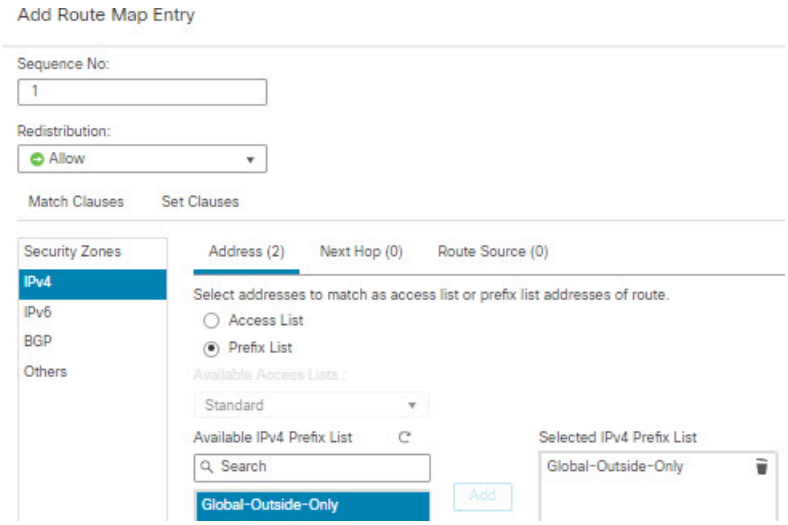
e) [保存（Save）] をクリックします。

f) [ルートマップ（Route Map）] をクリックします。[ルートマップの追加（Add Route Map）] をクリックし、*Import-from-Global* などの名前を付けて、[追加（Add）] をクリックします。

g) [シーケンス番号（Sequence Number）]（1 など）を指定し、[再配布（Redistribution）] ドロップダウンリストから [許可（Allow）] を選択します。

h) [match 句（Match Clause）] タブで [IPv4] をクリックします。[アドレス（Address）] タブで、[プレフィックスリスト（Prefix List）] をクリックします。

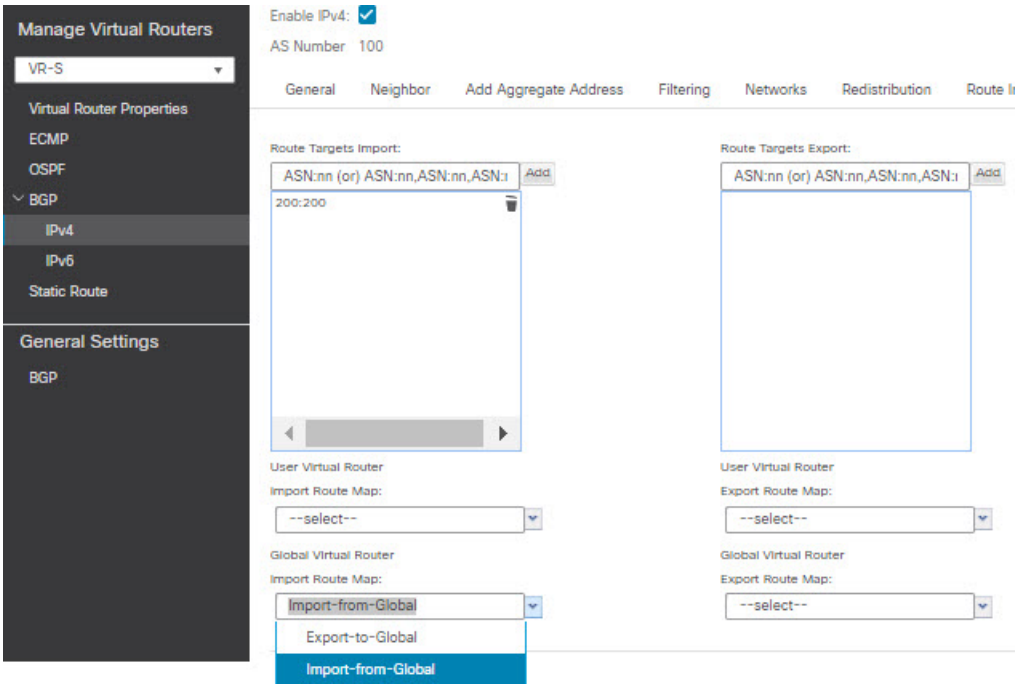
i) [利用可能なIPv4プレフィックスリスト（Available IPv4 Prefix List）] で、[Global-Outside-Only] を選択し、[追加（Add）] をクリックします。



j) [保存（Save）] をクリックします。

k) デバイスの [ルーティング（Routing）] タブに移動し、VR-S を選択します。**[BGP]** > **[IPv4]** > **[ルートのインポート/エクスポート（Route Import/Export）]**をクリックします。

l) [グローバル仮想ルータのインポートルートマップ（Global Virtual Router Import Route Map）] ドロップダウンリストから、[Import-from-Global] を選択します。

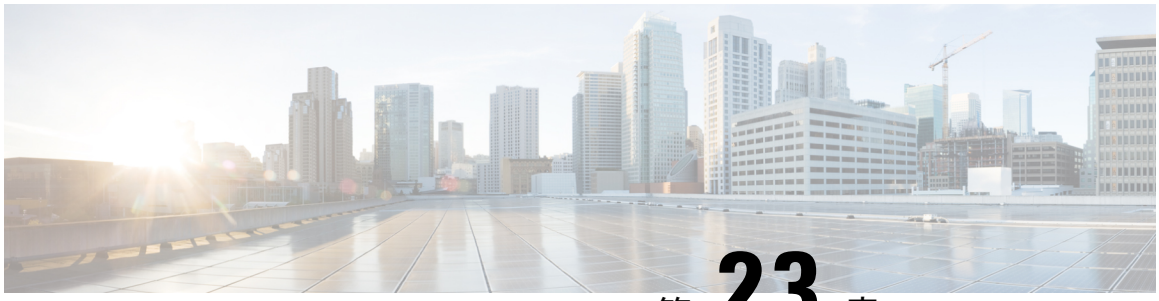


ステップ 5 [保存（Save）]、[展開（Deploy）] の順にクリックします。

仮想ルータの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ISA 3000 の仮想ルータサポート。	7.0	7.0	ISA 3000 には最大 10 の仮想ルータを設定できます。
ユーザー定義の仮想ルータでの SNMP サポート	7.0	7.0	ユーザー定義の仮想ルータで SNMP を設定できるようになりました。
仮想ルータの一括削除。	6.7	6.6	一度に複数の仮想ルータを Threat Defense から削除できます。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [仮想ルータの管理（Manage Virtual Routers）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Threat Defense の仮想ルータと VRF-Lite。	6.6	6.6	複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できるようになりました。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。仮想ルータは、Virtual Routing and Forwarding の「軽量」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。作成できる仮想ルータの最大数は 5 ～ 100 の範囲で、デバイスのモデルによって異なります。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**のデバイスの編集の **[ルーティング（Routing）]** タブ 新規/変更された CLI コマンド：。 • **show vrf** • ［**vrf** *name* | **all**］キーワードセットを CLI コマンド **clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters** に追加し、必要に応じて出力が仮想ルータ情報を表示するように変更 プラットフォームの制限：Firepower 1010 および ISA 3000 ではサポートされていません。



第 23 章

ECMP

この章では、ルーティングプロトコルでネットワークトラフィックの負荷分散に使用される等コストマルチパス（ECMP）ルーティングを設定する手順について説明します。

- ECMP について （1153 ページ）
- ECMP の注意事項と制限事項 （1153 ページ）
- ECMP の管理ページ （1154 ページ）
- ECMP ゾーンの作成 （1155 ページ）
- 等コストスタティックルートの設定 （1156 ページ）
- ECMP ゾーンの変更 （1157 ページ）
- ECMP ゾーンの削除 （1158 ページ）
- ECMP の設定例 （1158 ページ）
- Secure Firewall Threat Defense の ECMP の履歴 （1162 ページ）

ECMP について

Firepower Threat Defense デバイスは、等コストマルチパス（ECMP）ルーティングをサポートしています。インターフェイスのグループを含むように、仮想ルータごとにトラフィックゾーンを設定できます。各ゾーンにある最大 8 つのインターフェイス間に最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

ECMP の注意事項と制限事項

ファイアウォール モードのガイドライン

ECMP ゾーンは、ルーテッド ファイアウォール モードでのみサポートされています。

インターフェイスのガイドライン

dVTI とループバック インターフェイスはサポートされていません。

その他のガイドライン

- デバイスには、最大 256 の ECMP ゾーンを設定できます。
- ECMP ゾーンごとに 8 つのインターフェイスのみを関連付けられます。
- 1 つのインターフェイスがメンバーになれる ECMP ゾーンは 1 つだけです。
- 等コストのスタティックルートに関連付けられているインターフェイスは、ECMP ゾーンから削除できません。
- インターフェイスに等コストのスタティックルートが関連付けられている場合、ECMP ゾーンは削除できません。
- ルーテッドインターフェイスのみを ECMP ゾーンに関連付けられます。
- 次のインターフェイスは、ECMP ゾーンに関連付けられません。
  - BVI インターフェイス。
  - EtherChannel のメンバーインターフェイス。
  - フェールオーバーまたはステート リンク インターフェイス。
  - 管理専用インターフェイスまたは管理アクセスインターフェイス。
  - クラスタ制御リンクインターフェイス。
  - VNI。
  - VLAN インターフェイス
  - SSL が有効になっているリモートアクセス VPN 設定のインターフェイス。
- ECMP ゾーン内のインターフェイスでは DHCP リレーはサポートされていません。
- デュアル ISP/WAN Firewall Threat Defense の展開：プライマリおよびセカンダリ データ インターフェイス用に単一の ECMP ゾーンを作成します。この構成により、同じメトリック値を持つ両方のインターフェイスのスタティックルートを作成できます。
- Firewall Threat Defense は、IPsec セッションでの NAT を使用した ECMP をサポートしていません。標準の IPsec 仮想プライベートネットワーク（VPN）トンネルは、IPsec パケットの提供パス内の NAT ポイントでは機能しません。

ECMP の管理ページ

[ルーティング（Routing）] ペインで [ECMP] をクリックすると、仮想ルータに対応する ECMP ページが表示されます。このページには、仮想ルータの関連インターフェイスを持つ既存の

ECMPゾーンが表示されます。このページでは、仮想ルータにECMPゾーンを追加できます。ECMP の[編集（Edit）]（）と[削除（Delete）]（）もできます。

次を実行します。

- ECMP ゾーンの作成 （1155 ページ）
- 等コストスタティックルートの設定 （1156 ページ）
- ECMP ゾーンの変更 （1157 ページ）
- ECMP ゾーンの削除 （1158 ページ）

ECMP ゾーンの作成

ECMP ゾーンは、仮想ルータごとに作成されるため、ECMP が作成されている仮想ルータのインターフェイスのみを ECMP に関連付けることができます。

手順

ステップ 1 **[デバイス（Devices）]>[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 仮想ルータのドロップダウンから、ECMP ゾーンを作成する仮想ルータを選択します。

グローバル仮想ルータおよびユーザー定義の仮想ルータにECMPゾーンを作成できます。仮想ルータの作成については、仮想ルータの作成 （1103 ページ）を参照してください。

ステップ 4 [ECMP] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [ECMPの追加（Add ECMP）] ボックスに ECMP ゾーンの名前を入力します。

（注）
ECMP 名は、ルーテッドデバイスに対して一意である必要があります。

ステップ 7 インターフェイスを関連付けるには、[使用可能なインターフェイス（Available Interfaces）] ボックスでインターフェイスを選択し、[追加（Add）] をクリックします。

次の点を忘れないでください。

- 割り当てに使用できるのは、仮想ルータに属しているインターフェイスだけです。
- 論理名を持つインターフェイスのみが [Available Interfaces] ボックスの下にリストされます。インターフェイスを編集し、[インターフェイス（Interfaces）] で論理名を指定できます。設定を有効にするには、必ず変更を保存してください。

ステップ 8 [OK] をクリックします。

[ECMP] ページに、新しく作成された ECMP が表示されます。

ステップ 9 [保存（Save）] をクリックして、設定を展開します。

ECMP ゾーンインターフェイスを等コストのスタティックルートに関連付けるには、同じ宛先とメトリック値、および異なるゲートウェイを指定してインターフェイスを定義します。

次のタスク

- 等コストスタティックルートの設定 （1156 ページ）
- ECMP ゾーンの変更 （1157 ページ）
- ECMP ゾーンの削除 （1158 ページ）

等コストスタティックルートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
すべて	該当なし	Firewall Threat DefenseおよびFirewall Threat Defense Virtual	任意	Admin/Network Admin/Security Approver

グローバル仮想ルータとユーザー定義仮想ルータのどちらも、そのインターフェイスをデバイスの ECMP ゾーンに割り当てることができます。

始める前に

- インターフェイスの等コストスタティックルートを設定する場合は、必ず、それを ECMP ゾーンに関連付けてください。ECMP ゾーンの作成 （1155 ページ） を参照してください。
- 非 VRF 対応デバイスのすべてのルーティング設定は、グローバル仮想ルータでも使用できます。
- インターフェイスを ECMP ゾーンに関連付けずに、同じ宛先とメトリックでインターフェイスのスタティックルートを定義することはできません。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** ページで、Firewall Threat Defense デバイスを編集します。[ルーティング（Routing）] タブをクリックします。

ステップ 2 ドロップダウンリストから、インターフェイスが ECMP ゾーンに関連付けられている仮想ルータを選択します。

ステップ 3 インターフェイスの等コストスタティックルートを設定するには、[スタティックルート（Static Route）] をクリックします。

ステップ 4 [ルートを追加（Add Route）] をクリックして新しいルートを追加するか、既存のルートの場合は [編集（Edit）]（✎） をクリックします。

ステップ 5 [インターフェイス（Interface）] ドロップダウンから、仮想ルータと ECMP ゾーンに属するインターフェイスを選択します。

ステップ 6 [使用可能なネットワーク（Available Networks）] ボックスから宛先ネットワークを選択し、[追加（Add）] をクリックします。

ステップ 7 ネットワークのゲートウェイを入力します。

ステップ 8 メトリック値を入力します。1 ～ 254 の数値を指定できます。

ステップ 9 設定を保存するには、[保存（Save）] をクリックします。

ステップ 10 等コストスタティックルーティングを設定するには、手順を繰り返して、同じ ECMP ゾーンに含まれる別のインターフェイスのスタティックルートを、同じ宛先ネットワークとメトリック値で設定します。必ず、別のゲートウェイを指定してください。

次のタスク

- ECMP ゾーンの変更 （1157 ページ）
- ECMP ゾーンの削除 （1158 ページ）

ECMP ゾーンの変更

手順

ステップ 1 **[Devices]** > **[Device Management]** を選択し、FTD デバイスを編集します。

ステップ 2 [Routing] をクリックします。

ステップ 3 [ECMP] をクリックします。

ECMP ゾーンおよび関連付けられたインターフェイスが [ECMP] ページに表示されます。

ステップ 4 ECMP を変更するには、目的の ECMP に対する [編集（Edit）]（✎）をクリックします。[ECMP の編集（Edit ECMP）] ボックスでは、次のことができます。

- [ECMP名（ECMP Name）]：変更された名前がデバイスに対して一意であることを確認します。
- [インターフェイス（Interfaces）]：インターフェイスを追加または削除できます。すでに別の ECMP に関連付けられているインターフェイスを含めることはできません。また、等コストのスタティックルートに関連付けられているインターフェイスは削除できません。

ステップ 5 [OK] をクリックします。

ステップ 6 変更を保存するには、[Save] をクリックします。

次のタスク

- 等コストスタティックルートの設定 （1156 ページ）
- ECMP ゾーンの削除 （1158 ページ）

ECMP ゾーンの削除

手順

ステップ 1 **[Devices]** > **[Device Management]** を選択し、FTD デバイスを編集します。

ステップ 2 [Routing] をクリックします。

ステップ 3 [ECMP] をクリックします。

ECMP ゾーンおよび関連付けられたインターフェイスが [ECMP] ページに表示されます。

ステップ 4 ECMP ゾーンを削除するには、その ECMP ゾーンに対する [削除（Delete）]（🗑） をクリックします。

インターフェイスのいずれかが等コストのスタティックルートに関連付けられている場合、ECMP ゾーンは削除できません。

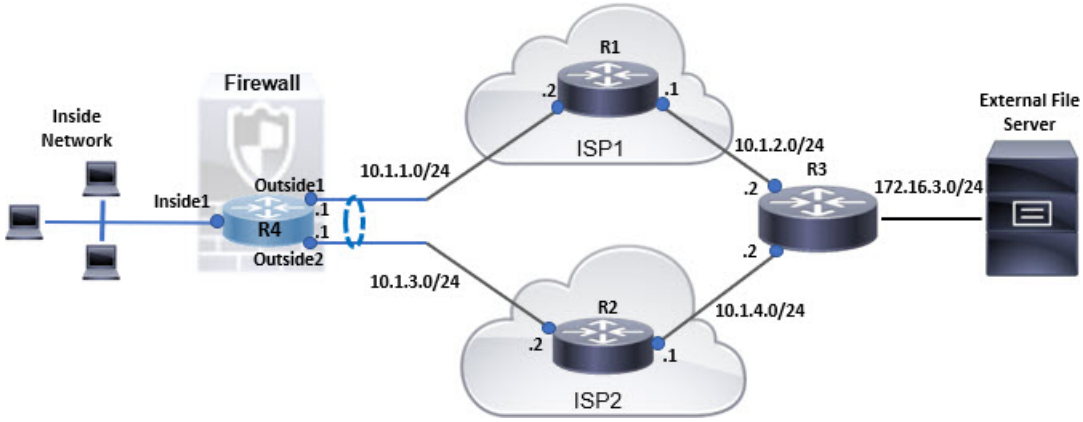
ステップ 5 確認メッセージで [削除（Delete）] をクリックします。

ステップ 6 変更を保存するには、[Save] をクリックします。

ECMP の設定例

この例では、Firewall Management Center を使用して、デバイスを通過するトラフィックが効率的に処理されるように Firewall Threat Defense の ECMP ゾーンを設定する方法を示しています。ECMP が設定されていると、Firewall Threat Defense ではゾーンごとにルーティングテーブルが維持されるため、可能な限り最良のルートでパケットを再ルーティングできます。そのため、ECMP は非対称ルーティング、負荷分散をサポートし、トラフィックの損失をシームレスに処理します。この例では、R4 は外部ファイルサーバーに到達する 2 つのパスを記録します。

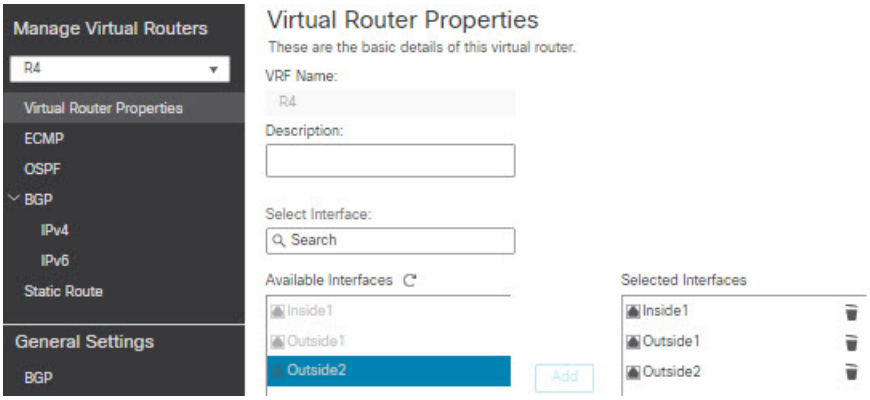
図 *292 : ECMP* の設定例



手順

ステップ 1 仮想ルータを作成します（*Inside1*、*Outside1*、*Outside2* インターフェイスを備えた *R4*）。

図 *293 : R4* 仮想ルータの設定



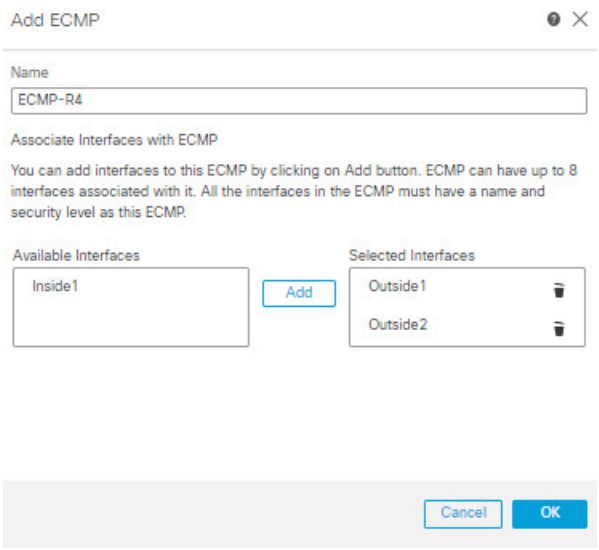
ステップ 2 ECMP ゾーンを作成します。

a) [ルーティング（Routing）] タブで、ユーザー定義の R4 仮想ルータを選択し、[ECMP] をクリックします。

b) [追加（Add）] をクリックします。

c) ECMP 名を入力し、[利用可能なインターフェイス（Available Interfaces）] リストから [Outside1] および [Outside2] を選択します。

図 *294 : ECMP* ゾーンの作成



d) [OK]、[保存（Save）] の順にクリックします。

ステップ 3 ゾーンインターフェイスのスタティックルートを作成します。

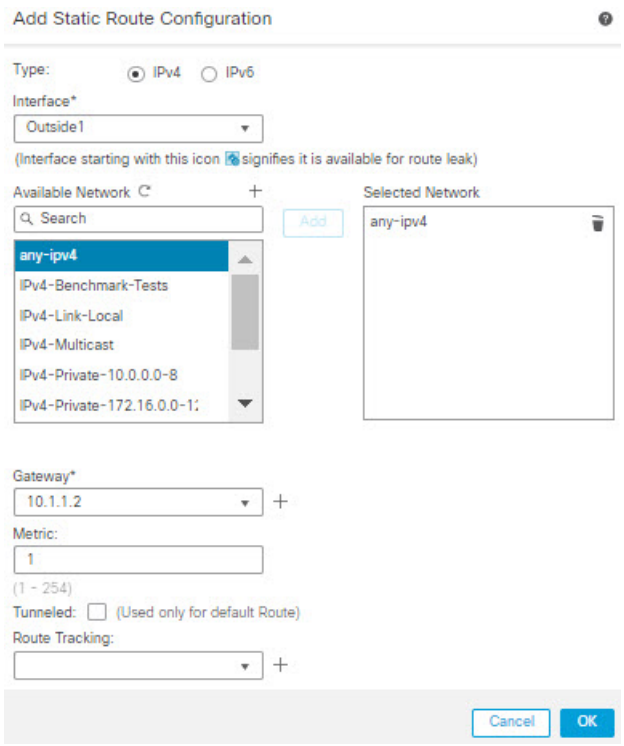
a) [ルーティング（Routing）] タブで、[スタティックルート（Static Route）] をクリックします。

b) [インターフェイス（Interface）] ドロップダウンリストから、[Outside1] を選択します。

c) [利用可能なネットワーク（Available Network）] で、any-ipv4 を選択し、[追加（Add）] をクリックします。

d) [ゲートウェイ（Gateway）] フィールドにネクストホップアドレス 10.1.1.2 を指定します。

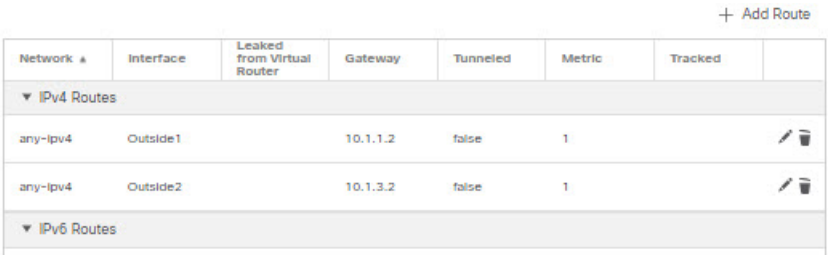
図 *295 : Outside1* のスタティックルートの設定



e) 手順 3b ～ 3d を繰り返して、Outside2 のスタティックルートを設定します。

同じメトリックを指定しますが、スタティックルートには異なるゲートウェイを指定します。

図 *296 : ECMP* ゾーンインターフェイスの設定済みスタティックルート

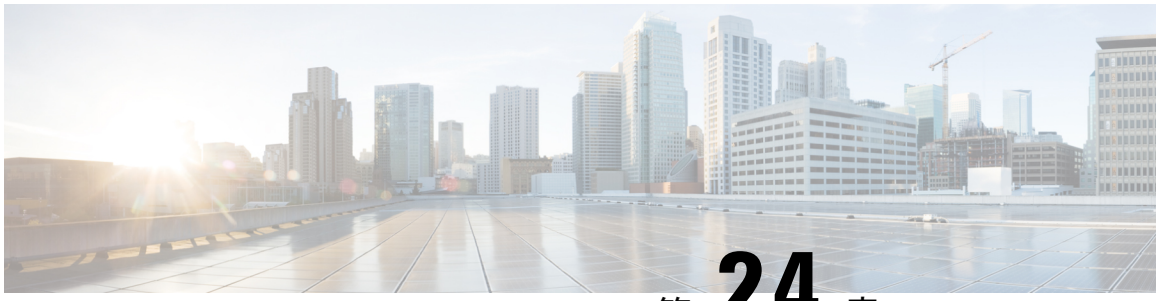


ステップ 4 [保存（Save）]、[展開（Deploy）] の順にクリックします。

ネットワークパケットは、ECMP アルゴリズムに基づいて、R4>R1>R3 または R4>R2>R3 に従って宛先 R3 に到達します。R1>R3 ルートが失われた場合、トラフィックはパケットドロップなしで R2 を通過します。同様に、*Outside1* からパケットを送信しても、R3 からの応答を *Outside2* が受信する可能性があります。さらに、ネットワークトラフィックが多い場合、R4 は 2 つのルート間でトラフィックを分散させ、負荷のバランスを取ります。

Secure Firewall Threat Defense の ECMP の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ルーティングポリシーとしての ECMP のサポート	7.1	任意（Any）	Secure Firewall Threat Defenseでは、以前は FlexConfig ポリシーを介して ECMP ルーティングがサポートされていました。このリリースから、インターフェイスをトラフィックゾーンにグループ化し、Secure Firewall Management Center でECMP ルーティングを設定できます。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [ECMP]**



第 24 章

双方向フォワーディング検出ルーティング

この章では、双方向フォワーディング検出（BFD）ルーティングプロトコルを使用するように Firewall Threat Defense を設定する方法について説明します。

- BFD ルーティングについて （1163 ページ）
- BFD ルーティングのガイドライン （1163 ページ）
- BFD の設定 （1165 ページ）
- BFD ルーティングの履歴 （1168 ページ）

BFD ルーティングについて

BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。BFD は、2 つのシステム間の転送データ プロトコルすべてに加えて、ユニキャストのポイントツーポイントモードで動作します。ただし、Firewall Threat Defense では、BFD は BGP プロトコルでのみサポートされます。パケットは、メディアやネットワークに対して適切なカプセル化プロトコルのペイロードで送信されます。

BFD は高速転送パス障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。ネットワーク管理者は BFD を使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

BFD ルーティングのガイドライン

コンテキスト モードのガイドライン

BFD は、すべての Firewall Threat Defense プラットフォームでサポートされています。また、マルチインスタンスモードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードではサポートされていますが、トランスペアレントモードではサポートされていません。

フェールオーバーとクラスタのガイドライン

- BFD は、フェールオーバー インターフェイスではサポートされていません。
- クラスタリングでは、BFD は制御ノードでのみサポートされています。

ルーティングとプロトコルのガイドライン

- BGP IPv4および BGP IPv6 プロトコルがサポートされています。

（注） 最適なルーティングを行うため、NSF の BGP グレースフル リスタートがデバイスで設定されている場合は、BFD を設定しないでください。

OSPFv2、OSPFv3、IS-IS、および EIGRP プロトコルはサポートされていません。

- スタティックルートの BFD はサポートされていません。BFD は、仮想ルータに属するインターフェイスでのみ設定できます。
- 名前付きインターフェイスのみサポートされています。
- BVI、VTI、およびループバック インターフェイスの BFD はサポートされていません。

シングルホップのガイドライン

- エコーモードはデフォルトで無効になっています。エコーモードはシングルホップでのみ有効にできます。
- エコー モードは IPv6 ではサポートされません。
- シングルホップポリシーを設定する場合は、シングルホップテンプレートのみを使用します。
- シングルホップテンプレートの認証は任意です。
- 同一インターフェイスには複数の BFD を設定できません。

マルチホップのガイドライン

- 送信元 IP アドレスを宛先 IP アドレスとしても設定しないでください。
- 送信元アドレスと宛先アドレスは、同じ IP タイプ（IPV4 または IPV6）である必要があります。

- ホストまたはネットワークタイプのネットワークオブジェクトのみが許可されます。
- マルチホップポリシーを設定する場合は、マルチホップテンプレートのみを使用します。
- マルチホップテンプレートの認証は必須です。

アップグレードのガイドライン

バージョン 7.3 にアップグレードし、以前のバージョンに FlexConfig BFD ポリシーがある場合、展開中に Management Center に警告メッセージが表示されます。ただし、展開プロセスは停止しません。アップグレード後の展開後、UI（**[デバイスの編集（Device (Edit)）] > [ルーティング（Routing）] > [BFD]**）から BFD ポリシーを管理するには、**[デバイスの編集（Device (Edit)）] > [ルーティング（Routing）] > [BFD]**ページで BFD ポリシーを設定し、デバイスの FlexConfig ポリシーから設定を削除する必要があります。を参照してください。

BFD の設定

ここでは、システムで BFD ルーティングプロセスを有効にして設定する方法について説明します。

手順

ステップ 1 BFD テンプレート （1326 ページ） を作成する。

ステップ 2 BFD ポリシーの設定 （1165 ページ）。

ステップ 3 BGP ネイバー設定で BFD サポートを設定します。ステップ 12 （1231 ページ）を参照してください。

BFD ポリシーの設定

BFDテンプレートは、仮想ルータに属するインターフェイス、または送信元アドレスと宛先アドレスのペアにバインドできます。

始める前に

- BFDポリシーは、仮想ルータに属するインターフェイスでのみ設定できます。「仮想ルータへのインターフェイスの設定」を参照してください。

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]**ページで、仮想ルータでサポートされているデバイスを編集します。[ルーティング（Routing）] に移動します。

ステップ 2 ドロップダウンリストから目的の仮想ルータを選択し、[BFD] をクリックします。

ステップ 3 インターフェイスで BFD を設定するには、[シングルホップ（Single-Hop）] タブまたは [マルチホップ（Multi-Hop）] タブをクリックします。

（注）
シングルホップポリシーの場合、BFDテンプレートはインターフェイスで設定されます。マルチホップポリシーの場合、BFDテンプレートは送信元アドレスと宛先アドレスのペアで設定されます。

ステップ 4 [追加（Add）] をクリックします。設定された BFD ポリシーを変更するには、[編集（Edit）]（✎）をクリックします。

（注）
BFDテンプレートによるインターフェイスマッピングを編集し、それを新しいBFDテンプレートに置き換える場合、Firewall Management Centerは **no** コマンドを使用してインターフェイスからテンプレートマッピングを削除し、新しいテンプレートをインターフェイスに適用します。これにより、OSPFv2、OSPFv3、または BGP フラップを発生させる可能性のある BFD フラップが発生します。ただし、BFD 間隔を大きくすると、BFD フラップが発生しなくなる可能性があります。または、フラッピングを回避するために、既存の BFD テンプレートマッピングを削除できます。インターフェイスを展開してから、新しいBFDテンプレートをインターフェイスに追加して、設定を展開します。

- シングルホップ BFD ポリシーの設定 （1166 ページ）を参照してください。
- 「マルチホップ BFD ポリシーの設定 （1167 ページ）」を参照してください。

シングルホップ BFD ポリシーの設定

シングルホップBFDポリシーは、仮想ルータに属するインターフェイスでのみ設定できます。

始める前に

- シングルホップBFDテンプレートを作成します。マルチホップテンプレートを使用して、インターフェイスにシングルホップ BFD ポリシーを設定することはできません。

手順

ステップ 1 [シングルホップ（Single-Hop）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

ステップ 2 [BFDシングルホップの追加（Add BFD Single-Hop）] ダイアログボックスで、次のように設定します。

a) [インターフェイス（Interface）] ドロップダウンリストには、仮想ルータに属するインターフェイスが表示されます。BFD ポリシーを設定するインターフェイスを選択します。

b) [テンプレート名（Template Name）] ドロップダウンリストに、シングルホップテンプレートが表示されます。適用するテンプレートを選択します。

シングルホップテンプレートを作成していない場合は、[追加（Add）] (+)を使用し、シングルホップ BFD テンプレートを使用して作成します。

ステップ 3 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

マルチホップ BFD ポリシーの設定

送信元と宛先のアドレスペアにマルチホップ BFD ポリシーを設定できます。

始める前に

- マルチホップ BFD テンプレートを作成します。シングルホップテンプレートを使用してマルチホップ BFD ポリシーを設定することはできません。

手順

ステップ 1 [BFDマルチホップの追加（Add BFD Multi-Hop）] ダイアログボックスで、次のように設定します。

a) BFD 送信元アドレスタイプ：[IPv4] または [IPv6] オプションボタンをクリックします。

b) [送信元アドレス（Source Address）] ドロップダウンリストに、ネットワークオブジェクトが一覧表示されます。BFD ポリシーに設定する送信元アドレスを選択します。any-ipv4 や any-ipv6 は選択できません。

必要なネットワークオブジェクトを作成していない場合は、[追加（Add）] (+)を使用して、ホスト/ネットワークオブジェクトを作成します。

（注）
作成されたネットワークオブジェクトの IP タイプが、選択した送信元 IP タイプと一致している必要があります。

c) [宛先アドレス（Destination Address）] ドロップダウンリストに、ネットワークオブジェクトが一覧表示されます。BFD に設定する宛先アドレスを選択します。any-ipv4 や any-ipv6 は選択できません。

必要なネットワークオブジェクトを作成していない場合は、[追加（Add）] (+)を使用して、ホスト/ネットワークオブジェクトを作成します。

（注）
作成されたネットワークオブジェクトの IP タイプが、選択した送信元 IP タイプと一致している必要があります。

注目
送信元アドレスと同じIPアドレスを持つネットワークオブジェクトを選択しないでください。

d) [テンプレート名（Template Name）] ドロップダウンリストに、マルチホップテンプレートが一覧表示されます。BFD ポリシーに適用するテンプレートを選択します。

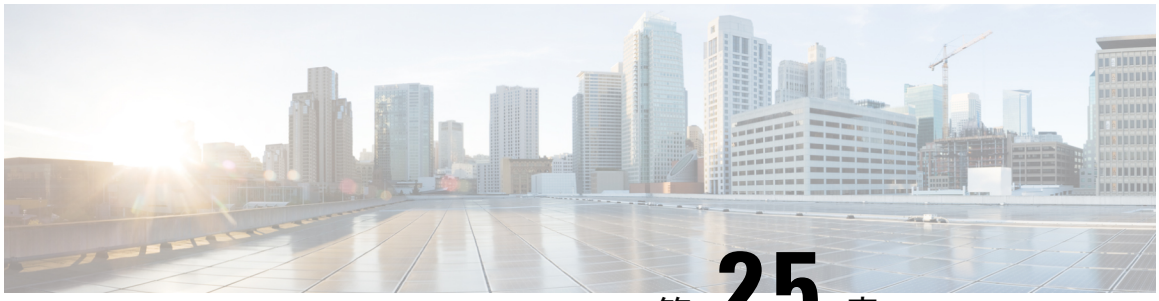
マルチホップテンプレートを作成していない場合は、[追加（Add）] (+)を使用して、マルチホップ BFD テンプレートを作成します。BFD テンプレート （1326 ページ）

ステップ 2 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

マルチホップマップ（テーブルビュー）は、[マルチホップ（Multi-Hop）] タブページに表示されます。

BFD ルーティングの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
BFD コンフィギュレーション	7.4	7.4	以前のリリースでは、BFD は FlexConfig を介してのみ Threat Defense で設定可能でした。FlexConfig は、BFD 設定をサポートしなくなりました。Management Center の UI で Threat Defense の BFD ポリシーを設定できるようになりました。Threat Defense では、BFD は BGP プロトコルでのみサポートされます。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BFD]**。



第 25 章

Open Shortest Path First（OSPF）

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firewall Threat Defense を設定する方法について説明します。

- Open Shortest Path First（OSPF） （1169 ページ）
- OSPF の要件と前提条件 （1173 ページ）
- OSPF のガイドライン （1173 ページ）
- OSPFv2 の設定 （1176 ページ）
- OSPFv3 の設定 （1192 ページ）
- OSPF の履歴 （1204 ページ）

Open Shortest Path First（OSPF）

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firewall Threat Defense を設定する方法について説明します。

OSPF について

OSPF は、パスの選択にディスタンス ベクターではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF は、ルーティング テーブル更新ではなく、リンクステート アドバタイズメントを伝達します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP と比べ OSPF には次の利点があります。

- OSPF では、リンクステート データベースの更新が RIP ほど頻繁に送信されません。また、ステート情報がタイムアウトすると、リンクステート データベースは徐々にではなく、すぐに更新されます。
- ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。Firewall Threat Defense デバイスは、インターフェイスのコストをリンク帯域幅に基づいて計算し、接続先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。

最短パスを優先するアルゴリズムの欠点は、CPUサイクルとメモリが大量に必要になることです。

Firewall Threat Defense デバイス は、OSPF プロトコルのプロセスを 2 つ同時に異なるインターフェイスセット上で実行できます。同じIPアドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスが共存可能ですが、OSPF ではアドレスは重複できません）がある場合に、2 つのプロセスを実行できます。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの2つのプロセス間で再配布することもできます。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、またはOSPF対応インターフェイスに設定されているスタティック ルートおよび接続ルートから、ルートを再配布できます。

Firewall Threat Defense デバイス では、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）。
- 仮想リンク。
- LSA フラッディング。
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）。
- Firewall Threat Defense デバイス の代表ルータまたはバックアップ代表ルータとしての設定。Firewall Threat Defense デバイス は、ABR として設定することもできます。
- スタブ エリアと Not-So-Stubby Area。
- エリア境界ルータのタイプ 3 LSA フィルタリング。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。OSPF と他のプロトコル（RIP など）の間のルート再配布にあたっては、攻撃者によるルーティング情報の悪用の可能性があるため、できる限りすべてのルーティング プロトコルで認証を行う必要があります。

NAT を使用していて、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使

用しているルータの間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA により、プライベートエリアとパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）は、プライベート ネットワークをアドバタイズしなくても NAT と OSPF を一緒に使用できるように、1 つのエリアから他のエリアにフィルタリングできます。

（注） フィルタリングできるのはタイプ 3 LSA のみです。プライベート ネットワーク内の ASBR として設定されている Firewall Threat Defense デバイス は、プライベート ネットワークを記述するタイプ 5 LSA を送信しますが、これは AS 全体（パブリック エリアも含む）にフラッディングされます。

NAT が採用されているが、OSPF がパブリック エリアだけで実行されている場合は、パブリック ネットワークへのルートを、デフォルトまたはタイプ 5 AS 外部 LSA としてプライベート ネットワーク内で再配布できます。ただし、Firewall Threat Defense デバイスにより保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一の Firewall Threat Defense デバイス インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

Firewall Threat Defense デバイス では、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでのコンバージェンスがより迅速になります。

Fast Hello パケットに対する OSPF サポートの前提条件

OSPF がネットワークですでに設定されているか、Fast Hello パケット機能向けの OSPF のサポートと同時に設定される必要があります。

OSPF Hello インターバルと dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、dead 間隔中に受信したすべてのネイバーのリストが含まれます。dead 間隔も設定可能なインターバル（秒単位）で送信されます。デフォルトは Hello インターバルの値の 4 倍です。Hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。dead 間隔の値も、ネットワーク内ですべて同一にする必要があります。

この2つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータが dead 間隔内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短い間隔で送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルと dead 間隔との関係についてあらかじめ理解しておく必要があります。OSPF Hello インターバルと dead 間隔 （1171 ページ）を参照してください。

OSPF fast hello パケットは、ospf dead-interval コマンドで設定されます。dead 間隔は 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる Hello インターバルは 0 に設定されます。このインターフェイス経由で受信した hello パケットの Hello インターバルは無視されます。

dead 間隔は、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。dead 間隔内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF Fast Hello パケットの利点

OSPF Fast Hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、コンバージェンス時間が短くなります。この機能によって、失われたネイバーを 1 秒以内に検出できるようになります。この機能は、ネイバーの損失がオープン システム相互接続（OSI）物理層またはデータリンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との後方互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。

- 2 つの LSA タイプの追加。
- 未知の LSA タイプの処理。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF の要件と前提条件

モデルのサポート

Threat Defense

Firewall Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

OSPF のガイドライン

ファイアウォール モードのガイドライン

OSPF は、ルーテッド ファイアウォール モードのみをサポートしています。OSPF は、トランスペアレント ファイアウォール モードをサポートしません。

高可用性 ガイドライン

OSPFv2 および OSPFv3 は、ステートフル 高可用性 をサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- Firewall Threat Defense デバイス は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。

OSPFv3 Hello パケットと GRE

通常、OSPF トラフィックは GRE トンネルを通過しません。IPv6 の OSPFv3 が GRE 内でカプセル化されている場合、マルチキャスト宛先などのセキュリティチェックで IPv6 ヘッダー検証が失敗します。このパケットは、宛先が IPv6 マルチキャストであるため、暗黙的なセキュリティチェックの検証でドロップされます。

GRE トラフィックをバイパスするプレフィルタルールを定義できます。ただし、プレフィルタルールでは、内部パケットはインスペクションエンジンによって問い合わせられません。

クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラー メッセージが表示されます。
- スパンド インターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスではサポートされません。
- 個別インターフェイスモードで、OSPFv2 または OSPFv3 ネイバーとして制御ユニットおよびデータユニットが確立されていることを確認します。
- 個別インターフェイスモードでは、OSPFv2 との隣接関係は、制御ユニットの共有インターフェイスの 2 つのコンテキスト間でのみ確立できます。スタティック ネイバーの設定は、ポイントツーポイン リンクでのみサポートされます。したがって、インターフェイスで許可されるのは 1 つのネイバー ステートメントだけです。
- クラスタで制御ロールの変更が発生した場合、次の挙動が発生します。
  - スパンド インターフェイス モードでは、ルータプロセスは制御ユニットでのみアクティブになり、データユニットでは停止状態になります。コンフィギュレーションが制御ユニットと同期されているため、各クラスタユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。
  - 個別インターフェイスモードでは、ルータ プロセスはすべての個別のクラスタユニットでアクティブになります。各クラスタ ユニットは設定されたクラスタ プールから独自の個別のルータ ID を選択します。クラスタで制御ロールが変更されても、ルーティングトポロジは変更されません。

マルチプロトコル ラベル スイッチング（MPLS）と OSPF のガイドライン

MPLS 設定ルータから送信されるリンク ステート（LS）アップデート パケットに、Opaque Type-10 リンクステート アドバタイズメント（LSA）が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデート パケットを確認せずにサイレントにドロップします。ピア ルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、アプライアンスでノンストップ フォワーディング（NSF）が無効であることを確認します。

- Firewall Management Center の [ノンストップ フォワーディング（Non Stop Forwarding）] ページに移動します（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**（**目的のデバイスを選択**） > **[ルーティング（Routing）]** > **[OSPF]** > **[詳細（Advanced）]** > **[ノンストップ フォワーディング（Non Stop Forwarding）]**）。

  [Non Stop Forwarding Capability] のボックスがオンになっていないことを確認します。

（注） Firepower 4100/9300 モデルでは、複数の受信キュー間のロードバランシング不足のため、MPLS を使用した際に遅延が大きくなる可能性があります。

ルートの再配布のガイドライン

- IPv4 プレフィックス リストを使用した OSPFv2 でのルートマップの再配布はサポートされています。ただし、IPv6 プレフィックス リストを使用した OSPFv3 でのルートマップの再配布はサポートされていません。再配布には、OSPF のルートマップでアクセス リストを使用します。
- OSPF が、EIGRP ネットワークの一部であるデバイスで設定されている場合、またはその逆の場合は、ルートにタグを付けるように OSPF ルータが設定されていることを確認します（EIGRP はルートタグをまだサポートしていません）。

  OSPF を EIGRP に再配布し、EIGRP を OSPF に再配布する場合は、いずれかのリンクまたはインターフェイスで障害が発生したときや、ルート発信元がダウンしたときにも、ルーティングループが発生します。あるドメインから同じドメインに再度ルートを再配布することを避けるため、ルータは、再配布する際にドメインに属しているルートにタグ付けすることができます。そして、そのタグに基づいて、リモートルータでそれらのルートをフィルタ処理できます。それらのルートはルーティングテーブルにインストールされないため、再度同じドメインに再配布されることはありません。

その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。
- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフル リスタートおよび IETF NSF グレースフル リスタート メカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフル リスタート メカニズムをサポートします。
- 配布可能なエリア内（タイプ 1）ルートの数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケット

サイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。

- 仮想ルーティングを使用するデバイスの場合は、グローバル仮想ルータの OSPFv2 と OSPFv3 を設定できます。ただし、ユーザー定義の仮想ルータには OSPFv2 のみ設定できます。
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。
- パケット サイズが 8190 を超えた場合、OSPFv3 は LS アップデートをドロップします。その結果、隣接関係は終了します。そのため、「ospfv3 mtu-ignore」コマンドを使用してスイッチを設定し、隣接関係の終了を回避してください。

OSPFv2 の設定

ここでは、OSPFv2 ルーティング プロセスの設定に関連するタスクについて説明します。仮想ルーティングを使用するデバイスでは、グローバルおよびユーザー定義の仮想ルータに対して OSPFv2 を設定できます。

OSPF エリア、範囲、仮想リンクの設定

認証の設定、スタブエリアの定義、デフォルトの集約ルートへの特定コストの割り当てが含まれる複数の OSPF エリア パラメータを設定できます。最大 2 つの OSPF プロセス インスタンスを有効にできます。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。認証では、エリアへの不正アクセスに対してパスワードベースで保護します。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

ステップ 4 [OSPF] をクリックします。

ステップ 5 [プロセス1（Process 1）] のチェックボックスをオンにします。それぞれのコンテキスト/仮想ルータで最大 2 つの OSPF プロセスインスタンスを有効にできます。エリアパラメータを設定するには、OSPF プロセスを選択する必要があります。

デバイスが仮想ルーティングを使用する場合、ID フィールドには選択された仮想ルータに対して生成された一意のプロセス ID が表示されます。

ステップ 6 [OSPFロール（OSPF Role）] をドロップダウンリストから選択し、次のフィールドにそれぞれの説明を入力します。オプションは、[内部（Internal）]、[ABR]、[ASBR]、[ABRおよびASBR（ABR & ASBR）] です。OSPF の権限の説明については、OSPF について （1169 ページ）を参照してください。

ステップ 7 **[エリア（Area）] > [追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、[編集（Edit）]（✎） をクリックするか、右クリックしてメニューを表示、選択します。

ステップ 8 以下のエリアのオプションを、それぞれの OSPF プロセスで設定します。

- [OSPF Process]：プロセス ID を選択します。仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [エリア ID（Area ID）]：：ルートをサマライズするエリアの接続先。
- [エリア タイプ（Area Type）]：次のいずれかを選択します。
  - [Normal]：（デフォルト）標準 OSPF エリア。
  - [スタブ（Stub）]：スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、自律システム（AS）External LSA（タイプ 5 LSA）がスタブ エリアにフラッディングされないようにします。スタブ エリアを作成すると、[サマリー スタブ（Summary Stub）] チェックボックスをオフにすることによって、集約 LSA（タイプ 3 および 4）がそのエリアにフラッディングされるのを防ぐことができます。
  - [NSSA]：エリアを Not-So-Stubby Area にします。NSSA は、タイプ 7 LSA を受け入れます。[再配布（Redistribute）] チェックボックスをオフにし、[デフォルト情報起点（Default Information Originate）] チェックボックスをオンにすることで、ルートの再配布を無効化することができます。[集約 NSSA（Summary NSSA）] チェックボックスをオフにすることによって、集約 LSA でエリアへのフラッディングを防止できます。
- [メトリック値（Metric Value）]：デフォルトルートの生成に使用するメトリックを指定します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

- [利用可能なネットワーク（Available Network）]：利用可能なネットワークの 1 つを選択して [追加（Add）] をクリックするか、[追加（Add）] (＋) をクリックして新しいネットワークオブジェクトを追加します。ネットワークの追加手順については、ネットワーク（1349 ページ）を参照してください。
- [認証（Authentication）]：OSPF 認証を選択します。
  - [なし（None）]：（デフォルト）OSPF エリアの認証を無効にします。
  - [パスワード（Password）]：クリアテキストパスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
  - [MD5]：MD5 認証を許可します。
- [デフォルト コスト（Default Cost）]：接続先までの最短パスを割り出す OSPF エリアのデフォルトのコスト。有効値の範囲は、0 ～ 65535 です。デフォルト値は 1 です。

ステップ 9 [OK] をクリックして、エリア設定を保存します。

ステップ 10 **[範囲（Range）] > [追加（Add）]** を選択します。

- 使用可能なネットワークのいずれかを選択して、アドバタイズするかを決めます。
- [追加（Add）](＋)をクリックして、新しいネットワークオブジェクトを追加します。ネットワークの追加手順については、ネットワーク （1349 ページ）を参照してください。

ステップ 11 [OK] をクリックして、範囲設定を保存します。

ステップ 12 [仮想リンク（Virtual Link）] を選択して、[追加（Add）]（＋） をクリックし、それぞれの OSPF プロセスに以下のオプションを設定します。

- [ピア ルータ（Peer Router）]：ピア ルータの IP アドレスを選択します。新しいピアルータを追加するには、[追加（Add）] (＋) をクリックします。ネットワークの追加手順については、ネットワーク （1349 ページ）を参照してください。
- [Hello 間隔（Hello Interval）]：hello パケットがインターフェイスで送信される秒単位の間隔です。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は 1 ～ 65535 です。デフォルトは 10 です。

  hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。
- [転送遅延（Transmit Delay）]：インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒単位）。ゼロよりも大きい整数値を指定します。有効値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

  アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

- [再転送間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 65535 の範囲で指定できます。デフォルトは 5 です。

  ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [デッド間隔（Dead Interval）]：ルータがダウンしていることをネイバーが示す前に hello パケットを非表示にする秒単位の時間。Dead 間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効値の範囲は 1 ～ 65535 です。

- [認証（Authentication）]：以下から OSPF 仮想リンクの認証を選択します。
  - [なし（None）]：（デフォルト）仮想リンク エリアの認証を無効にします。
  - [エリア認証（Area Authentication）]：MD5 を使用して、エリア認証を有効にします。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。
  - [パスワード（Password）]：クリアテキストパスワードが仮想リンクの認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
  - [MD5]：MD5 認証を許可します。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

    （注）
    MD5 キー ID として数字のみを入力してください。
  - [キー チェーン（Key Chain）]：キー チェーン認証を許可します。[追加（Add）] をクリックしてキーチェーンを作成した後、[保存（Save）] をクリックします。詳細な手順については、キー チェーンのオブジェクトの作成（1347 ページ）を参照してください。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。

ステップ 13 [OK] をクリックして、仮想リンクの設定を保存します。

ステップ 14 ルーティング ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

Configure OSPF Redistribution を続けます。

OSPF 再配布の設定

Firewall Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1 つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。EIGRP、RIP および BGP で検出されたルートを、OSPF ルーティングプロセスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

ステップ 4 [OSPF] をクリックします。

ステップ 5 [OSPFロール（OSPF Role）] ドロップダウンから、ロールを選択します。

ステップ 6 **[再配布（Redistribution）]** > **[追加（Add）]** をクリックします。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、[編集（Edit）]（ ） をクリックするか、右クリックしてメニューを表示、選択します。

ステップ 7 OSPF プロセスごとに、次の再配布オプションを設定します。

- [OSPF Process]：プロセス ID を選択します。仮想ルーティングを使用するデバイスの場合、このドロップダウンリストに選択した仮想ルータ用に生成された一意のプロセス ID が表示されます。
- [ルート タイプ（Route Type）]：次のいずれかのタイプを選択します。
  - [スタティック（Static）]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
  - [接続済み（Connected）]：接続されたルート（インターフェイス上で IP アドレスを有効にすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、デバイスの外部として再配布されます。[オプション（Optional）] リストのサブネットを使用するかどうかを選択できます。
  - [OSPF]：別の OSPF ルーティング プロセスからルートを再配布します（内部、外部 1 と 2、NSSA 外部 1 と 2、またはサブネットを使用するかどうか）。[オプション（Optional）] リストでこれらのオプションを選択できます。
  - [BGP]：BGP ルーティング プロセスからルートを再配布します。AS 番号およびサブネットを使用するかどうかを追加します。
  - [RIP]：RIP ルーティング プロセスからルートを再配布します。[オプション（Optional）] リストのサブネットを使用するかどうかを選択できます。

（注）
ユーザー定義の仮想ルータでは RIP がサポートされていないため、RIP からルートを再配布することはできません。

- [EIGRP]：EIGRP ルーティングプロセスからルートを再配布します。AS 番号およびサブネットを使用するかどうかを追加します。

- [メトリック値（Metric Value）]：再配布するルートのメトリック値。デフォルト値は 10 です。有効な値の範囲は 0 ～ 16777214 です。

  同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

- [タグ値（Tag Value）]：タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ～ 4294967295 です。

- [RouteMap]：送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。または、[追加（Add）](＋)をクリックして新しいルートマップを追加できます。新しいルートマップの追加については、「ルート マップ エントリの設定」を参照してください。

ステップ 8 [OK] をクリックして、再配布設定を保存します。

ステップ 9 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF エリア間フィルタリングの設定 （1181 ページ）に進みます。

OSPF エリア間フィルタリングの設定

ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他の

すべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

ステップ 4 [OSPF] をクリックします。

ステップ 5 **[エリア間（InterArea）]** > **[追加（Add）]** を選択します。

エリア間を切り取り、コピー、貼り付け、挿入、削除するには、[編集（Edit）]（✎）をクリックするか、右クリックしてメニューを表示、選択します。

ステップ 6 OSPF プロセスごとに、次のエリア間フィルタリング オプションを設定します。

- [OSPF Process]：仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [エリア ID（Area ID）]：ルートを要約するエリア。
- [PrefixList]：プレフィックスの名前。新しいプレフィックス リスト オブジェクトを追加するには、ステップ 5 を参照してください。
- [トラフィックの方向（Traffic Direction）]：着信または発信。OSPF エリアへの LSA をフィルタリングするには [着信（Inbound）] を選択し、OSPF エリアからの LSA をフィルタリングするには [発信（Outbound）] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 7 [追加（Add）] (＋) をクリックして、新しいプレフィックスリストの名前と、オーバーライドを許可するかどうかを入力します。

プレフィックス ルールを設定する前に、プレフィックス リストを設定する必要があります。

ステップ 8 [追加（Add）] をクリックしてプレフィックス ルールを設定し、次のパラメータを設定します。

- [アクション（Action）]：再配布アクセスに対して [ブロック（Block）] または [許可（Allow）] を選択します。
- [シーケンス番号（Sequence No）]：ルーティング シーケンス番号。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。
- [IP アドレス（IP Address）]：プレフィックス番号を IP アドレス/マスク長の形式で指定します。
- [最小プレフィックス長（Min Prefix Length）]：（オプション）最小のプレフィックス長。
- [最大プレフィックス長（Max Prefix Length）]：（オプション）最大のプレフィックス長。

ステップ 9 [OK] をクリックして、エリア間フィルタリング設定を保存します。

ステップ 10 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF フィルタルールの設定 （1183 ページ）に進みます。

OSPF フィルタルールの設定

OSPF プロセスごとに ABR タイプ 3 LSA フィルタを設定できます。ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリア フィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

ステップ 4 [OSPF] をクリックします。

ステップ 5 **[フィルタルール（Filter Rule）]** > **[追加（Add）]** を選択します。

[編集（Edit）]（✎） をクリックするか、右クリックメニューを使用して、フィルタルールの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 6 OSPF プロセスごとに、次のフィルタ ルール オプションを設定します。

- [OSPF Process]：仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [アクセス リスト（Access List）]：この OSPF プロセスのアクセス リスト。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）]（＋）をクリックし、標準 ACL オブジェクトの設定 （1322 ページ）を参照してください。
- [トラフィックの方向（Traffic Direction）]：フィルタリングするトラフィックの方向として [イン（In）] または [アウト（Out）] を選択します。OSPF エリアへの LSA をフィルタリングするには [イン（In）] を選択し、OSPF エリアからの LSA をフィルタリングするには [アウト（Out）] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- [インターフェイス（Interface）]：このフィルタ ルールのインターフェイス。

ステップ 7 [OK] をクリックしてルール設定を保存します。

ステップ 8 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF サマリーアドレスの設定 （1184 ページ）に進みます。

OSPF サマリーアドレスの設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。ただし、再配布されるルートのうち、指定のネットワーク アドレスとマスクに含まれるすべてのものを 1 つのルートで表し、そのルートだけをアドバタイズするように Firewall Threat Defense デバイスを設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。指定した IP アドレス マスク ペアと一致するルートは抑制できます。ルートマップで再配布を制御するために、タグ値を一致値として使用できます。

他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

ステップ 4 [OSPF] をクリックします。

ステップ 5 **[サマリーアドレス（Summary Address）] > [追加（Add）]** を選択します。

[編集（Edit）]（）をクリックして編集するか、右クリックメニューを使用して、サマリーアドレスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 6 OSPF プロセスごとに、次のサマリー アドレス オプションを設定します。

- [OSPF Process]：仮想ルーティングを使用するデバイスの場合、選択した仮想ルータ用に生成された一意のプロセス ID がドロップダウンにリストされます。
- [利用可能なネットワーク（Available Networks）]：サマリーの IP アドレス。利用可能なネットワークリストから 1 つを選択して [追加（Add）] をクリックするか、[追加（Add）]()をクリックして新しいネットワークを追加します。ネットワークを追加する手順については、ネットワーク （1349 ページ）を参照してください。
- [タグ（Tag）]：各外部ルートに付加される 32 ビットの 10 進数値。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。
- [アドバタイズ（Advertise）]：集約ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェック ボックスはオンになっています。

ステップ 7 [OK] をクリックしてサマリー アドレス設定を保存します。

ステップ 8 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF インターフェイスとネイバーの設定 （1185 ページ）に進みます。

OSPF インターフェイスとネイバーの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを変更することは必須ではありませんが、hello インターバル、Dead 間隔、認証キーというインターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

ステップ 4 [OSPF] をクリックします。

ステップ 5 **[インターフェイス（Interface）]** > **[追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、[編集（Edit）]（ ） をクリックするか、右クリックしてメニューを表示、選択します。

ステップ 6 OSPF プロセスごとに、次のインターフェイス オプションを設定します。

- [インターフェイス（Interface）]：設定するインターフェイス。

  （注）
  デバイスが仮想ルーティングを使用している場合、このドロップダウンリストには、ルータに属するインターフェイスだけが表示されます。

- [デフォルトコスト（Default Cost）]：インターフェイスを介したパケット送信のコスト。デフォルト値は 10 です。

- [優先順位（Priority）]：ネットワークの代表ルータ。有効な値の範囲は 0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。

  2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。この設定は、ポイントツーポイントのインターフェイスとして設定されているインターフェイスには適用されません。

- [MTU無視（MTU Ignore）]：OSPF は、共通のインターフェイス上でネイバーが同一の MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケット内の受信した MTU が、受信インターフェイスに設定されている IP MTU より大きい場合は、OSPF 隣接関係は確立されません。

- [データベースフィルタ（Database Filter）]：この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰使用につながることがあります。このチェックボックスをオンにすると、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。

- [Hello 間隔（Hello Interval）]：インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 10 秒です。

  hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。

- [伝送遅延（Transmit Delay）]：インターフェイス上で LSA パケットを送信するのに必要な予想時間（秒単位）。有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。

  更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

- [再送信間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

  ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [Dead 間隔（Dead Interval）]：hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間（秒単位）。この値は、ネットワーク上のすべてのノードで同じである必要があり、1 ～ 65535 の範囲で指定できます。

- [Hello 乗数（Hello Multiplier）]：1 秒ごとに送信される hello パケットの数を指定します。有効な値は 3 ～ 20 です。

- [ポイント ツー ポイント（Point-to-Point）]：VPN トンネルで OSPF ルートを送信できます。

- [認証（Authentication）]： OSPF のインターフェイス認証を次から選択します。
  - [なし（None）]：（デフォルト）インターフェイス認証を無効にします。
  - [エリア認証（Area Authentication）]：MD5 を使用したインターフェイス認証を有効にします。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。
  - [パスワード（Password）]：クリア テキスト パスワードが仮想リンクの認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
  - [MD5]：MD5 認証を許可します。[追加（Add）] をクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

    （注）

MD5 キー ID として数字のみを入力してください。

- [キー チェーン（Key Chain）]：キー チェーン認証を許可します。[追加（Add）] をクリックしてキーチェーンを作成した後、[保存（Save）] をクリックします。詳細な手順については、キーチェーンのオブジェクトの作成（1347ページ）を参照してください。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキーチェーン）とキー ID を使用します。

- [パスワードの入力（Enter Password）]：認証のタイプとして [パスワード（Password）] を選択した場合に、設定するパスワード。
- [パスワードの確認（Confirm Password）]：選択したパスワードを確認します。

ステップ 7 **[ネイバー（Neighbor）] > [追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、[編集（Edit）]（✎） をクリックするか、右クリックしてメニューを表示、選択します。

ステップ 8 OSPF プロセスごとに、次のパラメータを設定します。

- [OSPF プロセス（OSPF Process）]：1 または 2 を選択します。
- [ネイバー（Neighbor）]：ドロップダウンリストでネイバーの 1 つを選択するか、[追加（Add）](＋)をクリックして新しいネイバーを追加します。名前、説明、ネットワーク、およびオーバーライドを許可するかどうかを入力し、[保存（Save）] をクリックします。
- [インターフェイス（Interface）]：ネイバーに関連付けられたインターフェイスを選択します。

ステップ 9 [OK] をクリックして、ネイバー設定を保存します。

ステップ 10 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

OSPF 詳細プロパティの設定

[高度なプロパティ（Advanced Properties）] を使用すると、syslog メッセージ生成、アドミニストレーティブ ルート ディスタンス、LSA タイマー、グレースフルリスタートなどのオプションを設定できます。

グレースフル リスタート

Firewall Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。

（注） NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、OSPF を設定する仮想ルータを選択します。

ステップ 4 [OSPF] > [詳細（Advanced）] をクリックします。 >

ステップ 5 [一般（General）] を選択し、次のように設定します。

- [ルータID（Router ID）]：[自動（Automatic）] または [IP アドレス（IP Address）]（非クラスタおよびスパンド EtherChannel モードのクラスタの場合に表示）またはルータ ID の [クラスタプール（Cluster Pool）]（個別インターフェイスモードのクラスタの場合に表示）を選択します。[IPアドレス（IP address）] を選択する場合は、隣接するフィールドに IP アドレスを入力します。[クラスタプール（Cluster Pool）] を選択した場合は、隣接するドロップダウンフィールドで IPv4 クラスタプールの値を選択します。クラスタプールアドレスの作成については、アドレス プール （1323 ページ）を参照してください。
- [LSA MOSPF を無視（Ignore LSA MOSPF）]：ルートがサポートされていない LSA タイプ 6 マルチキャスト OSPF（MOSPF）パケットを受信した場合、syslog メッセージを抑制します。
- [RFC 1583 互換（RFC 1583 Compatible）]：集約ルートのコストを計算するための手段として RFC 1583 の互換性を設定します。RFC 1583 の互換性が有効な場合、ルーティング ループが発生することがあります。ルーティング ループを防止するには、これを無効にしま

す。OSPF ルーティング ドメイン内のすべての OSPF ルータの RFC 互換設定が同じである必要があります。

- [隣接関係の変更（Adjacency Changes）]：syslog メッセージが送信される隣接関係の変更内容を定義します。

  デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。

  - [隣接関係の変更のログ記録（Log Adjacency Changes）]：OSPF ネイバーが起動または停止したときに、Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
  - [隣接関係の変更の詳細のログ記録（Log Adjacency Change Details）]：ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

- [アドミニストレーティブ ルート ディスタンス（Administrative Route Distance）]：**エリア間**、**エリア内**、および**外部** IPv6 ルートのアドミニストレーティブ ルート ディスタンスの設定に使用された設定を変更できます。アドミニストレーティブ ルート ディスタンスは 1 ～ 254 の整数です。デフォルトは 110 です。
- [LSA グループ ペーシング（LSA Group Pacing）]：LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [デフォルト情報の発信を有効にする（Enable Default Information Originate）]：デフォルトの外部ルートを OSPF ルーティング ドメインに生成するには、[有効化（Enable）] チェックボックスをオンにして、次のオプションを設定します。
  - [デフォルト ルートを常にアドバタイズする（Always advertise the default route）]：デフォルト ルートが常にアドバタイズされるようにします。
  - [メトリック値（Metric Value）]：デフォルトルートの生成に使用するメトリックを指定します。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。
  - [メトリック タイプ（Metric Type）]：OSPFv3 ルーティング ドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンク タイプ。有効な値は1（タイプ 1 の外部ルート）および 2（タイプ 2 の外部ルート）です。デフォルトはタイプ 2 外部ルートです。
  - [ルートマップ（RouteMap）]：ルートマップが満たされている場合にデフォルトルートを生成するルーティングプロセスを選択するか、[追加（Add）] (＋) をクリックして、新しいルーティングプロセスを追加します。新しいルートマップの追加については、「ルート マップ エントリの設定」を参照してください。

ステップ 6 [OK] をクリックして、一般設定を保存します。

ステップ 7 [ノンストップフォワーディング（Non Stop Forwarding）] を選択し、NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフルリスタートを設定します。

（注）
OSPFv2 には、Cisco NSF と IETF NSF の 2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

a) [Cisco Non Stop Forwarding 機能を有効にする（Enable Cisco Non Stop Forwarding Capability）] チェックボックスをオンにします。
b) （オプション）必要に応じて、[非 NSF 認識隣接ネットワーキング デバイスが検出されたときに NSF リスタートをキャンセルする（Cancel NSF restart when non-NSF-aware neighboring networking devices are detected）] チェックボックスをオンにします。
c) （オプション）[Cisco Non Stop Forwarding ヘルパー モードを有効にする（Enable Cisco Non Stop Forwarding Helper mode）] チェックボックスをオフにして、NSF 認識デバイスでのヘルパー モードを無効にします。

ステップ 8 NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定します。

a) [IETF Non Stop Forwarding 機能を有効にする（Enable IETF Non Stop Forwarding Capability）] チェックボックスをオンにします。
b) [グレースフル リスタート間隔（秒）（Length of graceful restart interval (seconds)）] フィールドにリスタート間隔を秒単位で入力します。デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。
c) （オプション）[ヘルパー モードの IETF Nonstop Forwarding（NSF）を有効にする（Enable IETF nonstop forwarding (NSF) for helper mode）] チェックボックスをオフにして、NSF 認識デバイスでの IETF NSF ヘルパー モードを無効にします。
d) [厳密なリンク ステートのアドバタイズメント チェックを有効にする（Enable Strict Link State advertisement checking）]：有効にすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させます。
e) [IETF Non Stop Forwarding を有効にする（Enable IETF Non Stop Forwarding）]：スイッチオーバー後にルーティング プロトコル情報が復元される間、データのパケットの転送が既知のルートで続行される Non Stop Forwarding を有効にします。OSPF は OSPF プロトコルの拡張を使用して、隣接する OSPF デバイスからステートを回復します。リカバリが機能するためには、ネイバーが NSF プロトコル拡張をサポートし、再起動するデバイスの「ヘルパー」として積極的に動作する必要があります。ネイバーはまた、プロトコル ステートのリカバリが行われる間、再起動するデバイスにデータ トラフィックを転送し続ける必要もあります。

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。仮想ルーティングを使用しているデバイスの場合、ユーザー定義の仮想ルータではなく、グローバル仮想ルータに対してのみ OSPFv3 を設定できます。

OSPFv3 エリア、ルート集約、および仮想リンクの設定

OSPFv3 を有効にするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスを有効にする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPFv3] を選択します。

ステップ 3 デフォルトでは、[プロセス 1 を有効にする（Enable Process 1）] が選択されています。最大 2 つの OSPF プロセス インスタンスを有効にできます。

ステップ 4 OSPFv3 ロールをドロップダウン リストから選択し、それに対応する説明を入力します。オプションは、[内部（Internal）]、[ABR]、[ASBR]、[ABR および ASBR（ABR and ASBR）] です。OSPFv3 ロールの説明については、OSPF について （1169 ページ）を参照してください。

ステップ 5 **[エリア（Area）]** > **[追加（Add）]** を選択します。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、[編集（Edit）]（✎） をクリックするか、右クリックしてメニューを表示、選択します。

ステップ 6 [一般（General）] を選択し、各 OSPF プロセスについて次のオプションを設定します。

- [エリア ID（Area ID）]：ルートを要約するエリア。
- [コスト（Cost）]：この集約ルートのメトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ～ 16777215 です。
- [タイプ（Type）]：[標準（Normal）]、[NSSA]、[スタブ（Stub）] を指定します。[標準（Normal）] を選択した場合、設定するその他のパラメータはありません。[スタブ（Stub）] を選択した場合、エリアでサマリー LSA を送信することができます。[NSSA] を選択した場合、次の 3 つのオプションを設定できます。
  - [このエリアへのサマリー LSA の送信を許可する（Allow Sending summary LSA into this area）]：エリアにサマリー LSA を送信することを許可します。

- [標準およびNSSAエリアにルートをインポート（Imports routes to normal and NSSA area）]：再配布でルートをスタブエリアでなく標準エリアにインポートできるようになります。
- [デフォルト情報生成（Defaults information originate）]：OSPFv3 ルーティング ドメインへのデフォルト外部ルートを生成します。

- [メトリック（Metric）]：デフォルトルートを生成するために使用するメトリック。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

ステップ 7 [OK] をクリックして、一般設定を保存します。

ステップ 8 （内部 OSPFv3 ロールには適用されません）**[ルート集約（RouteSummary）]** > **[ルート集約の追加（Add Route Summary）]** を選択します。

[編集（Edit）]（） をクリックするか、右クリックメニューを使用して、ルート集約の切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 9 OSPF プロセスごとに、次のルート集約オプションを設定します。

- [IPv6 プレフィックス/長さ（IPv6 Prefix/Length）]：IPv6 プレフィックス。新しいネットワークオブジェクトを追加するには、[追加（Add）]（+）をクリックします。ネットワークを追加する手順については、ネットワーク （1349 ページ）を参照してください。
- [コスト（Cost）]：この集約ルートのメトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ～ 16777215 です。
- [アドバタイズ（Advertise）]：集約ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェック ボックスはオンになっています。

ステップ 10 [OK] をクリックして、ルート集約設定を保存します。

ステップ 11 （内部 OSPFv3 ロールには適用されません）[仮想リンク（Virtual Link）] を選択し、[仮想リンクの追加（Add Virtual Link）] をクリックして、各 OSPF プロセスについて次のオプションを設定します。

- [ピア ルータ ID（Peer RouterID）]：ピア ルータの IP アドレスを選択します。新しいネットワークオブジェクトを追加するには、[追加（Add）]（+）をクリックします。ネットワークを追加する手順については、ネットワーク （1349 ページ）を参照してください。
- [TTL セキュリティ（TTL Security）]：TTL セキュリティ チェックを有効にします。このホップカウントの値は、1 ～ 254 の数値です。デフォルトは 1 です。

  OSPF は、IP ヘッダー存続可能時間（TTL）の値が 255 の発信パケットを送信し、設定可能なしきい値よりも低い TTL 値の入力パケットを廃棄します。IP パケットを転送する各

デバイスはTTLが低下するため、直接（1ホップ）接続により受信されたパケットのTTL値は255になります。2つのホップを通過するパケットの値は254というようになります。受信しきい値は、パケットが移動する可能性がある最大ホップ数で設定されます。

- [Dead 間隔（Dead Interval）]：helloパケットが届かなかった場合にネイバーがルータのダウンを示すまでの時間（秒単位）。デフォルトはhello間隔の4倍または40秒です。有効な値の範囲は1 ～ 65535です。

  Dead間隔は符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。

- [Hello 間隔（Hello Interval）]：helloパケットがインターフェイスで送信される間隔（秒単位）。有効な値の範囲は1 ～ 65535です。デフォルトは10です。

  hello間隔は、helloパケットでアドバタイズされる符号なし整数です。この値は、特定のネットワーク上のすべてのルータおよびアクセスサーバーで同じである必要があります。hello間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。

- [再転送間隔（Retransmit Interval）]：インターフェイスに属する隣接関係のLSA再送信間の時間（秒単位）。再送信間隔は、接続されているネットワーク上の任意の2台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 65535の範囲で指定できます。デフォルトは5です。

  ルータが自身のネイバーにLSAを送信する場合、ルータは確認応答メッセージを受信するまでそのLSAを保持します。確認応答を受信しなかった場合、ルータではLSAを再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [転送遅延（Transmit Delay）]：インターフェイス上でLSAパケットを送信するために必要と推定される時間（秒単位）。ゼロよりも大きい整数値を指定します。有効な値の範囲は1 ～ 8192です。デフォルトは1です。

  アップデート パケット内のLSA自体の経過時間は、転送前にこの値の分だけ増分されます。リンクでの送信前に遅延が加算されていない場合、LSAがリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

ステップ 12 [OK] をクリックして、仮想リンク設定を保存します。

ステップ 13 [ルータ（Router）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPFv3 再配布の設定を続けます。

OSPFv3 再配布の設定

Secure Firewall Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1 つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。EIGRP、RIP および BGP で検出されたルートを、OSPF ルーティングプロセスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPF] を選択します。

ステップ 3 [再配布（Redistribution）] を選択し、[追加（Add）] をクリックします。

エリアを切り取り、コピー、貼り付け、挿入、削除するには、[編集（Edit）]（✎） をクリックするか、右クリックしてメニューを表示、選択します。

ステップ 4 OSPF プロセスごとに、次の再配布オプションを設定します。

- [ソース プロトコル（Source Protocol）]：ルートの再配布元となるソース プロトコル。サポートされるプロトコルは、接続済み、OSPF、静的、EIGRP、BGP です。OSPF を選択した場合は、[プロセス ID（Process ID）] フィールドにプロセス ID を入力する必要があります。BGP を選択した場合は、[AS番号（AS Number）] フィールドに AS 番号を追加する必要があります。
- [メトリック（Metric）]：配布されるルートのメトリック値。デフォルト値は 10 です。有効な値の範囲は 0 ～ 16777214 です。

  同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [タグ（Tag）]：タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ～ 4294967295 です。
- [ルート マップ（Route Map）]：送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータ

を指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルートマップ タグが表示されていない場合、ルートはインポートされません。または、[追加（Add）] (+) をクリックして新しいルートマップを追加できます。新しいルート マップを追加する手順については、ルート マップ （1380 ページ）を参照してください。

- [プロセス ID（Process ID）]：OSPF プロセス ID。1 または 2。

  （注）
  プロセス ID が有効であると、OSPFv3 プロセスは別の OSPFv3 プロセスから認識したルートを再配布します。

- [一致（Match）]：OSPF ルートを他のルーティング ドメインに再配布できるようにします。
  - [内部（Internal）] は、特定の自律システムの内部にあるルートです。
  - [外部 1（External 1）] は、自律システムの外部であるが、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。
  - [外部 2（External 2）] は、自律システムの外部であるが、OSPFv3 にタイプ 2 外部ルートとしてインポートされるルートです。
  - [NSSA 外部 1（NSSA External 1）] は、自律システムの外部であるが、IPv6 用の NSSA の OSPFv3 にタイプ 1 の外部ルートとしてインポートされるルートです。
  - [NSSA 外部 2（NSSA External 2）] は、自律システムの外部であるが、IPv6 用の NSSA の OSPFv3 にタイプ 2 の外部ルートとしてインポートされるルートです。

ステップ 5 [OK] をクリックして、再配布設定を保存します。

ステップ 6 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPFv3 サマリー プレフィックスの設定 （1196 ページ）に進みます。

OSPFv3 サマリー プレフィックスの設定

指定された IPv6 プレフィックスとマスクのペアに一致するルートをアドバタイズするように Firewall Threat Defense デバイスを設定できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPFv3] を選択します。

ステップ 3 **[サマリープレフィックス（Summary Prefix）] > [追加（Add）]** を選択します。

[編集（Edit）]（✎）をクリックするか、右クリックメニューを使用して、サマリープレフィックスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 4 OSPF プロセスごとに、次のサマリー プレフィックス オプションを設定します。

- [IPv6 プレフィックス/長さ（IPv6 Prefix/Length）]：IPv6 プレフィックスとプレフィックス長のラベル。リストから 1 つを選択するか、[追加（Add）]（＋）をクリックして新しいネットワークオブジェクトを追加します。ネットワークを追加する手順については、ネットワーク （1349 ページ）を参照してください。
- [アドバタイズ（Advertise）]：指定されたプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。
- （オプション）[タグ（Tag）]：ルート マップで再配布を制御するための「match」値として使用できるタグ値。

ステップ 5 [OK] をクリックして、サマリー プレフィックス設定を保存します。

ステップ 6 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPFv3 インターフェイス、認証、およびネイバーの設定 （1197 ページ）に進みます。

OSPFv3 インターフェイス、認証、およびネイバーの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

Nexus スイッチで OSPFv3 認証を正常に実装するには、互換性のあるバージョンのスイッチ（Nexus 3000、7000、9000 シリーズ スイッチなど）があることを確認します。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPFv3] を選択します。

ステップ 3 **[インターフェイス（Interface）] > [追加（Add）]** を選択します。

[編集（Edit）] をクリックしてエリアを編集するか、右クリックメニューを使用してエリアを切り取り、コピー、貼り付け、挿入、削除することができます。

ステップ 4 各 OSPFv3 プロセスについて、次のインターフェイス オプションを設定します。

- [インターフェイス（Interface）]：設定するインターフェイス。
- [OSPFv3 を有効にする（Enable OSPFv3）]：OSPFv3 を有効にします。
- [OSPF プロセス（OSPF Process）]：1 または 2 を選択します。
- [エリア（Area）]：このプロセスのエリア ID。
- [インスタンス（Instance）]：インターフェイスに割り当てるエリア インスタンス ID を指定します。インターフェイスは、OSPFv3エリアを1つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

ステップ 5 [プロパティ（Properties）] を選択し、各 OSPFv3 プロセスについて次のオプションを設定します。

- [発信リンク ステート アドバタイズメントをフィルタ（Filter Outgoing Link Status Advertisements）]：OSPFv3 インターフェイスへの発信 LSA をフィルタ処理します。デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。
- [MTU 不一致検出を無効にする（Disable MTU mismatch detection）]：DBD パケットが受信された場合、OSPF MTU 不一致検出を無効にします。OSPF MTU 不一致検出は、デフォルトで有効になっています。
- [フラッドの削減（Flood Reduction）]：エリア全体で 3600 秒ごとにフラッディングしないように、標準の LSA を [LSA をエージングしない（Do Not Age LSAs）] に変更します。

  OSPF LSA は 3600 秒ごとに更新されます。大規模な OSPF ネットワークでは、これにより大量の不要な LSA フラッディングがエリアからエリアに発生する可能性があります。
- [ポイントツーポイント ネットワーク（Point-to-Point Network）]：OSPF ルートを VPN トンネル経由で送信できます。インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。
  - インターフェイスにはネイバーを 1 つだけ定義できます。
  - ネイバーは手動で設定する必要があります。
  - クリプト エンドポイントを指すスタティック ルートを定義する必要があります。
  - トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリーム ルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
  - OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバ

インドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。

- [ブロードキャスト（Broadcast）]：インターフェイスがブロードキャストインターフェイスであることを指定します。デフォルトでは、イーサネットインターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャストインターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。
- [コスト（Cost）]：インターフェイスでパケットを送信するコストを指定します。この設定の有効値の範囲は 0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツーポイントの非ブロードキャストインターフェイスとして設定されているインターフェイスには適用されません。

  2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。
- [優先順位（Priority）]：ネットワークの代表ルータを指定します。有効な値の範囲は 0 ～ 255 です。
- [Dead 間隔（Dead Interval）]：hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間（秒単位）。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。
- [Hello間隔（Hello Interval）]：ネイバーとの隣接関係が確立される前にルータが送信する OSPF パケット間の期間（秒単位）。ルーティング デバイスがアクティブなネイバーを検出すると、hello パケット間隔はポーリング間隔で指定された時間から Hello 間隔で指定された時間に変更されます。有効な値の範囲は、1 ～ 65535 秒です。
- [再送信間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
- [転送遅延（Transmit Delay）]：インターフェイス上でリンクステート更新パケットを送信する予想時間（秒単位）。有効な値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

ステップ 6 [OK] をクリックして、プロパティ設定を保存します。

ステップ 7 [認証（Authentication）] を選択し、各 OSPFv3 プロセスについて次のオプションを設定します。

- [タイプ（Type）]：認証のタイプ。使用可能なオプションは、[エリア（Area）]、[インターフェイス（Interface）]、[なし（None）] です。[なし（None）] オプションを選択すると、認証が行われません。

- [セキュリティ パラメータ インデックス（Security Parameters Index）]：256 ～ 4294967295 の数値。タイプとして [インターフェイス（Interface）] を選択した場合、このオプションを設定します。
- [認証（Authentication）]：認証アルゴリズムのタイプ。サポートされる値は、[SHA-1] および [MD5] です。タイプとして [インターフェイス（Interface）] を選択した場合、このオプションを設定します。
- [認証キー（Authentication Key）]：MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。
- [認証キーを暗号化する（Encrypt Authentication Key）]：認証キーの暗号化を有効にします。
- [暗号化を含める（Include Encryption）]：暗号化を有効にします。
- [暗号化アルゴリズム（Encryption Algorithm）]：暗号化アルゴリズムのタイプ。サポートされる値は DES です。ヌルのエントリは暗号化されません。[暗号化を含める（Include Encryption）] を選択した場合、このオプションを設定します。
- [暗号化キー（Encryption Key）]：暗号キーを入力します。[暗号化を含める（Include Encryption）] を選択した場合、このオプションを設定します。
- [キーを暗号化する（Encrypt Key）]：キーを暗号化できるようにします。

ステップ 8 [OK] をクリックして、認証設定を保存します。

ステップ 9 [ネイバー（Neighbor）] を選択し、[追加（Add）] をクリックして、各 OSPFv3 プロセスについて次のオプションを設定します。

- [リンク ローカル アドレス（Link Local Address）]：スタティック ネイバーの IPv6 アドレス。
- [コスト（Cost）]：コストを有効にします。アドバタイズする場合は、[コスト（Cost）] フィールドにコストを入力し、[発信リンク ステート アドバタイズメントをフィルタ（Filter Outgoing Link State Advertisements）] をオンにします。
- （オプション）[ポーリング間隔（Poll Interval）]：ポーリング間隔を有効にします。[優先順位（Priority）] レベルと [ポーリング間隔（Poll Interval）]（秒単位）を入力します。

ステップ 10 [追加（Add）] をクリックして、ネイバーを追加します。

ステップ 11 [OK] をクリックして、インターフェイス設定を保存します。

OSPFv3 詳細プロパティの設定

[高度なプロパティ（Advanced Properties）] を使用すると、syslog メッセージ生成、アドミニストレーティブ ルート ディスタンス、パッシブ OSPFv3 ルーティング、LSA タイマー、グレースフルリスタートなどのオプションを設定できます。

グレースフル リスタート

Firewall Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。グレースフル リスタート（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

（注） NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[OSPFv3]** > **[高度（Advanced）]** を選択します。

ステップ 3 [ルータID（Router ID）] で、[自動（Automatic）] または [IPアドレス（IP Address）]（非クラスタおよびスパンド EtherChannel モードのクラスタの場合に表示）または [クラスタプール（Cluster Pool）]（個別インターフェイスモードのクラスタの場合に表示）を選択します。[IPアドレス（IP address）] を選択する場合は、[IPアドレス（IP Address）] フィールドに IPv6 アドレスを入力します。[クラスタプール（Cluster Pool）] を選択した場合は、[クラスタプール

（Cluster Pool）] ドロップダウンフィールドで IPv6 クラスタプール値を選択します。クラスタプールアドレスの作成については、アドレス プール （1323 ページ）を参照してください。

ステップ 4 ルートがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信する場合に syslog メッセージを抑制するには、[LSA MOSPF を無視（Ignore LSA MOSPF）] チェックボックスをオンにします。

ステップ 5 [一般（General）] を選択し、次のように設定します。

- [隣接関係の変更（Adjacency Changes）]：syslog メッセージが送信される隣接関係の変更内容を定義します。

  デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。

  - [隣接関係の変更（Adjacency Changes）]：OSPF ネイバーが起動または停止したときに、Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
  - [詳細を含める（Include Details）]：ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firewall Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

- [アドミニストレーティブ ルート ディスタンス（Administrative Route Distances）]：エリア間、エリア内、および外部 IPv6 ルートのアドミニストレーティブ ルート ディスタンスの設定に使用された設定を変更できます。アドミニストレーティブ ルート ディスタンスは 1 ～ 254 の整数です。デフォルトは 110 です。

- [デフォルト情報の発信（Default Information Originate）]：デフォルトの外部ルートを OSPFv3 ルーティング ドメインに生成するには、[有効化（Enable）] チェックボックスをオンにして、次のオプションを設定します。

  - [常にアドバタイズする（Always Advertise）]：デフォルト ルートが存在するかどうかにかかわらず、常にアドバタイズします。
  - [メトリック（Metric）]：デフォルト ルートを生成するために使用するメトリック。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。
  - [メトリック タイプ（Metric Type）]：OSPFv3 ルーティング ドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンク タイプ。有効な値は1（タイプ 1 の外部ルート）および 2（タイプ 2 の外部ルート）です。デフォルトはタイプ 2 外部ルートです。
  - [ルートマップ（Route Map）]：ルートマップが満たされている場合にデフォルトルートを生成するルーティングプロセスを選択するか、[追加（Add）] (＋) をクリックして、新しいルーティングプロセスを追加します。新しいルート マップを追加するには、ルート マップ （1380 ページ）を参照してください。

ステップ 6 [OK] をクリックして、一般設定を保存します。

ステップ 7 [パッシブインターフェイス（Passive Interfaces）] を選択して、[使用可能なインターフェイス（Available Interfaces）] リストからパッシブ OSPFv3 ルーティングを有効にするインターフェイスを選択し、[追加（Add）]をクリックして[選択したインターフェイス（Selected Interfaces）] リストにこれらを移動します。

パッシブ ルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信を無効にします。

ステップ 8 [OK] をクリックしてパッシブ インターフェイス設定を保存します。

ステップ 9 [タイマー（Timer）] を選択し、次の LSA ペーシングと SPF 計算タイマーを設定します。

- [到着（Arrival）]：ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。有効な範囲は 0 ～ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
- [フラッド ペーシング（Flood Pacing）]：フラッディング キュー内の LSA が更新間にペーシング処理される時間を指定します（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。
- [グループ ペーシング（Group Pacing）]：LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [再送信ペーシング（Retransmission Pacing）]：再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。
- [LSA スロットル（LSA Throttle）]：LSA の最初のオカレンスを生成する遅延を指定します（ミリ秒単位）。デフォルト値は、0 ミリ秒です。最小値は、同じ LSA を送信する最小遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最大値は、同じ LSA を送信する最大遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。

  （注）
  LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

- [SPF スロットル（SPF Throttle）]：SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最小値は、最初と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。デフォルト値は、10000 ミリ秒です。最大値は、SPF 計算の最大待機時間をミリ秒単位で指定します。デフォルト値は、10000 ミリ秒です。

  （注）
  SPF スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

ステップ 10 [OK] をクリックして LSA タイマー設定を保存します。

ステップ 11 [ノンストップフォワーディング（Non Stop Forwarding）] を選択し、[グレースフルリスタートヘルパーを有効にする（Enable graceful-restart helper）] チェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスでグレースフル リスタート ヘルパー モードを無効にするには、このチェックボックスをオフにします。

ステップ 12 [リンク ステート アドバタイズメントを有効にする（Enable link state advertisement）] チェックボックスをオンにして、厳密なリンク ステートアドバタイズメントチェックを有効にします。

有効にすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

ステップ 13 [グレースフル リスタートを有効にする（スパンド クラスタまたはフェールオーバーが設定されている場合に使用）（Enable graceful-restart (Use when Spanned Cluster or Failover Configured)）] をオンにして、グレースフル リスタート間隔を秒単位で入力します。範囲は 1 ～ 1800 です。デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

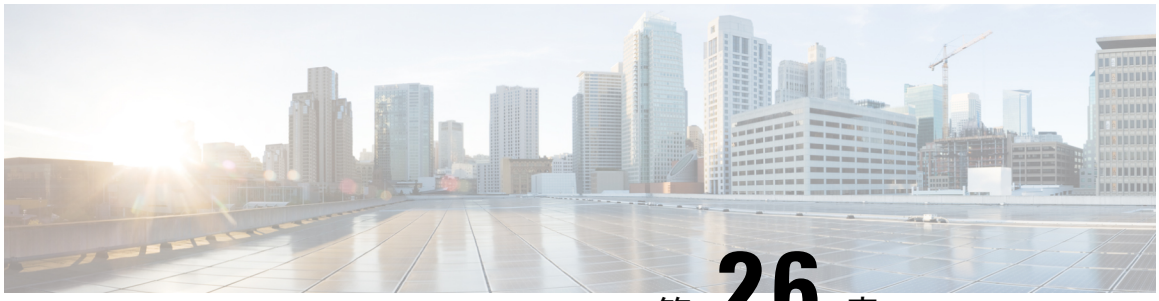
ステップ 14 [OK] をクリックしてグレースフル リスタート設定を保存します。

ステップ 15 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

OSPF の履歴

表 *65 : OSPF* の機能履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
OSPF v2 および v3 に対する BFD サポート	7.4	7.4	OSPFv2 および OSPFv3 インターフェイスで BFD を有効にできます。 新規/変更された画面： • **[設定（Configuration）] > [デバイスセットアップ（Device Setup）] > [ルーティング（Routing）] > [OSPFv2]** • **[設定（Configuration）] > [デバイスセットアップ（Device Setup）] > [ルーティング（Routing）] > [OSPFv3]**



第 26 章

EIGRP

このセクションでは、Enhanced Interior Gateway Routing Protocol（EIGRP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firewall Threat Defense を設定する方法について説明します。

- EIGRP ルーティングについて （1205 ページ）
- EIGRP の要件と前提条件 （1206 ページ）
- EIGRP ルーティングのガイドラインと制限事項 （1207 ページ）
- EIGRP の設定 （1208 ページ）
- EIGRP の履歴 （1217 ページ）

EIGRP ルーティングについて

シスコによって開発された Enhanced Interior Gateway Routing Protocol（EIGRP）は、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネットマスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリは、代替ルートが検出されるまで伝搬されます。EIGRP では可変長サブネットマスクがサポートされているため、ルートはネットワークの境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。

EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときに、部分的なアップデートを送信します。部分的アップデートの伝搬では、その情報を必要とするルータだけがアップデートされるように境界が自動的に設定されます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

脅威防御では、直接接続されているネットワーク上にある他のルータをダイナミックに把握するために、ネイバー探索が使用されます。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。EIGRP デバイスは、新し

いネイバーから hello パケットを受信すると、トポロジテーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジテーブルをデバイスに返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。スタティックに定義されたネイバーは、このルールの例外です。ネイバーを手動で設定すると、hello メッセージ、ルーティングアップデート、および確認応答がユニキャストメッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。保持時間は、その間に脅威防御がそのネイバーから hello パケットを受信すると想定できる時間です。デバイスは、保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、そのネイバーを使用不能と見なします。

EIGRP は、ネイバー探索/回復、Reliable Transport Protocol（RTP）、および Diffusing Update Algorithm（DUAL）をルート計算に使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジテーブルに保存します。最小コストのルートはルーティングテーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブル サクセサから別のルートが選択されます。サクセサとは、宛先への最小コストパスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティングループを形成しないことが保証されます。

フィジブルサクセサがトポロジテーブル内にない場合は、ルートが再計算されます。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリを送信します。このクエリは、連続するネイバーに伝播されます。フィジブルサクセサが見つからない場合は、到達不能メッセージが返されます。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、脅威防御は、ネイバーから応答が返ってくるのを 3 分間待ちます。デバイスがネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

EIGRP の要件と前提条件

モデルのサポート

Threat Defense

Firewall Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

EIGRP ルーティングのガイドラインと制限事項

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでのみサポートされています。

デバイスのガイドライン

- デバイスごとに許可される EIGRP プロセスは 1 つだけです。
- EIGRP は、Firewall Threat Defense 6.6 以降のバージョンの Management Center の UI を使用して設定できます。

インターフェイスのガイドライン

- EIGRP ルーティングプロセスに関連付けられるのは、論理名と IP アドレスを持つルーテッドインターフェイスだけです。
- グローバル仮想ルータに属するインターフェイスのみ EIGRP の一部にできます。EIGRP は、グローバル仮想ルータのルーティングプロトコル全体でルートを学習、フィルタ処理、および再配布できます。
- 物理、EtherChannel、冗長インターフェイス、サブインターフェイスのみをサポートします。ただし、EtherChannel インターフェイスのメンバーはサポートされていません。
- BVI および VNI は EIGRP の一部にできません。
- パッシブインターフェイスはネイバーインターフェイスとして設定できません。

IP アドレスとネットワークオブジェクトのサポート

- IPv4 アドレスのみサポートされています。
- 範囲、FQDN、およびワイルドカードマスクはサポートされていません。
- 標準アクセスリストオブジェクトのみがサポートされています。

再配布のガイドライン

- グローバル仮想ルータの BGP、OSPF、および RIP は、EIGRP に再配布できます。
- EIGRP では、グローバル仮想ルータ内の BGP、OSPF、RIP、スタティック、および接続済みルートに再配布できます。

- EIGRP が、OSPF ネットワークの一部であるデバイスで設定されている場合、またはその逆の場合は、ルートにタグを付けるように OSPF ルータが設定されていることを確認します（EIGRP はルートタグをサポートしていません）。

  EIGRP を OSPF に再配布し、OSPF を EIGRP に再配布する場合は、いずれかのリンクまたはインターフェイスで障害が発生したときや、ルート発信元がダウンしたときにも、ルーティングループが発生します。あるドメインから同じドメインに再度ルートを再配布することを避けるため、ルータは、再配布する際にドメインに属しているルートにタグ付けすることができます。そして、そのタグに基づいて、リモートルータでそれらのルートをフィルタ処理できます。それらのルートはルーティングテーブルにインストールされないため、再度同じドメインに再配布されることはありません。

展開プロセスのガイドライン

展開された EIGRP 設定の既存の AS 番号を変更する場合は、EIGRP を無効にして展開する必要があります。この手順により、Threat Defense に展開された EIGRP 設定がクリアされます。次に、新しい AS 番号で EIGRP 設定を再作成して展開します。このプロセスにより、Threat Defense に展開されている同じ EIGRP 設定による展開の失敗を阻止できます。

アップグレードのガイドライン

バージョン 7.2 以降にアップグレードし、以前のバージョンに FlexConfig EIGRP ポリシーがある場合、展開中に Management Center に警告メッセージが表示されます。ただし、展開プロセスは停止しません。ただし、展開後、UI（**[デバイスの編集（Device (Edit)）]** > **[ルーティング（Routing）]** > **[EIGRP]**）から EIGRP ポリシーを管理するには、**[デバイスの編集（Device (Edit)）]** > **[ルーティング（Routing）]** > **[EIGRP]**ページで設定をやり直し、FlexConfig から設定を削除する必要があります。を参照してください。UI でのポリシーの作成を自動化するために、Firewall Management Center にはポリシーを FlexConfig から UI に移行するオプションがあります。詳細については、FlexConfig ポリシーの移行 （2737 ページ）、を参照してください。

EIGRP の設定

[ルーティング（Routing）] タブで、ファイアウォールデバイスの EIGRP を有効にして設定することができます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [グローバル（Global）] で、[EIGRP] をクリックします。

ステップ 4 [EIGRPの有効化（Enable EIGRP）] チェックボックスをオンにして EIGRP ルーティングプロセスを有効にします。

ステップ 5 [AS番号（AS Number）] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。AS 番号には、複数の自律番号が含まれます。AS 番号は 1 ～ 65535 であり、固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。

ステップ 6 他の EIGRP プロパティを設定するには、次のトピックを参照してください。

1. EIGRP の設定 （1209 ページ）。
2. EIGRP ネイバー設定の設定 （1210 ページ）。
3. EIGRP のフィルタルールの設定 （1210 ページ）。
4. EIGRP 再配布の設定 （1211 ページ）。
5. EIGRP サマリーアドレスの設定 （1213 ページ）。
6. EIGRP インターフェイス設定の指定 （1213 ページ）。
7. EIGRP の高度な設定の指定 （1214 ページ）。

EIGRP の設定

手順

ステップ 1 [EIGRP] ページで [セットアップ（Setup）] タブをクリックします。

ステップ 2 [自動サマリー（Auto Summary）] チェックボックスをオンにして、EIGRP がネットワーク番号境界を集約できるようにします。

（注）
[自動サマリー（Auto Summary）] を有効にすると、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。

ステップ 3 [使用可能なネットワーク/ホスト（Available Networks/Hosts）] ボックスで、EIGRP ルーティングプロセスに参加する必要があるネットワークまたはホストをクリックし、[追加（Add）] をクリックします。新しいネットワークオブジェクトを追加するには、[追加（Add）] (＋) をクリックします。ネットワークを追加する手順については、ネットワーク （1349ページ）を参照してください。

ステップ 4 パッシブインターフェイスを構成するには、[パッシブインターフェイス（Passive Interface）] チェックボックスをオンにします。EIGRP の場合、受動インターフェイスではルーティングアップデートが送受信されません。

a) 選択したインターフェイスをパッシブとして指定するには、[選択したインターフェイス（Selected Interface）] オプションボタンをクリックします。[使用可能なインターフェイス（Available Interfaces）] ボックスでインターフェイスを選択し、[追加（Add）] をクリックします。

b) すべてのインターフェイスをパッシブとして指定するには、[すべてのインターフェイス（All Interfaces）] オプションボタンをクリックします。

ステップ 5 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP ネイバー設定の設定

EIGRP プロセスのスタティックネイバーを定義できます。EIGRP ネイバーを定義すると、hello パケットがそのネイバーにユニキャストされます。

手順

ステップ 1 [EIGRP] ページで [ネイバー（Neighbors）] タブをクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 [インターフェイス（Interface）] ドロップダウンリストから、ネイバーが使用可能になるインターフェイスを選択します。

ステップ 4 [ネイバー（Neighbor）] ドロップダウンから、スタティックネイバーの IP アドレスを選択します。ネットワークオブジェクトを追加するには、[追加（Add）] (+) をクリックします。ネットワークオブジェクトの追加手順については、ネットワーク （1349 ページ）を参照してください。

ステップ 5 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP のフィルタルールの設定

EIGRP ルーティングプロセスのルートフィルタルールを設定できます。フィルタルールによって、EIGRP ルーティングプロセスで受け入れまたはアドバタイズされるルートを制御できます。

手順

ステップ 1 [EIGRP] ページで、[フィルタルール（Filter Rules）] タブをクリックします。

ステップ 2 [追加（Add）] (+) をクリックします。

ステップ 3 [フィルタルールの追加（Add Filter Rules）] ダイアログボックスで、[フィルタ方向（Filter Direction）] ドロップダウンからルールの方向を選択します。

- [インバウンド（Inbound）]：このルールは、着信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。

- [アウトバウンド（Outbound）]：このルールは、発信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。

ステップ 4 フィルタルールを適用するインターフェイスを選択するには、[インターフェイス（Interface）] オプションボタンをクリックし、ドロップダウンからインターフェイスを選択します。

（注）
VTI インターフェイス上では、EIGRP フィルタリング ルールを適用できません。

ステップ 5 フィルタルールを適用するプロトコルを選択するには、[プロトコル（Protocol）] オプションボタンをクリックし、ドロップダウンからプロトコル（[BGP]、[RIP]、[静的（Static）]、[接続（Connected）]、または [OSPF]）を選択します。BGP および OSPF プロトコルの場合は、関連するプロセス ID を指定できます。

ステップ 6 [Access List] ドロップダウンから、アクセスリストを選択します。このリストは、受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義します。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）] (+) をクリックし、詳細な手順について 標準 ACL オブジェクトの設定 （1322 ページ） を参照してください。

ステップ 7 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP 再配布の設定

他のルーティングプロトコルから EIGRP ルーティングプロセスにルートを再配布するためのルールを定義できます。

手順

ステップ 1 [EIGRP] ページで、[再配布（Redistribution）] タブをクリックします。

ステップ 2 [追加（Add）] (+) をクリックします。

ステップ 3 [再配布の追加（Add Redistribution）] ダイアログボックスの [プロトコル（Protocol）] ドロップダウンから、ルートが再配布されるソースプロトコルを選択します。

- [BGP]：BGP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。
- [RIP]：RIP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。
- [Static]：スタティックルートを EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティックルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。ただし、EIGRP で VTI インターフェイスを指すスタティック ルートを再配布する場合は、メトリックを指定する必要があります。他のタイプのインターフェイスを指すスタティック ルートの場合、メトリックの指定は必須ではありません。

- [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [OSPF]：OSPF ルーティングプロセスで検出されたルートを EIGRP に再配布します。このプロトコルを選択すると、[オプションのOSPF再配布（Optional OSPF Redistribution）] で、このダイアログボックスの [一致（Match）] オプションが表示されます。
  - [Internal]：特定の AS の内部のルート。
  - [External1]：AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
  - [External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。
  - [Nsaa-External1]：AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area（NSSA）ルート。
  - [Nsaa-External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる（NSSA）ルート。

（注）
これらのオプションは、スタティック、接続済み、RIP、またはBGPルートを再配布するときには使用できません。

ステップ 4 [オプションメトリック（Optional Metrics）] で、関連する値を入力します。

- [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。
- [遅延時間（Delay Time）]：10 マイクロ秒単位のルート遅延です。有効値の範囲は、0 ～ 4294967295 です。
- [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。
- [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は、1 ～ 255 です。255 は 100% のロードを意味します。
- [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。

ステップ 5 [ルートマップ（Route Map）] ドロップダウンから、再配布エントリに適用するルートマップオブジェクトを選択します。新しいルートマップオブジェクトを作成するには、[追加（Add）]（＋）をクリックします。新しいルートマップを追加する手順については、「ルートマップエントリの設定」を参照してください。

ステップ 6 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP サマリーアドレスの設定

インターフェイスごとにサマリーアドレスを設定できます。ネットワークの境界以外でサマリーアドレスを作成する場合、または自動ルート集約が無効になったThreat Defenseでサマリーアドレスを使用する場合は、手動でサマリーアドレスを定義する必要があります。より具体的なルートがルーティングテーブルにある場合、EIGRPは、より具体的なすべてのルートの最小に等しいメトリックを持つサマリーアドレスをアドバタイズします。

手順

ステップ1 [EIGRP] ページで、[サマリーアドレス（Summary Address）] タブをクリックします。

ステップ2 [Add] をクリックします。

ステップ3 [インターフェイス（Interface]） ドロップダウンで、どのインターフェイスからこのサマリーアドレスをアドバタイズするかを選択します。

ステップ4 [ネットワーク（Network）] ドロップダウンから、集約する特定のIPアドレスとネットワークマスクを持つネットワークオブジェクトを選択します。新しいネットワークを追加するには、[追加（Add）] (+) をクリックします。ネットワークを追加する手順については、ネットワーク （1349 ページ）を参照してください。

ステップ5 [アドミニストレーティブ ディスタンス（Administrative Distance）] フィールドに、サマリールートのアドミニストレーティブ ディスタンスを入力します。有効値の範囲は、1 ～ 255 です。

ステップ6 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP インターフェイス設定の指定

[インターフェイス（Interfaces）] タブで、インターフェイス固有のEIGRPルーティングプロパティを設定できます。

手順

ステップ1 [EIGRP] ページで、[インターフェイス（Interfaces）] タブをクリックします。

ステップ2 [追加（Add）] (+) をクリックします。

ステップ3 [インターフェイス（Interface）] ドロップダウンから、設定が適用されるインターフェイスの名前を選択します。

ステップ4 [hello間隔（Hello Interval）] フィールドに、インターフェイスで送信されるEIGRP helloパケットの間隔を秒単位で入力します有効値の範囲は1 ～ 65535 です。デフォルト値は5秒です。

ステップ 5 [ホールド時間（Hold Time）] フィールドに、EIGRP hello パケットでデバイスによってアドバタイズされるホールド時間を入力します。有効値の範囲は 3 ～ 65535 です。デフォルト値は 15 秒です。

ステップ 6 インターフェイスで EIGRP スプリットホライズンを有効にするには、[スプリットホライズン（Split Horizon）] チェックボックスをオンにします。

ステップ 7 [遅延時間（Delay Time）] フィールドに、遅延時間を 10 マイクロ秒単位で入力します。有効な値は、1 ～ 16777215 です。このオプションは、マルチコンテキストモードのデバイスではサポートされています。

ステップ 8 認証プロパティの値を指定します。

- [MD5認証の有効化（Enable MD5 Authentication）]：EIGRP パケットの認証に MD5 ハッシュアルゴリズムを使用するには、このチェックボックスをオンにします。
- [キータイプ（Key Type）]：このドロップダウンから、次のいずれかのキータイプを選択します。
  - [なし（None）]：認証が必要ないことを示します。
  - [非暗号化（Unencrypted）]：使用されるキー文字列がクリアテキストの認証用パスワードであることを示します。
  - [暗号化（Encrypted）]：使用されるキー文字列が暗号化された認証用パスワードであることを示します。
  - [認証キー（Auth Key）]：使用されるキー文字列が EIGRP 認証キーであることを示します。
- [キーID（Key ID）]：EIGRP 更新の認証に使用されるキーの ID。数値のキー ID を入力します。有効値の範囲は 0 ～ 255 です。
- [キー（Key）]：最大 17 文字の英数字文字列。暗号化された認証タイプの場合は、このフィールドに 17 文字以上の文字列が必要です。
- [キーの確認（Confirm Key）]：キーを再入力します。

ステップ 9 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP の高度な設定の指定

ルータ ID、スタブルーティング、隣接関係の変更など、EIGRP の詳細設定を設定します。

手順

ステップ 1 [EIGRP] ページで [詳細（Advanced）] タブをクリックします。

ステップ 2 [デフォルトルート情報（Default Route Information）] で、EIGRP アップデート内のデフォルトルート情報の送受信を指定できます。

- （非クラスタおよびスパンド EtherChannel モードのクラスタの場合に表示）[ルータID（IP アドレス）（Router ID (IP Address)）]：外部ルートの発信元ルータを識別するために使用される ID を入力します。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。この問題を回避するには、ルータ ID のグローバルアドレスを指定します。各 EIGRP ルータには、一意の値を設定する必要があります。
- （個別インターフェイスモードのクラスタの場合にのみ表示）[IPv4アドレスプール（IPv4 Address Pool）]：関連するクラスタプール値（IPv4 アドレスプールオブジェクト）を選択します。アドレスプールを作成するには、アドレス プール （1323 ページ） を参照してください。
- [デフォルトのルート情報を受け入れる（Accept Default Route Info）]：外部のデフォルトルーティング情報を受け入れるように EIGRP を設定するには、このチェックボックスをオンにします。
  - [アクセスリスト（Access List）]：[アクセスリスト（Access List）] ドロップダウンから、デフォルトルート情報の受信時に許可するネットワークと許可しないネットワークを定義する標準アクセスリストを指定します。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）] (+) をクリックし、詳細な手順について 標準 ACL オブジェクトの設定 （1322 ページ） を参照してください。
- [デフォルトのルート情報を送信する（Send Default Route Info）]：外部のデフォルトルーティング情報をアドバタイズするように EIGRP を設定するには、このチェックボックスをオンにします。
  - [アクセスリスト（Access List）]：[アクセスリスト（Access List）] ドロップダウンから、デフォルトルート情報の送信時に許可するネットワークと許可しないネットワークを定義する標準アクセスリストを指定します。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）] (+) をクリックし、詳細な手順について 標準 ACL オブジェクトの設定 （1322 ページ） を参照してください。

ステップ 3 [アドミニストレーティブ ディスタンス（Administrative Distance）] で、次の項目を指定します。

- [内部ディスタンス（Internal Distance）]：EIGRP 内部ルートのアドミニストレーティブディスタンスです。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効値の範囲は、1 ～ 255 です。デフォルトは 90 です。
- [外部ディスタンス（External Distance）]：EIGRP 外部ルートのアドミニストレーティブディスタンスです。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効値の範囲は、1 ～ 255 です。デフォルト値は 170 です。

ステップ 4 [隣接関係の変更（Adjacency Changes）] で、次の項目を指定します。

- [ログネイバーの変更（Log Neighbor Changes）]：EIGRP ネイバーの隣接関係の変更に関するロギングを有効にするには、このチェックボックスをオンにします。
- [ログネイバーの警告（Log Neighbor Warnings）]：EIGRP ネイバーの警告メッセージのロギングを有効にするには、このチェックボックスをオンにします。
- （任意）ネイバー警告メッセージの反復時間間隔（秒数）を入力します。有効値の範囲は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

ステップ 5 EIGRP スタブルーティングプロセスとしてデバイス有効にするには、[スタブ（Stub）] にある次の EIGRP スタブルーティングプロセスのチェックボックスを 1 つ以上オンにします。

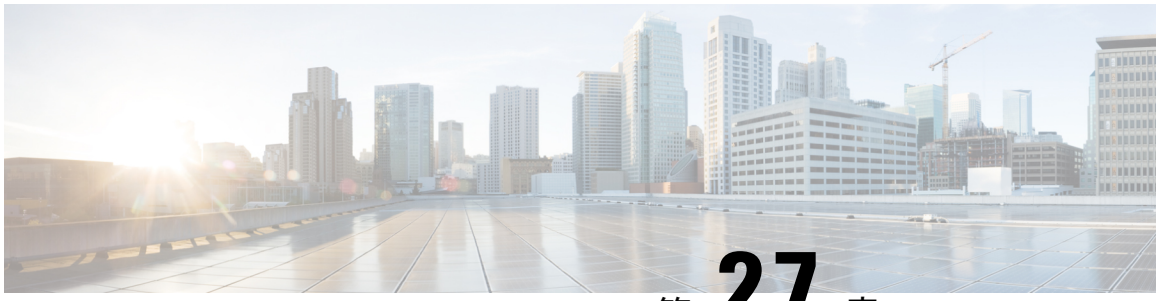
- [受信のみ（Receive only）]：ネイバールータからルート情報を受信しても、そのネイバールータにはルート情報を送信しない EIGRP スタブルーティングプロセスを設定します。このオプションを選択する場合は、他のスタブ ルーティング オプションを選択できません。
- [接続済み（Connected）]：接続済みルートをアドバタイズします。
- [再配布済み（Redistributed）]：再配布済みルートをアドバタイズします。
- [スタティック（Static）]：スタティックルートをアドバタイズします。
- [サマリー（Summary）]：サマリールートをアドバタイズします。

ステップ 6 [デフォルトのメトリック（Default Metrics）] で、EIGRP ルーティングプロセスに再配布されるルートのデフォルトのメトリックを定義します。

- [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。
- [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。
- [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。
- [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。
- [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。

EIGRP の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
EIGRP 設定	7.2	任意（Any）	以前のリリースでは、EIGRP は FlexConfig を介してのみ Threat Defense で設定できました。FlexConfig は、EIGRP 設定をサポートしなくなりました。Management Center の UI で Threat Defense 用の EIGRP 設定を構成できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[EIGRP]**。



第 27 章

BGP

この項では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように Firewall Threat Defense を設定する方法について説明します。

- BGPについて （1219 ページ）
- BGP の要件と前提条件 （1223 ページ）
- BGP のガイドライン （1223 ページ）
- BGP の設定 （1224 ページ）
- BGP の履歴 （1242 ページ）

BGPについて

BGP は相互および内部の自律システムのルーティングプロトコルです。自律システムとは、共通の管理下にあり、共通のルーティングポリシーを使用するネットワークまたはネットワークのグループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGP ルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

（注） AS ループの検出は、完全な AS パス（AS_PATH 属性で指定される）をスキャンし、ローカルシステムの AS 番号が AS パスに現れないことを確認することによって実行されます。デフォルトでは、EBGP は学習したルートを同じピアにアドバタイズすることで、ループチェックを実行するときにデバイスで追加の CPU サイクルが発生することを防ぐとともに、既存の発信更新タスクの遅延を防ぎます。

BGPにより学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。次のプロパティはBGP属性と呼ばれ、ルート選択プロセスで使用されます。

- Weight: これはシスコ定義の属性で、ルータに対してローカルです。Weight属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、[重み（Weight）] 属性値が最も大きいルートが優先されます。
- Local preference: Local preference属性は、ローカルASからの出口点を選択するために使用されます。Weight属性とは異なり、Local preference属性は、ローカルAS全体に伝搬されます。ASからの出口点が複数ある場合は、Local preference属性が最も高い出口点が特定のルートの出口点として使用されます。
- Multi-exit discriminator: メトリック属性であるMulti-exit discriminator (MED)は、メトリックをアドバタイズしているASへの優先ルートに関して、外部ASへの提案として使用されます。これが提案と呼ばれるのは、MEDを受信している外部ASがルート選択の際に他のBGP属性も使用している可能性があるためです。MEDメトリックが小さい方のルートが優先されます。
- Origin: Origin属性は、BGPが特定のルートについてどのように学習したかを示します。Origin属性は、次の3つの値のいずれかに設定することができ、ルート選択に使用されます。
  - IGP: ルートは発信側ASの内部にあります。この値は、ネットワークルータコンフィギュレーションコマンドを使用してBGPにルートを挿入する場合に設定されます。
  - EGP: ルートはExterior Border Gateway Protocol (EBGP)を使用して学習されます。
  - Incomplete: ルートの送信元が不明であるか、他の方法で学習されています。IncompleteのOriginは、ルートがBGPに再配布されるときに発生します。
- AS_path：ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティングテーブルにインストールされます。
- Next hop: EBGPのnext-hop属性は、アドバタイジングルータに到達するために使用されるIPアドレスです。EBGP ピアの場合、ネクストホップアドレスは、ピア間の接続のIPアドレスです。IBGP の場合、EBGP のネクストホップアドレスがローカル AS に伝送されます。ただし、ネクストホップが eBGP ピアのピアリングアドレスと同じサブネットにある場合、ネクストホップは変更されません。この動作は、サードパーティのネクストホップと呼ばれます。

  VPN でアドバタイズされたルートを iBGP ピアに再配布する場合は、**next-hop-self** コマンドを使用して、ルートが正しいネクストホップ IP で再配布されるようにします。
- Community: Community属性は、ルーティングの決定(承認、優先順位、再配布など)を適用できる接続先をグループ化する方法、つまりコミュニティを提供します。ルートマップは、Community 属性を設定するために使用されます。事前定義済みのCommunity属性は次のとおりです。

- no-export: EBGPピアにアドバタイズしません。
- no-advertise: どのピアにもこのルートをアドバイタイズしません。
- internet：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP を使用する状況

通常、大学や企業などの顧客ネットワークではネットワーク内でルーティング情報を交換するために OSPF などの Interior Gateway Protocol（IGP）を採用しています。カスタマーはISPに接続し、ISPはBGPを使用してカスタマーおよびISPルートを交換します。自律システム（AS）間でBGPを使用する場合、このプロトコルは外部BGP（EBGP）と呼ばれます。サービスプロバイダーがBGPを使用してAS内のルートを交換する場合、このプロトコルは内部BGP（IBGP）と呼ばれます。

BGPは、IPv6ネットワーク上でIPv6プレフィックスのルーティング情報を伝送するためにも使用することができます。

BGP パスの選択

BGPは、異なる送信元から同じルートに対する複数のアドバタイズメントを受信する場合があります。BGP はベストパスとして 1 つのパスだけを選択します。ベストパスを選択すると、BGPは選択したパスをIPルーティングテーブルに格納し、そのネイバーにパスを伝達します。BGP は、次に示す順序で次の条件を使用して、宛先のパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、更新はドロップされます。
- 重みが最大のパスが優先されます。
- 重みが同じ場合、ローカルプリファレンスが最大のパスが優先されます。
- ローカルプリファレンスが同じ場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_pathが最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じ場合、Origin タイプが最下位のパス（IGP は EGP よりも低く、EGP は Incomplete よりも低い）が優先されます。
- Origin コードが同じ場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じ場合、内部パスより外部パスが優先されます。
- それでもパスが同じ場合、最も近い IGP ネイバーを経由するパスが優先されます。
- BGPマルチパス （1222ページ） 用のルーティングテーブルに複数のパスをインストールする必要があるか判断します。
- 両方のパスが外部のときは、先に受信したパス(最も古いパス)が優先されます。

- BGPルータIDで指定された、IPアドレスが最も小さいパスが優先されます。
- 発信元 ID またはルータ ID が複数のパスで同じ場合は、最小のクラスタ リスト長を持つパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同じ宛先プレフィックスへの複数の等コスト BGP パスの IP ルーティングテーブルへのインストールが許可されます。その場合、宛先プレフィックスへのトラフィックは、インストールされたすべてのパス間で共有されます。

これらのパスは、ロードシェアリング用にベストパスとともにテーブルにインストールされます。BGPマルチパスはベストパスの選択には影響しません。たとえば、ルータではアルゴリズムに従って、ベストパスとしてパスの 1 つが引き続き指定され、そのベストパスが BGP ピアにアドバタイズされます。

マルチパスの候補になるためには、同じ宛先へのパスに、最適パスの特性に等しいこれらの特性が備わっている必要があります。

- 重量
- ローカル プリファレンス
- AS-PATH length
- オリジン コード
- Multi Exit識別子(MED)
- 次のいずれか。
  - ネイバー AS または sub-AS（BGP マルチパス機能が追加される前）
  - AS-PATH（BGP マルチパス機能が追加された後）

一部の BGP マルチパス機能により、マルチパス候補に関する追加要件が加わりました。

- パスは、外部またはコンフェデレーション外部の近接ルータ（eBGP）から学習されます。
- BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

内部 BGP（iBGP）マルチパスの候補には次の追加要件があります。

- パスは、内部の近接ルータ（iBGP）から学習されます。
- ルータが不等コスト iBGP マルチパスで設定されない限り、BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

BGP は、マルチパス候補から最近受信した最大 *n* 個のパスを IP ルーティングテーブルに挿入します。ここで、*n* は、BGPマルチパスを設定するときに指定した、ルーティングテーブルに

インストールするルートの数です。マルチパスがディセーブルになっている場合のデフォルト値は 1 です。

不等コスト ロード バランシングでは、BGP リンク帯域幅も使用できます。

（注） 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP の要件と前提条件

モデルのサポート

Threat Defense

Firewall Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

BGP のガイドライン

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルーテッドモードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

その他のガイドライン

- BGP の場合、ルートのネクストホップ IP アドレスはネットワーク IP アドレスであり、0.0.0.0 ではありません。

- システムは、PPPoE 経由で受信した IP アドレスのルートエントリを CP ルートテーブルに追加しません。BGP は常に CP ルートテーブルを調べて TCP セッションを開始するため、BGP は TCP セッションを形成しません。

  つまり、PPPoE 経由の BGP はサポートされません。

- 管理専用または BVI インターフェイスでは、BGP はサポートされません
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。
- PATH MTU（PMTU）を使用した BGP は、特に ECMP ルーティングで MTU ディスカバリが失敗した場合に、隣接関係（アジャセンシー）フラップを引き起こす可能性があります。したがって、何らかの理由で MTU ディスカバリが失敗した場合にパケットドロップが発生する可能性があるため、BGP、PMTU、および ECMP の使用時には注意が必要です。
- メンバーユニットの BGP テーブルは、制御ユニットテーブルと同期されません。ルーティングテーブルだけが、制御ユニットのルーティングテーブルと同期されます。
- 静的または動的な VTI インターフェイスを使用してルートベースのサイト間 VPN を構成する場合、ルーティングプロトコルとして BGP を使用している場合は、TTL ホップの値が 2 以上であることを確認してください。

BGP の設定

BGP を設定するには、以下のトピックを参照してください。

手順

ステップ 1 BGP 基本設定 （1225 ページ）
ステップ 2 BGP 一般設定 （1228 ページ）
ステップ 3 BGP ネイバーの設定 （1230 ページ）
ステップ 4 BGP 集約アドレス設定の設定 （1234 ページ）
ステップ 5 BGPv4 フィルタリング設定 （1236 ページ）

（注）
フィルタリング セクションは、IPv4 設定にのみ適用されます。

ステップ 6 BGP ネットワーク設定 （1236 ページ）
ステップ 7 BGP 再配布設定 （1237 ページ）
ステップ 8 BGP ルート注入の設定 （1238 ページ）

ステップ 9 BGP ルートのインポート/エクスポート設定の設定 （1239 ページ）

BGP 基本設定

BGP の多くの基本設定が可能です。

仮想ルーティングを使用するデバイスの場合、このセクションで説明する基本設定は、[BGP] ページの [一般設定（General Settings）] で設定する必要があります。詳細については、Firewall Management Center Web インターフェイスの変更：[ルーティング（Routing）] ページ （1102 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] を選択します。

ステップ 3 （仮想ルータ対応デバイスの場合）[一般設定（General Settings）] で [BGP] をクリックします。

ステップ 4 [BGP の有効化（Enable BGP）] チェックボックスをオンにして、BGP ルーティングプロセスを有効にします。

ステップ 5 [AS 番号（AS Number）] フィールドに、BGP プロセスの自律システム（AS）番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。AS 番号は固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。

ステップ 6 [ルータ ID（Router ID）] ドロップダウンリストで、[自動（Automatic）] または [手動（Manual）]（非クラスタおよびスパンド EtherChannel モードのクラスタの場合に表示）または [クラスタプール（Cluster Pool）]（個別インターフェイスモードのクラスタの場合に表示）を選択します。自動を選択すると、Firewall Threat Defense デバイス上で最上位の IP アドレスがルータ ID として使用されます。[手動（Manual）] を選択した場合は、[IPアドレス（IP Address）] フィールドに IP アドレスを入力します。[クラスタプール（Cluster Pool）] を選択した場合は、[クラスタプール（Cluster Pool）] フィールドにクラスタプール値を入力します。クラスタプールアドレスの作成については、アドレス プール （1323 ページ）を参照してください。

ステップ 7 固定ルータ ID を使用するには、[手動（Manual）] を選択して、[IPアドレス（IP Address）] フィールドに IPv4 アドレスを入力します。デフォルト値は [自動（Automatic）] です。仮想ルータ対応デバイスの場合は、**[仮想ルータ（Virtual Routers）] > [BGP]** ページでルータ ID の設定をオーバーライドできます。

ステップ 8 （オプション）[General] でさまざまな BGP 設定を編集します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。[編集（Edit）]（✎）をクリックして、グループの設定を編集します。

a) ネクストホップの検証用に BGP ルータの**スキャン間隔**を入力します。有効な値は 5 ～ 60 秒です。デフォルト値は 60 です。

b) [AS_PATH属性のAS番号の数（Number of AS numbers in AS_PATH attribute）] を入力します。AS パス属性は、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。有効な値は、1 ～ 254 です。デフォルト値は None です。

c) [ログ ネイバー変更（Log Neighbor Changes）] チェックボックスをオンにして、BGP ネイバーの変更（アップ状態またはダウン状態）およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。この設定はデフォルトで有効になっています。

d) [TCP パス MTU ディスカバリ使用（Use TCP path MTU discovery）] チェックボックスをオンにし、パス MTU 手法を使用して 2 つの IP ホスト間のネットワーク パスにおける最大伝送単位（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。この設定はデフォルトで有効になっています。

e) [フェールオーバー後すぐにセッションをリセット（Reset session upon Failover）] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。この設定はデフォルトで有効になっています。

f) [最初の AS を EBGP ルートのピアの AS として実行（Enforce that first AS is peer's AS for EBGP routes）] チェックボックスをオンにして、その AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストしていない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。この設定はデフォルトで有効になっています。

g) [AS 番号のドット表記を使用（Use dot notation for AS numbers）] チェックボックスをオンにして、完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。これは、デフォルトでは無効になっています。

h) [OK] をクリックします。

ステップ 9 （オプション）[ベスト パス選択（Best Path Selection）] セクションを編集します。

a) [デフォルトローカル優先度（Default Local Preference）] で 0 ～ 4294967295 の値を入力します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバに送信されます。

b) [異なるネイバーからの MED 比較を許可（Allow comparing MED from different neighbors）] チェックボックスをオンにして、さまざまな自律システムのネイバーからのパスにおいて Multi-exit discriminator（MED）の比較ができるようにします。これは、デフォルトでは無効になっています。

c) [同一 EBGP パスのルータ ID を比較（Compare Router ID for identical EBGP paths）] チェックボックスをオンにして、最適なパスの選択プロセス中に、外部 BGP ピアから受信した類似のパスを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。これは、デフォルトでは無効になっています。

d) [隣接する AS がアドバタイズしたパス間の最適 MED を選別（Pick the best MED path among paths advertised from the neighboring AS）] チェックボックスをオンにして、連合ピアから学習したパス間における MED 比較を有効にします。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。これは、デフォルトでは無効になっています。

e) [欠落 MED を最低優先度として処理（Treat missing MED as the least preferred one）] チェックボックスをオンにして、欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。これは、デフォルトでは無効になっています。

f) [OK] をクリックします。

ステップ 10 （オプション）[ネイバー タイマー（Neighbor Timers）] セクションを編集します。

a) [キープアライブインターバル（Keep alive interval）] フィールドに、BGP ネイバーがキープアライブメッセージを送信しなくなった後アクティブな状態を継続する時間を入力します。このキープアライブインターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。

b) [維持時間（Hold Time）] フィールドで、BGP 接続が開始、設定されている間、BGP ネイバーがアクティブな状態を維持する時間間隔を入力します。デフォルト値は 180 秒です。0 ～ 65535 の値を指定します。

c) （オプション）[最小維持時間（Min Hold time）] フィールドで、BGP 接続が開始、設定されている間、BGP ネイバーがアクティブな状態を維持する最小時間間隔を入力します。3 ～ 65535 の値を指定します。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

d) [OK] をクリックします。

ステップ 11 [ネクストホップ（Next Hop）] セクションで、必要に応じて BGP ネクストホップアドレス追跡を有効にする [アドレス追跡を有効にする（Enable address tracking）] チェックボックスをオンにし、ルーティングテーブルにインストールされた更新ネクストホップルートのチェック間隔として [遅延インターバル（Delay Interval）] を入力します。[OK] をクリックします。

（注）
[ネクスト ホップ（Next Hop）] セクションは、IPv4 設定にのみ適用されます。

ステップ 12 （オプション）[グレースフル リスタート（Graceful Restart）] セクションを編集します。

（注）
このセクションは、Firewall Threat Defenseデバイスがフェールオーバーまたはスパンドクラスタモードになっているときにのみ使用できます。フェールオーバー設定のデバイスの 1 つが失敗した場合に、トラフィック フローのパケットでドロップがないように行われるものです。

a) [グレースフルリスタートを有効にする（Enable Graceful Restart）] チェックボックスをオンにして、Firewall Threat Defense ピアがスイッチオーバー後のルートフラップを回避できるようにします。

b) [リスタート時間（Restart Time）] フィールドで BGP オープン メッセージが受信される前に、Firewall Threat Defenseピアが古いルートを削除するまでの待機時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。

c) [Stalepath時間（Stalepath Time）] フィールドで、リスタートする Firewall Threat Defenseから End Of Record（EOR）メッセージを受信した後、Firewall Threat Defenseが古いルートを

削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

d) [OK] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

ステップ 14 BGP の基本設定を表示するには、[仮想ルータ（Virtual Routers）] ドロップダウンから目的のルータを選択し、[BGP] をクリックします。

このページには、[設定（Settings）]ページで設定された基本設定が表示されます。このページでルータ ID の設定を編集できます。

ステップ 15 ルータ ID の設定を編集するには、[IPアドレス（IP Address）] フィールドの IP アドレスを変更します。変更された値で、[BGP] ページの [一般設定（General Settings）] で設定されたルータ ID の設定がオーバーライドされます。

BGP 一般設定

ルートマップ、アドミニストレーティブルートディスタンス、同期、ネクストホップ、パケット転送を設定します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [General] をクリックします。

ステップ 5 [一般（General）] で、次のセクションを更新します。

a) [設定（Settings）] セクションの [ルートマップ（Route Map）] でルートマップオブジェクトを入力または選択し、[OK] をクリックします。

（注）
[ルート マップ（Route Map）] フィールドは、IPv4 設定にのみ適用されます。

b) [アドミニストレーティブルートディスタンス（Administrative Route Distances）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- [外部（External）] : 外部 BGP ルートのアドミニストレーティブ ディスタンスを入力します。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 20 です。

- [内部（Internal）]：内部 BGP ルートのアドミニストレーティブ ディスタンスを入力します。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。
- [ローカル（Local）]：ローカル BGP ルートのアドミニストレーティブ ディスタンスを入力します。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ表示コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。

c) [ルートと同期化（Routes and Synchronization）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- （オプション）[デフォルトルートの生成（Generate default routes）]：デフォルトの情報発信元を設定するには、このオプションのチェックボックスをオンにします。
- （オプション）[サブネットルートのネットワーク レベルルートへの集約（Summarize subnet routes into network-level routes）]：このオプションのチェックボックスをオンにして、ネットワーク レベルのルートへのサブネットルートの自動集約を設定します。このチェックボックスは、IPv4 設定にのみ適用されます。
- （オプション）[非アクティブなルートのアドバタイズ（Advertise inactive routes）]：このオプションのチェックボックスをオンにして、ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。
- （オプション）[BGP と IGP システム間の同期化（Synchronize between BGP and IGP system）]：このオプションのチェックボックスをオンにして、BGP と内部ゲートウェイ プロトコル（IGP）システムの間の同期を有効にします。通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。この機能により、自律システム内のルータおよびアクセス サーバは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。
- （オプション）[IBGP の IGP への再配布（Redistribute IBGP into IGP）]：このオプションのチェックボックスをオンにして、OSPF などの内部ゲートウェイ プロトコル（IGP）への iBGP の再配布を設定します。

d) [多重パスでパケットを転送（Forward Packets over Multiple Paths）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- （オプション）[パスの数（Number of Paths）]：ルーティング テーブルにインストール可能な Border Gateway Protocol ルートの最大数を入力します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。
- （オプション）[IBGP パスの数（IBGP Number of Paths）]：ルーティング テーブルにインストール可能な並行内部ボーダー ゲートウェイ プロトコル（IBGP）ルートの最大数を入力します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。

ステップ 6 [保存（Save）] をクリックします。

BGP ネイバーの設定

BGP ルータは、更新を交換する前に各ピアと接続する必要があります。これらのピアは BGP ネイバーと呼ばれます。この手順を実行して、BGP IPv4 または IPv6 ネイバーとネイバーの設定を定義します。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Neighbor] クリックします。

ステップ 5 [追加（Add）] をクリックして、BGP ネイバーとネイバーの設定を定義します。

ステップ 6 BGP ネイバーの **IP アドレス**を入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。静的 VTI で BGP IPv6 を設定する場合は、ネイバーの仮想トンネル IP アドレスを入力します。

ステップ 7 BGP ネイバーのインターフェイスを選択します。

（注）
[インターフェイス（Interface）] フィールドは、IPv6 の設定にのみ適用されます。

ステップ 8 [リモート AS（Remote AS）] フィールドに、BGP ネイバーが属する自律システムを入力します。

ステップ 9 [有効アドレス（Enabled address）] チェックボックスをオンにして、この BGP ネイバーとの通信を有効にします。[有効アドレス（Enabled address）] チェックボックスがオンの場合にのみ、追加のネイバー設定が行われます。

ステップ 10 （オプション）[管理シャットダウン（Shutdown administratively）] チェックボックスをオンにして、ネイバーまたはピアグループを無効化します。

ステップ 11 （オプション）**[グレースフルリスタートの設定（Configure graceful restart）]** チェックボックスをオンにして、このネイバーの BGP グレースフルリスタート機能の設定を有効にします。このオプションを選択した後、**[グレースフルリスタート（フェールオーバー/スパンドモード）（Graceful Restart（failover/spanned mode））]** チェックボックスを使用して、このネイバーに対してグレースフルリスタートを有効にするか、無効にするかを指定する必要があります。

（注）
- [グレースフル リスタート（graceful restart）] フィールドは、IPv4 の設定にのみ適用されます。

- グレースフルリスタートは、デバイスがHAモードの場合、またはL2クラスタ（同じネットワークのすべてのノード）が設定されている場合にのみ有効になります。

ステップ 12 （オプション）BGP の BFD サポートの設定を有効にするには、[BFDフェールオーバー（BFD Failover）] ドロップダウンリストから BFD タイプ（single-hop、multi-hop、auto-detect-hop）を選択します。この選択により、BFD から転送パス検出失敗メッセージを受信するように BGP ネイバーが登録されます。BFD サポートが必要ない場合は、[なし（None）] を選択します。

ステップ 13 （オプション）BGP ネイバーの**説明**を入力します。

ステップ 14 （オプション）[ルートのフィルタリング（Filtering Routes）] で、必要に応じてアクセスリスト、ルートマップ、プレフィックスリスト、および AS パスのフィルタを使用して、BGP ネイバー情報を配布します。次の各セクションを更新します。

a) 適切な着信または発信**アクセスリスト**を入力または選択して、BGP ネイバー情報を配布します。

（注）
アクセスリストは、IPv4 の設定にのみ適用されます。

b) 適切な着信または発信**ルートマップ**を入力または選択して、着信または発信ルートにルートマップを適用します。

c) 適切な着信または発信**プレフィックスリスト**を入力または選択して、BGP ネイバー情報を配布します。

d) 適切な着信または発信 **AS パスフィルタ**を入力または選択して、BGP ネイバー情報を配布します。

e) [ネイバーから許可されるプレフィックスの数を制限する（Limit the number of prefixes allowed from the neighbor）] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。

- [最大プレフィックス数（Maximum Prefixes）] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
- [しきい値レベル（Threshold Level）] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。

f) [ピアから受信したプレフィックスの制御（Control prefixes received from the peer）] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。

- プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する（Terminate peering when prefix limit is exceeded）] チェックボックスをオンにします。[再起動間隔（Restart interval）] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
- 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する（Give only warning

message when prefix limit is exceeded）] チェックボックスをオンにします。この場合、BGP ネイバーは終了しません。

g) [OK] をクリックします。

ステップ 15 （オプション）[ルート（Routes）] で、その他のネイバールートパラメータを指定します。次を更新します。

a) [Advertisement Interval] フィールドに、BGP ルーティング アップデートが送信される最小間隔（秒）を入力します。有効な値は、1 ～ 600 です。

b) [発信ルーティング更新からプライベートAS番号を削除する（Remove private AS numbers from outbound routing updates）] チェックボックスをオンにして、プライベート AS 番号を発信ルートにおけるアドバタイズ対象から除外します。

c) [デフォルトルートの生成（Generate default routes）] チェックボックスをオンにして、ローカルルータにネイバーへのデフォルトルート 0.0.0.0 の送信を許可して、このルートがデフォルトルートとして使用されるようにします。[ルート マップ（Route map）] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを入力または選択します。

d) 条件に応じてアドバタイズされるルートを追加するには、[行を追加（Add Row）]（+）をクリックします。[アドバタイズ対象ルートの追加（Add Advertised Route）] ダイアログボックスで、次の手順を実行します。

1. [アドバタイズマップ（Advertise Map）] フィールドで、exist-map または非存在マップの条件が満たされた場合にアドバタイズされるルートマップを追加または選択します。
2. [存在マップ（Exist Map）] をクリックし、[ルートマップ オブジェクト セレクタ（Route Map Object Selector）] からルートマップを選択します。このルートマップは、アドバタイズマップルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
3. [非存在マップ（Non-Exist Map）] をクリックし、[ルートマップ オブジェクト セレクタ（Route Map Object Selector）] からルートマップを選択します。このルートマップは、アドバタイズマップルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
4. [OK] をクリックします。

ステップ 16 [タイマー（Timers）] で [BGP ピアのタイマーを設定する（Set timers for the BGP peer）] チェックボックスをオンにし、キープアライブ頻度、保留時間、最小保留時間を設定します

- [キープアライブインターバル（Keep alive interval）]：Firewall Threat Defense がキープアライブメッセージをネイバーに送信する頻度（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。
- [保留時間（Hold time）]：キープアライブメッセージを受信できない状態が継続し、ピアがデッドであると Firewall Threat Defense が宣言するまでの間隔（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 180 秒です。

- [最小保留時間（Min hold time）]：（オプション）キープアライブメッセージを受信できない状態が継続して、ピアがデッドであるとFirewall Threat Defenseが宣言するまでの最小間隔（秒）を入力します。有効な値は、3 ～ 65535 です。デフォルト値は 3 秒です。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 17 [詳細（Advanced）] で、次を更新します。

a) （オプション）[認証を有効にする（Enable Authentication）] チェックボックスをオンにして、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。

1. [暗号化を有効にする（Enable Encryption）] ドロップダウン リストから暗号化タイプを選択します。
2. パスワードを [パスワード（Password）] フィールドに入力します。[Confirm Password] フィールドにパスワードを再入力します。パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字まで指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注）
数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

b) （オプション）[このネイバーにコミュニティ属性を送信する（Send Community attribute to this neighbor）] チェックボックスをオンにして、コミュニティ属性を BGP ネイバーに送信することを指定します。

c) （オプション）[このネイバーのネクスト ホップとして FTD を使用する（Use FTD as next hop for this neighbor）] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

d) [接続の検証を無効にする（Disable Connection Verification）] チェックボックスをオンにして、シングルホップで到達可能な eBGP ピアリング セッションについての接続の検証プロセスを無効にします。これにより、ループバック インターフェイスで設定されたピアや直接接続されないIPアドレスが設定されたピアとの間でセッションを確立することができます。オフ（デフォルト）にすると、シングルホップ eBGP ピアリング セッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリング セッションは確立されません。

e) [直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）] を選択して、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。（オプション）[TTL ホップ（TTL hops）] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。または、[ネイバーへのTTLホップの制限数（Limited number of TTL hops to neighbor）] を選択して、BGP ピアリングセッションを保護します。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。

f) （オプション）[TCP MTU パス検出の使用（Use TCP MTU path discovery）] チェックボックスをオンにして、BGP セッションの TCP トランスポート セッションを有効にします。

g) [TCPトランスポートモード（TCP Transport Mode）] ドロップダウンリストから TCP 接続モードを選択します。オプションは [デフォルト（Default）]、[アクティブ（Active）]、または [パッシブ（Passive）] です。

h) （オプション）BGP ネイバー接続の**ウェイト**を入力します。

i) ドロップダウンリストから Firewall Threat Defense が受け入れる [BGP バージョン（BGP version）] を選択します。[4 のみ（4-Only）] に設定すると、指定されたネイバーとの間でバージョン 4 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 18 AS 移行を考慮する場合にのみ [移行（Migration）] を更新します。

（注）
AS 移行カスタマイズは、遷移の完了後に削除される必要があります。

a) （オプション）[ネイバーから受信したルータのAS番号をカスタマイズ（Customize the AS number for routes received from the neighbor）] チェックボックスをオンにし、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

b) [ローカル AS 番号（Local AS number）] フィールドにローカル自律システム番号を入力します。有効な値は、1 ～ 4294967295 または 1.0 ～ 65535.65535 の有効な自律システム番号です。

c) （オプション）[ローカルAS番号をネイバーから受信したルートの前に付加しない（Do not prepend local AS number to routes received from neighbor）] チェックボックスをオンにして、ローカル AS 番号が eBGP ピアから受信したルートの前に付加されないようにします。

d) （オプション）[実AS番号をネイバーから受信したルートのローカルAS番号に置き換える（Replace real AS number with local AS number in routes received from neighbor）] チェックボックスをオンにして、実自律システム番号を eBGP 更新のローカル自律システム番号に置き換えます。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。

e) （オプション）[実AS番号またはネイバーから受信したルートのローカルAS番号を受け入れる（Accept either real AS number or local AS number in routesreceived from neighbor）] チェックボックスをオンにして、実自律システム番号（ローカル BGP ルーティングプロセスより）またはローカル自律システム番号を使用するピアリングセッションを確立するように eBGP ネイバーを設定します。

ステップ 19 [OK] をクリックします。

ステップ 20 [保存（Save）] をクリックします。

BGP 集約アドレス設定の設定

BGP ネイバーはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約は、複数の異なるルートの属性を合成し、1 つのルートだけがアドバタイズされるようにするプロセスです。集約プレ

フィックスは、クラスレス ドメイン間ルーティング（CIDR）の原則を使用して、複数の隣接するネットワークを、ルーティング テーブルに要約できる IP アドレスのクラスレス セット 1 つに合成します。結果として、アドバタイズの必要なルートは少なくなります。[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

手順

ステップ 1 Firewall Threat Defense デバイスを編集する場合は、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [集約アドレスの追加（Add Aggregate Address）] をクリックします。

ステップ 5 [集約タイマー（Aggregate Timer）] フィールドで、集約タイマーの値（秒）を入力します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。

ステップ 6 （＋）[追加（Add）] をクリックして、[集約アドレスの追加（Add Aggregate Address）] ダイアログボックスを更新します。

a) [ネットワーク（Network）]：IPv4 アドレスを入力するか、任意のネットワーク/ホスト オブジェクトを選択します。

b) [集約マップ（Attribute Map）]：（オプション）集約ルートの属性の設定に使用されるルート マップを入力または選択します。

c) [アドバタイズマップ（Advertise Map）]：（オプション）AS 設定の元のコミュニティを作成するルートの選択に使用されるルート マップを入力または選択します。

d) [抑制マップ（Suppress Map）]：（オプション）抑制するルートの選択に使用されるルートマップを入力または選択します。

e) [AS設定パス情報の生成（Generate AS set path Information）]：（オプション）自律システム設定パス情報の生成を有効にするには、チェックボックスをオンにします。

f) [更新から全ルートをフィルタ処理（Filter all routes from updates）]：（オプション）更新からのすべての特定のルートをフィルタ処理するには、チェックボックスをオンにします。

g) [OK] をクリックします。

次のタスク

- BGPv4 設定については、BGPv4 フィルタリング設定 （1236 ページ）に進みます。
- BGPv6 設定については、BGP ネットワーク設定 （1236 ページ）に進みます。

BGPv4 フィルタリング設定

フィルタリング設定は、受信される BGP 更新プログラムのフィルタ処理ルートまたはネットワークに使用されます。フィルタリングは、ルータが学習またはアドバタイズするルーティング情報を制限するために使用されます。

始める前に

フィルタリングは、BGP の IPv4 ルーティング ポリシーでのみ適用されます。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** を選択します。

ステップ 4 [Filtering] をクリックします。

（注）
[フィルタリング（Filtering）] フィールドは、IPv4 設定にのみ適用されます。

ステップ 5 （＋）[追加（Add）] をクリックして、[フィルタの追加（Add Filter）] ダイアログボックスを更新します。

a) [アクセスリスト（Access List）] : 受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセス制御リストを選択します。
b) [指示（Direction）] : （オプション）インバウンド更新、アウトバウンド更新のどちらにフィルタを適用するかを指定する指示を選択します。
c) [プロトコル（Protocol）] : （オプション）なし、BGP、接続中、OSPF、RIP または静的のルーティングプロセスのうち、フィルタ処理するものを選択します。
d) [プロセス ID（Process ID）] : （オプション）OSPF ルーティング プロトコルのプロセス ID を入力します。
e) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

BGP ネットワーク設定

ネットワーク設定は、BGP ルーティングプロセスによってアドバタイズされるネットワーク、アドバタイズされるネットワークのフィルタ処理で確認されるルートマップを追加するために使用されます。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Networks] をクリックします。

ステップ 5 [追加（Add）] をクリックして、[ネットワークの追加（Add Networks）] ダイアログボックスを更新します。

a) [ネットワーク（Network）]：BGP ルーティングプロセスによってアドバタイズされるネットワークを選択します。

（注）
ネットワークプレフィックスをアドバタイズするには、デバイスへのルートがルーティングテーブルに存在する必要があります。

新しいネットワークオブジェクトを追加するには、ネットワーク オブジェクトの作成（1351 ページ）を参照してください。

b) （オプション）[ルートマップ（Route Map）]：アドバタイズされるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。新しいルートマップオブジェクトを追加するには、ルート マップ （1380 ページ）を参照してください。

c) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

BGP 再配布設定

再配布設定により、別のルーティング ドメインから BGP にルートを再配布する条件を定義できます。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Redistribution] をクリックします。

ステップ 5 [追加（Add）] をクリックして、[再配布の追加（Add Redistribution）] ダイアログを更新します。

a) [送信元プロトコル（Source Protocol）]：送信元プロトコル ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。

（注）
ユーザ定義の仮想ルータは、RIP からのトラフィックの再配布をサポートしていません。

b) [プロセス ID（Process ID）]：選択されている送信元プロトコルの識別子を入力します。OSPF プロトコルに適用されます。仮想ルーティングを使用しているデバイスの場合、このドロップダウンリストには、BGP 設定を設定する仮想ルータに割り当てられたプロセス ID が表示されます。

c) [メトリック（Metric）]：（オプション）再配布されているルートのメトリックを入力します。

d) [ルートマップ（Route Map）]：再配布されるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。新しいルートマップオブジェクトを作成するには、[追加（Add）]（＋）をクリックします。新しいルートマップを追加する手順については、「ルートマップエントリの設定」を参照してください。

e) [一致（Match）]：1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。

- 内線
- 外部 1
- 外部 2
- NSSA 外部 1
- NSSA 外部 2

f) [OK] をクリックします。

BGP ルート注入の設定

ルート注入設定により、条件に応じて BGP ルーティングテーブルに注入されるルートを定義できます。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Route Injection] をクリックします。

ステップ 5 [追加（Add）] をクリックして、[ルート注入の追加（Add Route Injection）] ダイアログボックスを更新します。

a) [マップ注入（Inject Map）]：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルートマップを入力または選択します。新しいルートマップオブジェクトを作成するには、[追加（Add）] (+) をクリックします。新しいルートマップを追加する手順については、「ルートマップエントリの設定」を参照してください。

b) [マップ存在（Exist Map）]：BGP スピーカーが追跡するプレフィックスを含むルート マップを入力または選択します。

c) [注入されたルートが集約ルートの属性を継承（Injected routes will inherit the attributes of the aggregate route）]：このチェックボックスをオンにして、集約ルートの属性を継承するよう注入されたルートを設定します。

d) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

BGP ルートのインポート/エクスポート設定の設定

BGP では、宛先仮想ルータと送信元仮想ルータの各ルートターゲット拡張コミュニティを使用してルートをインポートまたはエクスポートすることで、仮想ルータ間ルートリークを実装できます。ルーティングテーブル全体をリークする代わりに、ルートマップを使用して目的のルートターゲットをフィルタ処理できます。また、グローバル仮想ルータのルートをユーザ定義の仮想ルータにリークすることも、その逆も可能です。

- ルートターゲット拡張コミュニティを使用して、2 つのユーザ定義の仮想ルータ間でルートをリークするように BGP を設定できます。
  - ルートターゲットエクスポートを使用して、送信元仮想ルータからのルートターゲットでルートにタグを付けます。
  - ルートターゲットインポートを使用して、ルートターゲットに一致するルートを宛先仮想ルータにインポートします。
  - オプションで、エクスポートルートマップまたはインポートルートマップをそれぞれ使用して、送信元仮想ルータからのルート、または宛先仮想ルータへのルートをフィ

ルタ処理できます。ルートをフィルタリングするために、一致拡張コミュニティリストを使用してルートマップを設定できます。同様に、拡張コミュニティ ルート ターゲットを設定してルートマップを設定し、ルートターゲット拡張コミュニティにルートをタグ付けできます。

- グローバル仮想ルータからユーザ定義の仮想ルータにルートをインポートするには、[グローバル仮想ルータのインポートルートマップ（Global Virtual Router Import Route Map）] で IPv4/IPv6 ルートマップを指定して、ユーザ定義の仮想ルータにインポートします。
- ユーザ定義の仮想ルータからグローバル仮想ルータにルートをエクスポートするには、ルートターゲットのエクスポートに加えて、[グローバル仮想ルータのエクスポートルートマップ（Global Virtual Router Export Route Map）] を指定して、ユーザ定義の仮想ルータからエクスポートすることもできます。

BGP 仮想ルータ間ルートリークは、IPv4 と IPv6 の両方のプレフィックスをサポートします。

始める前に

- 仮想ルータを作成します。仮想ルータの作成 （1103 ページ）
- 仮想ルータ上で BGP を有効にします。BGP 基本設定 （1225 ページ）
- BGP の設定 （1224 ページ）。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 （仮想ルータでのみサポート）[ルートのインポート/エクスポート（Route Import/Export）] をクリックします。

ステップ 5 [ルートターゲットのインポート（Route Targets Import）] フィールドに、インポートするルートに一致するルートターゲット拡張コミュニティを入力します。展開時に、この値に一致する宛先仮想ルータのルートが送信元仮想ルータの BGP テーブルにインポートされます。

（注）
- ルートターゲットは ASN:nn 形式である必要があります。
- 複数のルートターゲットをカンマ区切り値として入力できます。
- この値の範囲は 0:1 ー 65534:65535 です。

ステップ 6 [ルートターゲットのエクスポート（Route Targets Export）] フィールドに、ルートターゲット拡張コミュニティを入力して、送信元仮想ルータのルートにルートターゲット値をタグ付けします。展開時に、送信元仮想ルータのルートはこの値でタグ付けされます。

（注）
- ルートターゲットは ASN:nn 形式である必要があります。
- 複数のルートターゲットをカンマ区切り値として入力できます。
- この値の範囲は 0:1 ー 65534:65535 です。

ステップ 7 ルートマップを使用すると、ルーティングテーブル全体をリークすることなく、共有するルートを絞り込めます。ルートマップフィルタリングは、指定されたルートターゲット値で取得されたルートのリストに適用されます。

a) （オプション）[ユーザ仮想ルータ（User Virtual Router）] で、[インポートルートマップ（Import Route Map）] ドロップダウンリストからルートマップを選択し、宛先仮想ルータでルートをフィルタ処理します。

（注）
ユーザ仮想ルータのインポートルートマップは、ルートターゲットのインポートが設定されている場合にのみ有効です。

b) （オプション）[ユーザー仮想ルータ（User Virtual Router）] で、[エクスポートルートマップ（Export Route Map）] ドロップダウンリストからルートマップを選択し、ルートが他の仮想ルータにエクスポートされる前に、送信元仮想ルータでルートをフィルタ処理します。

（注）
ルートマップの match 句と set 句をルートターゲット拡張コミュニティリストとともに使用して、他の基準に基づいてフィルタリングしたり、ルート ターゲット コミュニティ値でルートにタグ付けしたりできます。詳細については、ルートマップ（1380ページ）を参照してください。

ステップ 8 ユーザ定義の仮想ルータとグローバル仮想ルータの間でルートを共有するには、[グローバル仮想ルータ（Global Virtual Router）] でルートマップを指定します。

a) グローバル仮想ルータルートをユーザ定義の仮想ルータにリークするには、[インポートルートマップ（Import Route Map）] ドロップダウンリストからルートマップを選択します。IPv4 または IPv6 ルートマップがユーザ定義の仮想ルータにインポートされます。

b) ユーザ定義の仮想ルータルートをグローバル仮想ルータにリークするには、[エクスポートルートマップ（Export Route Map）] ドロップダウンリストからルートマップを選択します。IPv4 または IPv6 ルートマップがグローバル仮想ルータにエクスポートされます。

（注）
ルートマップの指定とは別に、エクスポートのルートターゲットを指定する必要があります。

（注）

ルートマップオブジェクトの match 句を使用して、リークのルートをフィルタ処理できます。詳細については、ルート マップ （1380 ページ）を参照してください。

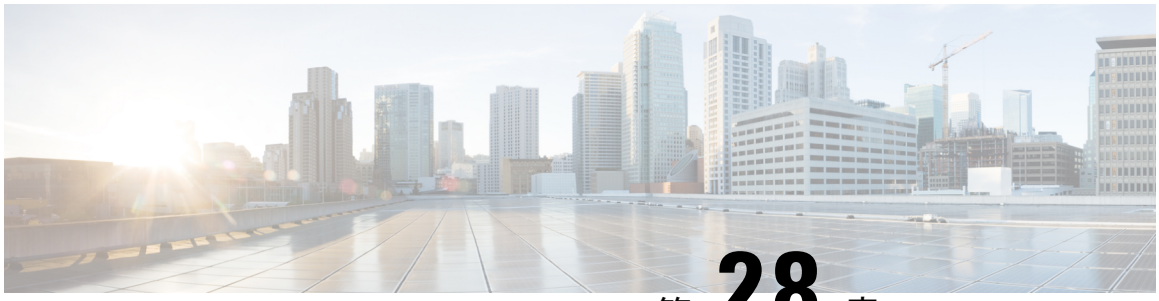
ステップ 9 手順（ステップ 3 ー 8）に従って、他の仮想ルータの関連する BGP ルートインポートおよびエクスポート設定も設定します。ステップ 3 （1240 ページ） ステップ 8 （1241 ページ）

ステップ 10 [保存して展開（Save and Deploy）] をクリックします。

パケットが入力仮想ルータに流れると、BGP は一致するルートターゲット値を持つ宛先仮想ルータからルートをインポートします。ルートマップも設定されている場合、ルートはさらにフィルタ処理され、パケットをルーティングするベストパスルートを特定するために使用されます。

BGP の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
仮想ルータを相互接続するための BGP 設定	7.1	任意（Any）	ユーザー定義の仮想ルータ間、およびグローバル仮想ルータとユーザー定義の仮想ルータ間でルートを動的にリークするように BGP 設定を構成できます。ルートのインポートおよびエクスポート機能が導入され、仮想ルータにルートターゲットのタグを付け、必要に応じて、一致したルートをルートマップでフィルタリングすることにより、仮想ルータ間でルートを交換します。この BGP 機能は、ユーザー定義の仮想ルータを選択した場合にのみ利用できます。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[BGPv4/v6]** > **[ルートのインポート/エクスポート（Route Import/Export）]** タブ。
ユーザー定義の仮想ルータでの BGPv6 サポート	7.1	任意（Any）	Secure Firewall Threat Defense は、ユーザー定義の仮想ルータでの BGPv6 の設定をサポートするようになりました。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[BGPv6]** ページ。



第 28 章

RIP

この章では、ルーティング情報プロトコル（RIP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するようにFirewall Threat Defenseを設定する方法について説明します。仮想ルーティングを使用しているデバイスの場合、ユーザ定義の仮想ルータではなく、グローバル仮想ルータに対してのみRIPを設定できます。

- RIP について （1243 ページ）
- RIP の要件と前提条件 （1245 ページ）
- RIP のガイドライン （1246 ページ）
- RIP の設定 （1246 ページ）

RIP について

RIPと呼ばれることが多いRouting Information Protocolは、すべてのルーティング プロトコルの中で最も堅牢なものの1つです。RIPには、ルーティング アップデート プロセス、RIPルーティング メトリック、ルーティング安定性、ルーティング タイマーの4つの基本的なコンポーネントがあります。RIPをサポートしているデバイスは、ルーティング アップデート メッセージを定期的に、またネットワーク トポロジが変更されたときに送信します。これらのRIPパケットには、デバイスが到達可能なネットワークに関する情報、さらに宛先アドレスに到達するためにパケットが通過しなければならないルータやゲートウェイの数が含まれています。RIPでは、生成されるトラフィックはOSPFより多くなりますが、設定はOSPFより容易です。

RIPは、ホップ カウントをパス選択のメトリックとして使用するディスタンス ベクター ルーティング プロトコルです。インターフェイス上でRIPが有効になっている場合、インターフェイスは、ネイバー デバイスとRIPブロードキャストを交換して、ルートの動的な学習およびアドバタイズを行います。

Secure Firewall Threat Defense デバイス は、RIP バージョン 1 と RIP バージョン 2 の両方をサポートしています。RIP バージョン 1 では、ルーティング アップデートでサブネットマスクは送信されません。RIP バージョン 2 では、ルーティング アップデートでサブネットマスクが送信され、可変長サブネット マスクがサポートされています。さらに、RIP バージョン 2 では、ルーティング アップデートを交換するときのネイバー認証がサポートされています。この認証により、信頼性の高い送信元から信頼できるルーティング情報が Secure Firewall Threat Defense デバイス で受信できるようになります。

RIP は、初期設定が簡単で、トポロジが変更されても設定を更新する必要がないため、スタティック ルーティングより有利です。RIP の欠点は、スタティック ルーティングよりネットワークや処理オーバーヘッドが大きいことです。

ルーティング アップデート プロセス

RIPは、ルーティングアップデートメッセージを定期的に送信するだけでなく、ネットワークトポロジが変更された場合にも送信します。ルータは、エントリの変更が含まれるルーティング アップデートを受け取ると、新しいルートを反映するようにそのルーティング テーブルを更新します。パスのメトリック値は1ずつ大きくなり、送信者はネクスト ホップとして示されます。RIP ルータは、宛先に対する最適なルート（メトリック値が最も小さいルート）だけを保持します。ルータは、そのルーティング テーブルを更新した後、他のネットワーク ルータに変更を通知するために、ルーティングアップデートの送信をただちに開始します。これらのアップデートは、RIP ルータが送信する定期的にスケジュールされたアップデートとは独立して送信されます。

RIP のルーティング メトリック

RIP は、1 つのルーティング メトリック（ホップ カウント）を使用して発信元と宛先ネットワークとの距離を測定します。発信元から宛先までのパスの各ホップにはホップ カウント値（通常は1）が割り当てられます。ルータが、新しいまたは変更された宛先ネットワーク エントリが含まれるルーティングアップデートを受け取ると、アップデートで示されたメトリック値に 1 を加算し、そのネットワークをルーティング テーブルに入れます。送信者の IP アドレスがネクスト ホップとして使用されます。

RIP 安定性機能

RIP は、送信元から宛先へのパスで許可されるホップ数に制限を導入することにより、ルーティング ループが無限に続くことを防止しています。パス内のホップの最大数は 15 です。新しいまたは変更されたエントリが含まれるルーティングアップデートをルータが受信し、メトリック値に1を加えた結果、メトリックが無限（つまり16）になる場合は、ネットワークの宛先は到達不能と見なされます。この安定性機能の欠点は、この機能によってRIPネットワークの直径の最大値が 16 ホップ未満に制限されることです。

RIPには、その他にも、多くのルーティングプロトコルに共通の安定性機能がいくつか含まれます。ネットワークトポロジは急激に変化する可能性がありますが、これらの機能は、安定性を提供するように設計されています。たとえば、RIPでは、スプリットホライズンとホールドダウン メカニズムを実装して、間違ったルーティング情報が伝搬されることを防止しています。

RIP タイマー

RIP では、多数のタイマーを使用してそのパフォーマンスを調整しています。RIP のタイマーステージは次のとおりです。

- 更新：ルーティングアップデートタイマーは、定期的なルーティングアップデートの間隔を測ります。これは、デバイスがルーティングアップデートを送信する頻度です。通常は30秒に設定されており、タイマーがリセットされたときにはランダムな時間がわずかに追加されます。これは、すべてのルータがそのネイバーを同時にアップデートしようとした結果発生する輻輳を防ぐためです。
- 無効：ルーティングテーブルの各エントリには、ルートタイムアウトタイマーが関連付けられています。これは、デバイスが最後の有効な更新を受信してからの秒数です。ルートタイムアウトタイマーが期限切れになると、ルートには無効のマークが付きますが、ルートフラッシュタイマーが期限切れになるまではテーブル内に保持されます。このタイマーが期限切れになると、ルートはホールドダウン状態になります。デフォルト値は180秒（3分）です。
- ホールドダウン：ホールドダウン期間は、ホールドダウン状態のルート（つまり、無効とマークされたルート）の新しい更新を受け入れる前にシステムが待機する秒数です。デフォルト値は 180 秒（3 分）です。
- フラッシュ：ルートフラッシュタイマーは、システムが最後の有効な更新を受信してから、ルートが破棄されてルーティングテーブルから削除されるまでの秒数です。デフォルトは 240 秒（4 分）です。

たとえば、隣接ルータのインターフェイスがダウンすると、システムは隣接ルータからルーティングアップデートを受信しなくなります。この時点で、無効タイマーとフラッシュタイマーが増加し始めます。最初の 180 秒間は何も起こりません。180 秒後、無効タイマーが期限切れになり、ルートが無効になりますが、ホールドダウンタイマーが開始され、ルートはさらに 60 秒間保持されます。隣接ルータのインターフェイスステータスに関する更新がまだない場合（つまり、まだダウンしている場合）、ルートはフラッシュ状態になり、システムは最後の更新から合計 240 秒（無効タイマーの 180 秒とホールドダウンタイマーの 60 秒）待機してから、ルートをフラッシュします。隣接ルータインターフェイスがすぐに起動しても、ホールドダウンタイマーが残りの120秒を完了するまで、システムはルーティングアップデートを受け入れません。

RIP の要件と前提条件

モデルのサポート

Threat Defense

Firewall Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

RIP のガイドライン

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 アップデートをそのインターフェイスに提供するすべてのネイバーデバイス上で同じにする必要があります。
- RIP バージョン 2 の場合、Secure Firewall Threat Defense デバイス は、マルチキャスト アドレス 224.0.0.9 を使用してデフォルト ルート アップデートを送受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイス上で設定されると、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上で登録されます。RIP バージョン 2 設定がインターフェイスから削除されると、そのマルチキャスト アドレスの登録は解除されます。

制限事項

- RIP アップデートは、Secure Firewall Threat Defense デバイス のインターフェイス間を通過できません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。
- Secure Firewall Threat Defense デバイス では、RIP プロセスを 1 つだけイネーブルにできます。

RIP の設定

RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル ルーティング プロトコルです。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] を選択します。

ステップ 3 コンテンツ テーブルから [RIP] を選択します。

ステップ 4 [RIPを有効にする（Enable RIP）] チェックボックスをオンにして、RIP を設定します。

ステップ 5 [RIPバージョン（RIP Version）] ドロップダウンリストから、RIP の更新を送受信するための RIP バージョンを選択します。

ステップ 6 （オプション）[デフォルトルートの生成（Generate Default Route）] チェックボックスをオンにして、指定したルートマップに基づく配布用のデフォルトルートを生成します。

a) [ルート マップ（Route map）] フィールドで、デフォルト ルートの生成に使用するルート マップ名を指定します。
[ルート マップ（Route map）] フィールドで指定したルート マップが存在する場合、特定のインターフェイスで配布されるデフォルト ルート 0.0.0.0/0 が生成されます。

ステップ 7 [RIP バージョン（RIP Version）] として [バージョン 2 の送受信（Send and Receive Version 2）] を選択した場合、[自動集約の有効化（Enable Auto Summary）] オプションが使用可能になります。[自動集約の有効化（Enable Auto Summary）] チェックボックスをオンにすると、自動ルート集約が有効になります。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズをディセーブルにします。自動サマライズをディセーブルにすると、サブネットがアドバタイズされます。

（注）
RIP バージョン 1 では、常に自動サマライズが使用されます。無効にすることはできません。

ステップ 8 [Networks] をクリックします。RIP ルーティングに対して 1 つ以上のネットワークを定義します。IP アドレスを入力するか、目的のネットワーク/ホスト オブジェクトを入力または選択します。セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。このコマンドで定義されるネットワークに属しているインターフェイスは、RIP ルーティング プロセスに参加します。RIP ルーティング更新は、指定したネットワークのインターフェイスだけを介して送受信されます。また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP 更新でアドバタイズされません。

（注）
RIP では、IPv4 オブジェクトのみがサポートされます。

ステップ 9 （オプション）[パッシブインターフェイス（Passive Interfaces）] をクリックします。このオプションを使用して、アプライアンスでパッシブ インターフェイスを指定してから、アクティブ インターフェイスを指定します。デバイスは、そのルーティング テーブルを入力するための情報を使用して、パッシブ インターフェイスでの RIP ルートのブロードキャストをリッスンしますが、パッシブ インターフェイスでのルーティング更新はブロードキャストしません。パッシブとして指定されていないインターフェイスは、更新を送受信します。

ステップ 10 [再配布（Redistribution）] をクリックして、再配布ルートを管理します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。

a) [追加（Add）] をクリックして、再配布ルートを指定します。

b) [プロトコル（Protocol）] ドロップダウンリストから、RIP ルーティングプロセスに再配布するルーティングプロトコルを選択します。

（注）
OSPF プロトコルの場合は、プロセス ID を指定します。同様に、BGP の場合は AS パスとして指定します。[プロトコル（Protocol）] ドロップダウン リストで [接続済み（Connected）] オプションを選択すると、直接接続されたネットワークを RIP ルーティング プロセスに再配布できます。

c) （オプション）OSPF ルートを RIP ルーティング プロセスに再配布する場合、[一致（Match）] ドロップダウン リストで、再配布する特定のタイプの OSPF ルートを選択できます。複数のタイプを選択するには、Ctrl を押しながらクリックします。

- [内部（Internal）]：自律システム（AS）に対して内部のルートが再配布されます。
- [外部1（External 1）]：AS に対して外部のタイプ 1 ルートが再配布されます。
- [外部2（External 2）]：AS に対して外部のタイプ 2 ルートが再配布されます。
- [NSSA外部1（NSSA External 1）]：Not-So-Stubby Area（NSSA）の外部のタイプ 1 ルートが再配布されます。
- [NSSA外部2（NSSA External 2）]：NSSA の外部のタイプ 2 ルートが再配布されます。

（注）
デフォルトの一致は、[内部（Internal）]、[外部 1（External 1）]、および [外部 2（External 2）] です。

d) [メトリック（Metric）] ドロップダウン リストから、再配布されたルートに適用する RIP メトリック タイプを選択します。選択肢は次の 2 つです。

- [トランスペアレント（Transparent）]：現在のルートメトリックを使用します。
- [指定値（Specified Value）]：特定のメトリック値を割り当てます。[メトリック値（Metric Value）] フィールドに 0 ～ 16 の特定の値を入力します。
- [なし（None）]：メトリックが指定されません。再配布されたルートに適用するメトリック値を使用しないでください。

（注）
[なし（None）] オプションは、静的プロトコルと接続済みプロトコルにのみ適用されます。

e) （オプション）[ルート マップ（Route Map）] フィールドに、ルートが RIP ルーティング プロセスに再配布される前に満たす必要のあるルートマップの名前を指定します。ルートは、IP アドレスがルートマップ アドレス リストの許可文と一致する場合にのみ再配布さ

れます。新しいルートマップオブジェクトを作成するには、[追加（Add）] (+) をクリックします。新しいルートマップを追加する手順については、「ルートマップエントリの設定」を参照してください。

f) [OK] をクリックします。

ステップ 11 （オプション）[フィルタリング（Filtering）] をクリックして、RIP ポリシーのフィルタを管理します。このセクションでは、インターフェイスでのルーティング更新の回避、ルーティング更新でのルートのアドバタイズ制御、ルーティング更新の処理制御、およびルーティング更新の送信元フィルタリングに、フィルタを使用します。

a) [追加（Add）] をクリックして、RIP フィルタを追加します。

b) [トラフィックの方向（Traffic Direction）] フィールドでフィルタリングされるトラフィックのタイプ（[着信（Inbound）] または [発信（Outbound）]）を選択します。

（注）
トラフィックの方向が着信の場合、インターフェイス フィルタだけを定義できます。

c) [フィルタオン（Filter On）] フィールドで適切な項目を選択して、フィルタがインターフェイスまたはルートのいずれに基づくかを指定します。[インターフェイス（Interface）] をクリックした場合、ルーティング更新がフィルタリングされるインターフェイスの名前を入力または選択します。[ルート（Route）] をクリックした場合、ルートタイプを選択します。

- [スタティック（Static）]：スタティックルートだけがフィルタリングされます。
- [接続済み（Connected）]：接続されたルートだけがフィルタリングされます。
- [OSPF]：指定した OSPF プロセスによって検出された OSPFv2 ルートだけがフィルタリングされます。フィルタリングされる OSPF プロセスの [プロセス ID（Process ID）] を入力します。
- [BGP]：指定した BGP プロセスによって検出された BGPv4 ルートだけがフィルタリングされます。フィルタリングされる BGP プロセスの AS パスを入力します。

d) [アクセスリスト（Access List）] フィールドで、許可されるネットワークまたは RIP ルートアドバタイズメントから削除されるネットワークを定義する 1 つ以上のアクセスコントロールリスト（ACL）の名前を入力または選択します。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）] (+) をクリックし、標準 ACL オブジェクトの設定 （1322 ページ）を参照してください。

e) [OK] をクリックします。

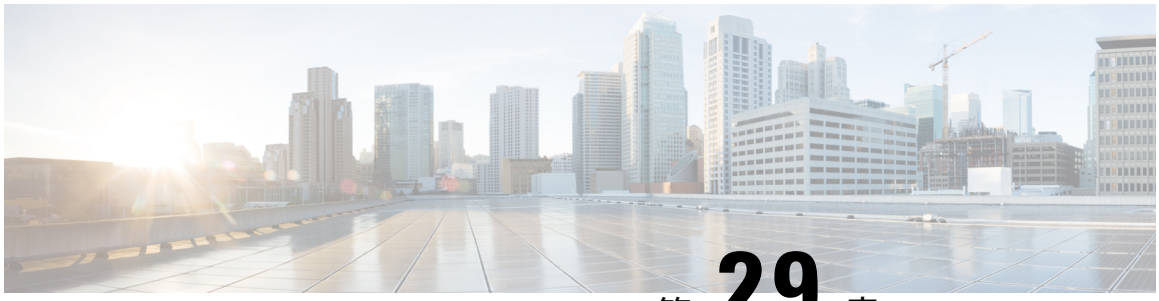
ステップ 12 （オプション）[ブロードキャスト（Broadcast）] をクリックして、インターフェイス設定を追加または編集します。[ブロードキャスト（Broadcast）] を使用して、インターフェイスごとに送受信するグローバル RIP バージョンをオーバーライドできます。また、有効な RIP アップデートを確認するための認証を実装する場合は、インターフェイスごとの認証パラメータを定義できます。

a) [追加（Add）] をクリックして、インターフェイス設定を追加します。

b) [インターフェイス（Interface）]フィールドで、このアプライアンスで定義されるインターフェイスを入力または選択します。
c) [送信（Send）]オプションで、該当するボックスを選択して、RIP バージョン1、バージョン 2、または両方を使用して更新を送信するように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな送信バージョンをオーバーライドできます。
d) [受信（Receive）] オプションで、該当するボックスを選択して、RIP バージョン 1、バージョン 2、または両方を使用して更新を受け入れるように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな受信バージョンをオーバーライドできます。
e) RIP ブロードキャストに対してこのインターフェイスで使用される**認証**を選択します。
   - [なし（None）]：認証はありません。
   - [MD5]：MD5 を使用します。
   - [クリアテキスト（Clear Text）]：クリアテキスト認証を使用します。

   [MD5] または [クリア テキスト（Clear Text）] を選択した場合、次の認証パラメータも指定する必要があります。
   - [キー ID（Key ID）]：認証キーの ID。有効な値は 0 ～ 255 です。
   - [キー（Key）]：選択した認証方式で使用されるキー。最大 16 文字まで使用できます
   - [確認（Confirm）]：確認のために、認証キーを再度入力します。

f) **[OK]** をクリックします。



第 29 章

マルチキャスト

この章では、マルチキャスト ルーティング プロトコルを使用するように Secure Firewall Threat Defense デバイス を設定する方法について説明します。

- マルチキャスト ルーティングについて （1251 ページ）
- マルチキャストルーティングの要件と前提条件 （1256 ページ）
- マルチキャスト ルーティングのガイドライン （1256 ページ）
- IGMP 機能の設定 （1258 ページ）
- PIM 機能の設定 （1264 ページ）
- マルチキャスト ルートの設定 （1272 ページ）
- マルチキャスト境界フィルタの設定 （1273 ページ）

マルチキャスト ルーティングについて

マルチキャストルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャストルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャスト ルーティング プロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、送信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャスト パケットは、Protocol Independent Multicast（PIM）やサポートする他のマルチキャスト プロトコルを使用した Firewall Threat Defense デバイス によりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

Firewall Threat Defense デバイス は、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つの Firewall Threat Defense デバイス に両方を同時に設定することはできません。

（注） マルチキャスト ルーティングでは、UDP トランスポートおよび非 UDP トランスポートの両方がサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

IGMP プロトコル

IP ホストは、Internet Group Management Protocol（IGMP）を使用して、そのグループ メンバーシップを、直接接続されているマルチキャスト ルータに報告します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージをリッスンし、定期的にクエリを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP は、グループ アドレス（クラス D IP アドレス）をグループ識別子として使用します。ホスト グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の範囲で使用できます。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

（注） Firewall Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、IGMP バージョン 2 がすべてのインターフェイスで自動的に有効になります。

マルチキャスト グループへのクエリ メッセージ

Firewall Threat Defense デバイスは、クエリ メッセージを送信して、インターフェイスに接続されているネットワークにメンバーを持つマルチキャスト グループを検出します。メンバーは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリ メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、Firewall Threat Defense デバイスに保存されているメンバーシップ情報が更新されます。Firewall Threat Defense デバイスで、ローカル メンバーがいなくなったマルチキャスト グループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャスト パケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニング メッセージを戻します。

デフォルトでは、サブネット上の PIM 代表ルータがクエリ メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。

クエリ応答時間を変更する場合は、IGMP クエリでアドバタイズする最大クエリ応答所要時間はデフォルトで 10 秒になります。Firewall Threat Defense デバイスがこの時間内にホスト クエリの応答を受信しなかった場合、グループを削除します。

スタブ マルチキャスト ルーティング

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、Firewall Threat Defense デバイス は IGMP のプロキシ エージェントとして動作します。Firewall

Threat Defense デバイス は、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、Firewall Threat Defense デバイス を PIM スパース モードまたは双方向モード用に設定できません。IGMP スタブ マルチキャスト ルーティングに参加するインターフェイス上で PIM を有効にする必要があります。

Firewall Threat Defense デバイス は、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイント（RP）をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

PIM マルチキャスト ルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する指定フォワーダ（DF）選択プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイント（RP）に転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF の選択は RP の検出中に行われ、これによってデフォルト ルートが RP に提供されます。

（注） Firewall Threat Defense デバイスが PIM RP の場合は、Firewall Threat Defense デバイスの変換されていない外部アドレスを RP アドレスとして使用してください。

PIM Source Specific Multicast のサポート

Firewall Threat Defense デバイスは PIM Source Specific Multicast（SSM）の機能や関連設定をサポートしていません。ただし、Firewall Threat Defense デバイスは最終ホップ ルータとして配置されていない限り、SSM 関連のパケットの通過を許可します。

SSM は、IPTV などの 1 対多のアプリケーションのデータ送信メカニズムとして分類されます。SSM モデルは、（S、G）ペアで示される「チャネル」の概念を使用します。S は発信元アドレス、G は SSM 宛先アドレスです。チャネルに登録するには、IGMPv3 などのグループ管理プロトコルを使用して行います。SSM は、特定のマルチキャスト送信元について学習した後、受信側のクライアントを有効にします。これにより、共有ランデブー ポイント（RP）からではなく、直接送信元からマルチキャスト ストリームを受信できるようになります。アクセス制御メカニズムは SSM 内に導入され、現在のスパースまたはスパース - デンス モードの実装では提供されないセキュリティ拡張機能を提供します。

PIM-SSM は、RP または共有ツリーを使用しない点で PIM-SM とは異なります。代わりに、マルチキャスト グループの発信元アドレスの情報は、ローカル受信プロトコル（IGMPv3）経由で受信者から提供され、送信元固有のツリーを直接作成するために使用されます。

マルチキャスト双方向 PIM

マルチキャスト双方向 PIM は、ビデオ会議、Webex ミーティング、およびグループチャットなどのように、同時に通信を行う送信元と受信者が多く存在し、各参加者がマルチキャスト トラフィックの送信元、受信者のどちらにもなりうるネットワークで有効です。PIM 双方向モードを使用すると、RP は共有ツリーの（*,G）エントリのみを作成します。（S,G）エントリはありません。各（S,G）エントリの状態テーブルを維持しないので、RP のリソースの節約になります。

PIM スパース モードでは、トラフィックは共有ツリーを下りにのみ流れます。PIM 双方向モードでは、トラフィックは共有ツリーの上りと下りの双方向に流れます。

PIM 双方向モードでは、PIM 登録/登録停止メカニズムを使って RP に送信元の登録をしません。送信元はそれぞれ、いつでもソースへの送信を開始できます。マルチキャスト パケットが RP に到達すると、共有ツリーで下りに転送されるか（受信者がいる場合）、ドロップされます（受信者がいない場合）。ただし、RP から送信元に対してマルチキャスト トラフィックの送信停止を命令する方法はありません。

設計の観点から、ネットワークのどこに RP を配置するかを考える必要があります。ネットワーク内の送信元と受信者の中間のどこかに配置する必要があるからです。

PIM 双方向モードには、リバース パス フォワーディング（RPF）のチェックがありません。ループを回避するため、代わりに代表フォワーダ（DF）の概念を使用します。この DF は、セグメント内で唯一、RP にマルチキャスト トラフィックの送信を許可されたルータです。マルチキャスト トラフィックを転送するルータがセグメントあたり 1 台だけであれば、ループは発生しません。DF は次のメカニズムを使って選択されます。

- RP へのメトリックが最も小さいルータが DF になる。
- メトリックが等しい場合は、IP アドレスが最も大きいルータが DF になる。

PIM ブートストラップ ルータ（BSR）

PIM ブートストラップ ルータ（BSR）は、RP 機能およびグループの RP 情報をリレーするために候補のルータを使用する動的ランデブーポイント（RP）セレクション モデルです。RP 機能には RP の検出が含まれており、RP にデフォルト ルートを提供します。これは、一連のデバイスを BSR の選択プロセスに参加する候補の BSR（C-BSR）として設定し、その中から BSR を選択することで実現します。BSR が選択されると、候補のランデブー ポイント（C-RP）として設定されたデバイスは、選定された BSR にグループ マッピングの送信を開始します。次に、BSR はホップ単位で PIM ルータ間を移動する BSR メッセージ経由で、マルチキャスト ツリーに至る他のすべてのデバイスにグループ/RP マッピング情報を配布します。

この機能は、RP を動的に学習する方法を提供するため、RP が停止と起動を繰り返す複雑で大規模なネットワークには不可欠です。

PIM ブートストラップ ルータ（BSR）の用語

PIM BSR の設定では、次の用語がよく使用されます。

- ブートストラップ ルータ（BSR）：BSR はホップバイホップ ベースの PIM が設定された他のルータに、ランデブー ポイント（RP）情報をアドバタイズします。選択プロセスの後に、複数の候補 BSR の中から 1 つの BSR が選択されます。このブートストラップ ルータの主な目的は、すべての候補 RP（C-RP）通知を RP-set というデータベースに収集し、これをネットワーク内の他のすべてのルータに定期的に BSR メッセージとして送信することです（60 秒ごと）。
- ブートストラップ ルータ（BSR）メッセージ：BSR メッセージは、TTL が 1 に設定された All-PIM-Routers グループへのマルチキャストです。これらのメッセージを受信するすべての PIM ネイバーは、メッセージを受信したインターフェイスを除くすべてのインターフェイスからそのメッセージを再送信します（TTL は 1 に設定）。BSR メッセージには、現在アクティブな BSR の RP-set と IP アドレスが含まれています。この方法で、C-RP は C-RP メッセージのユニキャスト先を認識します。
- 候補ブートストラップ ルータ（C-BSR）：候補 BSR として設定されるデバイスは、BSR 選択メカニズムに参加します。最も優先順位の高い C-BSR が BSR として選択されます。C-BSR の最上位の IP アドレスはタイブレイカーとして使用されます。BSR の選択プロセスはプリエンプティブです。たとえば、より優先順位の高い C-BSR が新たに見つかると、新しい選択プロセスがトリガーされます。
- 候補ランデブーポイント（C-RP）：RP はマルチキャストデータの送信元と受信者が対面する場所として機能します。C-RP として設定されているデバイスは、マルチキャスト グループ マッピング情報を、ユニキャスト経由で直接、選択された BSR に定期的にアドバタイズします。これらのメッセージには、グループ範囲、C-RP アドレス、および保留時間が含まれています。現在の BSR の IP アドレスは、ネットワーク内のすべてのルータが受信した定期的な BSR メッセージから学習されます。このようにして、BSR は現在動作中で到達可能な RP 候補について学習します。

（注） C-RP は BSR トラフィックの必須要件ですが、Firewall Threat Defense デバイス は C-RP としては機能しません。ルータのみが C-RP として機能できます。したがって、BSR のテスト機能では、トポロジにルータを追加する必要があります。

- BSR 選択メカニズム：各 C-BSR は、BSR 優先順位フィールドを含むブートストラップ メッセージ（BSM）を生成します。ドメイン内のルータは、ドメイン全体に BSM をフラッディングします。自身より優先順位の高い C-BSR に関する情報を受け取った BSR は、一定期間、BSM の送信を抑止します。残った単一の C-BSR が選択された BSR となり、その BSM により、選択された BSR に関する通知がドメイン内の他のすべてのルータに対して送信されます。

マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータ ストリームを受信することに関心があります。このグループには物理的または地理的な境界

がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMPを使用してグループに加入する必要があります。ホストがデータ ストリームを受信するには、グループのメンバでなければなりません。

マルチキャスト アドレス

マルチキャストアドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

クラスタ

マルチキャストルーティングは、クラスタリングをサポートします。スパンドEtherChannelクラスタリングでは、ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを送信します。ファーストパス転送が確立されると、データユニットがマルチキャストデータ パケットを転送できます。すべてのデータ フローは、フル フローです。スタブ転送フローもサポートされます。スパンドEtherChannelクラスタリングでは 1 つのユニットだけがマルチキャストパケットを受信するため、制御ユニットへのリダイレクションは共通です。

マルチキャストルーティングの要件と前提条件

モデルのサポート

Threat Defense

Firewall Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

マルチキャスト ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6

IPv6 はサポートされません。

マルチキャスト グループ

224.0.0.0 ー 224.0.0.255 のアドレス範囲は、ルーティングプロトコル、およびゲートウェイディスカバリやグループ メンバーシップ レポートなどのその他のトポロジディスカバリまたはメンテナンスプロトコルを使用するために予約されています。したがって、アドレス範囲224.0.0/24からのインターネット マルチキャスト ルーティングはサポートされません。予約されたアドレスのマルチキャストルーティングを有効にすると、IGMP グループは作成されません。

クラスタリング

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

その他のガイドライン

- 224.1.2.3 などのマルチキャスト ホストへのトラフィックを許可するには、インバウンド セキュリティ ゾーン上のアクセス制御またはプレフィルタ ルールを設定する必要があります。ただし、ルールの宛先セキュリティゾーンを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。
- PIM が設定されているインターフェイスは無効にできません。インターフェイスで PIM を設定している場合（PIMプロトコルの設定（1264ページ）を参照）、マルチキャストルーティングと PIM を無効にしても PIM 設定は削除されません。インターフェイスを無効にするには、PIM 設定を削除する必要があります。
- PIM/IGMP マルチキャストルーティングは、トラフィックゾーン内のインターフェイスではサポートされません。
- Firewall Threat Defense を同時にランデブーポイント（RP）とファーストホップルータになるように設定しないでください。
- HSRP スタンバイ IP アドレスは、PIM ネイバーシップに参加しません。したがって、RP ルータ IP が HSRP スタンバイ IP アドレスを介してルーティングされる場合、マルチキャストルーティングはFirewall Threat Defenseで機能しません。マルチキャストトラフィックが正常に通過するようにするには、RP アドレスのルートが HSRP スタンバイ IP アドレスではないことを確認し、代わりに、ルートアドレスをインターフェイス IP アドレスに設定します。
- 仮想ルーティングを使用しているデバイスの場合、ユーザ定義の仮想ルータではなく、グローバル仮想ルータに対してのみマルチキャストを設定できます。

IGMP 機能の設定

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージをリッスンし、定期的にクエリを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

手順

ステップ 1 マルチキャスト ルーティングの有効化 （1258 ページ）。
ステップ 2 IGMP プロトコルの設定 （1259 ページ）。
ステップ 3 IGMP アクセスグループの設定 （1261 ページ）。
ステップ 4 IGMP スタティック グループの設定 （1262 ページ）。
ステップ 5 IGMP 参加グループの設定 （1263 ページ）。

マルチキャスト ルーティングの有効化

Firewall Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、デフォルトですべてのインターフェイス上の IGMP と PIM が有効になります。IGMP は、直接接続されているサブネット上にグループのメンバーが存在するかどうか学習するために使用されます。ホストは、IGMP レポート メッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

（注） マルチキャスト ルーティングでは、UDP トランスポート層だけがサポートされています。

以下の一覧に、特定のマルチキャストテーブルに追加されるエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

- MFIB：30,000
- IGMP グループ：30,000
- PIM ルート：72,000

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 Choose **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [IGMP]** を選択します。

ステップ 3 [マルチキャスト ルーティングの有効化（Enable Multicast Routing）] チェックボックスをオンにします。

このチェックボックスをオンにすると、デバイス上で IP マルチキャストルーティングが有効になります。このチェックボックスをオフにすると、IP マルチキャスト ルーティングが無効になります。デフォルトでは、マルチキャストは無効になっています。マルチキャスト ルーティングを有効にすると、すべてのインターフェイス上でマルチキャストが有効になります。

マルチキャストはインターフェイスごとに無効にできます。この情報が役に立つのは、あるインターフェイス上にマルチキャスト ホストがないことがわかっている場合に、そのインターフェイス上で Firewall Threat Defense デバイスからホスト クエリ メッセージが送信されないように設定するときです。

IGMP プロトコルの設定

転送インターフェイス、クエリ メッセージ、時間間隔などのインターフェイスごとに、IGMP パラメータを設定できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [IGMP]** を選択します。

ステップ 3 [Protocol] で、[Add] または [Edit] をクリックします。

[IGMP パラメータの追加（Add IGMP parameters）] ダイアログボックスで、Firewall Threat Defense デバイスに新しい IGMP パラメータを追加します。既存のパラメータを変更する場合は、[IGMP パラメータの編集（Edit IGMP parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウンリストから、IGMP プロトコルを設定するインターフェイスを選択します。

- [IGMP を有効にする（Enable IGMP）]：IGMP を有効にするには、このチェックボックスをオンにします。

  （注）
  特定のインターフェイスでIGMPを無効にすることは、あるインターフェイス上にマルチキャストホストがないことがわかっている場合に、そのインターフェイス上でデバイスがホストクエリーメッセージを送信しないように設定するときに役に立ちます。

- [インターフェイスの転送（Forward Interface）]：ドロップダウンリストから、どのインターフェイスから IGMP メッセージを送信するかを選択します。

  これは Secure Firewall Threat Defense デバイスを、IGMP プロキシ エージェントとして設定し、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送します。

- [バージョン（Version）]：IGMP バージョン 1 または 2 を選択します。

  デフォルトでは、Firewall Threat Defense デバイスで IGMP バージョン 2 が実行されるため、多数の追加機能が使用できるようになります。

  （注）
  サブネットのマルチキャストルータはすべて、同じIGMPバージョンをサポートしている必要があります。Firewall Threat Defense デバイスが自動的にバージョン 1 ルータを検出してバージョン 1 に切り替えることはありません。ただ、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストを混在させることも可能です。IGMP バージョン 2 を実行している Firewall Threat Defense デバイスは、IGMP バージョン 1 のホストが存在しても正常に動作します。

- [クエリー インターバル（Query Interval）]：指定したルータから IGMP ホストクエリー メッセージが送信される秒単位の時間間隔。指定できる範囲は 1 ～ 3600 です。デフォルトは 125 です。

  （注）
  指定されたタイムアウト値の時間が経過しても、Firewall Threat Defense デバイスがインターフェイス上でクエリーメッセージを検出できなかった場合は、そのデバイスが指定ルータになり、クエリーメッセージの送信を開始します。

- [応答時間（Response Time）]：Firewall Threat Defense デバイスでグループが削除される前の秒単位の時間間隔。指定できる範囲は 1 ～ 25 です。デフォルトは 10 です。

  Firewall Threat Defenseデバイスがこの時間内にホストクエリーの応答を受信しなかった場合、グループを削除します。

- [グループ制限（Group Limit）]：インターフェイス上で加入する最大ホスト数。指定できる範囲は 1 ～ 500 です。デフォルトは 500 です。

  IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告はIGMPキャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

- [クエリータイムアウト（Query Timeout）]：秒単位の時間で、前のリクエスタがリクエスタとしての動作を停止してからこの時間が経過すると、この Firewall Threat Defense デバイスがそのインターフェイスのリクエスタの役割を引き継ぎます。指定できる範囲は 60 ～ 300 です。デフォルトは 255 です。

ステップ 5 [OK] をクリックして、IGMP プロトコル構成を保存します。

IGMP アクセスグループの設定

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

手順

ステップ 1 **[デバイス（Devices）]>[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）]>[マルチキャストルーティング（Multicast Routing）]>[アクセスグループ（Access Group）] を選択します。 > >

ステップ 3 [アクセスグループ（Access Group）] で、[追加（Add）] または [編集（Edit）] をクリックします。

[IGMP アクセス グループ パラメータを追加（Add IGMP Access Group parameters）] ダイアログボックスを使用して、新しい IGMP アクセスグループをアクセスグループ テーブルに追加します。既存のパラメータを変更する場合は、[IGMP アクセス グループ パラメータを編集（Edit IGMP Access Group parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

a) [インターフェイス（Interface）] ドロップダウンリストから、アクセスグループが関連付けられるインターフェイスを選択します。既存のアクセス グループを編集しているときは、関連インターフェイスは変更できません。

b) 次のいずれかをクリックします。

- [標準アクセスリスト（Standard Access List）]：[標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋) をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定 （1322 ページ）を参照してください。
- [拡張アクセスリスト（Extended Access List）]：[拡張アクセスリスト（Extended Access List）] ドロップダウンリストから、拡張 ACL を選択するか、または [追加（Add）] (＋) をクリックして新しい拡張 ACL を作成します。手順については、拡張 ACL オブジェクトの設定 （1320 ページ）を参照してください。

ステップ 5 [OK] をクリックして、アクセスグループ構成を保存します。

IGMP スタティック グループの設定

グループ メンバーがグループのメンバーシップをレポートできなかったり、ネットワーク セグメントにグループのメンバーが存在しない場合でも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信しなければならないことがあります。そのようなグループのマルチキャスト トラフィックをそのセグメントに送信するには、スタティック加入した IGMP グループを設定します。この方法の場合、Firewall Threat Defense デバイスはパケットそのものを受信せず、転送だけを実行します。そのため、スイッチングが高速に実施されます。発信インターフェイスは IGMP キャッシュ内に存在しますが、このインターフェイスはマルチキャスト グループのメンバーではありません。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [IGMP]** を選択します。

ステップ 3 [スタティックグループ（Static Group）] で、[追加（Add）] または [編集（Edit）] をクリックします。

インターフェイスに対してマルチキャストグループをスタティックに割り当てる場合は、[IGMP スタティック グループ パラメータの追加（Add IGMP Static Group parameters）] ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更する場合は、[IGMP スタティック グループ パラメータの編集（Edit IGMP Static Group parameters）] ダイアログボックスを使用します。

（注）
IGMP 静的グループを使用すると、PIM は送信元またはランデブーポイント（RP）向けに参加要求を送信できます。ただし、このコマンドのファイアウォールは、コマンドが適用されるインターフェイス上の PIM 代表ルータ（DR）であることが条件です。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウンリストから、マルチキャストグループを静的に割り当てるインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [マルチキャストグループ（Multicast Groups）] ドロップダウンリストから、インターフェイスを割り当てるマルチキャストグループを選択するか、[追加（Add）] (＋) をクリックして新しいマルチキャストグループを作成します。手順については、Creating Network Objects を参照してください。

ステップ 5 [OK] をクリックして、スタティック グループ設定を保存します。

IGMP 参加グループの設定

インターフェイスをマルチキャスト グループのメンバーとして設定できます。マルチキャスト グループに加入するように Firewall Threat Defense デバイスを設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

（注） IGMP スタティック グループの設定（1262 ページ）を参照して、特定のグループのマルチキャスト パケットを特定のインターフェイスに転送する必要がある場合に、Firewall Threat Defense デバイスがそのパケットをそのグループの一部として受け付けることがないようにする方法を確認してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [IGMP] を選択します。 > >

ステップ 3 [参加グループ（Join Group）] で、[追加（Add）] または [編集（Edit）] をクリックします。

Firewall Threat Defense デバイスをマルチキャスト グループのメンバーに設定する場合は、[IGMP 参加グループ パラメータの追加（Add IGMP Join Group parameters）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[IGMP 参加グループ パラメータの編集（Edit IGMP Join Group parameters）] ダイアログボックスを使用します。

（注）
IGMP 参加グループを使用すると、PIM は送信元またはランデブーポイント（RP）向けに参加要求を送信できます。ただし、このコマンドのファイアウォールは、コマンドが適用されるインターフェイス上の PIM 代表ルータ（DR）であることが条件です。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウンリストから、マルチキャストグループのメンバーにするインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [参加グループ（Join Group）] ドロップダウンリストから、インターフェイスを割り当てるマルチキャストグループを選択するか、[プラス（Plus）] をクリックして、新しいマル

チキャストグループを作成します。手順については、Creating Network Objects を参照してください。

PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。Secure Firewall Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、PIM および IGMP がすべてのインターフェイスで自動的に有効になります。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

手順

ステップ 1 PIM プロトコルの設定 （1264 ページ）。
ステップ 2 PIM ネイバー フィルタの設定 （1265 ページ）。
ステップ 3 PIM 双方向ネイバー フィルタの設定 （1266 ページ）。
ステップ 4 PIM ランデブー ポイントの設定 （1268 ページ）。
ステップ 5 PIM ルート ツリーの設定 （1269 ページ）。
ステップ 6 PIM リクエスト フィルタの設定 （1270 ページ）。
ステップ 7 マルチキャスト境界フィルタの設定 （1273 ページ）。

PIM プロトコルの設定

PIM は、特定のインターフェイスで有効または無効にすることができます。

代表ルータ（DR）のプライオリティを設定することもできます。DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャスト ルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。デフォルトでは、Firewall Threat Defense デバイスの DR プライオリティは 1 です。

ルータ クエリ メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリ メッセージを送信します。デフォルトでは、ルータ クエリ メッセージは 30 秒間隔で送信されま

す。さらに、60秒ごとに、Firewall Threat Defenseデバイスは PIM 加入メッセージおよびプルーニング メッセージを送信します。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [Protocol] で、[Add] または [Edit] をクリックします。

インターフェイスに新しい PIM パラメータを追加する場合は、[PIM パラメータの追加（Add PIM parameters）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM パラメータの編集（Edit PIM parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウン リストから、PIM プロトコルを設定するインターフェイスを選択します。
- [PIM を有効にする（Enable PIM）]：PIM を有効にするには、このチェックボックスをオンにします。
- [DR プライオリティ（DR Priority）]：選択したインターフェイスの DR の値。サブネット上のルータのうち、DR プライオリティが最も大きいものが指定ルータになります。有効な値の範囲は 0 ～ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値を 0 に設定した場合は、その Firewall Threat Defense デバイスインターフェイスが指定ルータになることはありません。
- [Hello 間隔（Hello Interval）]：インターフェイスから PIM hello メッセージが送信される時間間隔（秒単位）。指定できる範囲は 1 ～ 3600 です。デフォルトは 30 です。
- [参加プルーニング間隔（Join Prune Interval）]：インターフェイスから PIM の加入アドバタイズメントおよびプルーニング アドバタイズメントが送信される時間間隔（秒単位）。指定できる範囲は 10 ～ 600 です。デフォルトは 60 です。

ステップ 5 [OK] をクリックして、PIM プロトコル設定を保存します。

PIM ネイバー フィルタの設定

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャストルーティング（Multicast Routing）]** > **[PIM]** を選択します。

ステップ 3 [ネイバーフィルタ（Neighbor Filter）] で、[追加（Add）] または [編集（Edit）] をクリックします。

インターフェイスに新しい PIM ネイバー フィルタを追加する場合は、[PIM ネイバー フィルタの追加（Add PIM Neighbor Filter）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM ネイバー フィルタの編集（Edit PIM Neighbor Filter）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウンリストから、PIM ネイバーフィルタを追加するインターフェイスを選択します。
- [標準アクセスリスト（Standard Access List）]：[標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋) をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定（1322 ページ）を参照してください。

（注）
[標準アクセス リスト エントリの追加（Add Standard Access List Entry）] ダイアログボックスで [許可（Allow）] を選択すると、マルチキャスト グループ アドバタイズメントはこのインターフェイスを通過できるようになります。[ブロック（Block）] を選択すると、指定したマルチキャスト グループ アドバタイズメントはこのインターフェイスを通過できなくなります。インターフェイスに対してマルチキャスト境界を設定すると、ネイバー フィルタ エントリで許可されていない限り、すべてのマルチキャスト トラフィックが、インターフェイスの通過を拒否されます。

ステップ 5 [OK] をクリックして、PIM ネイバー フィルタ設定を保存します。

PIM 双方向ネイバー フィルタの設定

PIM 双方向ネイバー フィルタは、Designated Forwarder（DF）選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。DF を選択するために、セグメント内のすべてのマルチキャスト ルータが双方向で有効になっている必要があります。

PIM 双方向ネイバー フィルタが有効な場合、その ACL によって許可されるルータは、双方向に対応しているとみなされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向モードをサポートしていない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしている場合、DF選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしていない場合、DF 選択が実行される可能性があります。

手順

ステップ 1 **[デバイス（Devices）]>[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [マルチキャスト ルーティング（Multicast Routing）]> [PIM] を選択します。

ステップ 3 [双方向ネイバーフィルタ（Bidirectional Neighbor Filter）] で、[追加（Add）] または [編集（Edit）] をクリックします。

PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成する場合は、[PIM 双方向ネイバーフィルタの追加（Add PIM Bidirectional Neighbor Filter）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM 双方向ネイバーフィルタの編集（Edit PIM Bidirectional Neighbor Filter）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウン リストから、PIM 双方向ネイバー フィルタの ACL エントリを設定するインターフェイスを選択します。
- [標準アクセスリスト（Standard Access List）] : [標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋)をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定（1322 ページ）を参照してください。

  （注）
  [標準アクセス リスト エントリの追加（Add Standard Access List Entry）] ダイアログボックスで [許可（Allow）] を選択すると、指定したデバイスが DR 選択プロセスに参加できます。[ブロック（Block）]を選択すると、指定したデバイスはDR選択プロセスに参加できなくなります。

ステップ 5 [OK] をクリックして、PIM 双方向ネイバー フィルタ設定を保存します。

PIM ランデブー ポイントの設定

Firewall Threat Defense デバイスを複数のグループの RP として機能するように設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。ACL が指定されていない場合は、マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。双方向 PIM の詳細については、マルチキャスト双方向 PIM（1254 ページ）を参照してください。

RP には、次の制約事項が適用されます。

- 同じ RP アドレスは、2 度使用できません。
- 複数の RP に対しては、[すべてのグループ（All Groups）] を指定できません。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [ランデブーポイント（Rendezvous Points）] で、[追加（Add）] または [編集（Edit）] をクリックします。

[ランデブーポイント（Rendezvous Points）]テーブルに新しいエントリを作成する場合は、[ランデブー ポイントの追加（Add Rendezvous Point）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[ランデブー ポイントの編集（Edit Rendezvous Point）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [ランデブーポイントのIPアドレス（Rendezvous Point IP address）] ドロップダウンリストから、RP として追加する IP アドレスを選択するか、[追加（Add）] (＋) をクリックして新しいネットワークオブジェクトを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。
- [双方向転送の使用（Use bi-directional forwarding）] チェックボックスをオンにすると、指定されているマルチキャスト グループは双方向モードで動作します。双方向モードでは、Firewall Threat Defense デバイスがマルチキャスト パケットを受信したときに、直接接続されたメンバーも PIM ネイバーも存在しない場合は、送信元にプルーニング メッセージが返されます。
- 指定した RP をインターフェイス上のすべてのマルチキャストグループに対して使用する場合は、[すべてのマルチキャストグループに対してこのRPを使用する（Use this RP for All Multicast Groups）] をクリックします。
- [次に指定するようにすべてのマルチキャストグループに対してこのRPを使用する（Use this RP for all Multicast Groups as specified below）] をクリックして、指定の RP とともに使

用するマルチキャストグループを指定します。次に[標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋) をクリックして、新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定（1322 ページ）を参照してください。

ステップ 5 [OK] をクリックして、ランデブー ポイント設定を保存します。

PIM ルート ツリーの設定

デフォルトでは、PIM リーフルータは、新しい送信元から最初のパケットが到着した直後に、最短パス ツリーに加入します。この方法では、遅延が短縮されますが、共有ツリーに比べて多くのメモリが必要になります。すべてのマルチキャスト グループまたは特定のマルチキャスト アドレスに対して、Firewall Threat Defense デバイスを最短パス ツリーに加入させるか、共有ツリーを使用するかを設定できます。

[Multicast Groups] テーブルで指定されていないグループには最短パス ツリーが使用されます。[Multicast Groups] テーブルには、共有ツリーを使用するマルチキャスト グループが表示されます。テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループが含まれるエントリを作成し、その範囲の中から特定のグループを除外するには、その除外するグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

（注） この動作は Shortest Path Switchover（SPT）と呼ばれます。[共有ツリー（Shared Tree）] オプションを常に使用することをお勧めします。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [ルートツリー（Route Tree）] で、ルートツリーのパスを選択します。

- すべてのマルチキャストグループに最短パスツリーを使用する場合は、[最短パス（Shortest Path）] をクリックします。
- すべてのマルチキャストグループに共有ツリーを使用する場合は、[共有ツリー（Shared Tree）] をクリックします。
- [次に示すグループの共有ツリー（Shared tree for below mentioned group）] をクリックして、[マルチキャストグループ（Multicast Groups）] テーブルで指定されたグループを指定しま

す。次に [標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）](+)をクリックして、新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定 （1322 ページ）を参照してください。

ステップ 4 [OK] をクリックして、ルート ツリー設定を保存します。

PIM リクエスト フィルタの設定

Firewall Threat Defense デバイスが RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。Firewall Threat Defense デバイスが PIM 登録メッセージを受け入れるマルチキャスト送信元を定義できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [リクエストフィルタ（Request Filter）] で、RP として動作する Firewall Threat Defense デバイスに登録できるマルチキャスト送信元を定義します。

- [PIM 登録メッセージのフィルタ方法：（Filter PIM register messages using:）] ドロップダウン リストから [なし（None）]、[アクセス リスト（Access List）]、または [ルート マップ（Route Map）] を選択します。
- ドロップダウンリストから [アクセスリスト（Access List）] を選択した場合は、拡張 ACL を選択するか、[追加（Add）](+) をクリックして新しい拡張 ACL を作成します。手順については、拡張 ACL オブジェクトの設定 （1320 ページ）を参照してください。

  （注）
  [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、ドロップダウンリストから [許可（Allow）] を選択して、指定したマルチキャストトラフィックの指定した送信元を Firewall Threat Defense デバイスに登録することを許可するルールを作成します。または、[ブロック（Block）] を選択して、指定したマルチキャストトラフィックの指定した送信元がデバイスに登録されることを防ぐルールを作成します。

- [ルートマップ（Route Map）] を選択した場合は、[ルートマップ（Route Map）] ドロップダウンリストからルートマップを選択するか、[追加（Add）] (+) をクリックして新しいルートマップを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。

ステップ 4 [OK] をクリックして、リクエスト フィルタ設定を保存します。

Secure Firewall Threat Defense デバイスのブートストラップ ルータ設定

Firewall Threat Defense デバイスを BSR 候補として設定できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャスト ルーティング（Multicast Routing）]** > **[PIM]** を選択します。

ステップ 3 [ブートストラップルータ（Bootstrap Router）] で、[このFTDをブートストラップルータ候補として設定（Configure this FTD as a Candidate Bootstrap Router (C-BSR)）] チェックボックスをオンにして、C-BSR の設定をします。

a) [インターフェイス（Interface）] ドロップダウンリストから、BSR アドレスが派生する Firewall Threat Defense デバイスのインターフェイスを選択して、候補にします。

このインターフェイスは PIM を使用して有効化する必要があります。

b) [ハッシュ マスク長（Hash mask length）] フィールドに、ハッシュ関数が呼び出される前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）を入力します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループアドレスの最初の24 ビットだけが使用されます。これにより、複数のグループについて 1 つの RP を取得できます。指定できる範囲は 0 ～ 32 です。

c) [優先度（Priority）] フィールドに、BSR 候補の優先度を入力します。プライオリティが大きな BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。指定できる範囲は 0 ～ 255 です。デフォルト値は 0 です。

ステップ 4 （オプション）[このFTDをボーダーブートストラップルータとして設定（Configure this FTD as a Border Bootstrap Router (BSR)）] セクションで、[追加（Add）] (+) をクリックして、PIM BSR メッセージを送受信しないインターフェイスを選択します。

- [インターフェイス（Interface）] ドロップダウンリストから、PIM BSR メッセージを送受信しないインターフェイスを選択します。

  RP または BSR アドバタイズメントは、フィルタリングされている効果的に隔てられた 2 つの RP 情報交換ドメインです。

- BSR を有効化するには、[ボーダー BSR を有効にする（Enable Border BSR）] チェックボックスをオンにします。

ステップ 5 [OK] をクリックして、ブートストラップ ルータ設定を保存します。

マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIM を使用する場合、Firewall Threat Defense デバイスは、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャストルーティング（Multicast Routing）]** > **[マルチキャストルート（Multicast Routes）]** > **[追加（Add）]** または **[編集（Edit）]** を選択します。

Firewall Threat Defense デバイスに新しいマルチキャスト ルートを追加する場合は、[マルチキャスト ルート設定の追加（Add Multicast Route Configuration）] ダイアログボックスを使用します。既存のマルチキャスト ルートを変更する場合は、[マルチキャスト ルート設定の編集（Edit Multicast Route Configuration）] ダイアログボックスを使用します。

ステップ 3 [送信元ネットワーク（Source Network）] ドロップダウンボックスから、既存のネットワークを選択するか、[追加（Add）] (+) をクリックして新しいネットワークを追加します。手順については、Creating Network Objects を参照してください。

ステップ 4 ルートを転送するようインターフェイスを設定するには、[インターフェイス（Interface）] をクリックして、以下のオプションを設定します。

- [送信元インターフェイス（Source Interface）] ドロップダウンリストから、マルチキャスト ルートの着信インターフェイスを選択します。
- [発信インターフェイス/デンス（Output Interface/Dense）] ドロップダウンリストから、ルートが転送される宛先インターフェイスを選択します。
- [距離（Distance）] フィールドに、マルチキャスト ルートの距離を入力します。指定できる範囲は 0 ～ 255 です。

ステップ 5 ルートを転送するよう RPF アドレスを設定するには、[アドレス（Address）] をクリックして、以下のオプションを設定します。

- [RPF アドレス（RPF Address）] フィールドに、マルチキャスト ルートの IP アドレスを入力します。
- [距離（Distance）] フィールドに、マルチキャスト ルートの距離を 0 ～ 255 で入力します。

ステップ 6 [OK] をクリックして、マルチキャスト ルータの設定を保存します。

マルチキャスト境界フィルタの設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界フィルタを定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界フィルタを設定できます。IANA では、239.0.0.0 ～ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープアドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であるとみなされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界フィルタが設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界フィルタを定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

管理スコープ境界での Auto-RP 検出および通知のメッセージの設定、検査、フィルタリングを行うことができます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界フィルタを通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [マルチキャスト境界フィルタ（Multicast Boundary Filter）]** を選択し、[追加（Add）] または [編集（Edit）] をクリックします。

[マルチキャスト境界フィルタの追加（Add Multicast Boundary Filter）] ダイアログボックスを使用して、新しいマルチキャスト境界フィルタをデバイスに追加します。既存のパラメータを変更するには、[マルチキャスト境界フィルタの編集（Edit Multicast Boundary Filter）] ダイアログボックスを使用します。

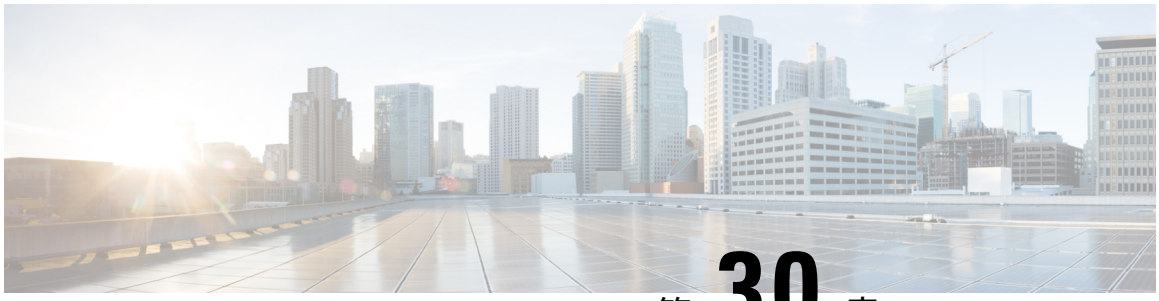
管理スコープ マルチキャスト アドレスのマルチキャスト境界を設定できます。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループアドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャスト トラフィックだけが、そのインターフェイスを通過します。

ステップ 3 [インターフェイス（Interface）] ドロップダウン リストから、マルチキャスト境界フィルタ ACL を設定するインターフェイスを選択します。

ステップ 4 [標準アクセスリスト（Standard Access List）] ドロップダウンリストから、使用する標準 ACL を選択するか、[追加（Add）](+)をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定 （1322 ページ）を参照してください。

ステップ 5 境界 ACL によって拒否されたソースからの Auto-RP メッセージをフィルタするには、[境界によって拒否された Auto-RP パケットからの Auto-RP グループ範囲通知の削除（Remove any Auto-RP group range announcement from the Auto-RP packets that are denied by the boundary）] チェックボックスをオンにします。このチェックボックスをオンにしていない場合、すべての Auto-RP メッセージが通過します。

ステップ 6 [OK] をクリックして、マルチキャスト境界フィルタの設定を保存します。



第 30 章

ポリシーベースルーティング

この章では、Firewall Management Centerの [ポリシーベースルーティング（Policy Based Routing）] ページを使用して、ポリシーベースルーティング（PBR）をサポートするようにFirewall Threat Defenseを設定する方法について説明します。次の項では、ポリシーベースルーティング、PBRのガイドライン、PBRの設定について説明します。

- ポリシーベース ルーティングについて （1275 ページ）
- ポリシーベースルーティングに関する注意事項と制約事項 （1277 ページ）
- パスモニタリング （1279 ページ）
- ポリシーベース ルーティング ポリシーの設定 （1281 ページ）
- ポリシーベースルーティングの設定例 （1285 ページ）
- パスモニタリングを使用した PBR の設定例 （1292 ページ）
- ポリシーベース ルーティングの履歴 （1294 ページ）

ポリシーベース ルーティングについて

従来のルーティングでは、パケットは宛先 IP アドレスに基づいてルーティングされます。ただし、宛先ベースのルーティングシステムでは特定トラフィックのルーティングを変更することが困難です。ポリシーベースルーティング（PBR）は、ルーティングプロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。

PBR を使用すると、IP プレジデンスを設定できます。高コスト リンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することもできます。PBR では、宛先ネットワークではなく条件（送信元ポート、宛先アドレス、宛先ポート、プロトコル、アプリケーション、またはこれらのオブジェクトの組み合わせなど）に基づいてルーティングを定義できます。

PBRを使用すると、アプリケーションに基づいてネットワークトラフィックを分類できます。このルーティング方法は、大規模なネットワーク展開で多数のデバイスがアプリケーションとデータにアクセスするシナリオに適用できます。従来、大規模な展開では、ルートベースのVPNの暗号化されたトラフィックとして、すべてのネットワークトラフィックをハブにバックホールするトポロジが設定されます。これらのトポロジでは、パケットの遅延、帯域幅の減少、パケットのドロップなどの問題が発生することがよくあります。これらの問題を克服するには、コストのかかる複雑な展開と管理が必要です。

PBR ポリシーを使用すると、指定したアプリケーションのトラフィックを安全にブレークアウトできます。Secure Firewall Management Center ユーザーインターフェイスで PBR ポリシーを設定して、アプリケーションに直接アクセスできるようにすることができます。

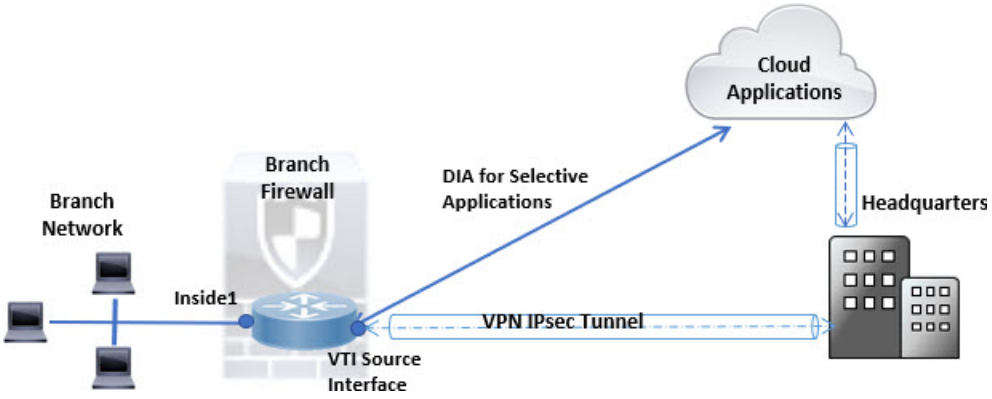
ポリシーベースルーティングを使用する理由

ロケーション間に 2 つのリンクが導入されている企業を例に説明します。1 つのリンクは高帯域幅、低遅延、高コストのリンクであり、もう 1 つのリンクは低帯域幅、高遅延、低コストのリンクです。従来のルーティングプロトコルを使用する場合、高帯域幅リンクで、リンクの（EIGRP または OSPF を使用した）帯域幅、遅延、または両方の特性により実現するメトリックの節約に基づいて、ほぼすべてのトラフィックが送信されます。PBR では、優先度の高いトラフィックを高帯域幅/低遅延リンク経由でルーティングし、その他のすべてのトラフィックを低帯域幅/高遅延リンクで送信します。

ポリシーベースルーティングを使用できるいくつかのシナリオを次に示します。

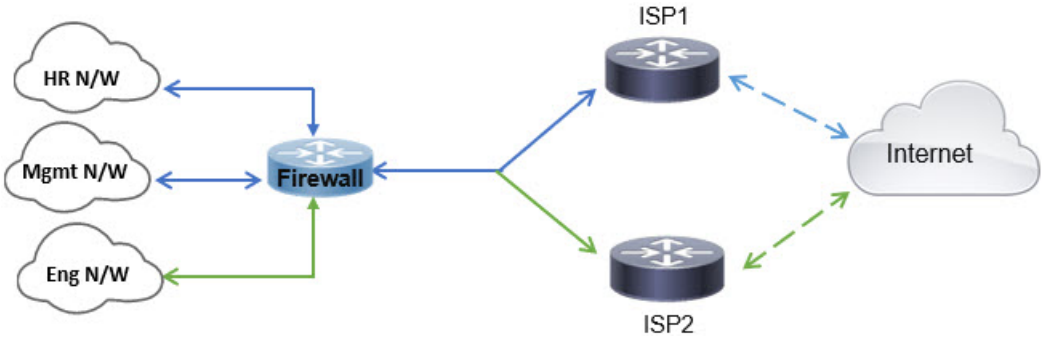
ダイレクト インターネット アクセス

このトポロジでは、ブランチオフィスからのアプリケーショントラフィックを、本社に接続する VPN トンネルを経由する代わりに、インターネットに直接ルーティングできます。ブランチ Firewall Threat Defense はインターネットの出口ポイントで構成され、PBR ポリシーは入力インターフェイス（*Inside 1*）に適用されて、ACL で定義されたアプリケーションに基づいてトラフィックを識別します。それに応じて、トラフィックは出力インターフェースを介して直接インターネットまたは IPsec VPN トンネルに転送されます。



同等アクセスおよび送信元依存ルーティング

このトポロジでは、HR ネットワークと管理ネットワークからのトラフィックは ISP1 を経由するように設定し、エンジニアリング ネットワークからのトラフィックは ISP2 を経由するように設定できます。したがって、ここに示すように、ネットワーク管理者は、ポリシーベースルーティングを使用して同等アクセスおよび送信元依存ルーティングを実現できます。



ロード シェアリング

ECMP ロード バランシングによって提供されるダイナミックなロード シェアリング機能に加え、ネットワーク管理者は、トラフィックの特性に基づいて複数のパス間にトラフィックを分散するためのポリシーを実装できます。

たとえば、同等アクセスおよび送信元依存ルーティングのシナリオに示すトポロジでは、管理者は、ISP1 を経由する HR ネットワークからのトラフィックと ISP2 を経由するエンジニアリング ネットワークからのトラフィックをルーティングしてロードシェアするように、ポリシーベースルーティングを設定できます。

ポリシーベースルーティングに関する注意事項と制約事項

ファイアウォール モードのガイドライン

PBR は、ルーテッド ファイアウォール モードでのみサポートされています。

デバイスのガイドライン

- PBR ～ Firewall Management Center の [ポリシーベースのルーティング（Policy Based Routing）] ページは、 バージョン 7.1 以降を搭載する Firewall Management Center およびデバイスでのみサポートされます。
- Firewall Management Center または Firewall Threat Defense をバージョン 7.1 以降にアップグレードすると、デバイスの PBR 設定が削除されます。[ポリシーベースのルーティング（Policy Based Routing）] ページを使用して PBR を再度設定する必要があります。管理対象デバイスがバージョン 7.1 以前の場合は、展開オプションを [毎回（every time）] に設定した FlexConfig を使用して PBR を再度設定する必要があります。
- クラスタデバイスでのアプリケーションベースの PBR ポリシーの設定は、サポートされていません。

インターフェイスのガイドライン

- グローバル仮想ルータに属するルーテッドインターフェイスおよび非管理専用インターフェイスのみ、入力インターフェイスまたは出力インターフェイスとして設定できます。
- ユーザー定義の仮想ルータでは PBR はサポートされません。
- ポリシーで定義できるのは、論理名を持つインターフェイスだけです。
- スタティック VTI は、出力インターフェイスとしてのみ設定できます。
- 設定に進む前に、特に NAT と VPN が使用されている場合に、非対称ルーティングによって引き起こされる予期しない動作を回避するために、各セッションの入力トラフィックと出力トラフィックが同じ ISP 側のインターフェイスを通過することを確認してください。

IPv6 のサポート

PBR は IPv6 をサポートしています。

アプリケーションベースの PBR と DNS の設定

- アプリケーションベースの PBR は、アプリケーション検出に DNS スヌーピングを使用します。アプリケーションの検出は、DNS 要求がクリアテキスト形式で Firewall Threat Defense を通過する場合にのみ成功します。DNS トラフィックは暗号化されません。
- 信頼できる DNS サーバーを設定する必要があります。

DNS サーバーの設定の詳細については、DNS （828 ページ）を参照してください。

出力ルート ルックアップに適用されない PBR ポリシー

ポリシーベース ルーティングは入力専用機能です。つまり、この機能は新しい着信接続の最初のパケットだけに適用され、この時点で接続のフォワードレグの出力インターフェイスが選択されます。着信パケットが既存の接続に属している場合、または NAT が適用され、NAT が出力インターフェイスを選択している場合には PBR がトリガーされないことに注意してください。

初期トラフィックに適用されない PBR ポリシー

（注） 初期接続とは、送信元と宛先の間で必要になるハンドシェイクが完了していない状態を指します。

新しい内部インターフェイスが追加され、一意のアドレスプールを使用して新しい VPN ポリシーが作成されると、新しいクライアントプールの送信元に一致する外部インターフェイスに PBR が適用されます。そのため、PBR はクライアントからのトラフィックを新しいインターフェイスの次のホップに送信します。ただし、PBR は、クライアントへの新しい内部インターフェイスルートとの接続をまだ確立していないホストからのリターントラフィックには関与しません。したがって、有効なルートがないため、ホストから VPN クライアントへのリターン

トラフィック、具体的には VPN クライアントの応答はドロップされます。内部インターフェイスにおいて、よりメトリックの高い重み付けされたスタティックルートを設定する必要があります。

その他のガイドライン

- ルートマップの設定に関する既存のすべての制限事項が、引き続き適用されます。
- ポリシー一致基準の ACL を定義するときに、事前定義されたアプリケーションのリストから複数のアプリケーションを選択してアクセス制御エントリ（ACE）を形成することができます。Firewall Threat Defense では、事前定義されたアプリケーションはネットワークサービス オブジェクトとして保存され、アプリケーションのグループはネットワーク サービス グループ（NSG）として保存されます。最大 1024 のそのような NSG を作成できます。アプリケーションまたはネットワーク サービス グループは、先頭パケット分類によって検出されます。現在、定義済みのアプリケーションリストへの追加やリストの変更はできません。
- Unicast Reverse Path Forwarding（uRPF）は、インターフェイスで受信したパケットの送信元 IP アドレスを、PBR ルートマップではなく、ルーティングテーブルと照合して検証します。uRPF が有効になっている場合、PBR を介してインターフェイスで受信されたパケットは、特定のルートエントリがない場合と同じようにドロップされます。したがって、PBR を使用する場合は、uRPF を無効にしてください。

パスモニタリング

PBR は、スタティック コストまたはパス モニタリング（ダイナミック メトリック）を使用してトラフィックをルーティングします。

パスモニタリングをインターフェイスに設定すると、ラウンドトリップ時間（RTT）、ジッター、平均オピニオン評点（MOS）、インターフェイスごとのパケット損失などのメトリックが得られます。これらのメトリックは、PBR トラフィックをルーティングするための最適なパスを決定するために使用されます。

インターフェイスのメトリックは、インターフェイスのデフォルトゲートウェイまたは指定されたリモートピアへの ICMP プローブメッセージを使用して動的に収集されます。

デフォルトのモニタリングタイマー

メトリックの収集とモニタリングには、次のタイマーが使用されます。

- インターフェイスモニタの平均間隔は 30 秒です。この間隔は、プローブで平均する頻度を示します。
- インターフェイスモニタの更新間隔は 30 秒です。この間隔は、収集された値の平均が計算され、PBR が最適なルーティングパスを決定するために使用できるようになる頻度を示します。

- ICMP によるインターフェースモニタのプローブ間隔は 1 秒です。この間隔は、ICMP ping が送信される頻度を示します。

（注） これらのタイマーの間隔は設定または変更できません。

PBR とパスモニタリング

通常、PBR では、トラフィックは、出力インターフェイスに設定された優先順位値（インターフェイスコスト）に基づいて、出力インターフェイスを介して転送されます。Management Center のバージョン 7.2 以降では、PBR は IP ベースのパスモニタリングを使用して、出力インターフェイスのパフォーマンスメトリック（RTT、ジッター、パケット損失、MOS）を収集します。PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェースを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパス モニタリング データベースから取得し、データパスを更新します。

パスモニタリングは、ダイナミックメトリックを使用した場合のみ、RTT、ジッター、packet-lost、または MOS 変更がインターフェイスに設定されている場合にのみ機能します。パスモニタリングは、静的メトリック、つまりインターフェイスコスト（インターフェイスで設定されたコスト）では機能しません。

インターフェイスのパスモニタリングを有効にし、モニタリングタイプを設定する必要があります。[PBRポリシー（PBR policy）] ページでは、パスの決定に必要なメトリックを指定できます。ポリシーベース ルーティング ポリシーの設定 （1281 ページ） を参照してください。

パスモニタリングの設定

PBR ポリシーは、往復時間（RTT）、ジッター、平均オピニオン評点（MOS）、インターフェイスのパケット損失などの柔軟なメトリックを使用して、そのトラフィックに最適なルーティングパスを識別します。パスモニタリングは、指定されたインターフェイスでこれらのメトリックを収集します。[インターフェイス（Interfaces）]ページで、パスモニタリングの設定を使用してインターフェイスを設定し、メトリック収集のために ICMP プローブを送信できます。

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [パスモニタリング（Path Monitoring）] タブをクリックします。

ステップ 4 [パスモニタリングの有効化（Enable Path Monitoring）] チェックボックスをオンにします。

ステップ 5 [モニタリングタイプ（Monitoring Type）] ドロップダウンリストから、該当するオプションを選択します。

- [自動（Auto）]：インターフェイスの IPv4 デフォルトゲートウェイに ICMP プローブを送信します。IPv4 ゲートウェイが存在しない場合、パスモニタリングはプローブをインターフェイスの IPv6 デフォルトゲートウェイに送信します。
- [ピアIPv4（Peer IPv4）]：モニタリングのために、指定されたピア IPv4 アドレス（ネクストホップ IP）に ICMP プローブを送信します。このオプションを選択した場合は、[モニターするピアIP（Peer IP To Monitor）] フィールドに IPv4 アドレスを入力します。
- [ピアIPv6（Peer IPv6）]：モニタリングのために、指定されたピア IPv6 アドレス（ネクストホップ IP）に ICMP プローブを送信します。このオプションを選択した場合は、[モニターするピアIP（Peer IP To Monitor）] フィールドに IPv6 アドレスを入力します。
- [自動IPv4（Auto IPv4）]：インターフェイスの IPv4 デフォルトゲートウェイに ICMP プローブを送信します。
- [自動IPv6（Auto IPv6）]：インターフェイスの IPv6 デフォルトゲートウェイに ICMP プローブを送信します。

（注）
- 自動オプションは、VTIインターフェイスでは使用できません。ピアアドレスを指定する必要があります。
- 宛先へ向かう 1 つのネクストホップのみがモニターされます。つまり、複数のピアアドレスを指定してインターフェイスをモニターすることはできません。

ステップ 6 [OK] をクリックし、[Save（保存）] をクリックして設定を保存します。

ポリシーベース ルーティング ポリシーの設定

[ポリシーベースルーティング（Policy Based Routing）] ページで、入力インターフェイス、一致基準（拡張アクセスコントロールリスト）および出力インターフェイスを指定することにより、PBR ポリシーを設定できます。

始める前に

出力インターフェイスでパスモニタリングメトリックを使用してトラフィック転送の優先順位を設定するには、インターフェイスのパスモニタリング設定を行う必要があります。パスモニタリングの設定 （1280 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 [ポリシーベースルーティング（Policy Based Routing）] をクリックします。

[ポリシーベースルーティング（Policy Based Routing）] ページに、設定されたポリシーが表示されます。グリッドには、入力インターフェイスのリストと、ポリシーベースのルートアクセスリストと出力インターフェイスの組み合わせが表示されます。

ステップ 4 ポリシーを設定するには、[追加（Add）] をクリックします。

ステップ 5 [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、ドロップダウンリストから [入力インターフェイス（Ingress Interface）] を選択します。

（注）
ドロップダウンには、論理名を持ち、グローバル仮想ルータに属するインターフェイスのみが表示されます。ただし、論理名を持つVLANインターフェイスを送信元（入力）インターフェイスとして設定することはできません。

ステップ 6 ポリシーで一致基準と転送アクションを指定するには、[追加（Add）] をクリックします。

ステップ 7 [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、次の操作を実行します。

a) （注）
ACEにアプリケーションアドレスと宛先アドレスの両方を定義することはできません。

着信インターフェイスに PBR を選択的に適用するには、ACE でブロック基準を定義します。トラフィックがACEのブロックルールに一致すると、トラフィックはルーティングテーブルに基づいて出力インターフェイスに転送されます。

b) [送信先（Send To）] ドロップダウンリストから：

- 構成されたインターフェイスを選択するには、[出力インターフェイス（Egress Interfaces）] を選択します。
- IPv4/IPv6 ネクストホップアドレスを指定するには、[IPアドレス（IP Address）] を選択します。手順 7.e （1283 ページ） に進みます

c) [出力インターフェイス（Egress Interfaces）] を選択した場合は、[インターフェイスの順位付け（Interface Ordering）] ドロップダウンから、関連するオプションを選択します。

- [インターフェイスの優先度（By Interface Priority）]：トラフィックはインターフェイスの優先度に基づいて転送されます。トラフィックは、優先度が最も低いインターフェイスに最初にルーティングされます。そのインターフェイスが使用できない場合、トラフィックは次に優先順位値が低いインターフェイスに転送されます。たとえば、*Gig0/1*、*Gig0/2*、および *Gig0/3* にそれぞれ優先順位値 *0*、*1*、および *2* が設定

されているとします。トラフィックは *Gig0/1* に転送されます。*Gig0/1* が使用できなくなった場合、トラフィックは *Gig0/2* に転送されます。

（注）
インターフェイスの優先度を構成するには、[ポリシーベースルーティング（Policy Based Routing）] ページで [インターフェイスの優先度の設定（Configure Interface Priority）] をクリックします。ダイアログボックスで、インターフェイスに対する優先度番号を指定し、[保存（Save）] をクリックします。インターフェイス設定でインターフェイスの優先度を設定することもできます。

すべてのインターフェイスで優先度値が同じである場合、トラフィックはインターフェイス間で分散されます。

- [順序（By Order）]：トラフィックは、ここで指定されたインターフェイスの順序に基づいて転送されます。たとえば、*Gig0/1*、*Gig0/2*、*Gig0/3* が、*Gig0/2*、*Gig0/3*、*Gig0/1* の順に選択されたとします。トラフィックは、優先度の値に関係なく、最初に *Gig0/2* に転送され、次に *Gig0/3* に転送されます。
- [最小ジッター（By Minimal Jitter）]：トラフィックは、ジッター値が最小のインターフェイスに転送されます。ジッター値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。
- [最大平均オピニオン評点（By Maximum Mean Opinion Score）]：トラフィックは、平均オピニオン評点（MOS）が最大のインターフェイスに転送されます。MOS 値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。
- [最短ラウンドトリップ時間（By Minimal Round Trip Time）]：トラフィックは、ラウンドトリップ時間（RTT）が最短のインターフェイスに転送されます。RTT 値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。
- [最小パケット損失（By Minimal Packet Loss）]：トラフィックは、パケット損失が最小のインターフェイスに転送されます。パケット損失値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。

d) [使用可能なインターフェイス（Available Interfaces）] ボックスに、すべてのインターフェイスとその優先度の値が一覧表示されます。インターフェイスのリストから、[追加（Add）]（＋）ボタンをクリックして、選択した出力インターフェイスに追加します。手順 7.k （1285 ページ） に進みます

（注）
選択したインターフェイスへのルートがルーティングテーブルに存在している必要があります。

e) [IPアドレス（IP Address）] を選択した場合は、[IPv4アドレス（IPv4 Addresses）] または [IPv6アドレス（IPv6 Addresses）] フィールドに IP アドレスをカンマで区切って入力します。トラフィックは、指定された IP アドレスの順序で転送されます。

（注）
複数のネクストホップIPアドレスが指定されている場合、ルーティングできる有効なネクストホップ IP アドレスが見つかるまで、トラフィックは指定された IP アドレスの順序に従って転送されます。設定済みのネクストホップは、直接接続する必要があります。

f) [フラグメント化しない（Don't Fragment）] ドロップダウンリストから、[はい（Yes）]、[いいえ（No）]、または [なし（None）] を選択します。DF（フラグメント化しない（Don't Fragment））フラグが [はい（Yes）] に設定されている場合、中間ルータはパケットのフラグメント化を実行しません。

g) 現在のインターフェイスを転送のデフォルトとして指定するには、[デフォルトインターフェイス（Default Interface）] チェックボックスをオンにします。

h) [IPv4設定（IPv4 Settings）] および [IPv6設定（IPv6 Settings）] タブでは、再帰設定とデフォルト設定を指定できます。

（注）
ルートマップの場合、IPv4 または IPv6 ネクストホップ設定のいずれかのみを指定できます。

- [再帰（Recursive）]：ルートマップ設定は、指定されたネクストホップアドレスとデフォルトのネクストホップアドレスが直接接続されたサブネット上で見つかった場合にのみ適用されます。ただし、再帰オプションを使用できます。この場合、ネクストホップアドレスが直接接続されている必要はありません。ネクストホップアドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータの現在のルーティングパスに従って、そのルートエントリで使用されているネクストホップに転送されます。
- [デフォルト（Default）]：一致するトラフィックに対する通常のルートルックアップが失敗すると、ここで指定されたネクストホップIPアドレスにトラフィックが転送されます。

i) ネクストホップアドレスをピアアドレスとして使用するには、[ピアアドレス（Peer Address）] チェックボックスをオンにします。

（注）
デフォルトのネクストホップアドレスとピアアドレスの両方を使用してルートマップを設定することはできません。

j) IPv4 設定の場合、[可用性の検証（Verify Availability）] でルートマップの次の IPv4 ホップが使用できるかどうかを確認できます。[追加（Add）] (＋) ボタンをクリックし、ネクストホップ IP アドレスエントリを追加します。

- [IP Address]：ネクスト ホップ IP アドレスを入力します。
- [シーケンス（Sequence）]：エントリはシーケンス番号を使用して順に評価されます。重複するシーケンス番号が入力されていないことを確認してください。有効な範囲は 1 ～ 65535 です。
- [トラック（Track）]：有効な ID を入力します。有効範囲は 1 ～ 255 です。

k) [保存（Save）] をクリックします。

ステップ 8 ポリシーを保存するには、[保存（Save）] および [展開（Deploy）] をクリックします。

Firewall Threat Defense は、ACL を使用してトラフィックを照合し、トラフィックのルーティングアクションを実行します。通常、トラフィックが照合される ACL を指定するルートマップを設定し、次にそのトラフィックに対して 1 つ以上のアクションを指定します。パスモニタリングにより、PBR でトラフィックのルーティングに最適な出力インターフェイスを選択できるようになりました。最後に、すべての着信トラフィックに PBR を適用するインターフェイスにルートマップを関連付けます。

パス監視ダッシュボードの追加

パスモニタリングメトリックを表示するには、パス監視ダッシュボードをデバイスの [ヘルスモニタリング（Health Monitoring）] ページに追加する必要があります。

手順

ステップ 1 **[システム（System）] > [正常性（Health）] > [モニター（Monitor）]**を選択します。

ステップ 2 デバイスを選択し、[新規ダッシュボードの追加（Add New Dashboard）] をクリックします。

ステップ 3 カスタムダッシュボードの名前を入力します。

ステップ 4 [メトリック（Metrics）] 領域で、[事前定義された相関関係から追加（Add from Predefined Correlations）] ボタンをクリックします。

ステップ 5 リストから、[インターフェイス - パスメトリック（Interface - Path Metrics）] をクリックします。

デフォルトでは、ダッシュボードにポートレットとして表示される 4 つのメトリックがすべて選択され、追加のメトリックフィールドも表示されます。[削除（Delete）]（ ） をクリックすると、いずれかのポートレットを除外できます。

ステップ 6 [ダッシュボードの追加（Add Dashboard）] をクリックします。

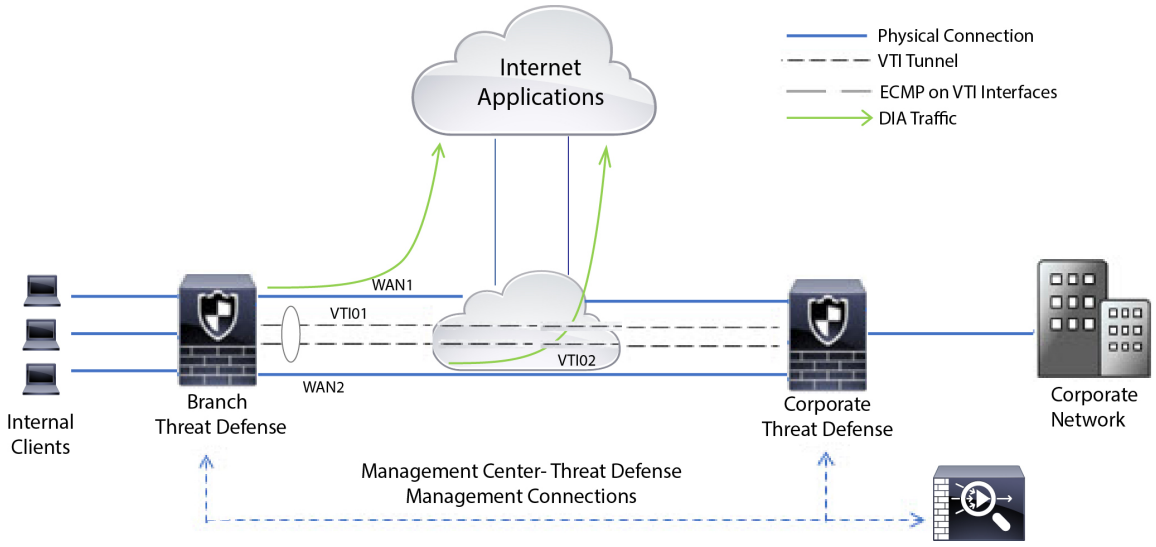
ポリシーベースルーティングの設定例

すべてのブランチ ネットワーク トラフィックが企業ネットワークのルートベースの VPN を通過し、必要に応じてエクストラネットに分岐する一般的な企業ネットワークシナリオを考えてください。企業ネットワークを介して日常業務に対処する Web ベースのアプリケーションにアクセスする場合、膨大なネットワーク拡張とメンテナンスコストが発生します。この例は、ダイレクト インターネット アクセスの PBR 設定手順を示しています。

次の図は、企業ネットワークのトポロジを示しています。ブランチネットワークは、ルートベースの VPN を介して企業ネットワークに接続されています。従来、企業 Firewall Threat Defense は、ブランチオフィスの内部トラフィックと外部トラフィックの両方を処理するように設定されていました。PBR ポリシーにより、ブランチ Firewall Threat Defense は、特定のトラフィックを仮想トンネルではなく WAN ネットワークにルーティングするポリシーで設定されます。残りのトラフィックは、通常どおり、ルートベースの VPN を通過します。

この例では、ロードバランシングを実現するための ECMP ゾーンを使用した WAN および VTI インターフェイスの設定も示しています。

図 *297 : Firewall Management Center* のブランチ *Firewall Threat Defense* でのポリシーベースルーティングの設定



始める前に

この例では、Firewall Management Center のブランチ Firewall Threat Defense の WAN および VTI インターフェイスがすでに設定されていることを前提としています。

手順

ステップ 1 ブランチ Firewall Threat Defense のポリシーベースルーティングを設定し、入力インターフェイスを選択します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) **[ルーティング（Routing）] > [ポリシーベースルーティング（Policy Based Routing）]** を選択し、[ポリシーベースルーティング（Policy Based Routing）] ページで、[追加（Add）] をクリックします。

c) [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストからインターフェイス（*[内部1（Inside 1）]* と *[内部2（Inside 2）]* など）を選択します。

ステップ 2 一致基準を指定します。

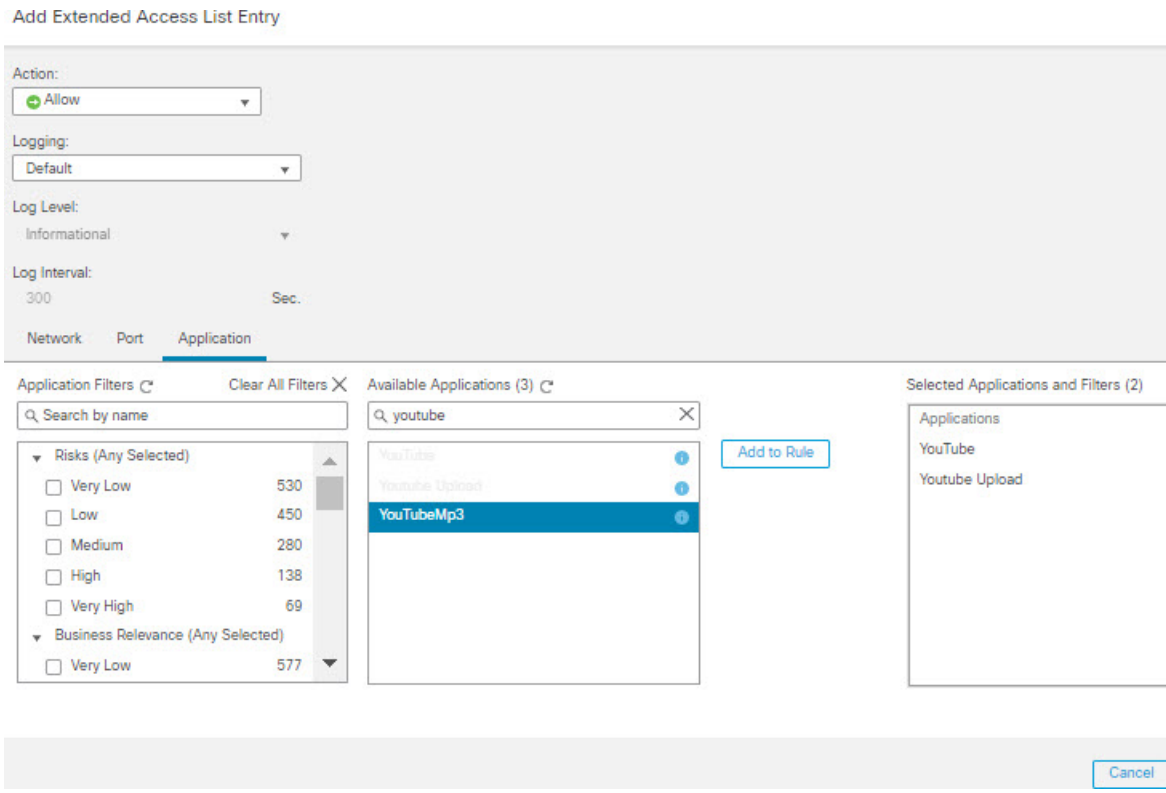
a) [追加（Add）] をクリックします。

b) 一致基準を定義するには、[追加（Add）] (+) ボタンをクリックします。

c) [新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] で、ACL の名前（たとえば、*DIA-FTD-Branch*）を入力し、[追加（Add）] をクリックします。

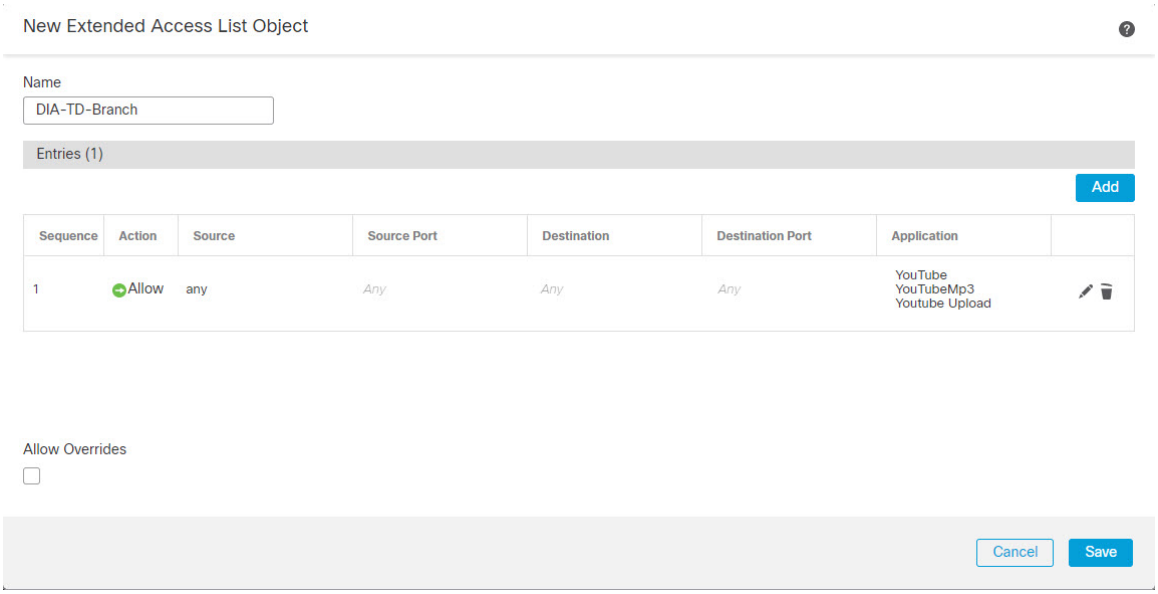
d) [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、[アプリケーション（Application）] タブから必要な Web ベースのアプリケーションを選択します。

図 *298 : [Applications]* タブ



Firewall Threat Defense では、ACL のアプリケーショングループがネットワーク サービス グループとして設定され、各アプリケーションがネットワーク サービス オブジェクトとして設定されます。

図 *299* : 拡張 *ACL*



e) [保存（Save）] をクリックします。

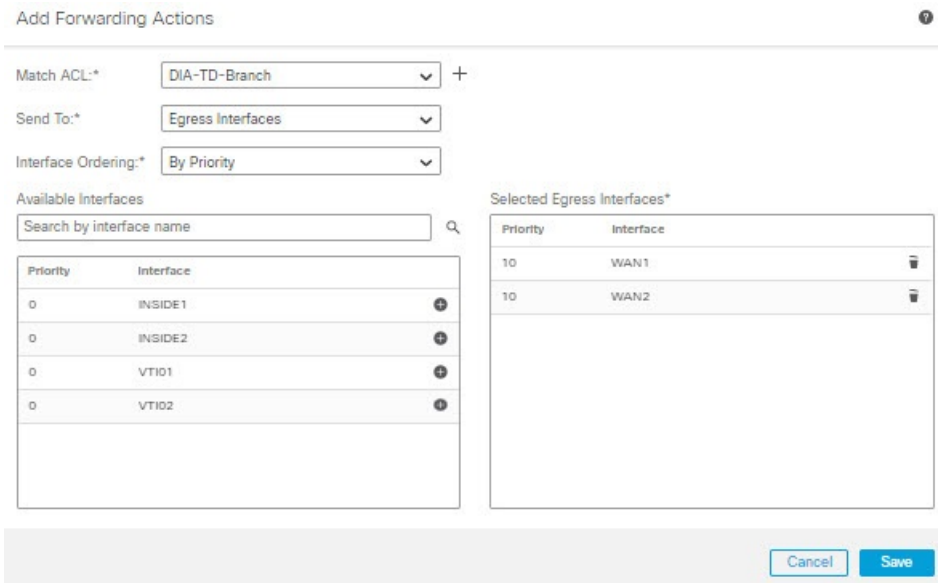
f) [ACLの照合（Match ACL）] ドロップダウンリストから [DIA-FTD-Branch] を選択します。

ステップ 3 出力インターフェイスを指定します。

a) **[宛先（Send To）]** および **[インターフェイスの順序付け（Interface Ordering）]** ドロップダウン リストから、[出力インターフェイス（Egress Interfaces）] と [インターフェイスの優先順位（Interface Priority）] をそれぞれ選択します。

b) [使用可能なインターフェイス（Available Interfaces）] で、それぞれのインターフェイス名の ⊕ ボタンをクリックして、[WAN1] と [WAN2] を追加します。

図 *300* : ポリシーベース ルーティングの設定



c) [保存（Save）] をクリックします。

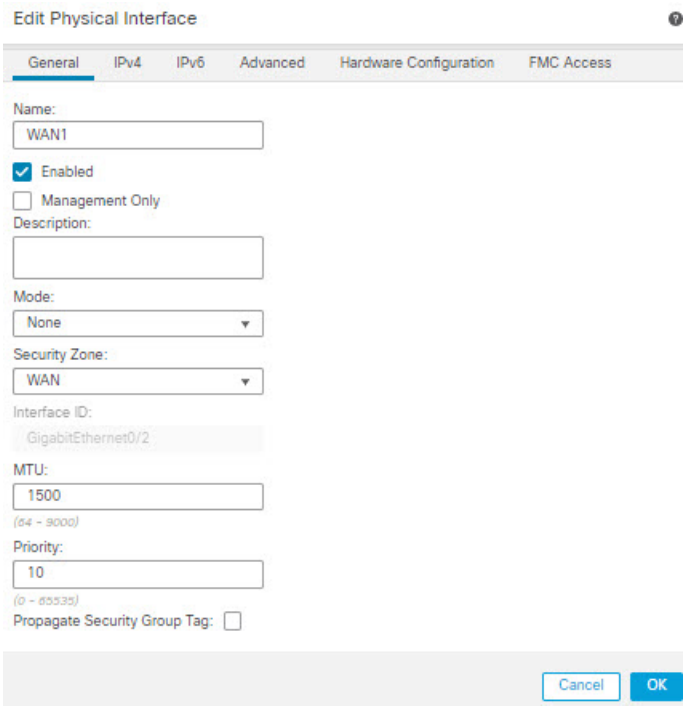
ステップ 4 インターフェイスの優先順位を設定します。

[物理インターフェイスの編集（Edit Physical Interface）] ページまたは [ポリシーベースルーティング（Policy Based Routing）] ページ（[インターフェイスの優先順位の設定（Configure Interface Priority）]）で、インターフェイスの優先順位の値を設定できます。この例では、[物理インターフェイスの編集（Edit Physical Interface）] のメソッドが示されています。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、ブランチ Firewall Threat Defense を編集します。

b) インターフェイスの優先順位を設定します。インターフェイスに対して [編集（Edit）] をクリックし、優先順位の値を入力します。

図 *301* : インターフェイスの優先順位の設定



c) [OK] をクリックし、[保存（Save）] をクリックして保存します。

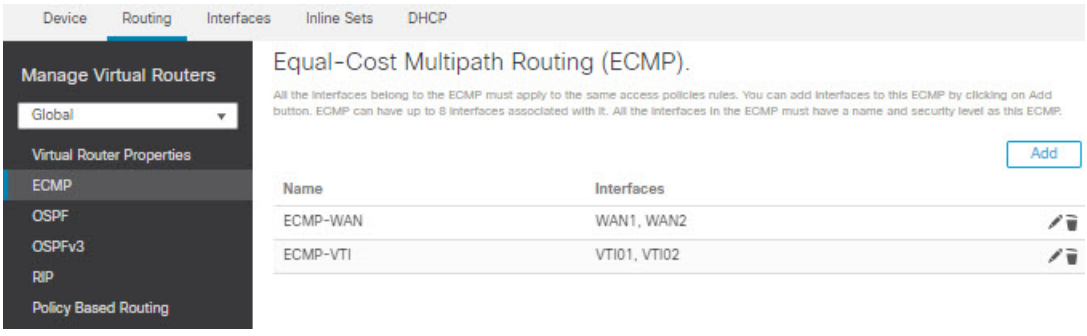
ステップ 5 ロードバランシング用の ECMP ゾーンを作成します。

a) [ルーティング（Routing）] ページで、[ECMP] をクリックします。

b) インターフェイスを ECMP ゾーンに関連付けるには、[追加（Add）] をクリックします。

c) [WAN1] と [WAN 2] を選択し、ECMP ゾーン（*ECMP-WAN*）を作成します。同様に、[VTI01] と [VTI02] を追加し、ECMP ゾーン（*ECMP-VTI*）を作成します。

図 *302* : インターフェイスと *ECMP* ゾーンの関連付け

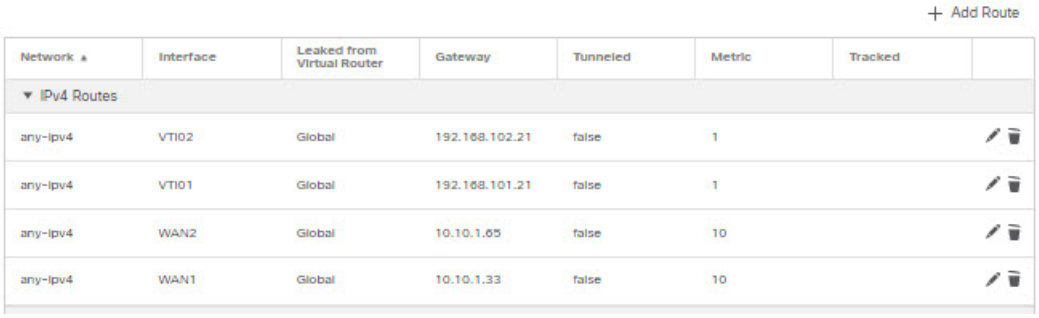


ステップ 6 ロードバランシング用のゾーンインターフェイスのスタティックルートを設定します。

a) [ルーティング（Routing）] ページで、[スタティックルート（Static Route）] をクリックします。

b) [追加（Add）]をクリックし、*WAN1*、*WAN2*、*VTI01*、および*VTI02*のスタティックルートを指定します。必ず、同じECMPゾーンに属するインターフェイスには同じメトリック値を指定してください（手順 5）。

図 *303 : ECMP* ゾーンインターフェイスのスタティックルートの設定



（注）
ゾーンインターフェイスの宛先アドレスとメトリックは同じであるが、ゲートウェイアドレスが異なることを確認してください。

ステップ 7 インターネットへの安全なトラフィックフローが確保されるように、ブランチ Firewall Threat Defense の WAN オブジェクトで信頼できる DNS を設定します。

a) **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]**を選択し、ブランチ Firewall Threat Defense で DNS ポリシーを作成します。

b) 信頼できるDNSを指定するには、[編集（Edit）]をクリックしてポリシーを編集し、[DNS]をクリックします。

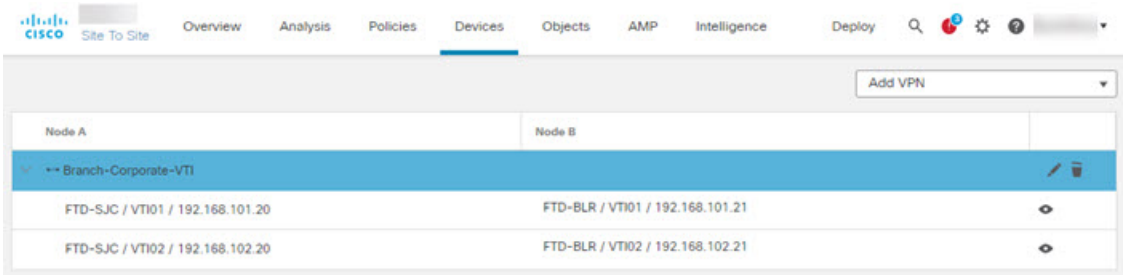
c) WAN オブジェクトが使用する DNS 解決用の DNS サーバーを指定するには、[DNS 設定（DNS Settings）]タブで、DNSサーバーグループの詳細情報を指定し、インターフェイスオブジェクトから WAN を選択します。

d) [信頼できるDNSサーバー（Trusted DNS Servers）] タブを使用して、DNS 解決のために信頼できる特定の DNS サーバーを指定します。

ステップ 8 [保存（Save）]、[展開（Deploy）] の順にクリックします。

ネットワーク *INSIDE1* または *INSIDE2* 内のブランチからの *YouTube* 関連のアクセス要求は、*DIA-FTD-Branch* ACL と一致するため、*WAN1* または *WAN2* にルーティングされます。*google.com* などの他のすべての要求は、サイト間 VPN 設定で指定されているように、*VTI01* または *VTI02* を介してルーティングされます。

図 *304* : サイト間 *VPN* の設定



ECMP が設定されていると、ネットワークトラフィックはシームレスに分散されます。

パスモニタリングを使用した PBR の設定例

この例では、柔軟なメトリックによる次のアプリケーションのパスモニタリングを備えた PBR の設定について詳しく説明します。

- ジッタのある、音声やビデオが不安定になる可能性があるアプリケーション（Webex Meetings など）。
- RTT のある、クラウドベースのアプリケーション（Office365 など）。
- パケット損失のある、ネットワークベースのアクセス制御（特定の送信元と宛先を使用）。

始める前に

1. この例は、PBR の基本的な設定手順を理解していることを前提としています。
2. 論理名による入力インターフェイスと出力インターフェイスの設定が完了しています。この例では、入力インターフェイスの名前は「Inside1」、出力インターフェイスの名前は「ISP01」、「ISP02」、および「ISP03」です。

手順

ステップ 1 インターフェイス ISP01、ISP02、および ISP03 でのパスモニタリングの設定：

出力インターフェイスでのメトリック収集については、それらのインターフェイスでパスモニタリングを有効にして設定する必要があります。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense を編集します。
b) [インターフェイス（Interfaces）] タブで、インターフェイス（この例では「ISP01」）を編集します。

c) [パスモニタリング（Path Monitoring）] タブをクリックし、[パスモニタリングの有効化（Enable Path Monitoring）] チェックボックスをオンにしてから、モニタリングタイプを指定します（パスモニタリングの設定 （1280 ページ）を参照）。

d) [OK] をクリックし、[保存（Save）] をクリックして保存します。

e) 同じ手順を繰り返し、ISP02 と ISP03 のパスモニタリングの設定を指定します。

ステップ 2 組織の Firewall Threat Defense に含まれるブランチのポリシーベースルーティングを設定し、入力インターフェイスを選択します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]** を選択し、[ポリシーベースルーティング（Policy Based Routing）] ページで、[追加（Add）] をクリックします。

c) [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから [内部 1（Inside 1）] を選択します。

ステップ 3 一致基準を指定します。

a) [追加（Add）] をクリックします。

b) 一致基準を定義するには、[追加（Add）] (＋) ボタンをクリックします。

c) [新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] で、ACL の名前（たとえば、*PBR-WebEx*）を入力し、[追加（Add）] をクリックします。

d) [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、[アプリケーション（Application）] タブから必要な Web ベースのアプリケーション（WebEx Meetings など）を選択します。

メモ
Firewall Threat Defense では、ACL のアプリケーショングループがネットワーク サービス グループとして設定され、各アプリケーションがネットワーク サービス オブジェクトとして設定されます。

e) [保存（Save）] をクリックします。

f) [ACLの照合（Match ACL）] ドロップダウンリストから [PBR-WebEx] を選択します。

ステップ 4 出力インターフェイスを指定します。

a) [宛先（Send to）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。

b) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [最小ジッターによる（By Minimal Jitter）] を選択します。

c) [使用可能なインターフェイス（Available Interfaces）] で、それぞれのインターフェイス名の [右矢印（right arrow）] （＞） ボタンをクリックして、[ISP01]、[ISP02]、および [ISP03] を追加します。

d) [保存（Save）] をクリックします。

ステップ 5 手順 2 と手順 3 を繰り返して、同じインターフェイス（*Inside1*）に、Office365 およびネットワークベースアクセス制御トラフィックをルーティングする PBR を作成します。

a) 一致基準オブジェクト（*PBR-Office365* など）を作成し、[アプリケーション（Application）] タブから Office365 アプリケーションを選択します。
b) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから、[最短ラウンドトリップ時間による（By Minimal Round Trip Time）] を選択します。
c) 出力インターフェイス「ISP01」、「ISP02」、および「ISP03」を指定し、[保存] をクリックします。
d) ここで、一致基準オブジェクト（*PBR-networks* など）を作成し、[ネットワーク（Network）] タブで送信元および宛先インターフェイスを指定します。
e) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [最小ラウンドトリップ時間による（By Minimal Packet Loss）] を選択します。
f) 出力インターフェイス「ISP01」、「ISP02」、および「ISP03」を指定し、[保存] をクリックします。

ステップ 6 [保存（Save）]、[展開（Deploy）] の順にクリックします。

ステップ 7 パスモニタリングメトリックを表示するには、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、[その他（More）] (⋮) から [ヘルスモニター（Health Monitor）] をクリックします。デバイスのインターフェイスのメトリックに関する詳細情報を表示するには、パスメトリックダッシュボードを追加する必要があります。詳細については、パス監視ダッシュボードの追加 （1285 ページ）を参照してください。

Webex、Office365、およびネットワークベース ACL トラフィックは、*ISP01*、*ISP02*、および *ISP03* で収集されたメトリック値から得られる最適ルートを介して転送されます。

ポリシーベース ルーティングの履歴

表 *66 :*

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
デュアル WAN/ISP Threat Defense 管理のサポート	7.3.0	7.3.0	デュアル WAN 対応の脅威防御では、単一のデータインターフェイスが Management Center と通信するように構成されました。現在、プライマリ データ インターフェイスに障害が発生した場合に通信チャネルが維持されるように、セカンダリ データ インターフェイスを構成するサポートが提供されています。Management Center は、優先順位と SLA メトリックに基づいて、SF-Tunnel トラフィックを Tapnlp（内部）インターフェイスから使用可能なデータインターフェイスの 1 つにルーティングするように PBR を自動設定します。

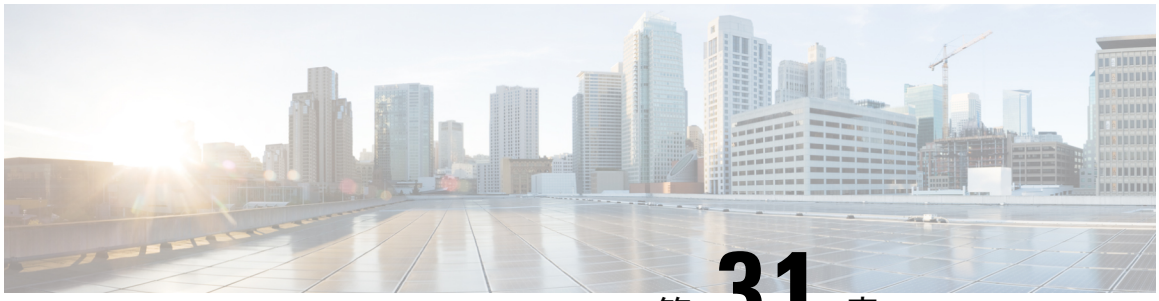
機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
PBR ルートマップのネクストホップの設定	7.3.0	7.1.0	パケット転送アクションを有効にしながら、PBR ルートマップのネクストホップを設定できます。 新規/変更された画面：出力インターフェイスを設定するための [転送アクションの追加/編集（Add/Edit Forwarding Actions）] ページの新しいフィールド：**[デバイス管理（Device Management）] > [ルーティング（Routing）] > [ポリシーベースルーティング（Policy Based Routing）] > [転送アクションの追加（Add Forwarding Actions）]**ページ。
PBR とパスモニタリング	7.2.0	7.2.0	PBR ではパスモニタリングを使用して、出力インターフェイスの評価指標（RTT、ジッター、パケット損失、MOS）が収集されます。インターフェイスのパスモニタリングを有効にし、モニタリングタイプを設定する必要があります。パスの決定に必要なメトリックを使用して PBR ポリシーを設定できます。 新規/変更された画面：パスモニタリングを有効にするための[インターフェイス（Interfaces）] ページの新しいタブ：**[デバイス（Device）] > [デバイス管理（Device Management）] > [インターフェイスの編集（Edit Interfaces）] > [パスモニタリング（Path Monitoring）]**タブ。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
FMC Web インターフェイスからポリシーベースルーティングを設定します。	7.1.0	7.1.0	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** FMC Web インターフェイスからポリシーベースルーティング（PBR）を設定できるようになりました。これにより、アプリケーションに基づいてネットワークトラフィックを分類し、ダイレクトインターネットアクセス（DIA）を実装して、ブランチ展開からインターネットにトラフィックを送信することができます。PBR ポリシーを定義し、入力インターフェイスに設定して、一致基準と出力インターフェイスを指定できます。アクセスコントロールポリシーに一致するネットワークトラフィックは、ポリシーで設定されている優先順位または順序に基づいて、出力インターフェイスを介して転送されます。 この機能を使用するには、FMC とデバイスの両方にバージョン 7.1 以降が必要です。FMC をバージョン 7.1 以降にアップグレードすると、既存のポリシーベースルーティング FlexConfig が削除されます。デバイスをバージョン 7.1 以降にアップグレードした後、FMC Web インターフェイスでポリシーベースルーティング設定をやり直します。バージョン 7.1 以降にアップグレードしないデバイスの場合は、FlexConfig を再実行し、「毎回」展開するように設定します。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [ポリシーベースルーティング（Policy Based Routing）]**

第 V 部

オブジェクトと証明書

- オブジェクト管理 （1299 ページ）
- 証明書 （1455 ページ）



第 31 章

オブジェクト管理

この章では、再利用可能なオブジェクトを管理する方法について説明します。

- オブジェクトの概要 （1300 ページ）
- オブジェクト マネージャ （1303 ページ）
- AAAサーバ （1313 ページ）
- アクセスリスト （1319 ページ）
- アドレス プール （1323 ページ）
- アプリケーション フィルタ （1325 ページ）
- ASパス （1325 ページ）
- BFD テンプレート （1326 ページ）
- 暗号スイート リスト （1327 ページ）
- コミュニティ リスト （1328 ページ）
- DHCP IPv6 プール （1332 ページ）
- 識別名 （1332 ページ）
- DNS サーバ グループ （1335 ページ）
- 外部属性 （1336 ページ）
- ファイル リスト （1338 ページ）
- FlexConfig （1344 ページ）
- 位置情報 （1345 ページ）
- インターフェイス（Interface） （1346 ページ）
- Key Chain （1346 ページ）
- ネットワーク （1349 ページ）
- PKI （1352 ページ）
- ポリシー リスト （1373 ページ）
- ポート （1376 ページ）
- プレフィックス リスト （1377 ページ）
- ルート マップ （1380 ページ）
- セキュリティ インテリジェンス （1384 ページ）
- シンクホール （1398 ページ）
- SLA モニタ （1399 ページ）

- 時間範囲 （1401 ページ）
- タイムゾーン （1403 ページ）
- トンネル ゾーン （1404 ページ）
- URL （1404 ページ）
- 変数セット （1406 ページ）
- VLAN タグ （1424 ページ）
- VPN （1425 ページ）
- オブジェクト管理の履歴 （1449 ページ）

オブジェクトの概要

柔軟性と Web インターフェイスの使いやすさを向上させるために、システムでは、名前を値に関連付ける再利用可能な構成である名前付きオブジェクトを使用します。その値を使用する場合は、代わりに名前付きオブジェクトを使用します。多くのポリシーとルール、イベント検索、レポート、ダッシュボードなど、Webインターフェイスのさまざまな場所でのオブジェクトの使用がサポートされています。よく使用される構成を表す多くの事前定義されたオブジェクトが提供されています。

オブジェクトを作成および管理するには、オブジェクトマネージャを使用します。オブジェクトを使用する多くの構成では、必要に応じて、その場でオブジェクトを作成することもできます。オブジェクト マネージャを使用して、次の操作も実行できます。

- ネットワーク、ポート、VLAN、またはURLオブジェクトが使用されているポリシー、設定、およびその他のオブジェクトを表示します。オブジェクトとその使用状況の表示（1307 ページ）を参照してください。
- 単一の構成で複数のオブジェクトを参照するための、オブジェクトのグループ化。オブジェクト グループ （1308 ページ）を参照してください。
- 選択したデバイスのオブジェクト値を上書きします。オブジェクトのオーバーライド（1310 ページ） を参照して ください。

アクティブなポリシーで使用されるオブジェクトを編集した後に、変更を有効にするには、変更した構成を再展開する必要があります。アクティブなポリシーで使用されているオブジェクトは削除できません。

（注） オブジェクトは、そのデバイスに割り当てられているポリシーでオブジェクトが使用される場合のみ、管理対象デバイスで設定されます。特定のデバイスに割り当てられているすべてのポリシーからオブジェクトを削除する場合、オブジェクトは、次の導入時にデバイス設定からも削除され、オブジェクトに対する後続の変更はデバイス設定に反映されません。

オブジェクト タイプ

次の表に、システムで作成できるオブジェクト、各オブジェクトタイプがグループ化可能かどうか、およびオーバーライドを許可するように構成できるかどうかを示します。

オブジェクト タイプ（Object Type）	グループ化可能	オーバーライドを許可
ネットワーク	○	○
[ポート（Port）]	○	○
インターフェイス： • セキュリティ ゾーン • インターフェイス グループ	×	×
トンネル ゾーン	×	×
アプリケーション フィルタ	×	×
VLAN タグ	○	○
外部属性：セキュリティグループタグ（SGT）およびダイナミックオブジェクト	×	×
URL	○	○
位置情報（GeoLocation）	×	×
時間範囲	×	×
変数セット	×	×
セキュリティ インテリジェンス：ネットワーク、DNS、URL のリストとフィード	×	×
シンクホール	×	×
ファイル リスト	×	×
暗号スイート リスト	×	×
識別名（Distinguished Name）	○	×
公開キー インフラストラクチャ（PKI）： • 内部および信頼できる CA • 内部および外部証明書	○	×
キーチェーン	×	○

オブジェクト タイプ（**Object Type**）	グループ化可能	オーバーライドを許可
DNS サーバー グループ	×	×
SLA モニター	×	×
プレフィックス リスト：IPv4 および IPv6	×	○
ルート マップ	×	○
アクセス リスト：標準および拡張	×	○
AS パス	×	○
コミュニティ リスト（Community List）	×	○
ポリシー リスト	×	○
FlexConfig：テキストおよびFlexConfig オブジェクト	×	○

オブジェクトおよびマルチテナンシー

マルチドメイン展開では、グローバルおよび子孫ドメインでオブジェクトを作成できます。ただし、グローバル ドメインでのみ作成できるセキュリティ グループ タグ（SGT）オブジェクトを除きます。現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。また、編集できない先祖ドメインで作成されたオブジェクトも表示されますが、セキュリティ ゾーンとインターフェイス グループを除きます。

（注） セキュリティゾーンとインターフェイスグループは、リーフレベルで設定したデバイスインターフェイスに関連するため、子孫ドメイン内の管理者は、先祖ドメインで作成されたとグループを表示および編集できます。サブドメインのユーザーは、先祖ゾーンとグループからインターフェイスを追加および削除できますが、ゾーン/グループを削除または名前変更することはできません。

オブジェクト名は、ドメイン階層内で一意である必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

グループ化をサポートするオブジェクトの場合、現在のドメインのオブジェクトを先祖ドメインから継承されたオブジェクトとグループ化できます。

オブジェクトのオーバーライドにより、ネットワーク、ポート、VLAN タグ、URL などの特定のオブジェクトタイプのデバイス固有またはドメイン固有の値を定義できます。マルチドメイン展開では、先祖ドメイン内のオブジェクトのデフォルト値を定義できますが、子孫ドメイン内の管理者は、そのオブジェクトのオーバーライドの値を追加できます。

オブジェクト マネージャ

オブジェクト マネージャを使用すると、オブジェクトおよびオブジェクト グループを作成、管理することができます。

オブジェクト マネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーション リンクを使用して追加ページを表示します。特定のページにアクセスしたり、[更新（Refresh）]（ ） をクリックしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ページのオブジェクトは、名前または値でフィルタ処理できます。

オブジェクトのインポート

オブジェクトは、カンマ区切り値ファイルからインポートできます。1回の試行で最大1000個のオブジェクトをインポートできます。カンマ区切り値ファイルの内容は、特定の形式に従う必要があります。形式はオブジェクトタイプごとに異なります。一部のタイプのオブジェクトのみをインポートできます。サポートされているオブジェクトタイプと対応するルールについては、次の表を参照してください。

オブジェクト タイプ	ルール

個々のオブジェクト	• 列ヘッダーは大文字で指定する必要があります。
	• ファイルには、次の列ヘッダーが必要です。
	  • NAME
	  • [DN]
	• エントリをインポートするには、NAME 列と DN 列の両方のエントリが必須です。
	• 個々のオブジェクトを既存の識別名オブジェクトグループに直接インポートできます。

オブジェクト タイプ	ルール
ネットワーク オブジェクト	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • DESCRIPTION • タイプ • 値 • LOOKUP • ホスト、範囲、またはネットワーク オブジェクト タイプのエントリをインポートするには、NAME 列と VALUE 列のエントリが必須です。 • FQDN オブジェクトの場合、TYPE 列のエントリは「fqdn」を指定する必要があり、LOOKUP 列エントリは「ipv4」、「ipv6」、または「ipv4_ipv6」を指定する必要があります。 • FQDN オブジェクトの LOOKUP 列エントリに内容が指定されていない場合、オブジェクトは ipv4_ipv6 フィールド値で保存されます。
ポート	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • プロトコル • ポート • ICMPCODE • ICMPTYPE • NAME 列のエントリは必須です。 • 「tcp」および「udp」プロトコルタイプの場合、PORT 列のエントリは必須です。 • 「icmp」および「icmp6」プロトコルタイプの場合、ICMPCODE 列および ICMPTYPE 列のエントリは必須です。

オブジェクト タイプ	ルール
URL	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • DESCRIPTION • URL • エントリをインポートするには、NAME 列と URL 列のエントリが必須です。
VLAN タグ	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • DESCRIPTION • TAG • エントリをインポートするには、NAME 列と TAG 列のエントリが必須です。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

ステップ 2 左ペインから、次のオブジェクトタイプのいずれかを選択します。

- **[識別名（Distinguished Name）] > [個々のオブジェクト（Individual Objects）] >**
- **[ネットワーク オブジェクト（Network Object）]**
- **ポート（Port）**
- **URL**
- **VLAN タグ**

ステップ 3 [追加 [オブジェクトタイプ]（Add [Object Type]）] ドロップダウンリストから [オブジェクトのインポート（Import Object）] を選択します。

（注）
前の手順で [個々のオブジェクト（Individual Objects）] を選択した場合は、[インポート（Import）] をクリックします。

ステップ 4 [参照（Browse）] をクリックします。

ステップ 5 システム上のカンマ区切りファイルを見つけて選択します。

ステップ 6 [Open] をクリックします。

（注）
識別名オブジェクトをインポートするときに、必要に応じて、[インポートされた識別名オブジェクトを以下のオブジェクトグループに追加する（Add imported Distinguished Name objects to the below object group）] チェックボックスをオンにして、ドロップダウンボックスからグループ名を選択することで、オブジェクトを既存の識別名オブジェクトグループに直接インポートすることができます。

ステップ 7 [インポート（Import）] をクリックします。

オブジェクトの編集

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 リストからオブジェクトタイプを選択します（オブジェクトの概要（1300ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある[編集（Edit）]（）をクリックします。

代わりに[表示（View）]（）が表示される場合、オブジェクトは先祖ドメインに属し、オーバーライドを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 必要に応じてオブジェクト設定を変更します。

ステップ 5 変数セットを編集する場合は、セット内の変数を管理します（変数の管理（1421ページ）を参照）。

ステップ 6 オーバーライドを許可するように設定できるオブジェクトの場合、次の操作をします。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可（1312ページ）を参照）。現在のドメインに属しているオブジェクトに対してのみ、この設定を変更できます。
- このオブジェクトにオーバーライド値を追加する場合は、[Override]セクションを展開し、[Add]をクリックします（オブジェクトのオーバーライドの追加（1312ページ）を参照）。

ステップ 7 **[保存（Save）]** をクリックします。

ステップ 8 変数セットを編集するときにそのセットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

オブジェクトとその使用状況の表示

[オブジェクト管理（Object Management）]ページで、オブジェクトの使用状況の詳細を表示できます。Firewall Management Center では、多くのオブジェクトタイプに対してこの機能を使用できます。ただし、一部のオブジェクトタイプはサポートされていません。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 次のいずれかのサポートされているオブジェクトタイプを選択します。

- [アクセスリスト（Access List）] > [拡張（Extended）]
- [アクセスリスト（Access List）] > [標準（Standard）]
- AS パス
- コミュニティ リスト（Community List）
- Interface
- ネットワーク（Network）
- ポリシー リスト
- ポート
- [プレフィックスリスト（Prefix List）] > [IPv4プレフィックスリスト（IPv4 Prefix List）]
- [プレフィックスリスト（Prefix List）] > [IPv6プレフィックスリスト（IPv6 Prefix List）]
- ルートマップ
- SLAモニター
- URL
- VLAN タグ

ステップ 3 オブジェクトの横にある**使用状況の検索**（）アイコンをクリックします。

[オブジェクトの使用率（Object Usage）] ウィンドウには、オブジェクトが使用されているすべてのポリシー、オブジェクト、およびその他の設定のリストが表示されます。オブジェクトの使用率の詳細を確認するには、リスト内のいずれかの項目をクリックします。オブジェクト

が使用されるポリシーおよびその他の設定については、対応するリンクをクリックすると、それぞれの UI ページにアクセスすることができます。

オブジェクトまたはオブジェクト グループのフィルタリング

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [フィルタ処理（Filter）] フィールドのフィルタ条件を入力します。

ページは入力に従って更新され、一致する項目が表示されます。

次のワイルドカードを使用できます。

- アスタリスク（*）文字は、ある文字の 0 回以上のオカレンスに一致します。
- キャレット記号（^）は文字列の先頭部分と一致します。
- ドル記号（$）は文字列の末尾と一致します。

ステップ 3 [未使用のオブジェクトを表示（Show Unused Object）] チェックボックスをオンにして、システム内のどこでも使用されていないオブジェクトとオブジェクトグループを表示します。

（注）
- オブジェクトが未使用オブジェクトのグループに含まれる場合、そのオブジェクトは使用済みと見なされます。ただし、[未使用のオブジェクトを表示（Show Unused Object）] チェックボックスをオンにすると、未使用オブジェクトのグループが表示されます。
- [未使用のオブジェクトを表示（Show Unused Object）] チェックボックスは、ネットワーク、ポート、URL、および VLAN タグのオブジェクトタイプでのみ使用できます。

オブジェクト グループ

オブジェクトをグループ化すると、複数のオブジェクトを 1 つの設定で参照できます。システムでは、Web インターフェイスでオブジェクトおよびオブジェクト グループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクト グループも使用できます。

ネットワーク、ポート、VLAN タグ、URL、および PKI オブジェクトをグループ化できます。ネットワーク オブジェクト グループはネストすることができます。つまり、ネットワーク オブジェクト グループを別のネットワーク オブジェクト グループに追加できます。許容されるネスト レベルは最大 10 です。

同じタイプのオブジェクトおよびオブジェクト グループには、同じ名前を付けることはできません。

ポリシーで使用されるオブジェクト グループ（たとえば、アクセス コントロール ポリシーで使用されるネットワーク オブジェクト グループ）を編集する場合、変更を適用するためには、変更後の設定を再展開する必要があります。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、アクティブ ポリシーで使用中のグループは削除できません。たとえば、保存されたアクセス コントロール ポリシーの VLAN 条件で使用している VLAN タグのグループは削除できません。

再利用可能オブジェクトのグループ化

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 グループ化するオブジェクト タイプが、[ネットワーク（Network）]、[ポート（Port）]、[URL]、[VLAN タグ（VLAN Tag）] の場合は、次のように操作します。

a) オブジェクト タイプのリストからオブジェクト タイプを選択します。

b) [追加 [オブジェクト タイプ]（Add [Object Type]）] ドロップダウンリストから [グループの追加（Add Group）] を選択します。

ステップ 3 グループ化するオブジェクト タイプが [識別名（Distinguished Name）] の場合は、次のように操作します。

a) [識別名（Distinguished Name）] ノードを展開します。

b) [オブジェクト グループ（Object Groups）] を選択します。

c) [識別名グループの追加（Add Distinguished Name Group）] をクリックします。

ステップ 4 グループ化するオブジェクト タイプが [PKI] の場合は、次のように操作します。

a) [PKI] ノードを展開します。

b) 次のいずれかを実行します。

- **内部 CA グループ（Internal CA Groups）**
- **信頼できる CA グループ（Trusted CA Groups）**
- **内部証明書グループ（Internal Cert Groups）**
- **外部証明書グループ（External Cert Groups）**

c) [[オブジェクトタイプ]グループの追加（Add [Object Type] Group）] をクリックします。

ステップ 5 一意の [名前（Name）] を入力します。

ステップ 6 リストから 1 つ以上のオブジェクトを選択して、[追加（Add）] をクリックします。

次のことも実行できます。

- 含める既存のオブジェクトを検索するには、フィルタ フィールド（[検索（Search）]（）を使用します。これは入力に従って更新され、一致する項目を表示します。検索文字列をクリアするには、検索フィールドの上にある**リロード**（）をクリックするか、検索フィールド内の[クリア（Clear）]（）をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、その場でオブジェクトを作成するには、[追加（Add）]()をクリックします。

ステップ 7 必要に応じて、[ネットワーク（Network）]、[ポート（Port）]、[URL]、および [VLAN タグ（VLAN Tag）] グループに対し、次の操作を実行します。

- [説明（Description）] を入力します。
- [オーバーライドを許可する（Allow Overrides）] チェックボックスをオンにして、このオブジェクト グループのオーバーライドを許可します。オブジェクトのオーバーライドの許可 （1312 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクト グループを参照する場合は、設定の変更を展開します。設定変更の展開 （172 ページ）を参照してください。

オブジェクトのオーバーライド

オブジェクトをオーバーライドすることにより、オブジェクトの代替値を定義できます。指定したデバイスに対して、システムはこの代替値を使用します。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクト オーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、社内のさまざまな部門への ICMP トラフィックを拒否する場合があります。それぞれの部門は、異なるネットワークに接続されています。これを実行するには、Departmental Network という名前のネットワーク オブジェクトを含むルールを使用して、アクセス コントロール ポリシーを定義します。このオブジェクトのオーバーライドを許可することによって、関連する各デバイスで、デバイスが接続されている実際のネットワークを指定するオーバーライドを作成できます。

オブジェクト オーバーライドのターゲットを特定のドメインに絞ることもできます。その場合、ユーザがデバイス レベルで値をオーバーライドしない限り、システムはターゲット ドメインのすべてのデバイスにオブジェクト オーバーライド値を使用します。

オブジェクトマネージャで、オーバーライド可能なオブジェクトを選択し、そのオブジェクトに対するデバイスレベルまたはドメインレベルのオーバーライドのリストを定義できます。

オブジェクト オーバーライドを使用できるオブジェクト タイプは以下に限られます。

- ネットワーク
- ポート
- VLAN タグ
- URL
- SLA モニタ
- プレフィックス リスト
- ルート マップ
- アクセス リスト
- AS パス
- コミュニティ リスト（Community List）
- ポリシー リスト
- 証明書の登録（PKI）
- キーチェーン

オブジェクト マネージャでは、オーバーライド可能なオブジェクトのオブジェクト タイプには [オーバーライド（Override）] 列が表示されます。この列の有効な値は以下のとおりです。

- 緑のチェックマーク：このオブジェクトにはオーバーライドを作成できます。オーバーライドはまだ追加されていません。
- 赤の X：このオブジェクトにはオーバーライドを作成できません。
- 数値：このオブジェクトに追加されているオーバーライドの数を表します（たとえば、「2」は 2 つのオーバーライドが追加されていることを意味します）。

オブジェクト オーバーライドの管理

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから選択します（オブジェクトの概要（1300 ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある[編集（Edit）]（✎）をクリックします。

代わりに[表示（View）]（ ）が表示される場合、オブジェクトは先祖ドメインに属し、オーバーライドを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 オブジェクト オーバーライドを管理します。

- 追加：オブジェクトオーバーライドを追加します（オブジェクトのオーバーライドの追加（1312 ページ）を参照）。
- 許可：オブジェクトオーバーライドを許可します（オブジェクトのオーバーライドの許可（1312 ページ） を参照）。
- 削除：オブジェクトエディタで、削除するオーバーライドの横にある[削除（Delete）]（）をクリックします。
- 編集：オブジェクト オーバーライドを編集します（オブジェクト オーバーライドの編集（1313 ページ）を参照）。

オブジェクトのオーバーライドの許可

手順

ステップ 1 オブジェクトエディタで、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします。

ステップ 2 **[Save]** をクリックします。

次のタスク

オブジェクトのオーバーライド値を追加します（オブジェクトのオーバーライドの追加 （1312 ページ） を参照）。

オブジェクトのオーバーライドの追加

始める前に

オブジェクトのオーバーライドを許可します（オブジェクトのオーバーライドの許可 （1312ページ） を参照）。

手順

ステップ 1 オブジェクトエディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 [Add] をクリックします。

ステップ 3 [ターゲット（Targets）] で、[使用可能なデバイスとドメイン（Available Devices and Domains）] リストからドメインまたはデバイスを選択し、[追加（Add）] をクリックします。

ステップ 4 [オーバーライド（Override）] タブで、[名前（Name）] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 オーバーライド値を入力します。

例：

ネットワークオブジェクトについては、ネットワーク値を入力します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

オブジェクト オーバーライドの編集

既存のオーバーライドの説明と値を変更できます。ただし、既存のターゲットリストは変更できません。代わりに、既存のオーバーライドを置き換える、新しいターゲットに対する新しいオーバーライドを追加する必要があります。

手順

ステップ 1 オブジェクトエディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 変更するオーバーライドの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 必要に応じて、[説明（Description）] を変更します。

ステップ 4 オーバーライド値を変更します。

ステップ 5 [保存（Save）] をクリックして、オーバーライドを保存します。

ステップ 6 [保存（Save）] をクリックして、オブジェクトを保存します。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

AAAサーバ

再利用可能な AAA サーバーオブジェクトを追加します。

RADIUS サーバーグループの追加

RADIUS サーバー グループ オブジェクトには、RADIUS サーバーへの参照が 1 つ以上含まれています。これらのサーバーは、リモート アクセス VPN 接続を通じてユーザーのログインを認証するために使用されます。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

始める前に

（注） RADIUS サーバー グループ オブジェクトは、オーバーライドできません。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAA サーバー（AAA Server）] > [RADIUS サーバーグループ（RADIUS Server Group）]** を選択します。

現在設定されているすべての RADIUS サーバーグループ オブジェクトがリスト表示されます。フィルタを使用して、リストを絞り込んでください。

ステップ 2 リストされた [RADIUS サーバ グループ（RADIUS Server Group）] オブジェクトを選択し、編集するか、新しいオブジェクトを追加します。

このオブジェクトを設定する場合は、RADIUS サーバー オプション （1316 ページ）およびRADIUS サーバー グループのオプション （1314 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックします。

RADIUS サーバー グループのオプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAA サーバー（AAA Server）] > [RADIUS サーバーグループ（RADIUS Server Group）]。設定済みの RADIUS サーバー グループ オブジェクトを選択して編集するか、または新しく追加します。

フィールド

- [名前（Name）] と [説明（Description）]：この RADIUS サーバー グループ オブジェクトを識別するための名前と、任意で説明を入力します。
- [グループ アカウンティング モード（Group Accounting Mode）]：グループ内の RADIUS サーバーにアカウンティング メッセージを送信するための方法です。[1 つ（Single）] を選択します。アカウンティング メッセージがグループ内の 1 つのサーバーに送信されま

す。これはデフォルトです。または、[同時（Multiple）] を選択します。アカウンティングメッセージがグループ内のすべてのサーバーに同時に送信されます。

- [間隔のリトライ（Retry Interval）]：RADIUS サーバへの接続を試みる間隔です。間隔の範囲は、1 ～ 10 秒です。
- [レルム（Realms）]（オプション）：この RADIUS サーバーグループに関連付ける Active Directory（AD）レルムを指定または選択します。その後、トラフィック フローの VPN 認証アイデンティティ ソースの判別時に、関連する RADIUS サーバー グループにアクセスするためにこのレルムがアイデンティティ ポリシーで選択されます。このレルムは実質的に、アイデンティティ ポリシーからこの Radius サーバ グループへのブリッジを提供します。この RADIUS サーバー グループにレルムを関連付けない場合、アイデンティティ ポリシーでトラフィック フローの VPN 認証アイデンティティ ソースを判別するために RADIUS サーバー グループに到達することができません。

（注） ユーザーアイデンティティと RADIUS をアイデンティティソースとしてリモートアクセス VPN を使用する場合、このフィールドは必須です。

- [許可のみを有効にする（Enable authorize only）]：この RADIUS サーバー グループが認証に使用されないが、許可またはアカウンティングに使用される場合は、このフィールドをオンにすると RADIUS サーバー グループの許可限定モードが有効になります。

  許可限定モードでは、アクセス要求に RADIUS サーバ パスワードを含める必要がありません。したがって、個別の RADIUS サーバに設定されたパスワードが無視されます。

- [アカウントの暫定更新（Enable interim account update）を有効にする] および [間隔（Interval）]：新たに割り当てられた IP アドレスを RADIUS サーバーに通知するために、RADIUS interim-accounting-update メッセージの生成を有効にします。[間隔（Interval）] フィールドの定期アカウンティング更新の間隔時間長を設定します。有効数は 1 ～ 120 であり、デフォルト値は 24 です。
- [ダイナミック認証の有効化（Enable Dynamic Authorization）] と [ポート（Port）]：この RADIUS サーバ グループの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にします。[ポート（Port）] フィールドで、RADIUS CoA 要求のリスニング ポートを指定します。有効数は 1024 ～ 65535 であり、デフォルト値は 1700 です。一旦定義されると、対応する RADIUS サーバ グループが CoA 通知用に登録され、Cisco Identity Services Engine（ISE）から CoA ポリシーの更新を行うポートにリッスンします。
- [RADIUSサーバー（RADIUS Servers）]：RADIUS サーバー オプション （1316 ページ） を参照してください。

関連トピック

RADIUS サーバーグループの追加 （1314 ページ）

RADIUS サーバー オプション

ナビゲーション パス

[オブジェクト（Objects）]>**[オブジェクト管理（Object Management）]**>**[AAAサーバー（AAA Server）]** > **[RADIUSサーバーグループ（RADIUS Server Group）]**。リストされた [RADIUS サーバー グループ（RADIUS Server Group）] オブジェクトを選択し、編集するか、新しいオブジェクトを追加します。次に、[RADIUS サーバ グループ（RADIUS Server Group）] ダイアログで、リストされた RADIUS サーバを選択して、編集するか、新しい RADIUS サーバを追加します。

フィールド

- [IPアドレス/ホスト名（IP Address/Hostname）]：認証要求が送信される RADIUS サーバーのホスト名または IP アドレスを特定するネットワーク オブジェクトです。ホスト名またはIPアドレスを1つのみ選択し、追加のサーバに追加し、更なるRADIUSサーバをRADIUS サーバ グループ リストに追加します。

（注） デバイスは、RADIUS 認証の IPv6 IP アドレスをサポートするようになりました。

- [認証ポート（Authentication Port）]：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [キー（Key）] および [キーの確認（Confirm Key）]：管理対象デバイス（クライアント）と RADIUS サーバ間でデータを暗号化するために使用される共有秘密です。

  キーでは、127 文字以下の英数字で、大文字と小文字を区別します。特殊文字も使用可能です。

  このフィールドで定義したキーは、RADIUS サーバのキーと一致している必要があります。確認フィールドでもう一度キーを入力します。
- [アカウンティング ポート（Accounting Port）]：RADIUS アカウンティングが実行されるポートです。デフォルトは 1813 です。
- [タイムアウト（Timeout）]：認証のセッション タイムアウト。

（注） RADIUS 二要素認証の場合、タイムアウト値は 60 秒以上必要です。デフォルトのタイムアウト値は 10 秒です。

- [使用して接続（Connect Using）]：ルートルックアップまたは特定のインターフェイスを使用して、デバイスから RADIUS サーバーへの接続を確立します。
  - [ルーティング（Routing）] オプションボタンをクリックして、ルーティングテーブルを使用します。

- [特定のインターフェイス（Specific Interface）] オプションボタンをクリックし、ドロップダウンリストからセキュリティゾーン/インターフェイスグループまたは [診断（Diagnostic）] インターフェイス（デフォルト）を選択します。

- [リダイレクトACL（Redirect ACL）]：リストからリダイレクト ACL を選択するか、新しいリダイレクト ACL を追加します。

（注） これは、リダイレクトされるトラフィックを決定するためにデバイスで定義されている ACL の名前です。ここでのリダイレクト ACL の名前は、ISE サーバーの *redirect-acl* の名前と同じである必要があります。ACL オブジェクトを設定する場合は、ISE サーバーと DNS サーバーに [Block（ブロック）] アクションを、残りのサーバーに [許可（Allow）] アクションを必ず選択してください。

関連トピック

RADIUS サーバーグループの追加 （1314 ページ）
RADIUS サーバー グループのオプション （1314 ページ）

シングルサインオンサーバーの追加

始める前に

SAML アイデンティティ プロバイダーから次のものを取得します。

- アイデンティティ プロバイダー エンティティ ID URL
- サインイン URL
- サインアウト URL
- アイデンティティ プロバイダー証明書と、Firewall Management Center Web インターフェイス（[デバイス（Devices）]>[証明書（Certificates）]）を使用した Firewall Threat Defense への証明書の登録

詳細については、「SAML シングルサインオン認証の設定 （1659 ページ）」を参照してください。

手順

ステップ 1 **[オブジェクト（Object）]>[オブジェクト管理（Object Management）]>[AAA サーバー（AAA Server）]>[シングルサインオンサーバー（Single Sign-on Server）]** を選択します。

ステップ 2 [シングルサインオンサーバーの追加（Add Single Sign-On Server）] をクリックし、次の詳細を入力します。

- [名前（Name）]：SAML シングル サインオン サーバー オブジェクトの名前。
- [アイデンティティ プロバイダー エンティティ ID（Identity Provider Entity ID）]：サービス プロバイダーを一意に識別するために SAML IdP で定義される URL。

  これは、SAML 発行元が要求に応答する方法を記述したメタデータ XML を提供するページの URL です。
- [SSO URL]：SAML アイデンティティ プロバイダー サーバーにサインインするための URL。
- [ログアウトURL（Logout URL）]：SAML アイデンティティ プロバイダー サーバーからサインアウトするための URL。
- [ベースURL（Base URL）]：アイデンティティ プロバイダー認証が完了するとユーザーを Firewall Threat Defense にリダイレクトする URL。これは、Firewall Threat Defense リモートアクセス VPN 用に設定されたアクセスインターフェイスの URL です。
- [アイデンティティプロバイダー証明書（Identity Provider Certificate）]：IdP によって署名されたメッセージを検証するために Firewall Threat Defense に登録される IdP の証明書。

  リストからアイデンティティプロバイダー証明書を選択するか、**[追加（Add）]** をクリックして新しい証明書登録オブジェクトを作成します。

  詳細については、「Firewall Threat Defense 証明書の管理 （1456 ページ）」を参照してください。

  Microsoft Azure に登録されたすべてのアプリケーション CA 証明書を Firewall Threat Defense のトラストポイントとして登録する必要があります。Microsoft Azure SAML アイデンティティ プロバイダーは、最初のアプリケーション用に Firewall Threat Defense で構成されます。すべての接続プロファイルは、構成された MS Azure SAML アイデンティティプロバイダーにマップされます。MS Azure アプリケーション（デフォルト以外）ごとに、リモートアクセス VPN の接続プロファイル構成で必要なトラストポイント（CA 証明書）を選択できます。

  詳細は、リモートアクセス VPN の AAA 設定 （1588 ページ）を参照してください。
- [サービスプロバイダー証明書（Service Provider Certificate）]：要求に署名し、IdP との信頼の輪を構築するために使用される Firewall Threat Defense 証明書。

  内部 Firewall Threat Defense 証明書を登録していない場合は、[+] をクリックして証明書を追加および登録します。詳細については、「Firewall Threat Defense 証明書の管理 （1456 ページ）」を参照してください。
- [要求の署名（Request Signature）]：SAML シングルサインオン要求に署名する暗号化アルゴリズムを選択します。

  署名（SHA1、SHA256、SHA384、SHA512）は、最も弱いものから最も強いものの順で一覧表示されます。暗号化を無効にする場合は、[なし（None）] を選択します。

- [要求タイムアウト（Request Timeout）]：ユーザーがシングルサインオン要求を完了するための SAML アサーション有効期間を指定します。SAML IdPには、*NotBefore* と *NotOnOrAfter* の 2 つのタイムアウトがあります。Firewall Threat Defense は、現在の時刻が（下限）*NotBefore*、および（上限） *NotBefore* + タイムアウト と *NotOnOrAfter* のうちの小さいほうの時間範囲内にあるかどうかを検証します。そのため、IdP の *NotOnOrAfter* タイムアウトよりも長いタイムアウトを設定した場合、指定したタイムアウトは無視され、*NotOnOrAfter* タイムアウトが選択されます。指定したタイムアウトと *NotBefore* タイムアウトの合計が *NotOnOrAfter* の時間より短い場合、そのタイムアウトは Firewall Threat Defense のタイムアウトによってオーバーライドされます。

  タイムアウトの範囲は 1 ー 7200 秒で、デフォルトは 300 秒です。

- [内部ネットワークでのみアクセス可能なIdPを有効にする（Enable IdP only accessible on Internal Network）]：SAML IdP が内部ネットワークに存在する場合は、このオプションを選択します。Firewall Threat Defense はゲートウェイとして機能し、匿名の webvpn セッションを使用してユーザーと IdP 間の通信を確立します。

- [ログイン時に IdP の再認証を要求する（Request IdP re-authentication on Login）]：このオプションをオンにすると、以前の IdP セッションが有効であっても、ログインのたびにユーザーが認証されます。

- [オーバーライドを許可する（Allow Overrides）]：このチェックボックスをオンにすると、このシングル サインオン サーバー オブジェクトのオーバーライドが許可されます。

ステップ 3 [保存（Save）] をクリックします。

関連トピック

リモートアクセス VPN の AAA 設定 （1588 ページ）

アクセスリスト

アクセス リスト オブジェクトは、アクセス コントロール リスト（ACL）とも呼ばれ、トラフィックに適用されるサービスを選択します。これらのオブジェクトは、Firewall Threat Defense デバイスの特定の機能（ルートマップなど）を設定するときに使用します。ACL で許可されたトラフィックはサービスを利用できますが、「ブロックされた」トラフィックはサービスから除外されます。サービスから除外されたトラフィックが必ずしも完全にドロップされるわけではありません。

次のタイプの ACL を設定できます。

- 拡張：送信元と宛先アドレスおよびポートに基づいてトラフィックを識別します。IPv4 および IPv6 アドレスをサポートしており、任意のルールで混在させることができます。

- 標準：宛先アドレスのみに基づいてトラフィックを識別します。IPv4 のみサポートしています。

ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）またはルールで構成されます。ACE の順番は重要です。パケットを「許可」 ACE と照合して ACL を評価する際、ACL に登録されている ACE の順番どおりに照合します。一致が見つかると、それ以降の ACE とは照合しません。たとえば、10.100.10.1 を「許可」して、10.100.10.0/24 の残りはすべて「ブロック」する場合、許可エントリがブロック エントリより前に登録されている必要があります。通常、具体性の高いルールを ACL の上部に置きます。

「許可」エントリに一致しないパケットはブロックされたと見なします。

次に、ACL オブジェクトの設定方法について説明します。

拡張 ACL オブジェクトの設定

送信元および宛先アドレス、プロトコルおよびポート、アプリケーショングループに基づいて、あるいはトラフィックが IPv6 の場合にトラフィックを照合するには、拡張 ACL オブジェクトを使用します。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択して、コンテンツテーブルから **[オブジェクト（Objects）]** > **オブジェクト管理（Object Management）]** > **[アクセスリスト（Access List）]** > **[拡張済み（Extended）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [拡張アクセスリストの追加（Add Extended Access List）] をクリックして、新しいオブジェクトを作成します。
- [編集（Edit）]（✎） をクリックして、既存のオブジェクトを編集します。

ステップ 3 [新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] ダイアログボックスで、オブジェクトの名前を入力し（スペースは使用不可）、アクセス コントロール エントリを設定します。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しいエントリを作成します。
- [編集（Edit）]（✎） をクリックして、既存のエントリを編集します。

b) トラフィック基準を許可（一致）するか、またはブロック（一致しない）するかの**アクション**を選択します。

（注）
[ログ（Logging）]、[ログ レベル（Log Level）]、および[ログ インターバル（Log Interval）] オプションはアクセス ルールに対してのみ使用されます（インターフェイスに接続されているか、グローバルで適用される ACL）。ACL オブジェクトがアクセス ルールで使用されていないため、これらの値にはデフォルトを使用します。

c) 次のテクニックのいずれかを使用して、[ネットワーク（Network）] タブで送信元および宛先アドレスを設定します。

- [利用可能（Available）] リストから目的のネットワーク オブジェクトまたはグループを選択し、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。リストの上の [+] ボタンをクリックすると、新しいオブジェクトを作成できます。IPv4 アドレスと IPv6 アドレスを組み合わせることができます。
- 送信元または宛先リストの下の編集ボックスにアドレスを入力し、[追加（Add）] をクリックします。1 つのホストアドレス（10.100.10.5、2001:DB8::0DB8:800:200C:417A など）またはサブネット（10.100.10.0/24 または 10.100.10.0 255.255.255.0 の形式。IPv6 の場合は 2001:DB8:0:CD30::/60）を指定できます。

d) [ポート（Port）] タブをクリックし、次のテクニックのいずれかを使用してサービスを設定します。

- [利用可能（Available）] リストから目的のポートオブジェクトを選択し、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。リストの上の [+] ボタンをクリックすると、新しいオブジェクトを作成できます。オブジェクトによって TCP/UDP ポート、ICMP/ICMPv6 メッセージ タイプ、その他のプロトコルを指定できます（「任意」を含む）。ただし、通常は空にしておく送信元ポートは TCP/UDP のみを受け入れます。ポートグループは選択できません。

  TCP/UDP の場合、送信元フィールドと宛先フィールドの両方を指定するときは、両方で同じプロトコルを使用する必要があることに注意してください。たとえば、UDP 送信元ポートと TCP 宛先ポートを指定することはできません。

- 送信元または宛先リストの下の編集ボックスでポートまたはプロトコルを入力または選択し、[追加（Add）] をクリックします。

（注）
すべての IP トラフィックに適用するエントリを取得するには、「すべて」のプロトコルを指定する宛先ポート オブジェクトを選択します。

e) [アプリケーション（Application）] タブをクリックし、ダイレクト インターネット アクセス ポリシー用にグループ化するアプリケーションを選択します。

重要
- クラスタデバイスのアプリケーションを設定することはできません。したがって、このタブはクラスタデバイスには適用されません。
- ポリシーベースルーティングのアプリケーションでのみ拡張 ACL を使用します。動作が不明でサポートされていないため、他のポリシーでは使用しないでください。拡張 ACL でユーザーアイデンティティと SGT を使用するポリシーベースルーティングのレルム/ISE 設定の移行を確認してください。

（注）
- [利用可能なアプリケーション（Available Applications）] リストには、事前定義されたアプリケーションの固定セットが表示されます。アプリケーションは最初のパケット

（IPアドレスとポートに解決されるFQDNエンドポイント）によってのみ検出できるため、このリストはアクセス コントロール ポリシーで使用できるアプリケーションのサブセットです。アプリケーション定義は、VDBの更新によって更新され、その後の展開中に Firewall Threat Defense にプッシュされます。

- ユーザー定義のカスタムアプリケーションまたはアプリケーションのグループはサポートされていません。
- 現在、Firewall Management Center ではユーザー定義のカスタムアプリケーションまたはアプリケーションのグループはサポートされておらず、事前定義されたアプリケーションリストを変更することもできません。
- [アプリケーションフィルタ（Application Filters）] にあるフィルタオプションを使用して、このリストを絞り込むことができます。

f) 必要なアプリケーションを選択し、[ルールの追加（Add Rule）] をクリックします。

（注）
- 拡張 ACL オブジェクトで宛先ネットワークとアプリケーションを構成しないでください。
- 各アクセス コントロール エントリで選択されたアプリケーション（ネットワーク サービス オブジェクト）は、ネットワーク サービス グループ（NSG）を形成し、このグループは Firewall Threat Defense で展開されます。NSG は、ダイレクト インターネット アクセスで使用され、選択したアプリケーショングループとの一致に基づいてトラフィックを分類します。

g) [追加（Add）] をクリックして、エントリをオブジェクトに追加します。
h) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

ステップ 4 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 5 [保存（Save）] をクリックします。

標準 ACL オブジェクトの設定

宛先 IPv4 アドレスのみに基づいてトラフィックを照合する場合は、標準 ACL オブジェクトを使用します。それ以外の場合は、拡張 ACL を使用します。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択して、コンテンツテーブルから **[オブジェクト（Objects）]** > **オブジェクト管理（Object Management）]** > **[アクセスリスト（Access List）]** > **[標準（Standard）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [標準アクセスリストの追加（Add Standard Access List）] をクリックして、新しいオブジェクトを作成します。
- [編集（Edit）]（✎） をクリックして、既存のオブジェクトを編集します。

ステップ 3 [新しい標準アクセスリストオブジェクト（New Standard Access List Object）] ダイアログボックスで、オブジェクトの名前を入力し（スペースは使用不可）、アクセス コントロール エントリを設定します。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しいエントリを作成します。
- [編集（Edit）]（✎） をクリックして、既存のエントリを編集します。

b) アクセス コントロール エントリごとに、次のプロパティを設定します。

- [アクション（Action）]：トラフィック基準を許可（一致）またはブロック（不一致）するかどうか。
- [ネットワーク（Network）]：IPv4 ネットワーク オブジェクトまたはトラフィックの宛先を特定するグループを追加します。

c) [追加（Add）] をクリックして、エントリをオブジェクトに追加します。

d) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

ステップ 4 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 5 [保存（Save）] をクリックします。

アドレス プール

クラスタリングの診断インターフェイス、またはVPN リモート アクセス プロファイルに使用できる IPv4 と IPv6 の両方で、IP アドレスプールを設定できます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレスプール（Address Pools）]** を選択します。

ステップ 2 [IPv4プール（IPv4 Pools）] をクリックしてから [IPv4プールの追加（Add IPv4 Pools）] をクリックし、次のフィールドを設定します。

- [名前（Name）]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [説明（Description）]：このプールのオプションの説明を追加します。
- [IP アドレス（IP Address）]：プールで使用できるアドレスの範囲を入力します。ドット付き 10 進表記および最初と最後のアドレスの間でハイフンを使用します。例：10.10.147.100-10.10.147.177。
- [マスク（Mask）]：この IP アドレスプールが常駐するサブネットを指定します。
- [オーバーライドを許可（Allow Overrides）]：このチェックボックスをオンにして、オブジェクトのオーバーライドを有効にします。展開矢印をクリックして、[オーバーライド（Overrides）] テーブルを表示します。[追加（Add）] をクリックして、新たなオーバーライドを追加することができます。詳細については、「オブジェクトのオーバーライド（1310 ページ）」を参照してください。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 [IPv6プール（IPv6 Pools）] をクリックしてから [IPv6プールの追加（Add IPv6 Pools）] をクリックし、次のフィールドを設定します。

- [名前（Name）]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [説明（Description）]：このプールのオプションの説明を追加します。
- [IPv6 アドレス（IPv6 Address）]：設定されたプールで使用できる最初の IP アドレスとビットのプレフィックス長を入力します。たとえば、2001:DB8::1/64 となります。
- [アドレスの数（Number of Addresses）]：開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。
- [オーバーライドを許可（Allow Overrides）]：このチェックボックスをオンにして、オーバーライドを有効にします。展開矢印をクリックして、[オーバーライド（Overrides）] テーブルを表示します。[追加（Add）] をクリックして、新たなオーバーライドを追加することができます。詳細については、「オブジェクトのオーバーライド（1310ページ）」を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

アプリケーション フィルタ

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。オブジェクト マネージャで、システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能アプリケーション フィルタを作成、管理できます。詳細については、アプリケーション ルール条件 （817 ページ）を参照してください。

ASパス

AS パスは BGP のセットアップの必須属性です。これは、ネットワークのアクセスを可能にする AS 番号のシーケンスです。AS パスは、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。異なる AS プレフィックスにリーチする方法に関するメッセージを交換、更新するのに、ネイバー自律システム（ASes）で BGP が使用されます。各ルータで宛先までの最適ルートに関する新たなローカル判断が行われた後、用意されている距離メトリックおよびパス属性とともに、ルートまたはパスの情報がそれぞれのピアに送信されます。この情報がネットワークを移動すると、パスに沿った各ルータは、固有の AS 番号を BGP メッセージの ASes リストの前に付加します。このリストは、ルートの AS パスです。AS パスは AS プレフィックスとともに、ネットワークを介した一方向の中継ルートの特定のハンドルになります。AS パス ページの設定を使用して、自律システム（AS）のパスのポリシー オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、または BGP ネイバー フィルタリングを設定するときに使用する、AS パス オブジェクトを作成できます。AS パスのフィルタにより、正規表現でルーティング アップデート メッセージをフィルタ処理できます。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択して、目次で [AS パス（AS Path）] を選択します。 >

ステップ 2 [AS パスの追加（Add AS Path）] をクリックします。

ステップ 3 [名前（Name）] フィールドに AS パス オブジェクトの名前を入力します。有効な値は、1 ～ 500 です。

ステップ 4 [新しい AS パス オブジェクト（New AS Path Object）] ウィンドウで、[追加（Add）] をクリックします。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [正規表現（Regular Expression）] フィールドで AS パスのフィルタ処理を定義する正規表現を指定します。

c) [追加（Add）] をクリックします。

ステップ 5 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 6 [保存（Save）] をクリックします。

BFD テンプレート

BFD テンプレートは、一連の BFD 間隔値を指定します。BFD テンプレートで指定された BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。また、シングルホップセッションとマルチホップセッションの認証も設定できます。エコーモードはデフォルトで無効になっています。エコーモードはシングルホップでのみ有効にできます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [BFDテンプレート（BFD Template）]**を選択します。

ステップ 2 [BFDテンプレートの追加（Add BFD Template）] または [編集（Edit）] をクリックします。

（注）
テンプレートを編集している場合、テンプレートの名前とタイプは変更できません。

ステップ 3 [Template] タブで、次の項目を設定します。

- [Template Name]：この BFD テンプレートの名前。テンプレートの残りのパラメータを設定するには、名前を割り当てる必要があります。テンプレート名にスペースを含めることはできず、数字だけの名前も指定できません。
- [タイプ（Type）] : [シングルホップ（Single-Hop）] または [マルチホップ（Multi-Hop）] オプションボタンをクリックします。
- [Enable Echo] :（オプション）シングルホップテンプレートでエコーをイネーブルにします。

エコー機能がネゴシエートされない場合、検出時間を満たすように高いレートで BFD 制御パケットが送信されます。エコー機能がネゴシエートされている場合、BFD制御パケットはより低速のネゴシエートされたレートで送信され、自己転送されるエコーパケットはより高速のレートで送信されます。可能であれば、エコーモードを使用することを推奨します。

ステップ 4 [Interval] タブで、次の項目を設定します。

a) [間隔タイプ（Interval Type）] ドロップダウンリストから、[マイクロ秒（Microseconds）]、または [ミリ秒（Milliseconds）] を選択します。

b) [乗数（Multiplier）] フィールドに、ホールドダウン時間の計算に使用する値を入力します。この値は、BFD ピアからの連続して見逃す必要がある BFD 制御パケットの数を示します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。デフォルトは 3 です。

c) [最小伝送（Minimum Transmit）] フィールドに最小伝送間隔機能の値を入力します。範囲は 50 ～ 999 ミリ秒または 50,000 ～ 999,000 マイクロ秒です。

d) [最小受信（Minimum Receive）] フィールドに最小受信間隔機能の値を入力します。範囲は 50 ～ 999 ミリ秒または 50,000 ～ 999,000 マイクロ秒です。

ステップ 5 [Authentication] タブで、次の項目を設定します。

- [認証タイプ（Authentication Type）]：ドロップダウンリストから、[NONE] 、[md5] 、[meticulous-sha-1] 、[meticulous-md5] 、または [sha-1] を選択します。
- [暗号化パスワード（Encrypted Password）]：（任意）認証パスワードの暗号化を有効にします。
- [パスワード（Password）]：認証されているルーティングプロトコルを使用してパケットで送受信される必要がある認証パスワード。有効な値は、1 ～ 29 文字の大文字と小文字の英数字からなる文字列です。ただし、最初の文字は数字にはできず、数字の後に空白を続けることはできません。たとえば、「1password」や「0 password」は無効です。
- [Key ID]：キー値と照合する共有キー ID。指定できる範囲は 0 ～ 255 です。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックして、BFD テンプレート コンフィギュレーションを保存します。

暗号スイート リスト

暗号スイートリストは複数の暗号スイートからなるオブジェクトです。定義済み暗号スイートの値は、SSL または TLS 暗号化セッションのネゴシエートに使われる暗号スイートを表しています。暗号スイートおよび暗号スイート リストを SSL ルールで使用すると、クライアントとサーバが暗号スイートを使って SSL セッションをネゴシエートしたかどうかに基づいて暗号化トラフィックを制御できます。SSL ルールに暗号スイート リストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされた SSL セッションがルールに一致します。

（注） Web インターフェイスでは暗号スイート リストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

暗号スイート リストの作成

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。
ステップ 2 オブジェクト タイプのリストから [暗号スイート リスト（Cipher Suite List）] を選択します。
ステップ 3 [暗号スイートの追加（Add Cipher Suites）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 [使用可能な暗号（Available Ciphers）] リストから、1 つ以上の暗号スイートを選択します。
ステップ 6 [追加（Add）] をクリックします。
ステップ 7 オプションで、[選択された暗号（Selected Ciphers）] リストで、削除する暗号スイートの隣にある[削除（Delete）]（）をクリックします。
ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

コミュニティ リスト

コミュニティは、遷移的 BGP 属性のオプションです。コミュニティは、共通するいくつかの属性を共有する宛先のグループです。これはルート タギングに使用されます。BGP のコミュニティ属性は、特定のプレフィックスに割り当てられ、他のネイバーにアドバタイズされる数値です。コミュニティは、一般的な属性を共有する一連のプレフィックスのマーキングに使用できます。アップストリームプロバイダーは、これらのマーカーを使用して、特定のローカル設定のフィルタリングまたは割り当て、あるいは他の属性の変更などの一般的なルーティングポリシーを適用します。コミュニティ リストの設定ページを使用して、コミュニティ リスト ポリシー オブジェクトを作成、コピー、編集します。ルート マップまたはポリシー マップを設定するときに使用する、コミュニティ リスト ポリシー オブジェクトを作成できます。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。コミュニティ リストは、一致ステートメントの番号付きリストです。接続先は、一致が見つかるまでルールと照合します。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 [オブジェクト（Objects）]>[オブジェクト管理（Object Management）] を選択して、目次で[コミュニティ リスト（Community List）] を選択します。 >

ステップ 2 [コミュニティ リストの追加（Add Community List）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、コミュニティ リスト オブジェクトの名前を指定します。

ステップ 4 [新しいコミュニティ リスト オブジェクト（New Community List Object）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 5 [標準（Standard）] オプション ボタンを選択して、コミュニティ ルールの種類を表示します。

標準コミュニティ リストは、ウェルノウン コミュニティやコミュニティ番号の指定に使用されます。

（注）
標準を使用したエントリ、コミュニティ ルールの拡張種類を使用したエントリを、同じコミュニティ リスト オブジェクトに含めることはできません。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [コミュニティ（Communities）] フィールドで、コミュニティ番号を指定します。有効な値は 1 ～ 4294967295 または 0:1 ～ 65534:65535 です。

c) 適切な [ルート タイプ（Route Type）] を選択します。

- [インターネット（Internet）]：インターネットのウェルノウン コミュニティを指定するために選択します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
- [非アドバタイズ（No Advertise）]：非アドバタイズのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。
- [非エクスポート（No Export）]：非エクスポートのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 6 [拡張（Expanded）] オプション ボタンを選択して、コミュニティ ルールの種類を表示します。

拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ属性の照合パターンの指定に使用されます。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [表現（Expressions）] フィールドで、正規表現を指定します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 9 [保存（Save）] をクリックします。

拡張コミュニティ

拡張コミュニティは、共通するいくつかの属性を共有する宛先の大規模なグループです。BGP 拡張コミュニティリストには、共通の属性を共有する一連のプレフィックスをマークするために使用できる属性があります。それらのマーカーは、仮想ルータ間のルートリークを実装するルートをフィルタ処理するために、ルートマップの match 句で使用されます。フィルタリング用の拡張コミュニティリストを使用してポリシーリストオブジェクトを定義することもできます。拡張コミュニティリストは、一致ステートメントの順序付きリストです。ルートは、指定されたルートターゲット（標準）または正規表現（拡張）と一致するものが見つかるまで、ルールと照合されます。[拡張コミュニティ（Extended Community）] ページを使用して、拡張コミュニティ リスト ポリシー オブジェクトを作成および編集します。

（注） 拡張コミュニティリストは、ルートのインポートまたはエクスポートの設定にのみ適用されます。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次から **[コミュニティリスト（Community List）]** > **[拡張コミュニティ（Extended Community）]** を選択します。

ステップ 2 [拡張コミュニティリストの追加（Add Extended Community List）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、拡張コミュニティ リスト オブジェクトの名前を指定します。名前の長さは 80 文字を超えることはできません。

ステップ 4 拡張コミュニティルールタイプを選択します。

- 1 つ以上のルートターゲットを指定するには、[標準（Standard）] オプションボタンをクリックします。
- 正規表現を指定するには、[拡張（Expanded）] オプションボタンをクリックします。

（注）
同じ拡張コミュニティ リスト オブジェクトに、[標準（Standard）] および [拡張（Expanded）] 拡張コミュニティルールタイプを使用するエントリを含めることはできません。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 拡張コミュニティルールタイプとして [標準（Standard）] を選択した場合は、次の内容を指定します。

a) [シーケンス番号（Sequence No）] フィールドに、ルールを実行する順序を入力します。

シーケンス番号は、リスト内で一意である必要があります。

b) ここで指定したルートターゲットと一致するルートを許可する場合は、[アクション（Action）] ドロップダウンリストから [許可（Allow）] を選択します。ここで指定したルートターゲットと一致するルートを拒否する場合は、[ブロック（Block）] を選択します。

c) [ルートターゲット（Route Target）] フィールドで、ルートターゲットを指定します。

- 1つのエントリに、単一のルートターゲットまたはカンマで区切った一連のルートターゲットを追加できます。例：1:2,1:4,1:6。
- 有効な値は 1:1 ～ 65534:65535 です。
- 1 つのエントリに最大 8 つのルートターゲットを設定できます。
- 複数のエントリに冗長なルートターゲットセットを設定することはできません。たとえば、seq1 に 1:200,100:100,1:300 のルートターゲットを設定し、seq2 に 1:300,100:100,1:200 のルートターゲットを設定するとします。この結果、冗長なルートターゲットセットになり、展開できません。

ステップ 7 拡張コミュニティルールタイプとして [拡張（Expanded）] を選択した場合は、次の内容を指定します。

a) [シーケンス番号（Sequence No）] フィールドに、ルールを実行する順序を入力します。

シーケンス番号は、リスト内で一意である必要があります。

b) ここで指定した正規表現と一致するルートを許可する場合は、[アクション（Action）] ドロップダウンリストから [許可（Allow）] を選択します。ここで指定した正規表現と一致するルートを拒否する場合は、[ブロック（Block）] を選択します。

c) [表現（Expressions）] フィールドで、正規表現を指定します。

- 1 つのエントリに、単一のルートターゲット、またはスペースで区切った一連のルートターゲットを追加できます。例：^((16) | (18)):(.)$。
- エントリには最大 16 の正規表現を追加できます。
- 複数のエントリに冗長な正規表現セットを設定することはできません。たとえば、seq1 に ^((16) | (18)):(.)$ ^4_[0-9]*$ のルートターゲットを設定し、seq2 に ^4_[0-9]*$ ^((16) | (18)):(.)$ のルートターゲットを設定するとします。この結果、冗長な正規表現セットになり、展開できません。

BGP 正規表現の詳細については、こちらを参照してください。

ステップ 8 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 9 [保存（Save）] をクリックします。

拡張コミュニティリストは、ルートマップオブジェクトまたはポリシーリストオブジェクトの match 句で参照できます。

- ルートマップオブジェクトでは、拡張コミュニティリストの名前は **[ルートマップエントリの追加（Add Route Map Entry）]** > **[Match句（Match Clause）]** > **[BGP]** > **[コミュニティリスト（Community List）]** > **[拡張コミュニティリストの追加（Add Extended Community List）]** ダイアログに表示されます。ルートマップでの BGP 設定の設定の詳細については、ルート マップ （1380 ページ）を参照してください。
- ポリシーリストオブジェクトでは、拡張コミュニティリストの名前は、**[ポリシーリストの追加（Add Policy List）]** > **[コミュニティルール（Community Rule）]** > **[拡張コミュニティリストの追加（Add Extended Community List）]** ダイアログに表示されます。ポリシーリストでの BGP 設定の設定の詳細については、ポリシー リスト （1373 ページ）を参照してください。

DHCP IPv6 プール

ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアント（IPv6プレフィックス委任クライアントの有効化 （732ページ））については、DHCP IPv6 プールを定義して DHCPv6 サーバーに割り当てることにより、これらのクライアントが情報要求（IR）パケットを Firewall Threat Defense に送信する際に（DNS サーバー、ドメイン名などの）情報を提供するように Firewall Threat Defense を設定できます。Firewall Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータアドバタイズメントメッセージで受信したプレフィックス（Firewall Threat Defense がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

プールを追加するには、DHCP IPv6 プールの作成 （788 ページ）を参照してください。

識別名

それぞれの識別名オブジェクトは、公開キー証明書のサブジェクトまたは発行元に識別名を表します。TLS/SSL ルールで識別名オブジェクトとグループを使用すると、サブジェクトまたは発行元として識別名を含むサーバー証明書を使ってクライアントとサーバーが TLS/SSL セッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

（識別名グループは、既存の識別名オブジェクトの名前付きコレクションです。）

識別名は、国コード、共通名、組織、および組織単位で構成できますが、通常は共通名のみで構成されます。たとえば、`https://www.cisco.com` の証明書の共通名は `cisco.com` です。（ただし、必ずしも単純な名前とは限りません。共通名を見つける方法については、識別名（DN）のルール条件 （2373ページ）を参照してください）。証明書には、ルール条件で DN として使用できる、複数のサブジェクト代替名（SAN）を含めることができます。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。

共通名を参照する識別名オブジェクトの形式は、CN=*name* です。CN= なしで DN ルール条件を追加すると、オブジェクトを保存する前に CN= が追加されます。

識別名（DN）のルール条件（2373 ページ）で詳しく説明されているように、可能な場合は常に Server Name Indication（SNI）を使用して TLS/SSL ルール内の DN が照合されます。

さらに、次の表に示す各属性を含む識別名を追加することもできます。属性はカンマで区切って使用します。

表 *67* : 識別名の属性

属性	説明	使用可能な値
C	国番号	2 つの英字
CN	共通名	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
O	組織	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
OU	組織単位	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字

DN ルール条件に関する重要な注意事項

- システムが新しいサーバーへの暗号化セッションを最初に検出したときは、DN データを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。

  サーバーで TLS 1.3 が要求される場合、TLS サーバーアイデンティティ検出を設定すると、復号ポリシーの判断が行われる前にサーバー証明書が既知の証明書であることを確認するのに役立ちます。詳細については、アクセスコントロールポリシーの詳細設定（1759 ページ）を参照してください。

- [復号-既知のキー（Decrypt - Known Key）] アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号用のサーバー証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われています。

ワイルドカードの例

ワイルドカードとして 1 つ以上のアスタリスク（*）を属性に定義できます。共通名属性では、ドメイン名ラベルごとに 1 つ以上のアスタリスクを定義できます。ワイルドカードはそのラベルでのみ一致しますが、ワイルドカードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 *68 :* 共通名属性のワイルドカードの例

属性	一致する	一致しない
CN=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

（注） DN オブジェクト `CN=amp.cisco.com` は、`CN=auth.amp.cisco.com` のような CN とは一致しないため、このような場合にワイルドカードを推奨します。

詳細および例については、識別名（DN）のルール条件 （2373 ページ）を参照してください。

関連トピック

識別名（DN）のルール条件 （2373 ページ）

識別名オブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [識別名（Distinguished Name）] ノードを展開し、[個別オブジェクト（Individual Objects）] を選択します。

ステップ 3 [識別名の追加（Add Distinguished Name）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、識別名 （1332ページ）に示されている属性をカンマで区切って含めることができます。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

DNS サーバ グループ

ドメイン ネーム システム（DNS）サーバーは、www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決します。

DNS サーバー グループ オブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

ステップ 2 ネットワーク オブジェクト リストから [DNSサーバー グループ（DNS Server Group）] をクリックします。

ステップ 3 [DNS サーバ グループの追加（Add DNS Server Group）] をクリックします。

ステップ 4 [名前（Name）]を入力します。

ステップ 5 状況に応じて、完全修飾されていないホスト名に追加するために使用される [デフォルト ドメイン（Default Domain）] を入力します。

この設定は、デフォルトのサーバーグループにのみ使用されます。

ステップ 6 デフォルトの [タイムアウト（Timeout）] と [再試行（Retries）] の値は事前入力されています。必要に応じて、これらの値を変更します。

- [再試行（Retries）]：システムが応答を受信しない場合に DNS サーバのリストを再試行する回数（0 ～ 10）。デフォルトは 2 です。
- [タイムアウト（Timeout）]：次の DNS サーバを試行する前に待機する秒数（1 ～ 30）。デフォルト値は 2 秒です。システムがサーバのリストを再試行するたびに、このタイムアウトは 2 倍に増えます。

ステップ 7 このグループの一部になる [DNS サーバ（DNS Servers）] を、IPv4 または IPv6 の形式のカンマ区切りのエントリとして入力します。

1 つのグループには、最大で 6 DNS サーバを含めることができます。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

DNS サーバ グループに設定されている DNS サーバは、DNS プラットフォーム設定でインターフェイス オブジェクトに割り当てる必要があります。詳細については、「DNS （828 ページ）」を参照してください。

外部属性

API で作成したダイナミックオブジェクトについて

ダイナミックオブジェクトは、REST API コールを使用するか、クラウドソースから IP アドレスを更新できる Cisco Secure 動的属性コネクタ を使用して取得した 1 つまたは複数の IP アドレスを指定するオブジェクトです。これらのダイナミック オブジェクトは、オブジェクトへの動的な変更を展開しなくても、アクセス制御ルールで使用できます。

動的属性コネクタ の詳細については、『*Cisco Secure Dynamic Attributes Configuration Guide*』（ガイドへのリンク）を参照してください。https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/200/cisco-secure-dynamic-attributes-connector-v200.html

ダイナミックオブジェクトとネットワークオブジェクトの違いは次のとおりです。

- 動的属性コネクタを使用して作成したダイナミックオブジェクトは、作成されるとすぐに Firewall Management Center にプッシュされ、定期的に更新されます。
- API によって作成されたダイナミックオブジェクト：
  - Classless Inter-Domain Routing（CIDR）の有無にかかわらず、ネットワークオブジェクト同様にアクセスコントロールルールで使用できる IP アドレス。
  - 完全修飾ドメイン名またはアドレス範囲をサポートしていません。
  - API を使用して更新する必要があります。

関連トピック

API で作成したダイナミックオブジェクトの追加または編集 （1336 ページ）

API で作成したダイナミックオブジェクトの追加または編集

この手順では、動的オブジェクトを追加または編集する方法について説明します。動的オブジェクトは、Classless Inter-Domain Routing（CIDR）の有無にかかわらず、ネットワークオブ

ジェクトと同様にアクセス制御ルールで使用できる、APIを使用するIPアドレスのグループです。

（注） Cisco Secure 動的属性コネクタ を使用する場合は、動的オブジェクトが自動的に作成されるため、この手順は不要です。

始める前に

オブジェクトサービスREST APIを使用してIPオブジェクトにアドレスを入力する方法については、『*Firepower Management Center REST API Quick Start Guide*』を参照してください。動的オブジェクトを展開する必要はありません。

手順

ステップ1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** をクリックします。

ステップ2 **[External Attributes]** > **[Dynamic Objects]** をクリックします。

ステップ3 [Add Dynamic Object] または [編集（Edit）]（✎） をクリックします。

ステップ4 オブジェクトの [Name] を入力し、任意で [Description] を入力します。

ステップ5 [Type] リストで [IP] をクリックします。

次のタスク

必要に応じて、APIを使用して動的オブジェクトを更新します。展開する必要はありません。

セキュリティグループタグ

セキュリティ グループ タグ（SGT）オブジェクトは、単一のSGT値を指定します。ルールでSGTオブジェクトを使用して、Cisco ISEで割り当てられたものでは**ない**SGT属性を持つトラフィックを制御できます。SGTオブジェクトをグループ化またはオーバーライドすることはできません。

関連トピック

カスタムセキュリティグループタグ（SGT）からISEセキュリティグループタグ（SGT）への自動遷移

カスタムSGT条件

ISE SGTとカスタムSGTルール条件との比較

セキュリティ グループ タグ オブジェクトの作成

これらのオブジェクトは、グローバルドメインでのみ作成できます。これらのオブジェクトを従来型デバイスで使用するには、制御ライセンスが必要です。スマートライセンスデバイスの場合は、どのライセンスでも使用できます。

始める前に

- ISE/ISE-PIC 接続を無効にします。アイデンティティ ソースとして ISE/ISE-PIC を使用している場合は、カスタム SGT オブジェクトを作成することはできません。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** をクリックします。

ステップ 2 **[外部属性（External Attributes）]** > **[セキュリティグループタグ（Security Group Tag）]** をクリックします。

ステップ 3 [Add Security Group Tag] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 [タグ（Tag）] フィールドに、単一の SGT を入力します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

ファイル リスト

マルウェア防御 を使用しており、AMP クラウドがファイルの性質を誤って特定した場合は、このファイルをファイル リストに追加して、今後さらに検出できます。このファイルは、SHA-256 ハッシュ値を使用して指定されます。各ファイル リストには、一意の SHA-256 値を最大 10000 個まで含めることができます。

ファイル リストには 2 種類の事前定義済みカテゴリがあります。

クリーン リスト

このリストにファイルを追加すると、システムは AMP クラウドがクリーンな性質を割り当てた場合と同様にファイルを扱います。

カスタム検出リスト

このリストにファイルを追加すると、システムは AMP クラウドがマルウェアの性質を割り当てた場合と同様にファイルを扱います。

これらのリストに含まれているファイルに手動でブロッキング動作を指定するため、システムはこれらのファイルの性質について AMP クラウドに照会しません。ファイルの SHA 値を計算するには、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションと [マルウェア ブロック（Block Malware）] アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があります。

⚠

注意 クリーン リストにマルウェアを**含めない**でください。クリーン リストによって、AMP クラウドおよびカスタム検出リストの両方がオーバーライドされます。

ファイル リストのソース ファイル

SHA-256 値のリストと説明を含むコンマ区切り値（CSV）ソース ファイルをアップロードすることによって、複数の SHA-256 値をファイル リストに追加できます。Firewall Management Center はその内容を検証し、有効な SHA-256 値をファイル リストに入れます。

ソース ファイルは、ファイル名拡張子 .csv の単純なテキスト ファイルである必要があります。見出しはポンド記号（#）で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1 つの SHA-256 値の後に説明が含まれる必要があり、LF または CR+LF 改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべての SHA-256 ハッシュもファイル リストから削除されます。
- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイル リストに含まれる場合は、複数のファイルをファイル リストにアップロードすることはできません。
- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にカンマを含める場合は、エスケープ文字（\）を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。
- 重複しないすべての SHA-256 値がこのファイル リストに追加されます。すでにファイル リストに存在する SHA-256 値を含むソース ファイルをアップロードした場合、新しくアップロードされた値によって既存の SHA--256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイル イベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。
- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。

- アップロードされた複数のソース ファイル内に同じ SHA--256 値に関するエントリが含まれる場合、システムは最も新しい値を使用します。
- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソースファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。
- ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイル リストからソース ファイルを削除すると、ファイル リストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

ファイル リスト別の SHA-256 値の追加

この手順を実行するには、マルウェア防御 ライセンスが必要です。

ファイルの SHA-256 値を送信して、それをファイル リストに追加できます。重複する SHA-256 値は追加できません。

始める前に

- イベント ビューからファイルまたはマルウェア イベントを右クリックし、コンテキスト メニューで [フル テキストの表示（Show Full Text）] を選択し、ファイルの SHA-256 値全体をコピーし、ファイルリストに貼り付けます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーンリストまたはカスタム検出リストの横の[編集（Edit）]（）をクリックします。

代わりに [表示（View）]（） が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加元（Add by）] ドロップダウンリストから [SHA 値の入力（Enter SHA Value）] を選択します。

ステップ 5 [説明（Description）] フィールドにソース ファイルの説明を入力します。

ステップ 6 [SHA-256] フィールドにファイル全体の値を入力し、または貼り付けます。システムでは値の部分的な一致はサポートされません。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストへの個々のファイルのアップロード

この手順を実行するには、マルウェア防御 ライセンスが必要です。

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルを Secure Firewall Management Center にアップロードできます。システムはファイルの SHA-256 値を計算し、ファイルをリストに追加します。SHA-256 を計算するとき、システムはファイル サイズを制限しません。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーンリストまたはカスタム検出リストの横の[編集（Edit）]（）をクリックします。

代わりに [表示（View）]（） が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加（Add by）] ドロップダウン リストから、[SHA の計算（Calculate SHA）] を選択します。

ステップ 5 オプションで、[Description] フィールドにファイルの説明を入力します。説明を入力しない場合、アップロード時にファイル名が説明として使用されます。

ステップ 6 [参照（Browse）] をクリックし、アップロードするファイルを選択します。

ステップ 7 [SHA の計算と追加（Calculate and Add SHA）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

（注） 設定の変更を導入すると、その後システムはそのリストのファイルを AMP クラウドでクエリしなくなります。

ファイル リストへのソース ファイルのアップロード

この手順を実行するには、マルウェア防御 ライセンスが必要です。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ソースファイルからの値の追加先となるファイルリストの横にある[編集（Edit）]（✎）をクリックします。

代わりに [表示（View）]（👁） が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加方法（**Add by**）] ドロップダウン リストで [SHA のリスト（List of SHAs）] を選択します。

ステップ 5 オプションで、[Description] フィールドにソース ファイルの説明を入力します。説明を入力しない場合、システムはファイル名を使用します。

ステップ 6 [参照（Browse）] をクリックしてソース ファイルを参照してから、[リストのアップロードと追加（Upload and Add List）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

（注） ポリシーを展開したら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストの SHA-256 値の編集

この手順を実行するには、マルウェア防御 ライセンスが必要です。

ファイル リストの個々の SHA-256 値を編集または削除することができます。オブジェクト マネージャ内でソース ファイルを直接編集できないことに注意してください。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ファイルの変更場所となるクリーンリストまたはカスタム検出リストの横の [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 次の操作を実行できます。

- 変更する SHA-256 値の横にある [編集（Edit）]（） をクリックし、必要に応じて [SHA-256] または [説明（Description）] の値を変更します。
- 削除する SHA-256 値の横にある [削除（Delete）]（） をクリックします。

ステップ 5 [保存（Save）] をクリックし、リストのファイル エントリを更新します。

ステップ 6 [保存（Save）] をクリックして、ファイル リストを保存します。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストからソース ファイルをダウンロードする

この手順を実行するには、マルウェア防御 ライセンスが必要です。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ソースファイルのダウンロード対象となるクリーンリストまたはカスタム検出リストの横の [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 ダウンロードするソースファイルの横にある [表示（View）]（👁） をクリックします。

ステップ 5 [SHA リストのダウンロード（Download SHA List）] をクリックし、プロンプトに従ってソース ファイルを保存します。

ステップ 6 [閉じる（Close）] をクリックします。

FlexConfig

FlexConfig ポリシーで FlexConfig ポリシー オブジェクトを使用して、他の方法では Secure Firewall Management Center を使用して設定できない Firewall Threat Defense デバイスの機能のカスタマイズされた設定を指定します。FlexConfig ポリシーの詳細については、FlexConfig ポリシーの概要 （2687 ページ）を参照してください。

FlexConfig の次のタイプのオブジェクトを設定できます。

テキスト オブジェクト

テキスト オブジェクトは、FlexConfig オブジェクトで変数として使用する自由形式のテキスト文字列を定義します。このオブジェクトに単一の値を設定したり、このオブジェクトを複数の値のリストにしたりすることができます。

事前定義済みの FlexConfig オブジェクトで使用される複数の事前定義済みテキスト オブジェクトがあります。関連付けられている FlexConfig オブジェクトを使用する場合は、単に、テキスト オブジェクトの内容を編集して、FlexConfig オブジェクトによる特定のデバイスの設定方法をカスタマイズすることだけが必要です。事前定義済みのオブジェクトを編集するには、一般に、これらのオブジェクトのデフォルト値を直接変更するのではなく、設定しているデバイスごとにデバイスの上書きを作成することをお勧めします。これは、他のユーザが別の一連のデバイスに同じ FlexConfig オブジェクトを使用する場合に、意図しない結果が発生しないようにするのに役立ちます。

テキスト オブジェクトの設定については、FlexConfig テキスト オブジェクトの設定 （2720 ページ）を参照してください。

FlexConfig オブジェクト

FlexConfig オブジェクトには、デバイス設定コマンド、変数、およびスクリプト言語の手順が含まれています。導入展開時に、これらの手順が処理されて、一連の設定コマンドが、ターゲットデバイスで特定の機能を設定するカスタマイズされたパラメータとともに作成されます。

これらの手順は、通常の Firewall Management Center ポリシーで定義されている機能が設定される前（先頭に付加）または後（付加）に設定されます。Secure Firewall Management Center で設定されたオブジェクト（ネットワーク オブジェクトなど）に依存する FlexConfig は、設定展開に付加される必要があります。付加されない場合、必要なオブジェクトが、FlexConfig がこのオブジェクトを参照する必要がある前に設定されません。

FlexConfig オブジェクトの設定の詳細については、FlexConfig オブジェクトの設定 （2714 ページ）を参照してください。

位置情報

設定済みの位置情報（ジオロケーション）オブジェクトは、モニタ対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。アクセス コントロール ポリシー、SSL ポリシー、リモートアクセス VPN、イベント検索など、システムの Web インターフェイスのさまざまな場所で地理位置情報オブジェクトを使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセス コントロール ルールを作成できます。

常に最新の情報を使用してネットワーク トラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

地理位置情報オブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [地理位置情報（Geolocation）] を選択します。

ステップ 3 [位置情報の追加（Add Geolocation）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 地理位置情報オブジェクトに含める国および大陸のチェック ボックスを選択します。大陸を選択すると、その大陸内のすべての国、および GeoDB 更新によってその大陸に今後追加されるすべての国が選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

インターフェイス（Interface）

各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てることができます。その上で、ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、「内部」インターフェイスを「内部」ゾーンに割り当て、「外部」インターフェイスを「外部」ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、外部から内部に向けては設定できません。ポリシーによっては、セキュリティゾーンだけをサポートする場合も、ゾーンとグループの両方をサポートする場合もあります。

インターフェイス オブジェクトの詳細については、セキュリティ ゾーンとインターフェイス グループ （631 ページ）を参照してください。

インターフェイス オブジェクトの追加方法については、セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成 （634 ページ）を参照してください。

Key Chain

デバイスのデータセキュリティと保護を向上させるため、IGP ピアを認証するために 180 日以下の期間の循環キーが展開されています。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キーチェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。循環キーは OSPFv2 プロトコルにのみ適用されます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

（注） 認証に使用されるのは MD5 暗号化アルゴリズムのみです。

キーのライフタイム

安定した通信を維持するためには、各デバイスがキー チェーンの認証キーを保存し、複数のキーを同時に機能に使用します。キーの送信と受け入れのライフタイムに基づき、キーのロールオーバーを処理するセキュアなメカニズムがキーチェーン管理によって提供されます。デバイスは、キーのライフタイムを使用してキーチェーン内でアクティブになっているキーを判断します。

キー チェーン内の各キーには 2 つのライフタイムがあります。

- 受け入れライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
- 送信ライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイム中、デバイスはルーティング アップデート パケットをキーとともに送信します。送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

ライフタイムが設定されていない場合は、タイムラインなしで MD5 認証を設定するのと同じことになります。

キーの選択

- キー チェンに複数の有効なキーがある場合、OSPF はライフタイムが最大のキーを選択します。
- ライフタイムが無限のキーが優先されます。
- ライフタイムが同じキーが複数ある場合は、もっとも大きなキー ID を持つキーが優先されます。

キー チェーンのオブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [キー チェーン（Key Chain）] を選択します。

ステップ 3 [キー チェーンの追加（Add Key Chain）] をクリックします。

ステップ 4 [キー チェーン オブジェクトの追加（Add Key Chain Object）] ダイアログボックスで、キー チェーンの名前を [名前（Name）] フィールドに入力します。

名前はアンダースコアまたはアルファベットから開始し、英数字文字または特殊文字（-、_、+、 .）を続けます。

ステップ 5 キーをキー チェーンに追加するには、[追加（Add）] をクリックします。

ステップ 6 [キー ID（Key ID）] フィールドにキー識別子を指定します。

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

ステップ 7 [アルゴリズム（Algorithm）] フィールドと [暗号化タイプ（Crypto Encryption Type）] フィールドにサポート対象のアルゴリズムと暗号化タイプ、つまり [MD5] と [プレーン テキスト（Plain Text）] がそれぞれ表示されます。

ステップ 8 [暗号キー文字列（Crypto Key String）] フィールドにパスワードを入力し、[暗号キー文字列の確認（Confirm Crypto Key String）] フィールドにパスワードを再入力します。

- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

ステップ 9 デバイスが他のデバイスとキー交換をしている間にキーを受領/送信する時間間隔をデバイスに設定するには、[受け入れライフタイム（Accept Lifetime）] フィールドと [送信ライフタイム（Send Lifetime）] フィールドにライフタイムの値を指定します。

（注）
デフォルトでは、日時の値は UTC タイムゾーンになります。

終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無期限です。デフォルトの終了時刻は、DateTime です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、それぞれの終了時刻よりも前である必要があります。

ステップ 10 [追加（Add）] をクリックします。

ステップ 5 ～ 10 を繰り返してキーを作成します。キー チェーンにはライフタイムが重複するキーを 2 つ以上作成します。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。

ステップ 11 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （1312ページ）を参照）。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

ネットワーク

ネットワーク オブジェクトは 1 つ以上の IP アドレスを表します。ネットワークオブジェクトおよびグループは、アクセス コントロール ポリシー、ネットワーク変数、アイデンティティ ルール、ネットワーク検出ルール、イベント検索、レポート、ID ポリシーなど、さまざまな場所で使用できます。

ネットワーク オブジェクトを必要とするオプションを設定する際は、リストが自動的にフィルタリングされて、そのオプションに有効なネットワーク オブジェクトだけが表示されます。たとえば、オプションのなかにはホスト オブジェクトが必要なものと、サブネットが必要なものがあります。

ネットワーク オブジェクトには、以下のいずれかのタイプを指定できます。

ホスト

単一の IP アドレス。

IPv4 の例：

```
209.165.200.225
```

IPv6 の例：

```
2001:DB8::0DB8:800:200C:417A
```
または
```
2001:DB8:0:0:0DB8:800:200C:417A
```

範囲

IP アドレスの範囲。

IPv4 の例：

```
209.165.200.225-209.165.200.250
```

IPv6 の例：

```
2001:db8:0:cd30::1-2001:db8:0:cd30::1000
```

ネットワーク（Network）

アドレス ブロック（別名サブネット）。

IPv4 の例：

```
209.165.200.224/27
```

IPv6 の例：

```
2001:DB8:0:CD30::/60
```

（注） セキュリティ インテリジェンスは、`/0` ネットマスクを使用して、IP アドレス ブロックを無視します。

[FQDN]

単独の完全修飾ドメイン名（FQDN）FQDN 解決を IPv4 アドレスのみ、IPv6 アドレスのみ、または IPv4 と IPv6 アドレスの両方に制限できます。FQDN は、数字または文字で始まって終わる必要があります。FQDN で内部文字として使用できるのは、文字、数字、およびハイフンだけです。

次に例を示します。

```
www.example.com
```

（注） FQDN オブジェクトは、アクセスコントロールルールとプレフィルタルールまたは手動 NAT ルールのみで使用できます。ルールは、DNS ルックアップを介して FQDN で取得された IP アドレスを一致させます。FQDN ネットワーク オブジェクトを使用するには、DNS サーバー設定を DNS サーバ グループ（1335 ページ） で設定し、DNS プラットフォーム設定を DNS （828 ページ） で設定していることを確認します。

アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

グループ

ネットワーク オブジェクトまたは他のネットワーク グループからなるグループ。あるネットワーク オブジェクト グループを別のネットワーク オブジェクト グループに追加することで、ネストされたグループを作成できます。グループをネストできるレベルは、最大で 10 レベルです。

ネットワーク ワイルドカード マスク

[オブジェクト管理（Object Management）] ページで、ワイルドカード マスク オブジェクトを作成および管理できます。

拡張サブネット IP アドレスを持つネットワークオブジェクトを作成できます。既存のネットワークオブジェクトは、ネットワークオブジェクトとネットワーク ワイルドカード オブジェクトの両方をサポートするように拡張されています。ワイルドカードマスクを使用するネットワークオブジェクトは、ネットワーク オブジェクト リスト ページの [タイプ（Type）] 列に [ネットワークワイルドカード（Network Wildcard）] としてリストされます。

ワイルドカードマスクは、ビットの不連続なマスクである IP アドレスです。連続したマスクを使用して標準ネットワークオブジェクトを作成し、不連続のマスクを使用してワイルドカード ネットワーク オブジェクトを作成できます。

IP アドレスの例	ネットワークワイルドカード ?	オブジェクト タイプ
192.0.0.0/8	なし	ネットワーク
10.10.0.0/255.255.0.0	なし	ネットワーク

IP アドレスの例	ネットワークワイルドカード?	オブジェクト タイプ
10.10.0.10/255.255.0.255	対応	ネットワークワイルドカード
72.0.240.10/255.255.240.255	対応	ネットワークワイルドカード

（注） ネットワーク ワイルドカード オブジェクトと、ネットワーク ワイルドカード オブジェクトを含むオブジェクトグループは、次のポリシーを設定している場合にのみ許可されます。

- プレフィルタ ポリシー
- アクセス コントロール ポリシー
- NAT ポリシー

注意事項と制約事項

- ネットワーク ワイルドカード オブジェクトを作成するには、Firewall Management Center UI で**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[ネットワーク（Network）]**を選択し、[ネットワークの追加（Add Network）] をクリックしてから [オブジェクトの追加（Add Object）] をクリックします。[ネットワーク（Network）] オプションを選択し、拡張サブネットマスクの値を入力します。例：10.0.10.10/255.255.0.255
- オブジェクトのオーバーライド、グループオブジェクトのサポート、グループオブジェクトのオーバーライド、ワイルドカードリテラル、およびワイルドカードオブジェクトのインポートがサポートされています。
- ネットワーク ワイルドカード オブジェクトは、IPv4 アドレスに対してのみサポートされます。
- ネットワーク ワイルドカード オブジェクトは、Firewall Management Center および Firewall Threat Defense 7.1 バージョン以降でサポートされます。
- ネットワーク ワイルドカード オブジェクトは、Snort-3 でのみサポートされます。

ネットワーク オブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
ステップ 2 オブジェクト タイプのリストから [ネットワーク（Network）] を選択します。

ステップ 3 [ネットワークを追加（Add Network）] ドロップダウン メニューで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 [ネットワーク（Network）] フィールドで、必要なオプションを選択して適切な値を入力します（ネットワーク （1349 ページ）を参照）。

ステップ 7 （FQDN オブジェクトのみ）[ルックアップ（Lookup）] ドロップダウン メニューから DNS 解決を選択して、IPv4、IPv6、または IPv4 と IPv6 の両方のアドレスを FQDN に関連付けるかを決定します。

ステップ 8 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （1312 ページ）を参照）。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

ネットワークオブジェクトのインポート

ネットワークオブジェクトのインポートの詳細については、オブジェクトのインポート （1303 ページ）を参照してください。

PKI

SSL アプリケーションの PKI オブジェクト

PKI オブジェクトは、導入をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局（CA）証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバー証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。

信頼できる認証局オブジェクトと内部証明書オブジェクトを使用して ISE/ISE-PIC への接続を設定する場合、ISE/ISE-PIC をアイデンティティ ソースとして使用できます。

内部証明書オブジェクトを使用してキャプティブ ポータルを設定する場合、システムはキャプティブ ポータル デバイスがユーザの Web ブラウザに接続する際に、デバイスのアイデンティティを検証できます。

信頼できる認証局オブジェクトを使用してレルムを設定する場合、LDAP または AD サーバへのセキュア接続を設定できます。

SSL ルールで PKI オブジェクトを使用する場合、以下のものを使用して暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

SSL ルールで PKI オブジェクトを使用する場合、以下のものを復号できます。

- 発信トラフィック：内部 CA オブジェクトを使ってサーバ証明書を再署名することによって復号します
- 受信トラフィック：内部証明書オブジェクトにある既知の秘密鍵を使用して復号します

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、システムは証明書のサブジェクト識別名をオブジェクト値として表示します。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。証明書に関する他の詳細を表示するには、PKI オブジェクトを編集します。

（注） Firewall Management Center および管理対象デバイスは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密キーを、保存前にランダムに生成されたキーを使って暗号化します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使って秘密キーを復号し、ランダムに生成されたキーを使ってそれを再暗号化してから保存します。

証明書の登録の PKI オブジェクト

証明書の登録オブジェクトには、証明書署名要求（CSR）を作成したり、指定された CA からアイデンティティ証明書を取得したりするために必要な証明機関（CA）サーバ情報や登録パラメータが含まれています。これらのアクティビティは、秘密キー インフラストラクチャ（PKI）で発生します。

証明書の登録オブジェクトには、証明書失効情報も含まれている場合があります。PKI、デジタル証明書、および証明書の登録の詳細については、PKI インフラストラクチャとデジタル証明書 （1479 ページ） を参照してください。

内部認証局オブジェクト

設定されたそれぞれの内部認証局（CA）オブジェクトは、組織で制御されるCAのCA公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA 証明書、およびペアになった秘密鍵からなります。SSL ルールで内部 CA オブジェクトとグループを使用すると、内部 CA によってサーバ証明書に再署名することにより、発信する暗号化トラフィックを復号できます。

（注） [復号 - 再署名（Decrypt - Resign）] SSL ルールで内部 CA オブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSLハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザーのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメイン リストに内部CAオブジェクト証明書を追加します。

次の方法で内部 CA オブジェクトを作成できます。

- RSA ベースまたは楕円曲線ベースの既存の CA 証明書と秘密キーをインポートする
- 新しい RSA ベースの自己署名 CA 証明書と秘密キーを生成する
- RSA ベースの未署名の CA 証明書と秘密キーを生成する内部 CA オブジェクトを使用する前に、証明書に署名するために証明書署名要求（CSR）を別の CA に送信する必要があります。

署名付き証明書を含む内部CAオブジェクトを作成した後で、CA証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システムで生成された場合でも、ユーザによって作成された場合でも、内部CAオブジェクトの名前は変更できますが、他のオブジェクト プロパティは変更できません。

使用中の内部 CA オブジェクトは削除できません。さらに、SSL ポリシーで使用される内部CAオブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を有効にするには、アクセス コントロール ポリシーを再度展開する必要があります。

CA 証明書と秘密キーのインポート

X.509 v3 CA 証明書と秘密キーをインポートすることによって、内部 CA オブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

秘密キー ファイルがパスワード保護されている場合は、復号パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

（注） ルールに [復号 - 再署名（Decrypt - Resign）] アクションを設定すると、そのルールでは、設定されているルール条件に加えて、参照される内部 CA 証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号するには、楕円曲線ベースの CA 証明書をアップロードする必要があります。

CA 証明書および秘密キーのインポート

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA のインポート（Import CA）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロード ファイルがパスワード保護されている場合は、[暗号化および次のパスワード:（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

新しい CA 証明書と秘密キーの生成

識別情報を提供することで、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。

生成される CA 証明書の有効期間は 10 年です。[有効期間の開始（Valid From）] の日付は、生成の一週間前です。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。
ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。
ステップ 3 [CA の生成（Generate CA）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ID 属性を入力します。
ステップ 6 [自己署名 CA の生成（Generate self-signed CA）] をクリックします。

新しい署名付き証明書

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求（CSR）が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できます。

未署名の CA 証明書と CSR の作成

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。
ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。
ステップ 3 [CA の生成（Generate CA）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ID 属性を入力します。
ステップ 6 [Generate CSR] をクリックします。
ステップ 7 CA に送信するために CSR をコピーします。
ステップ 8 [OK] をクリックします。

次のタスク

- CA によって発行される署名済み証明書をアップロードする必要があります。次のページを参照してください。CSR への応答として発行された署名付き証明書のアップロード（1357 ページ）

CSR への応答として発行された署名付き証明書のアップロード

一度アップロードすると、署名付き証明書は SSL ルールで参照できます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 CSR を待機している未署名の証明書を含む CA オブジェクトの横の [編集（Edit）]（） をクリックします。

ステップ 4 [Install Certificate] をクリックします。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 アップロード ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェック ボックスをオンにして、パスワードを入力します。

ステップ 7 [保存（Save）] をクリックして、CA オブジェクトに署名付き証明書をアップロードします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

CA 証明書および秘密キーのダウンロード

証明書および鍵の情報を含むファイルを内部 CA オブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。

注意 ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロードファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。

⚠

注意 システムバックアップの一部としてダウンロードされる秘密鍵は、復号されてから、非暗号化バックアップ ファイルに保存されます。

CA 証明書および秘密キーのダウンロード

現在のドメインおよび先祖ドメインの両方の CA 証明書をダウンロードできます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 証明書および秘密キーをダウンロードする対象となる内部CAオブジェクトの横の[編集（Edit）]（✎） をクリックします。

ステップ 4 [Download] をクリックします。

ステップ 5 [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに、暗号化パスワードを入力します。

ステップ 6 **[OK]** をクリックします。

信頼できる認証局オブジェクト

設定した信頼できる認証局（CA）オブジェクトは、それぞれ信頼できるCAに属するCA公開鍵証明書を表します。このオブジェクトは、オブジェクト名と CA 公開鍵証明書からなります。次のものに設定された外部 CA オブジェクトとグループを使用できます。

- 信頼できる CA、または信頼チェーン内のいずれかの CA によって署名された証明書で暗号化されたトラフィックを制御するための SSL ポリシー。
- LDAP または AD サーバへのセキュアな接続を確立するためのレルムの設定。
- ISE/ISE-PIC 接続。[pxGrid サーバ CA（pxGrid Server CA）] フィールドと [MNT サーバ CA（MNT Server CA）] フィールドで信頼できる認証局オブジェクトを選択します。

信頼できる CA オブジェクトを作成した後で、その名前を変更したり、証明書失効リスト（CRL）を追加したりすることはできますが、他のオブジェクトプロパティを変更することはできません。オブジェクトに追加できるCRLの数には制限がありません。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

（注） オブジェクトが ISE/ISE-PIC 統合設定で使用されている場合は、オブジェクトに CRL を追加しても影響はありません。

使用中の信頼できる CA オブジェクトを削除することはできません。また、使用中の信頼できる CA オブジェクトを編集すると、関連付けられているアクセス コントロール ポリシーが最新ではなくなります。変更を有効にするには、アクセス コントロール ポリシーを再度展開する必要があります。

信頼できる CA オブジェクト

外部 CA オブジェクトは、X.509 v3 CA 証明書をアップロードすることによって設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワードで保護されている場合は、復号パスワードを提供する必要があります。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA 証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

信頼できる CA オブジェクトの追加

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 [PKI] ノードを展開し、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3 [信頼できる CA の追加（Add Trusted CAs）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 ファイルがパスワード保護されている場合は、[暗号化、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

信頼できる CA オブジェクトの証明書失効リスト

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

CRL を追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切な CRL を含んでいるファイルのみをアップロードできます。信頼できる CA オブジェクトに追加できる CRL の数には制限がありません。ただし、CRL をアップロードした場合、別の CRL を追加する前に、オブジェクトをその都度保存する必要があります。

（注） オブジェクトが ISE/ISE-PIC 統合設定で使用されている場合は、オブジェクトに CRL を追加しても影響はありません。

信頼できる CA オブジェクトへの証明書失効リストの追加

（注） オブジェクトが ISE/ISE-PIC 統合設定で使用されている場合は、オブジェクトに CRL を追加しても影響はありません。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 [PKI] ノードを展開し、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3 信頼できる CA オブジェクトの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [CRL の追加（Add CRL）] をクリックして、DER または PEM でエンコードされた CRL ファイルをアップロードします。

ステップ 5 **[OK]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

外部証明書オブジェクト

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSL ルールで外部証明書オブジェクトとグループを使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。たとえば、信頼できる自己署名サーバ証明書をアップロードできますが、信頼できる CA 証明書を使って検証することはできません。

X.509 v3 サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

外部証明書オブジェクトの追加

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[外部証明書（External Certs）] を選択します。

ステップ 3 [外部証明書の追加（Add External Cert）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバー証明書ファイルをアップロードします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

内部証明書オブジェクト

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。内部証明書オブジェクトとグループは、以下で使用することができます。

- SSL ルール。既知の秘密キーを使用する組織のサーバの 1 つに着信するトラフィックを復号します。
- ISE/ISE-PIC 接続。[MC サーバ証明書（MC Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。
- キャプティブ ポータル設定。ユーザの Web ブラウザに接続する際にキャプティブ ポータル デバイスのアイデンティティを認証するように設定します。[サーバ証明書（Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。

X.509 v3 RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることにより、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワードで保護されている場合は、復号パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、使用中の内部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を有効にするには、アクセス コントロール ポリシーを再度展開する必要があります。

内部証明書オブジェクトの追加

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部証明書（Internal Certs）] を選択します。

ステップ 3 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバー証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロードする秘密キー ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 [保存（Save）] をクリックします。

証明書の登録オブジェクト

トラストポイントを使用すると、CA と証明書の管理およびトラックを行えます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

証明書の登録オブジェクトには、証明書署名要求（CSR）を作成したり、指定された CA からアイデンティティ証明書を取得したりするために必要な証明機関（CA）サーバ情報や登録パラメータが含まれています。これらのアクティビティは、秘密キー インフラストラクチャ（PKI）で発生します。

証明書の登録オブジェクトには、証明書失効情報も含まれている場合があります。PKI、デジタル証明書、および証明書の登録の詳細については、PKI インフラストラクチャとデジタル証明書 （1479 ページ） を参照してください。

証明書の登録オブジェクト の使用方法

証明書の登録オブジェクト は、管理対象デバイスを PKI インフラストラクチャに登録し、以下を実行することで VPN 接続をサポートするデバイス上にトラストポイント（CA オブジェクト）を作成するために使用されます。

1. 証明書の登録オブジェクトの CA 認証と登録のパラメータを定義します。共有パラメータを指定し、オーバーライド機能を使用して、異なるデバイスに固有のオブジェクト設定を指定します。
2. アイデンティティ証明書を必要とする各管理対象デバイスにこのオブジェクトを関連付けてインストールします。デバイス上で、そのオブジェクトはトラストポイントになります。

   証明書の登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに証明書の登録プロセスが開始されます。プロセスは、自己署名、SCEP、EST、およ

び PKCS12 ファイル登録タイプの場合は自動的に行われます。つまり、管理者による追加の操作は必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。

3. 作成されたトラストポイントを VPN の設定で指定します。

証明書の登録オブジェクト の管理

証明書の登録オブジェクト を管理するには、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動し、ナビゲーション ウィンドウから [PKI] > [証明書の登録（Certificate Enrollment）] を選択します。次の情報が表示されます。

- 既存の証明書の登録オブジェクトが [名前（Name）] 列に表示されます。

  リストをフィルタリングするには検索フィールド（虫めがね）を使用します。

- 各オブジェクトの登録タイプが [タイプ（Type）] 列に表示されます。次の登録方式を使用できます。

  - [自署（Self Signed）]：管理対象デバイスが独自の自己署名ルート証明書を生成します。
  - [EST]：Enrollment over Secure Transport は、CA からアイデンティティ証明書を取得するためにデバイスによって使用されます。
  - [SCEP]：（デフォルト）Simple Certificate Enrollment Protocol は、CA からアイデンティティ証明書を取得するためにデバイスで使用されます。
  - [手動（Manual）]：登録のプロセスは、管理者によって手動で実行されます。
  - [PKCS12 ファイル（PKCS12 File）]：VPN 接続をサポートしている Firewall Threat Defense 管理対象デバイスの PKCS 12 ファイルをインポートします。PKCS#12（PFX または P12）ファイルとは、サーバ証明書、中間証明書、秘密キーのすべてを暗号化して保持するファイルです。復号のための [パスフレーズ（Passphrase）] 値を入力します。

- [オーバーライド（Override）] 列は、オブジェクトがオーバーライド（緑のチェック マーク）を許可するかしないか（赤の X）を示します。数が表示される場合、これはオーバーライドの数です。

  [オーバーライド（Override）] オプションを使用して、VPN 設定の一部である各デバイスのオブジェクト設定をカスタマイズします。オーバーライドすると、各デバイスのトラストポイントの詳細が一意になります。通常、共通名またはサブジェクトは、VPN の設定内の各デバイスに対して上書きされます。

  任意のタイプのオブジェクトのオーバーライドに関する詳細および手順については、オブジェクトのオーバーライド （1310 ページ）を参照してください。

- 編集アイコン（鉛筆）をクリックして、前に作成した 証明書の登録オブジェクト を**編集**します。編集は、登録オブジェクトがどの管理対象デバイスにも関連付けられていない場合にのみ実行できます。証明書の登録オブジェクトの編集については、追加の手順を参照してください。失敗した登録オブジェクトを編集できます。

- 削除アイコン（ごみ箱）をクリックして、前に作成した 証明書の登録オブジェクト を**削除**します。管理対象デバイスに関連付けられている証明書の登録オブジェクトは削除できません。

（＋） [証明書登録の追加（Add Cert Enrollment）] をクリックして、[証明書登録の追加（Add Cert Enrollment）] ダイアログを開き、証明書の登録オブジェクト を設定します。証明書の登録オブジェクトの追加（1365ページ）を参照してください。次に、管理対象のヘッドエンドデバイスごとに証明書をインストールします。

関連トピック

自己署名登録を使用した証明書のインストール （1460 ページ）
EST 登録を使用した証明書のインストール （1461 ページ）
SCEP の登録を使用した証明書のインストール （1462 ページ）
手動登録を使用した証明書のインストール （1463 ページ）
PKCS12 ファイルを使用した証明書のインストール （1464 ページ）

証明書の登録オブジェクトの追加

これらのオブジェクトはFirewall Threat Defenseデバイスで使用できます。このタスクを実行するには、管理者権限またはネットワーク管理者権限が必要です。

手順

ステップ1 以下の方法のいずれかにより、[証明書登録の追加（Add Cert Enrollment）] ダイアログを開きます。

- オブジェクト管理から直接開く：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] 画面で、[ナビゲーション（Navigation）] ペインの [PKI] > [証明書の登録（Cert Enrollment）] を選択し、[証明書の登録の追加（Add Cert Enrollment）] を押します。
- 管理対象デバイスの設定中に開く：[デバイス（Devices）] > [証明書（Certificates）] 画面で、[追加（Add）] > [新しい証明書の追加（Add New Certificate）] を選択し、[証明書の登録（Certificate Enrollment）] フィールドの （＋） をクリックします。

ステップ2 [名前（Name）] を入力し、任意で登録するオブジェクトの [説明（Description）] を入力します。

登録が完了すると、この名前が関連付けられた管理対象デバイスのトラストポイントの名前になります。

ステップ3 [CA 情報（CA Information）] タブを開いてから、[登録タイプ（Enrollment Type）] を選択します。

- [自己署名証明書（Self-Signed Certificate）]：管理対象デバイスが CA として機能し、自己の署名付きルート証明書を生成します。このペインでは、さらに必要となる情報はありません。

（注）
自己署名証明書を登録するときには、証明書パラメータで共通名（CN）を指定する必要があります。

- [EST]：Enrollment over Secure Transport プロトコル。EST 情報を指定します。「証明書の登録オブジェクト EST オプション （1367 ページ）」を参照してください。
- [SCEP]：（デフォルト）Simple Certificate Enrollment Protocol。SCEP 情報を指定します。証明書の登録オブジェクト SCEP オプション （1368 ページ）を参照してください。
- **[手動（Manual）]**
  - [CAのみ（CA Only）]：選択したCAからCA証明書のみを作成するには、このチェックボックスをオンにします。この証明書のアイデンティティ証明書は作成されません。

    このチェックボックスをオンにしない場合、CA証明書は必須ではありません。CA証明書がなくてもCSRを生成し、アイデンティティ証明書を取得することができます。
  - [CA証明書（CA Certificate）]：CA 証明書を PEM 形式でボックスに貼り付けます。CA 証明書は別のデバイスからコピーして取得することもできます。

    CA 証明書なしで CSR を生成する場合は、このボックスを空のままにできます。
- [PKCS12 ファイル（PKCS12 File）]：VPN 接続をサポートしている Firewall Threat Defense 管理対象デバイスの PKCS 12 ファイルをインポートします。PKCS#12 ファイル、または PFX ファイルは、サーバー証明書、中間証明書、秘密キーが含まれる単一の暗号化ファイルです。 Enter the **Passphrase** value for decryption.
- [CA証明書の基本的な制約のCAフラグチェックをスキップする（Skip Check for CA flag in basic constraints of the CA Certificate）]：トラストポイント証明書の基本制約の拡張と CA フラグのチェックをスキップする場合は、このチェックボックスをオンにします。
- [検証用法（Validation Usage）]：VPN 接続中に証明書を検証するオプションから選択します。
  - [IPsecクライアント（IPsec Client）]：サイト間 VPN 接続の IPSec クライアント証明書を検証します。
  - [SSLクライアント（SSL Client）]：リモートアクセス VPN 接続の試行中に SSL クライアント証明書を検証します。
  - [SSLサーバー（SSL Server）]：Cisco Umbrella サーバー証明書など、SSL サーバー証明書を検証する場合に選択します。

ステップ 4 （任意）[証明書のパラメータ（Certificate Parameters）] タブを開き、証明書の内容を指定します。証明書の登録オブジェクト 証明書のパラメータ （1369 ページ）を参照してください。

この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

ステップ 5 （任意）[キー（Key）] タブを開き、キーの内容を指定します。証明書の登録オブジェクトの主要なオプション （1370 ページ）を参照してください。

ステップ 6 （任意）[失効（Revocation）] タブをクリックし、失効のオプションを指定します。証明書の登録オブジェクト 失効オプション （1373 ページ） を参照してください。

ステップ 7 必要に応じ、このオブジェクトについて [オーバーライドを許可（Allow Overrides）] しておきます。

オーバーライドを許可するように PKCS12 証明書の登録オブジェクトを変更するたびに、オーバーライドされるデバイスで証明書の [パスフレーズ（Passphrase）] を更新する必要があります。

オブジェクトのオーバーライドの詳細はオブジェクトのオーバーライド（1310ページ） を参照してください。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

デバイスのトラストポイントを作成するため、デバイスの登録オブジェクトの関連付けとインストールを行います。

関連トピック

自己署名登録を使用した証明書のインストール （1460 ページ）
EST 登録を使用した証明書のインストール （1461 ページ）
SCEP の登録を使用した証明書のインストール （1462 ページ）
手動登録を使用した証明書のインストール （1463 ページ）
PKCS12 ファイルを使用した証明書のインストール （1464 ページ）

証明書の登録オブジェクト EST オプション

Secure Firewall Management Center ナビゲーション パス

[Objects] > **[Object Management]** を選択し、ナビゲーションウィンドウから **[PKI]** > **[Cert Enrollment]** を選択します。（＋） [証明書の登録の追加（Add Cert Enrollment）] をクリックして、[証明書の登録の追加（Add Cert Enrollment）] ダイアログを開き、[CA情報（CA Information）] タブを選択します。

フィールド

[Enrollment Type]：[EST] に設定します。

（注）
- EST 登録タイプは、EdDSA キーをサポートしていません。
- 証明書の有効期限が切れたときにデバイスを自動登録する EST の機能はサポートされていません。

[登録 URL（Enrollment URL）]：デバイスが登録を試行する先の CA サーバーの URL。

https://CA_name:port の形式の HTTPS URL を使用します。ここで、CA_name は CA サーバーのホスト DNS 名または IP アドレスです。ポート番号は必須です。

[Username]：CA サーバーにアクセスするためのユーザー名。

[Password / Confirm Password]：CA サーバーにアクセスするためのパスワード。

[Fingerprint]：EST を使用して CA 証明書を取得する場合、CA サーバーのフィンガープリントを入力する必要があります。フィンガープリントを使用して CA サーバの証明書の真正性を確認すると、不正な第三者が、本物の証明書を偽の証明書に置き換えることを阻止できます。CA サーバの [フィンガープリント（Fingerprint）] には 16 進数形式で入力します。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。サーバーに直接接続して、CA のフィンガープリントを取得します。

[Source Interface]：CA サーバーと通信するインターフェイス。デフォルトでは、診断インターフェイスが表示されます。データインターフェイスを送信元インターフェイスとして設定するには、各インターフェイスのセキュリティゾーンまたはインターフェイス グループ オブジェクトを選択します。

[Ignore EST Server Certificate Validations]：EST サーバー証明書の検証はデフォルトで実行されます。Firewall Threat Defense による EST サーバー証明書の検証を無視する場合は、このチェックボックスをオンにします。

証明書の登録オブジェクト SCEP オプション

Secure Firewall Management Center ナビゲーション パス

[Objects] > [Object Management] を選択し、ナビゲーションウィンドウから [PKI] > [Cert Enrollment] を選択します。（＋）[証明書の登録の追加（Add Cert Enrollment）] をクリックして、[証明書の登録の追加（Add Cert Enrollment）] ダイアログを開き、[CA情報（CA Information）] タブを選択します。

フィールド

[登録タイプ（Enrollment Type）]：[SCEP] に設定します。

[登録 URL（Enrollment URL）]：デバイスが登録を試行する先の CA サーバの URL。

`http://CA_name:port` の形式の HTTP URL を使用します。ここで、CA_name は CA サーバのホスト DNS 名または IP アドレスです。ポート番号は必須です。

（注） SCEP サーバがホスト名/FQDN で参照されている場合は、FlexConfig オブジェクトを使用して DNS サーバを設定します。

CA での CA cgi-bin スクリプト位置がデフォルト（/cgi-bin/pkiclient.exe）でない場合は、その標準以外のスクリプト位置を http://CA_name:port/script_location の形式で URL に含める必要があります。ここで、script_location は CA スクリプトへのフル パスです。

[チャレンジ パスワード/パスワードの確認（Challenge Password/Confirm Password）]：CA サーバがデバイスのIDを検証するために使用するパスワード。CAサーバに直接アクセスして、またはWebブラウザにアドレス（**http://URLHostName/certsrv/mscep/mscep.dll**）を入力して、パスワードを取得できます。このパスワードは、CA サーバから取得した時間から60分間有効です。したがって、パスワードは、作成後、できるだけ迅速に配布する必要があります。

[再試行期間（Retry Period）]：証明書要求の試行間隔（分数）。値には1～60分を指定できます。デフォルトは1分です。

[再試行回数（Retry Count）]：最初の要求時に証明書が発行されていない場合、実行する再試行回数。1 ～ 100 の値を指定できます。デフォルトは 10 です。

[CA 証明書の取得元（CA Certificate Source）]：CA 証明書の取得方法を指定します。

- [SCEP を使用した取得（Retrieve Using SCEP）]（デフォルトであり、唯一サポートされているオプション）：Simple Certificate Enrollment Process（SCEP）を使用して CA サーバから証明書を取得します。SCEP を使用するにはデバイスと CA サーバとの間の接続が必要です。登録プロセスを開始する前に、デバイスからCAサーバへのルートがあることを確認します。

[フィンガープリント（Fingerprint）]：SCEP を使用して CA 証明書を取得する場合、CA サーバのフィンガープリントを入力する必要があります。フィンガープリントを使用してCAサーバの証明書の真正性を確認すると、不正な第三者が、本物の証明書を偽の証明書に置き換えることを阻止できます。CA サーバの [フィンガープリント（Fingerprint）] には 16 進数形式で入力します。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。サーバーに直接アクセスして、またはWebブラウザにアドレス（**http://<URLHostName>/certsrv/mscep/mscep.dll**）を入力して、CAのフィンガープリントを取得します。

証明書の登録オブジェクト 証明書のパラメータ

CA サーバに送信される証明書要求に、その他の情報を指定します。この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

Secure Firewall Management Center ナビゲーション パス

[Objects] > [Object Management] を選択し、ナビゲーションウィンドウから [PKI] > [Cert Enrollment] を選択します。（＋）[証明書の登録の追加（Add Cert Enrollment）] を押して、[証明書の登録の追加（Add Cert Enrollment）] ダイアログを開き、[証明書のパラメータ（Certificate Parameters）] タブを選択します。

フィールド

標準の LDAP X.500 形式を使用して、すべての情報を入力します。

- [FQDN を含む（Include FQDN）]：デバイスの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を証明書要求に含めるかどうかを指定します。選択肢は次のとおりです。

- **[デバイスのホスト名を FQDN として使用（Use Device Hostname as FQDN）]**
- **[証明書には FQDN を使用しない（Don't use FQDN in certificate）]**
- [カスタム FQDN（Custom FQDN）]：これを選択し、表示された [カスタム FQDN（Custom FQDN）] フィールドに指定します。

- [デバイスの IP アドレスを含める（Include Device's IP Address）]：IP アドレスが証明書要求に含まれているインターフェイス。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。

（注） 自己署名証明書を登録するときには、証明書パラメータで共通名（CN）を指定する必要があります。

- [組織単位（OU）（Organizational Unit (OU)）]：証明書に含める組織単位の名前（部門名など）。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [地域（L）（Locality (L)）]：証明書に含める地域。
- [都道府県（ST）（State (ST)）]：証明書に含める州または都道府県。
- [国コード（C）（County Code (C)）]：証明書に含める国。これらのコードは、ISO 3166 の国の省略形に準拠しています（たとえばアメリカ合衆国は「US」）。
- [電子メール（E）（Email (E)）]：証明書に含める電子メール アドレス。
- [デバイスのシリアル番号を含める（Include Device's Serial Number）]：デバイスのシリアル番号を証明書に含めるかどうかを指定します。CA は、このシリアル番号を使用して、証明書を認証するか、またはあとで証明書を特定のデバイスに関連付けます。シリアル番号を含めるかどうか判断できない場合は、デバッグに役立つため、含めてください。

証明書の登録オブジェクト の主要なオプション

Secure Firewall Management Center ナビゲーション パス

[Objects] > [Object Management] を選択し、ナビゲーションウィンドウから [PKI] > [Cert Enrollment] を選択します。（＋）[証明書の登録の追加（Add Cert Enrollment）] をクリックして、[証明書の登録の追加（Add Cert Enrollment）] ダイアログを開き、[キー（Key）] タブを選択します。

フィールド

- キータイプ：RSA、ECDSA、EdDSA。

（注）

- EST 登録タイプの場合、EdDSA キーはサポートされないため、選択しないでください。
- EdDSA は、サイト間 VPN トポロジでのみサポートされます。
- EdDSA は、リモートアクセス VPN のアイデンティティ証明書としてサポートされていません。

- [Key Name]：証明書に関連付けるキーペアがすでに存在する場合、このフィールドではそのキーペアの名前を指定します。キーペアが存在しない場合、このフィールドでは、登録時に生成されるキーペアに割り当てる名前を指定します。名前を指定しない場合、完全修飾ドメイン名（FQDN）キーペアが代わりに使用されます。
- [キー サイズ（Key Size）]：キー ペアが存在しない場合は、必要なキー サイズ（係数）をビットで定義します。推奨サイズは 2048 ビットです。係数のサイズが大きくなるほど、キーがよりセキュアになります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり（512 ビットより大きい場合は 1 分以上）、交換するときの処理にも時間がかかります。

重要

- Firewall Management Center と Firewall Threat Defense のバージョン 7.0 以降では、RSA キーサイズが 2,048 ビット未満の証明書と、SHA-1 と RSA 暗号化アルゴリズムを使用するキーは登録できません。ただし、Weak-Crypto を使用した証明書の PKI 登録を使用すると、SHA-1 と RSA 暗号化アルゴリズムおよび小さなキーサイズを使用する証明書を許可できます。Weak-Crypto を使用した証明書の PKI 登録（1372 ページ）
- Firewall Threat Defense 7.0 では、Weak-Crypto オプションを有効にしても、2048 ビット未満のサイズの RSA キーを生成できません。

- [Advanced Settings]：IPsec リモートクライアント証明書のキーの使用状況エクステンションおよび拡張キーの使用状況エクステンションの値を検証しない場合は、[Ignore IPsec Key Usage] を選択します。IPsec クライアント証明書のキーの使用状況チェックを行わないようにできます。デフォルトでは、このオプションは無効になっています。

（注） サイト間VPN接続では、Windows認証局（CA）を使用する場合、デフォルトのアプリケーション ポリシー拡張は **IP セキュリティ IKE 中間**です。このデフォルト設定を使用している場合は、選択したオブジェクトで [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）] オプションを選択する必要があります。それ以外の場合、エンドポイントはサイト間 VPN 接続を完了できません。

Weak-Crypto を使用した証明書の PKI 登録

SHA-1 ハッシュ署名アルゴリズム、および証明書の 2048 ビット未満の RSA キーサイズは、Firewall Management Center および Firewall Threat Defense バージョン 7.0 以降ではサポートされていません。RSA キーサイズが 2048 ビット未満の証明書は登録できません。

7.0 より前のバージョンを実行している場合、Firewall Management Center を管理する Firewall Threat Defense 7.0 でこれらの制限をオーバーライドするには、Firewall Threat Defense で Enable Weak-Crypto オプションを使用できます。Weak-Crypto キーを許可することは推奨しません。このようなキーは、キーサイズが大きいキーほど安全ではないためです。

（注） Firewall Threat Defense 7.0 以降では、Weak-Crypto を許可している場合でも、2048 ビット未満のサイズの RSA キーの生成はサポートされません。

デバイスで Weak-Crypto を有効にするには、[Devices] > [Certificates] ページに移動します。Firewall Threat Defense デバイスに対して表示される [Weak-Cryptoの有効化（Enable Weak-Crypto）]（🔒）ボタンをクリックします。Weak-Crypto オプションを有効にすると、ボタンが 🔓 に変わります。デフォルトでは、Weak-Crypto オプションは無効になっています。

（注） 弱い暗号の使用が原因で証明書の登録が失敗した場合、Firewall Management Center は Weak-Crypto オプションを有効にするように求める警告メッセージを表示します。同様に、[Enable Weak-Crypto] ボタンをオンにすると、Firewall Management Center はデバイスで Weak-Crypto の設定を有効にする前に警告メッセージを表示します。

Firewall Threat Defense の旧バージョンから 7.0 へのアップグレード

Firewall Threat Defense 7.0 にアップグレードする場合、既存の証明書の設定は保持されます。ただし、これらの証明書に 2048 ビット未満の RSA キーがあり、SHA-1 暗号化アルゴリズムを使用している場合は、それらを使用して VPN 接続を確立することはできません。2048 ビットより大きい RSA キーサイズの証明書を購入するか、または VPN 接続の Permit Weak-Crypto オプションを有効にする必要があります。

証明書の登録オブジェクト 失効オプション

証明書の失効ステータスを確認するかどうかを、方法を選択して設定することで指定します。失効の確認はデフォルトでオフになっており、どちらの方法（CRL または OCSP）もオンになっていません。

Secure Firewall Management Center ナビゲーション パス

[Objects] > [Object Management] を選択し、ナビゲーションウィンドウから [PKI] > [Cert Enrollment] を選択します。（＋）[証明書の登録の追加（Add Cert Enrollment）] をクリックして、[証明書の登録の追加（Add Cert Enrollment）] ダイアログを開き、[失効（Revocation）] タブを選択します。

フィールド

- [証明書失効リストの有効化（Enable Certificate Revocation Lists）]：CRL の確認を有効にするにはオンにします。
  - [証明書からのCRL分散ポイント（Use CRL distribution point from the certificate）]：証明書からの失効リスト配布 URL を取得するにはオンにします。
  - [設定された静的 URL を使用（Use static URL configured）]：失効リストのスタティックな事前定義された配布 URL を追加するには、これをオンにします。次に URL を追加します。

    [CRL サーバの URL（CRL Server URLs）]：CRL をダウンロード可能な LDAP サーバの URL。

    URL は、**http://** で始まる必要があります。URL にポート番号を含めてください。

- [Online Certificate Status Protocol（OCSP）の有効化（Enable Online Certificate Status Protocol）]：OCSP チェックを有効にするにはオンにします。

  [OCSP サーバ URL（OCSP Server URL）]：OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。

  URL は、**http://** で始まる必要があります。

- [失効情報にアクセスできない場合、証明書は有効と見なされます（Consider the certificate valid if revocation information cannot be reached）]：デフォルトでオンになっています。これを許可しない場合は、チェックボックスをオフにします。

ポリシー リスト

ポリシー リストのポリシー オブジェクトを作成、コピー、編集するには、[ポリシー リストの設定（Configure Policy List）] ページを使用します。ルート マップを設定するときに使用するポリシー リスト オブジェクトを作成できます。ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに

2 つ以上のポリシー リストを設定できる。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから [ポリシー リスト（Policy List）] を選択します。

ステップ 2 [ポリシー リストの追加（Add Policy List）] をクリックします。

ステップ 3 [名前（Name）] フィールドにポリシー リスト オブジェクトの名前を入力します。オブジェクト名では、大文字と小文字が区別されません。

ステップ 4 [アクション（Action）] ドロップダウン リストから、一致する条件へのアクセスを許可するかブロックするかを選択します。

ステップ 5 [インターフェイス（Interface）] タブをクリックして、指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。

[ゾーン/インターフェイス（Zones/Interfaces）] リストに、デバイスが管理ステーションとの通信を行うインターフェイスが含まれたゾーンを追加します。ゾーン内にないインターフェイスの場合は、[選択したゾーン/インターフェイス（Selected Zone/Interface）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

ステップ 6 [アドレス（Address）] タブをクリックして、標準アクセス リストまたはプレフィックス リストで許可された宛先アドレスを持つルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 7 [ネクスト ホップ（Next Hop）] タブをクリックして、指定したアクセス リストまたはプレフィックス リストの 1 つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 8 [ルート送信元（Route Source）] タブをクリックして、アクセス リストまたはプレフィックス リストで指定されたアドレスのルータおよびアクセス サーバによってアドバタイズされたルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 9 [AS パス（AS Path）] タブをクリックして、BGP 自律システム パスを一致させます。複数の AS パスを指定した場合、ルートはいずれかの AS パスと一致します。

ステップ 10 [コミュニティルール（Community Rule）] タブをクリックして、BGP コミュニティまたは拡張コミュニティを、指定されたコミュニティ リスト オブジェクトまたは拡張コミュニティ リスト オブジェクトとそれぞれ照合できるようにします。複数のルールを指定すると、一致する許可または拒否が満たされるまで、ルートがルールに対して検証されます。

a) ルールに対してコミュニティリストを指定するには、[選択したコミュニティリスト（Selected Community List）] フィールドで [既定（given）] をクリックします。[編集（Edit）]（✎）コミュニティリストが [使用可能なコミュニティリスト（Available Community List）] の下に表示されます。必要なリストを選択して [追加（Add）] をクリックし、[OK] をクリックします。

BGP コミュニティと指定したコミュニティの完全一致を有効にするには、[指定したコミュニティと完全に一致（Match the specified community exactly）] チェックボックスをオンにします。

b) 拡張コミュニティリストを追加するには、[選択した拡張コミュニティリスト（Selected Extended Community List）] フィールドで [既定（given）] をクリックします。[編集（Edit）]（✎）拡張コミュニティリストが [使用可能な拡張コミュニティリスト（Available Extended Community List）] の下に表示されます。必要なリストを選択して [追加（Add）] をクリックし、[OK] をクリックします。

（注）
拡張コミュニティリストは、ルートのインポートまたはエクスポートの設定にのみ適用されます。

ステップ 11 [メトリックとタグ（Metric & tag）] タブをクリックして、メトリックとルートのセキュリティグループ タグを照合します。

a) [Metric（メトリック）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

b) [タグ（Tag）] フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。

ステップ 12 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 13 [保存（Save）] をクリックします。

ポート

ポート オブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

TCP および UDP

ポートオブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例：`TCP(6)/22`。

ICMP および ICMPv6（IPv6-ICMP）

ポートオブジェクトはインターネット層プロトコルと、オプションでタイプおよびコードを表します。例：`ICMP(1):3:3`

ICMP または IPV6-ICMP ポート オブジェクトは、タイプ、および該当する場合はコードを基準に制限できます。ICMP のタイプとコードの詳細については、次の URL を参照してください。

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

その他

ポート オブジェクトは、ポートを使用しない他のプロトコルを表します。

システムには、ウェルノウンポート用にデフォルトのポートオブジェクトが用意されています。これらのデフォルト オブジェクトを変更または削除することはできません。デフォルト オブジェクトに加え、カスタム ポート オブジェクトを作成できます。

ポート オブジェクトおよびグループは、アクセス コントロール ポリシー、アイデンティティ ルール、ネットワーク検出ルール、ポート変数、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、組織が特定のポート範囲を使用するカスタム クライアントを使用していて、システムで過剰なイベントや誤解を与えるイベントが発生した場合、それらのポートをモニタ対象から除外するようネットワーク検出ポリシーを設定できます。

ポート オブジェクトを使用する際は、次のガイドラインに従ってください。

- アクセス コントロール ルールの送信元ポート条件には TCP/UDP 以外のプロトコルを追加できません。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポート プロトコルを混在させることはできません。
- 送信元ポート条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、設定を展開しても、その条件が使用されているルールは管理対象デバイスで適用されません。
- TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポート条件としてそのポート オブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

ポート オブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ポート（Port）] を選択します。

ステップ 3 [ポートの追加（Add Port）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

ステップ 5 [プロトコル（Protocol）] を選択します。

ステップ 6 選択したプロトコルに応じて、[ポート（Port）] で制限するか、または ICMP の [タイプ（Type）] および [コード（Code）] を選択します。

1 から 65535 のポートを入力できます。ポート範囲を指定するには、ハイフンを使用します。[すべて（All）] のプロトコルと一致させることを選択した場合は、[その他（Other）] ドロップダウン リストを使用して、ポートでオブジェクトを制限する必要があります。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （1312 ページ）を参照）。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

ポートオブジェクトのインポート

ポートオブジェクトのインポートの詳細については、オブジェクトのインポート （1303 ページ）を参照してください。

プレフィックス リスト

ルート マップ、ポリシー マップ、OSPF フィルタリング、BGP ネイバー フィルタリングを設定する際に使用する、IPv4 および IPv6 用のプレフィックス リスト オブジェクトを作成できます。

IPv6 プレフィックス リストの設定

IPv6 プレフィックス リストの設定ページを使用して、プレフィックス リスト オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[プレフィックス リスト（Prefix Lists）]** > **[IPv6 プレフィックス リスト（IPv6 Prefix List）]** を選択します。

ステップ 2 [プレフィックス リストの追加（Add Prefix List）] をクリックします。

ステップ 3 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウの [名前（Name）] フィールドで、プレフィックス リスト オブジェクトの名前を入力します。

ステップ 4 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 5 [アクション（Action）] ドロップダウンリストから適切なアクション、[許可（Allow）] または [ブロック（Block）] を選択して、再配布アクセスを指定します。

ステップ 6 このオブジェクトですでに設定されているプレフィックス リスト エントリのリストにおける、新しいプレフィックス リスト エントリの位置を示す固有の数字を、[シーケンス番号（Sequence No.）] フィールドに入力します。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。

ステップ 7 [IP アドレス（IP address）] フィールドの IP アドレス/マスク長形式で、IPv6 アドレスを指定します。マスク長は 1 ～ 128 の有効な値でなければなりません。

ステップ 8 [最小プレフィックス長（Minimum Prefix Length）] フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。

ステップ 9 [最大プレフィックス長（Maximum Prefix Length）] フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 12 [保存（Save）] をクリックします。

IPv4 プレフィックス リストの設定

IPv4 プレフィックス リストの設定ページを使用して、プレフィックス リスト オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、目次で [プレフィックス リスト（Prefix Lists）] > [IPv4 プレフィックス リスト（IPv4 Prefix List）] を選択します。 > >

ステップ 2 [プレフィックス リストの追加（Add Prefix List）] をクリックします。

ステップ 3 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウの [名前（Name）] フィールドで、プレフィックス リスト オブジェクトの名前を入力します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [アクション（Action）] ドロップダウンリストから適切なアクション、[許可（Allow）] または [ブロック（Block）] を選択して、再配布アクセスを指定します。

ステップ 6 このオブジェクトですでに設定されているプレフィックス リストエントリのリストにおける、新しいプレフィックス リストエントリの位置を示す固有の数字を、[シーケンス番号（Sequence No.）] フィールドに入力します。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。

ステップ 7 [IP アドレス（IP address）] フィールドの IP アドレス/マスク長形式で、IPv4 アドレスを指定します。マスク長は 1 ～ 32 の有効な値でなければなりません。

ステップ 8 [最小プレフィックス長（Minimum Prefix Length）] フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。

ステップ 9 [最大プレフィックス長（Maximum Prefix Length）] フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 12 [保存（Save）] をクリックします。

ルート マップ

ルート マップは、ルートをルーティング プロセスに再配布するときに使用できます。また、デフォルトルートをルーティングプロセスに生成するときにも使用します。ルートマップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。ルート マップを設定して、ルート マップ オブジェクトの新しいルート マップ エントリを作成したり、既存のルート マップ エントリを編集したりします。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

始める前に

ルートマップは、これらのオブジェクトの1つまたは複数を使用することができます。これらのオブジェクトをすべて追加する必要はありません。これらのオブジェクトを必要に応じて作成および使用して、ルート マップを設定します。

- ACL の追加
- プレフィックス リストの追加
- AS パスの追加
- コミュニティ リストの追加
- 拡張コミュニティリストを追加します。

（注） 拡張コミュニティリストは、ルートのインポートまたはエクスポートの設定にのみ適用されます。

- ポリシー リストの追加

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[ルート マップ（Route Map）]** を選択します。

ステップ 2 [ルート マップの追加（Add Route Map）] をクリックします。

ステップ 3 [新しいルートマップオブジェクト（New Route Map Object）] ウィンドウで [追加（Add）] をクリックします。

ステップ 4 [シーケンス番号（Sequence No.）] フィールドで、このルートマップオブジェクトにすでに設定されているルートマップエントリのリストでの新しいルートマップエントリの位置を示す 0 ～ 65535 の番号を入力します。

（注）

将来的に句を挿入する必要が生じた場合の番号の間隔を確保するために、少なくとも 10 間隔で句に番号を指定することをお勧めします。

ステップ 5 [再配布（Redistribution）] ドロップダウンリストから、再配布アクセスを示す適切なアクション（[許可（Allow）] または [ブロック（Block）]）を選択します。

ステップ 6 [句の照合（Match Clauses）] タブをクリックして、コンテンツテーブルで選択する次の条件に基づいて照合します（ルート/トラフィック）。

- [セキュリティゾーン（Security Zones）]：（入力/出力）インターフェイスに基づいてトラフィックを照合します。ゾーンを選択して追加するか、インターフェイス名を入力して追加します。
- [IPv4]：次の条件に基づいて IPv4（ルート/トラフィック）を照合します。条件を定義するタブを選択します。
  1. ルート アドレスに基づいてルートを照合するには、[アドレス（Address）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
  2. ルートのネクスト ホップ アドレスに基づいてルートを照合するには、[ネクスト ホップ（Next Hop）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
  3. ルートのアドバタイズ送信元アドレスに基づいてルートを照合するには、[ルート送信元（Route Source）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
- [IPv6]：ルートのルートアドレス、ネクストホップアドレス、またはアドバタイズ送信元アドレスに基づいて IPv6（ルート/トラフィック）を照合します。
- [BGP]：次の条件に基づいて BGP（ルート/トラフィック）を照合します。条件を定義するタブを選択します。
  1. BGP 自律システム パス アクセス リストと指定されたパス アクセス リストの照合を有効にするには、[AS パス（AS Path）] タブをクリックします。複数のパス アクセス リストを指定した場合、ルートはいずれかのパス アクセス リストと一致します。
  2. [コミュニティリスト（Community List）] タブをクリックして、BGP コミュニティまたは拡張コミュニティを、指定されたコミュニティ リスト オブジェクトまたは拡張コミュニティ リスト オブジェクトとそれぞれ照合できるようにします。
     - ルールに対してコミュニティリストを指定するには、[選択したコミュニティリスト（Selected Community List）] フィールドで [既定（given）] をクリックします。[編集（Edit）]（✎）コミュニティリストが [使用可能なコミュニティリスト（Available Community List）] の下に表示されます。必要なリストを選択して [追

加（Add）] をクリックし、[OK] をクリックします。コミュニティ リスト オブジェクトの作成方法については、コミュニティ リスト（1328 ページ）を参照してください。

- 拡張コミュニティリストを追加するには、[選択した拡張コミュニティリスト（Selected Extended Community List）] フィールドで [既定（given）] をクリックします。[編集（Edit）]（）拡張コミュニティリストが [使用可能な拡張コミュニティリスト（Available Extended Community List）] の下に表示されます。必要なリストを選択して [追加（Add）] をクリックし、[OK] をクリックします。拡張コミュニティリストオブジェクトの作成方法については、拡張コミュニティ （1330 ページ）を参照してください。

BGP コミュニティと指定したコミュニティ リスト オブジェクトの完全一致を有効にするには、[指定したコミュニティと完全に一致（Match the specified community exactly）] チェックボックスをオンにします。このオプションは、拡張コミュニティリストには適用されません。

（注）
複数のルールを指定すると、一致する許可または拒否条件が満たされるまで、ルートがルールに対して検証されます。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンド ルート マップにアドバタイズされません。

3. BGP ポリシーを評価および処理するためのルート マップを設定するには、[ポリシー リスト（Policy List）] タブをクリックします。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

- [その他（Others）]：次の条件に基づいてルートまたはトラフィックを照合します。

1. ルートのメトリックの照合を有効にするには、[メトリック ルート値（Metric Route Value）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。
2. [タグ値（Tag Values）] フィールドに、照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。
3. ルート タイプの照合を有効にするには、適切な**ルート タイプ** オプションをオンにします。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。複数のルート タイプをリストから選択することができます。

ステップ 7 [句の設定（Set Clauses）] タブをクリックして、コンテンツ テーブルで選択する次の条件に基づいてルート/トラフィックを設定します。

- [メトリック値（Metric Values）]：[帯域幅（Bandwidth）]、すべての値、または値なしを設定します。

1. [帯域幅（Bandwidth）] フィールドに、メトリック値または帯域幅（キロビット/秒）を入力します。有効な値は、0 ～ 4294967295 の範囲の整数値です。
2. [メトリック タイプ（Metric Type）] ドロップダウン リストから、宛先ルーティング プロトコルのメトリックのタイプを選択して指定します。有効な値は、internal、type-1、または type-2 です。

- [BGP句（BGP Clauses）]：次の条件に基づいて BGP ルートを設定します。条件を定義するタブを選択します。

1. BGP ルートの自律システム パスを変更するには、[AS パス（AS Path）] タブをクリックします。
   1. 任意の自律システム パス文字列を BGP ルートの前に付加するには、[AS パスを前に付加（Prepend AS Path）] タブをクリックします。通常、ローカルな AS 番号が複数回追加され、自律システム パス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。
   2. 最後の AS 番号を AS パスの前に付加するには、[最後の AS を AS パスの前に付加（Prepend Last AS to AS Path）] フィールドに AS パス番号を入力します。AS 番号の値を 1 ～ 10 の範囲で入力します。
   3. ルートのタグを自律システム パスに変換するには、[ルート タグを AS パスに変換する（Convert route tag into AS path）] チェックボックスをオンにします。
2. コミュニティ属性を設定するには、[コミュニティリスト（Community List）] タブをクリックします。

   [特定のコミュニティ（Specific Community）] の下で、次の手順を実行します。
   1. ルート マップをパスするプレフィックスからコミュニティ属性を除去するには、[なし（None）] ラジオ ボタンをクリックします。
   2. コミュニティ番号を入力するには、[コミュニティの指定（Specify Community）] ラジオ ボタンをクリックします（必要な場合）。有効な値は 1 ～ 4294967295 です。
   3. 既存のコミュニティにコミュニティを追加するには、[既存のコミュニティに追加する（Add to existing communities）] チェックボックスをオンにします。
   4. 既知のコミュニティのいずれかを使用するには、[インターネット（Internet）]、[アドバタイズなし（No-Advertise）]、または [エクスポートなし（No-Export）] チェックボックスをオンにします。

   [特定の拡張コミュニティ（Specific Extended Community）] の [ルートターゲット（Route Target）] フィールドに、ルートターゲット番号を ASN:nn 形式で入力します。

   - 1:1 ー 65534:65535 の範囲の値を入力できます。

     1 つのエントリに、単一のルートターゲットまたはカンマで区切った一連のルートターゲットを追加できます。例：1:2,1:4,1:6。

- 1 つのエントリに最大 8 つのルートターゲットを設定できます。
- ルートマップ間で冗長ルートターゲットエントリを設定することはできません。

3. 追加属性を設定するには、[その他（Others）] タブをクリックします。
   1. タグ値を自動的に計算するには、[自動タグを設定する（Set Automatic Tag）] チェックボックスをオンにします。
   2. [ローカル優先度の設定（Set Local Preference）] フィールドに自律システム パスの優先度値を入力します。0 から 4294967295 までの値を入力してください。
   3. [重み付けの設定（Set Weight）] フィールドにルーティング テーブルの BGP ウェイトを入力します。0 から 65535 までの値を入力してください。
   4. BGP の発信元コードを選択して指定します。有効な値は [ローカル IGP（Local IGP）] および [未完了（Incomplete）] です。
   5. [IPv4 設定（IPv4 Settings）] セクションで、パケットが出力されるネクストホップのネクストホップ IPv4 アドレスを指定します。隣接ルータである必要はありません。複数の IPv4 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。

      [プレフィックス リスト（Prefix List）] ドロップダウン リストから IPv4 プレフィックス リストを選択して指定します。
   6. [IPv6 設定（IPv4 Settings）] セクションで、パケットが出力されるネクストホップのネクストホップ IPv6 アドレスを指定します。隣接ルータである必要はありません。複数の IPv6 アドレスを指定した場合、任意の IP アドレスでパケットを出力できます。

      [プレフィックス リスト（Prefix List）] ドロップダウン リストから IPv6 プレフィックスを選択して指定します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

ステップ 10 [保存（Save）] をクリックします。

セキュリティ インテリジェンス

セキュリティ インテリジェンス機能には、IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

セキュリティインテリジェンスのリストとフィードは、リストまたはフィードのエントリに一致するトラフィックをすばやくフィルタリングするために使用できる IP アドレス、ドメイン名、および URL のコレクションです。

- リストは、手動で管理される静的コレクションです。
- フィードは、HTTP または HTTPS で一定期間更新する動的コレクションです。

セキュリティ インテリジェンスのリストとフィードは、次のようにグループ化されます。

- DNS（ドメイン名）
- ネットワーク（IP アドレス）
- URL

システムが提供するフィード

シスコでは、セキュリティインテリジェンス オブジェクトとして次のフィードを提供しています。

- Talosからの最新の脅威インテリジェンスで定期的に更新されるセキュリティインテリジェン スフィード。
  - Cisco-DNS-and-URL-Intelligence-Feed（[DNS Lists and Feeds] の下）
  - Cisco-Intelligence-Feed（IPアドレス用、[Network Lists and Feeds] の下）

  システムが提供するフィードは削除できませんが、更新頻度を変更（または無効に設定）できます。
- Cisco-TID-Feed（[Network Lists and Feeds] の下）

  このフィードは、アクセス コントロール ポリシーの [Security Intelligence] タブでは使用されません。

  代わりに、Secure Firewall Threat Intelligence Director を有効化および設定して、TID オブザーバブルデータのコレクションであるこのフィードを使用するようする必要があります。

  このオブジェクトを使用して、このデータが TID 要素に公開される頻度を設定します。

  詳細については、Secure Firewall Threat Intelligence Director （2941 ページ）を参照してください。

事前定義リスト：グローバルブロックリストとグローバルブロックしないリスト

システムには、ドメイン（DNS）、IP アドレス（ネットワーク）、および URL の定義済みグローバルブロックリストとブロックしないリストが付属しています。

これらのリストは、入力するまで空です。これらのリストを作成するには、グローバルおよびドメインのセキュリティインテリジェンスリスト （1387 ページ）を参照してください。

デフォルトで、アクセス コントロール ポリシーと DNS ポリシーは、セキュリティ インテリジェンスの一部としてこれらのリストを使用します。

カスタムフィード

サードパーティーのフィードやカスタム内部フィードを使用すると、複数の Secure Firewall Management Center アプライアンスからなる大規模な展開で企業全体のブロックリストを簡単に保守できます。

「カスタム セキュリティ インテリジェンス フィード（1394 ページ）」を参照してください。

カスタムリスト

カスタム リストを強化し、フィードとグローバル リストを微調整できます。

「カスタム セキュリティ インテリジェンス リスト（1396 ページ）」を参照してください。

セキュリティ インテリジェンスのリストとフィードが使われる状況

- IP アドレスとアドレスブロック：セキュリティ インテリジェンスの一部として、アクセス コントロール ポリシーでブロックリストとブロックしないリストを使用します。
- ドメイン名：セキュリティ インテリジェンスの一部として、DNS ポリシーでブロックリストとブロックしないリストを使用します。
- URL：セキュリティ インテリジェンスの一部として、アクセス コントロール ポリシーでブロックリストとブロックしないリストを使用します。また、セキュリティインテリジェンス後に分析およびトラフィック処理フェーズが実行されるアクセス コントロール ルールおよび QoS ルールで、URL リストを使用することもできます。

セキュリティ インテリジェンス オブジェクトの変更方法

ブロックリスト、ブロックしないリスト、フィード、またはシンクホールオブジェクトのエントリを追加または削除するには：

オブジェクト タイプ	機能の編集	編集後に再度展開しますか?
カスタムのブロックリストとブロックしないリスト	オブジェクト マネージャを使用して新しいリストと交換リストをアップロード。	×
デフォルト（カスタム入力）ブロックリストとブロックしないリスト：グローバル、子孫、ドメイン固有	コンテキストメニューを使用してエントリを追加するか、オブジェクトマネージャを使用してエントリを削除します。	×

オブジェクト タイプ	機能の編集	編集後に再度展開しますか?
システム提供インテリジェンス フィード	オブジェクト マネージャを使用して更新頻度を無効または変更。	×
カスタム フィード	オブジェクト マネージャを使用して完全に変更。	×
シンクホール	オブジェクト マネージャを使用して完全に変更。	はい

グローバルおよびドメインのセキュリティインテリジェンスリスト

Firewall Management Center には、グローバルブロックリストとブロックなしリストが含まれています。これらのリストを使用すると、セキュリティインテリジェンスを使用して、特定の接続を一貫してブロックできます。また、特定の接続のブロックを免除して、設定済みの別の脅威検出プロセスによるそれらの接続の評価を可能にすることができます。

たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な一連の IP アドレスに気付いた場合、それらの IP アドレスを即座にブロックリストに入れることができます。変更内容が伝達されるまでに数分かかる場合がありますが、再度展開する必要はありません。

デフォルトでは、アクセス コントロール ポリシーと DNS ポリシーがすべてのセキュリティゾーンに適用されるグローバル リストを使用します。ポリシーごとに、これらのリストを使用しないように選択することができます。

（注） これらのオプションは、セキュリティ インテリジェンスにのみ適用されます。セキュリティインテリジェンスは、すでにファーストパスされたトラフィックをブロックすることはできません。同様に、セキュリティインテリジェンスでブロックしないリストに登録しても、それに一致するトラフィックが自動的に信頼されることもファーストパスされることもありません。詳細については、「セキュリティインテリジェンスについて（1851 ページ）」を参照してください。

セキュリティ インテリジェンス リストとマルチテナンシー

マルチテナント追加：

- ドメインリスト：コンテンツが特定のサブドメインにのみ適用されるブロックリストまたはブロックしないリスト。グローバル リストは、グローバル ドメインのドメイン リストです。
- 子孫ドメインリスト：現在のドメインの子孫のドメインリストを集約するブロックリストまたはブロックしないリスト。

ドメイン リスト

グローバルリストに（編集ではなく）アクセスできることに加えて、各サブドメインには独自の名前付きリストがあり、そのコンテンツはそのサブドメインにのみ適用されます。たとえば、Company A という名前のサブドメインは、次のリストを所有するとします。

- ドメインブロックリスト：Company A、ドメインブロックしないリスト：Company A
- DNS のドメインブロックリスト：Company A、DNS のドメインブロックしないリスト：Company A
- URL のドメインブロックリスト：Company A、URL のドメインブロックしないリスト：Company A

現在のドメインより上位の管理者は、これらのリストに入力できます。コンテキストメニューを使用して、現在のドメインとすべての子孫ドメインの項目をブロックリストまたはブロックしないリストに追加できます。ただし、ドメインリストから項目を削除できるのは、関連付けられたドメインの管理者のみです。

たとえば、グローバル管理者は同じ IP アドレスをグローバルドメインと Company A のブロックリストに追加できますが、CompanyBのドメインのブロックリストには追加できません。このアクションにより、同じ IP アドレスが次のリストに追加されます。

- （グローバル管理者のみが削除できる）グローバルブロックリスト
- （Company A の管理者のみが削除できる）ドメインブロックリスト- Company A

子孫ドメイン リスト

子孫ドメインリストは、現在のドメインの子孫のドメインリストを集約するブロックしないリストまたはブロックリストです。リーフ ドメインには、子孫ドメイン リストはありません。

子孫ドメイン リストが便利なのは、上位レベルのドメインの管理者が一般的なセキュリティ インテリジェンス設定を適用できる一方で、サブドメインユーザーは独自の展開で項目をブロックリストやブロックしないリストに追加できるためです。

たとえば、グローバル ドメインには、次の子孫ドメイン リストがあります。

- 子孫ブロックリスト - Global、子孫のブロックしないリスト - Global
- DNS の子孫ブロックリスト - Global、子孫の DNS のブロックしないリスト - Global
- URL の子孫ブロックリスト - Global、子孫の URL のブロックしないリスト - Global

（注） 子孫ドメイン リストは、手動で入力されたリストではなく象徴的な集約であるため、オブジェクト マネージャには表示されません。それを使用できる場所、つまり、アクセス コントロール ポリシーと DNS ポリシーに表示されます。

グローバル セキュリティ インテリジェンス リストへのエントリの追加

イベントとダッシュボードを確認するときに、事前定義されたブロックリストに追加することで、それらのイベント内の IP アドレス、ドメイン、および URL を含む将来のトラフィックを即座にブロックできます。

同様に、セキュリティインテリジェンスのブロック後に脅威検出プロセスで評価する必要があるトラフィックをセキュリティインテリジェンスがブロックしている場合は、イベントからの IP アドレス、ドメイン、および URL を事前定義された「ブロックしない」リストに追加できます。

脅威検出のセキュリティ インテリジェンス フェーズで、これらのリストのエントリに照らしてトラフィックが評価されます。

これらリストの詳細については、グローバルおよびドメインのセキュリティインテリジェンス リスト （1387 ページ） を参照してください。

始める前に

セキュリティ インテリジェンス リストにエントリを追加するとアクセス制御に影響が出るため、次のユーザーロールのうち 1 つが必須です。

- 管理者
- ロールの組み合わせ：ネットワーク管理者（Network Admin）またはアクセス管理者（Access Admin）に加えてセキュリティアナリスト（Security Analyst）およびセキュリティ承認者（Security Approver）
- アクセス コントロール ポリシーの変更（Modify Access Control Policy）と設定をデバイスに展開（Deploy Configuration to Devices）の両方のアクセス許可を持つカスタム ロール。

必要に応じて、これらのリストが予定通りのポリシー内で使用されていることを確認してください。

手順

ステップ 1 セキュリティ インテリジェンスを使用して常にブロックするか、セキュリティ インテリジェンスのブロックから除外する IP アドレス、ドメイン、または URL を含むイベントに移動します。

ステップ 2 IP アドレス、ドメイン、または URL を右クリックし、適切なオプションを選択します。

項目タイプ	コンテキスト メニュー オプション
IP アドレス	ブロックリストに IP を追加 ブロックしないリストに IP を追加 これらのオプションは、ネットワークのそれぞれのリストに IP アドレスを追加します。

項目タイプ	コンテキスト メニュー オプション
URL	URL のグローバルブロックリストに URL を追加 URL のグローバルブロックしないリストに URL を追加
URL フィールドの URL ドメイン	URL のグローバルブロックリストにドメインを追加 URL のグローバルブロックしないリストにドメインを追加
DNS クエリフィールドのドメイン	DNS のグローバルブロックリストにドメインを追加 DNS のグローバルブロックしないリストにドメインを追加

次のタスク

これらの変更を有効にするために再展開する必要はありません。

リストから項目を削除する方法は、グローバル セキュリティ インテリジェンス リストからのエントリを削除する （1390 ページ） を参照してください。

グローバル セキュリティ インテリジェンス リストからのエントリを削除する

（注） これらのリストにエントリを追加するには グローバル セキュリティ インテリジェンス リストへのエントリの追加 （1389 ページ） を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [セキュリティ インテリジェンス] をクリックします。

ステップ 3 適切なオプションをクリックします。

- [ネットワークのリストとフィード（Network Lists and Feeds）]（IP アドレス用）
- [DNSのリストとフィード（DNS Lists and Feeds）]（ドメイン名用）
- [URLのリストとフィード（URL Lists and Feeds）]

ステップ 4 グローバルブロックリストまたはグローバルブロックしないリストの横にある鉛筆をクリックします。

ステップ 5 削除するエントリの横にあるごみ箱ボタンをクリックします。

セキュリティ インテリジェンスのリストとフィードの更新

リストとフィードの更新は、既存のリストまたはフィードファイルを新しいファイルの内容に置き換えます。既存ファイルと新しいファイルの内容は結合されていません。

システムが破損したフィードまたは認識不能なエントリがあるフィードをダウンロードした場合、システムは古いフィードデータを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内のエントリを1つでも認識できる場合、システムは認識できるエントリを使用します。

デフォルトでは、各フィードは2時間ごとにManagement Centerを更新します。この頻度は変更できます。Management Centerが受信したすべての更新は、すぐに管理対象デバイスに渡されます。また、管理対象デバイスは、変更について30分ごとにFirewall Management Centerをポーリングします。この周波数を変更することはできません。

フィードの更新間隔を変更するには、セキュリティ インテリジェンス フィードの更新頻度の変更 （1391 ページ）を参照してください。

セキュリティ インテリジェンス フィードの更新頻度の変更

Firewall Management Centerがセキュリティ インテリジェンス フィードを更新する間隔を指定できます。

フィードの更新の詳細については、セキュリティインテリジェンスのリストとフィードの更新（1391 ページ）を参照してください。

手順

ステップ1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、更新頻度を変更するフィードのタイプを選択します。

システムが提供するURLフィードは、[DNSリストとフィード（DNS Lists and Feeds）] の下のドメインフィードと結合されます。

ステップ3 更新するフィードの横にある [編集（Edit）]（ ） をクリックします。

代わりに [表示（View）]（ ） が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ4 [更新頻度（Update Frequency）] を編集します。

ステップ5 [保存（Save）] をクリックします。

カスタム セキュリティ インテリジェンスのリストとフィード

カスタムリストとカスタムフィード：要件

リストとフィードの書式設定

各リストまたはフィードは、500MB 未満の単純なテキスト ファイルでなければなりません。リスト ファイルの拡張子は .txt でなければなりません。1 行につきエントリまたはコメントを 1 つ（IP アドレス 1 つ、URL 1 つ、ドメイン名 1 つ）含めます。

ヒント　含めることができるエントリの数は、ファイルの最大サイズによって制限されます。たとえば、コメントがなく URL の長さの平均が 100 文字（Punycode または Unicode 表現と改行のパーセントを含む）の URL リストには、524 万を超えるエントリを含めることができます。

DNS リストエントリ内では、ドメインラベルとしてアスタリスク（*）ワイルドカード文字を指定できます。その場合、すべてのラベルがワイルドカードと一致します。たとえば、`www.example.*` のエントリは `www.example.com` と `www.example.co` の両方に一致します。

ソース ファイル内にコメント行を含める場合は、シャープ（#）文字で開始する必要があります。コメントが含まれるソースファイルをアップロードすると、システムによってアップロード中にコメントが削除されます。ダウンロードするソースファイルには、コメントを除くすべてのエントリが含まれます。

フィードの要件

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode エンコードすることができません。

フィードの更新間隔が 30 分以下の場合は、MD5 URL を指定する必要があります。これにより、変更されていないフィードの頻繁なダウンロードが防止されます。フィードサーバーが MD5 URL を提供しない場合は、30 分以上間隔を空けてダウンロードを使用する必要があります。

MD5 チェックサムを使用する場合は、チェックサムのみを含む単純なテキスト ファイルに保存する必要があります。コメントはサポートされていません。

URL リストとフィード：URL 構文と一致基準

セキュリティ インテリジェンスの URL リストとフィード（カスタムのリストとフィード、およびグローバルのブロックリストとブロックしないリストのエントリを含む）には、以下を含めることができます。これらは、説明されている一致の動作を持ちます。

- ホスト名

  たとえば、**www.example.com** などです。

- URL

example.com は、**example.com** とすべてのサブドメインと一致します（**www.example.com**、**eu.example.com**、**example.com/abc**、および **www.example.com/def** を含む）。ただし、**example.co.uk** または **examplexyz.com** または **example.com.malicious-site.com** とは一致しません

URL フィードまたはリストに 1 つのエントリが含まれている場合、それらのドメインで終わるすべての URL が識別されてブロックされます。

例：**www.netflix.com**, **www.amazon.***、**org**、**edu**、**www.hulu.*** の URL フィードがグローバルなブロックリストに追加されると、次のコンテンツがブロックされます。http://www.amazon.in、http://www.rajiv.org/、http://www.edu.edu/、http://www.edu.org/、http://org.org/ および http://edu.edu。

https://www.cisco.com/c/en/us/products/security/firewalls/index.html のように、URL パス全体を含めることもできます

（注） カスタム URL、ネットワーク、および DNS フィードを作成できます。ここでは、URL 自体にユーザー名とパスワードを追加できます（例：**https://admin:password@server.domain.com/list.txt**）。

ただし、パスワードにコロン（:）やアットマーク（@）などの特殊文字が含まれている場合、送信は失敗します。パスワードに特殊文字が含まれていないことを確認してください。または、URL でエンコードされたパスワードを使用することもできます。

- 完全一致を指定するための URL の末尾のスラッシュ

  example.com/ は、**example.com** のみと一致します。**www.example.com** またはその他の URL とは一致しません。

- URL 内の任意のドメインを表すワイルドカード（*）

  アスタリスクは、ドットで区切られた完全なドメイン文字列を表すことができますが、ドメイン文字列の一部を表すことはできません。また、最初のスラッシュの後に続く URL の一部を表すことはできません。

  有効な例：

  - ***.example.com**
  - **www.*.com**
  - **example.***

    （これは、**example.com**、**example.org**、および **example.de** などと一致しますが、**example.co.uk** とは一致しません）

  - ***.example.***
  - **example.*/**

無効な例：

- **example*.com**
- **example.com/***

- IP アドレス（IPv4）

  IPv6 アドレスの場合や、範囲または CIDR 表記を使用する場合は、セキュリティ インテリジェンス ネットワーク オブジェクトを使用します。

  10.10.10.* や 10.10.*.* などの、オクテットを表す 1 つ以上のワイルドカードを含めることができます。

カスタム セキュリティ インテリジェンス リスト （1396 ページ） も参照してください。

カスタム セキュリティ インテリジェンス フィード

カスタムまたはサードパーティのセキュリティインテリジェンスフィードを使用すると、インターネット上で定期的に更新される他の信頼できるブロックリストおよびブロックしないリストによって、システムが提供するインテリジェンスフィードを拡張することができます。内部フィードのセットアップもできます。内部フィードは、1 つのソースリストを使用して導入環境で複数の Secure Firewall Management Center アプライアンスを更新する場合に役立ちます。

（注） セキュリティ インテリジェンス フィードでは、/0 ネットマスクを使ってアドレス ブロックをブロックリストまたはブロックしないリストに追加することはできません。ポリシーですべてのトラフィックをモニターまたはブロックする場合は、[モニター（Monitor）] または [ブロック（Block）] ルール アクションを含むアクセス コントロール ルールを使用し、デフォルト値 any を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

MD5 チェックサムを使用して、更新されたフィードをダウンロードするかどうか判断するようにシステムを設定することもできます。システムが最後にフィードをダウンロードした後にチェックサムが変更されていない場合、再ダウンロードする必要はありません。特に内部フィードが大きい場合は、内部フィードに MD5 チェックサムを使用することをお勧めします。

（注） システムはカスタム フィードのダウンロード時にピア SSL 証明書の検証を実行**しません**。また、システムは、証明書のバンドルまたは自己署名証明書を使用したリモート ピアの検証もサポートしていません。

システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にできます。ただし、自動更新を行えば、最新の関連するデータであることが確実になります。

手動でセキュリティ インテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

完全な要件については、カスタムリストとカスタムフィード：要件（1392ページ）を参照してください。

セキュリティ インテリジェンス フィードの作成

IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、追加するフィードタイプを選択します。

ステップ 3 上記で選択したフィード タイプに適したオプションをクリックします。

- [ネットワークのリストとフィードの追加（Add Network Lists and Feeds）]（IP アドレス用）
- **[DNS リストとフィードの追加（Add DNS Lists and Feeds）]**
- **[URL リストとフィードの追加（Add URL Lists and Feeds）]**

ステップ 4 フィードの名前を [名前（Name）] に入力します。

ステップ 5 [タイプ（Type）] ドロップダウンリストから [フィード（Feed）] を選択します。

ステップ 6 [フィード URL（Feed URL）] を入力します。

ステップ 7 [MD5 URL] を入力します。

これは、フィードの内容が最後の更新以降に変更されたかどうかを判断するために使用され、システムは変更されていないフィードをダウンロードしません。

30 分より短い更新間隔には MD5 URL が必要です。

フィードサーバーが MD5 URL を提供しない場合は、30 分以上の間隔を選択する必要があります。

ステップ 8 [更新頻度（Update Frequency）] を選択します。

ステップ 9 [保存（Save）] をクリックします。
フィードの更新を無効にした場合を除き、システムはフィードをダウンロードして検証しようとします。

手動によるセキュリティ インテリジェンス フィードの更新

IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

始める前に

少なくとも 1 つのデバイスが管理センターに追加されている必要があります。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、フィード タイプを選択します。

ステップ 3 [フィードの更新（Update Feeds）] をクリックして、確認します。

ステップ 4 [OK] をクリックします。

フィードの更新をダウンロードして検証した後、Secure Firewall Management Center はすべての変更内容を管理対象デバイスに通知します。導入環境では、更新されたフィードを使用してトラフィックのフィルタリングが開始されます。

カスタム セキュリティ インテリジェンス リスト

セキュリティ インテリジェンス リストは、IP アドレス、アドレス ブロック、URL、またはドメイン名の単純なスタティック リストで、ユーザがシステムに手動でアップロードします。カスタム リストは、単一の Secure Firewall Management Center の管理対象デバイスで、フィードやグローバル リストの 1 つを増やしたり、微調整したりする場合に役立ちます。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしているものの、このフィードが全体的に部門にとって有用である場合、IP アドレス フィード オブジェクトをアクセス コントロール ポリシーのブロックリストから削除する代わりに、誤って分類された IP アドレスだけが含まれるカスタムブロックしないリストを作成できます。

（注） セキュリティ インテリジェンス リストでは、`/0` ネットマスクを使ってアドレス ブロックをブロックリストまたはブロックしないリストに追加することはできません。ポリシーですべてのトラフィックをモニターまたはブロックする場合は、[モニター（Monitor）] または [ブロック（Block）]ルールアクションを含むアクセス コントロール ルールを使用し、デフォルト値 `any` を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

リスト エントリのフォーマットについて、次の点に注意してください。

- アドレス ブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ `0` から `32`、または `0` から `128` までの整数になります。
- ドメイン名に含まれる Unicode は Punycode 形式でエンコードされる必要があります。大文字と小文字は区別されません。
- ドメイン名の文字の大文字と小文字は区別されません。
- URL に含まれる Unicode はパーセントエンコーディング形式でエンコードする必要があります。

- URL サブディレクトリの文字の大文字と小文字は区別されます。
- シャープ記号（#）で始まるリスト エントリは、コメントと見なされます。
- 追加のフォーマット要件については、カスタムリストとカスタムフィード：要件（1392ページ）を参照してください。

リスト エントリの照合について、次の点に注意してください。

- URL または DNS リストにより高位レベルのドメインが存在する場合、システムはそれより低いレベルのドメインを一致とします。たとえば、DNS リストに `example.com` を追加すると、システムは `www.example.com` と `test.example.com` の両方を一致とします。
- システムは DNS または URL リスト エントリに対して DNS ルックアップを（フォワード ルックアップ、リバース ルックアップともに）行いません。たとえば、URL リストに `http://192.168.0.2` を追加し、これがルックアップすれば `http://www.example.com` であったとします。この場合、システムは `http://192.168.0.2` のみ一致とし、`http://www.example.com` は一致となりません。

新しいセキュリティ インテリジェンス リストの Secure Firewall Management Center へのアップロード

セキュリティ インテリジェンス リストを変更するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があります。Web インターフェイスを使用してファイルの内容を変更することはできません。ソース ファイルへのアクセス権がない場合は、システムからコピーをダウンロードします。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 上記の手順で選択したリストに該当するオプションをクリックします。

- [ネットワークのリストとフィードの追加（Add Network Lists and Feeds）]（IP アドレス用）
- **[DNS リストとフィードの追加（Add DNS Lists and Feeds）]**
- **[URL リストとフィードの追加（Add URL Lists and Feeds）]**

ステップ 4 名前を入力します。

ステップ 5 [タイプ（Type）] ドロップダウン リストから、[リスト（List）] を選択します。

ステップ 6 [参照（Browse）] をクリックしてリストの `.txt` ファイルを位置指定し、[アップロード（Upload）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

これらの変更を有効にするために再展開する必要はありません。リストからエントリを削除する方法は、グローバルセキュリティインテリジェンスリストからのエントリを削除する（1390 ページ） を参照してください。

セキュリティ インテリジェンス リストの更新

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 更新するリストの横にある[編集（Edit）]（）をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 編集するリストのコピーが必要な場合、[ダウンロード（Download）]をクリックし、ブラウザのプロンプトに従ってリストをテキスト ファイルとして保存します。

ステップ 5 必要に応じてリストを変更します。

ステップ 6 [セキュリティ インテリジェンス（Security Intelligence）] ポップアップ ウィンドウで、[参照（Browse）]をクリックして、変更されたリストを参照し、[アップロード（Upload）]をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

これらの変更を有効にするために再展開する必要はありません。リストからエントリを削除する方法は、グローバルセキュリティインテリジェンスリストからのエントリを削除する（1390 ページ） を参照してください。

シンクホール

シンクホールオブジェクトとは、シンクホール内のすべてのドメイン名のルーティング不可アドレスか、またはサーバーに解決されない IP アドレスのいずれかを付与する DNS サーバーを表します。DNS ポリシー ルール内のシンクホール オブジェクトを参照して、一致するトラフィックをシンクホールにリダイレクトすることができます。オブジェクトには、IPv4 アドレスと IPv6 アドレスの両方を割り当てる必要があります。

シンクホール オブジェクトの作成

IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [Sinkhole] を選択します。

ステップ 3 [Add Sinkhole] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 シンクホールの [IPv4 アドレス（IPv4 Address）] と [IPv6 アドレス（IPv6 Address）] を入力します。

ステップ 6 次の選択肢があります。

- シンクホール サーバーへのトラフィックをリダイレクトする場合は、[Log Connections to Sinkhole] を選択します。
- トラフィックを非解決 IP アドレスにリダイレクトするには、[Block and Log Connections to Sinkhole] を選択します。

ステップ 7 侵入の痕跡（IoC）のタイプをシンクホールに割り当てるには、[タイプ（Type）] ドロップダウンからいずれかのタイプを選択します。

ステップ 8 [保存（Save）] をクリックします。

SLA モニタ

各インターネット プロトコル サービス レベル契約（SLA）モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。要求がタイムアウトすると、そのルートはルーティング テーブルから削除され、バックアップ ルートに置き換えられます。SLA モニタリング ジョブは、デバイス設定から SLA モニターを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージング アウトしません）。インターネット プロトコル サービス レベル契約（SLA）モニタ オブジェクトは、IPv4 スタティック ルート ポリシーの [ルートトラッキング（Route Tracking）] フィールドで使用されます。IPv6 ルートでは、ルート トラッキングによって SLA モニターを使用することはできません.

これらのオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから [SLA モニター（SLA Monitor）] を選択します。

ステップ 2 [SLA モニターの追加（Add SLA Monitor）] をクリックします。

ステップ 3 [名前（Name）] フィールドにオブジェクトの名前を入力します。

ステップ 4 （オプション）[説明（Description）] フィールドにオブジェクトの説明を入力します。

ステップ 5 [頻度（Frequency）] フィールドに、ICMP エコー要求送信の頻度（秒単位）を入力します。有効な値の範囲は、1 ～ 604800 秒（7 日）です。デフォルトは 60 秒です。

（注）
頻度はタイムアウト値未満にできません。これらの値を比較するには、頻度をミリ秒に換算する必要があります。

ステップ 6 [SLA モニタ ID（SLA Monitor ID）] フィールドに SLA 操作の ID 番号を入力します。値の範囲は 1 ～ 2147483647 です。1 つのデバイスには最大で 2000 個の SLA 操作を作成できます。各 ID 番号はポリシーとデバイス設定に対して一意である必要があります。

ステップ 7 [しきい値（Threshold）] フィールドに、上昇しきい値が宣言されるまでに、ICMP エコー要求の後に経過する必要のある時間（ミリ秒単位）を入力します。有効な値の範囲は、0 ～ 2147483647 ミリ秒です。デフォルトは 5000 ミリ秒です。しきい値は、定義された値を超過したイベントを示すためだけに使用されます。これらのイベントは、タイムアウト値が適切であるかどうかを評価するために使用できます。このイベントは、モニタリング対象のアドレスへの到達可能性を直接的に示すものではありません。

（注）
しきい値はタイムアウト値を超過しないようにします。

ステップ 8 [タイムアウト（Timeout）] フィールドに、SLA 操作が ICMP エコー要求への応答を待機する時間（ミリ秒単位）を入力します。値の範囲は 0 ～ 604800000 ミリ秒（7 日）です。デフォルトは 5000 ミリ秒です。モニタリング対象のアドレスからの応答がこのフィールドに定義された時間内に受信されない場合、スタティック ルートがルーティング テーブルから削除され、バックアップ ルートに置き換えられます。

（注）
タイムアウト値は頻度値を超過できません。2 つの数値を比較するには、頻度値をミリ秒に換算してください。

ステップ 9 [データ サイズ（Data Size）] フィールドに、ICMP 要求パケット ペイロードのサイズ（バイト単位）を入力します。値の範囲は 0 ～ 16384 バイトです。デフォルトは 28 バイトです。この場合、全体の ICMP パケットは 64 バイトとなります。この値には、プロトコルまたは Path Maximum Transmission Unit（PMTU）で許可される最大値を超える値を設定しないでください。場合によっては、到達可能性を確保するために、デフォルトのデータ サイズを大きくして、ソースとターゲットの間での PMTU の違いを検出できるようにすることが必要となります。PMTU が小さいと、セッションのパフォーマンスに影響を及ぼすことがあります。セッションのパフォーマンスへの影響が検出されると、セカンダリ パスが使用されます。

ステップ 10 [ToS] フィールドに、ICMP 要求パケットの IP ヘッダーで定義されたタイプ オブ サービス（ToS）の値を入力します。値の範囲は 0 ～ 255 です。デフォルトは 0 です。このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。この情報は、ポリシールーティングのためにネットワーク上の他のデバイスが使用する場合もあれば、専用アクセス レートなどの機能によって使用される場合もあります。

ステップ 11 [パケット数（Number of Packets）] フィールドに、送信されるパケットの数を入力します。値の範囲は 1 ～ 100 です。デフォルトは 1 パケットです。

（注）
パケット損失によって、Secure Firewall Threat Defense デバイスがモニタリング対象のアドレスに到達できないと誤って認識することが懸念される場合は、デフォルトのパケット数を大きくしてください。

ステップ 12 [モニタリング対象アドレス（Monitored Address）] フィールドに、SLA 操作によって可用性がモニターされている IP アドレスを入力します。

ステップ 13 [使用可能なゾーン（Available Zones）] リストには、ゾーンとインターフェイス グループの両方が表示されます。[ゾーン/インターフェイス（Zones/Interfaces）] リストで、デバイスが管理ステーションと通信するインターフェイスを含むゾーンまたはインターフェイス グループを追加します。1つのインターフェイスを指定するには、インターフェイスにゾーンまたはインターフェイスのグループを作成する必要があります。セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成 （634 ページ）を参照してください。デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

ステップ 14 [保存（Save）] をクリックします。

時間範囲

時間範囲オブジェクトを使用して、ルールをいつ適用するのかを決定するために使用する期間を定義します。

（注） 時間ベースの ACL は、Firewall Management Center 7.0 以降の Snort 3 でもサポートされています。

時間範囲オブジェクトの作成

指定した時間範囲の間にのみポリシーを適用する場合は、時間範囲オブジェクトを作成してから、そのオブジェクトをポリシーで指定します。このオブジェクトはFirewall Threat Defenseデバイスでのみ機能することに注意してください。

時間範囲オブジェクトは、このトピックの最後にリストされているポリシータイプでのみ指定できます。

（注） タイムゾーンはデバイスのローカル時間を表し、時間範囲をサポートするポリシーのルールでその時間範囲を適用するためにのみ使用されます。タイムゾーンによってデバイスの設定された時刻が変更されることはありません。設定を確認するには、Firewall Threat Defense CLI で **show time-range timezone** および **show time** コマンドを使用します（Cisco Secure Firewall Threat Defense コマンドリファレンス ガイドを参照）。さらに、シャーシのタイムゾーンは管理センターのタイムゾーンに優先します。

始める前に

時間範囲は、トラフィックを処理するデバイスに関連付けられているタイムゾーンに基づいて適用されます。デフォルトでは、これはUTCです。デバイスに関連付けられているタイムゾーンを変更するには、[デバイス（Device）] > [プラットフォーム設定（Platform Settings）] に移動します。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2 オブジェクト タイプのリストから [時間範囲（Time Range）] を選択します。

ステップ 3 [時間範囲の追加（Add Time Range）] をクリックします。

ステップ 4 値を入力します。

次のガイドラインに従ってください。

- 入力したオブジェクト名の周りに赤色のエラー ボックスが表示された場合は、[名前（Name）] フィールドの上にマウスを置くと名前付けの制限が表示されます。
- [デバイス（Device）] > [プラットフォーム設定（Platform Settings）] でデバイスのタイムゾーンを指定しないかぎり、すべての時間は UTC です。
- 24 時間制で時間を入力します。たとえば、1:30 PM は 13:30 と入力します。
- 通常の週末の時間（夕方および夜を含む、金曜日の 5pm から月曜日の 8am まで）など、1 つの連続する範囲を指定するには、[範囲タイプ（Range Type）] に [範囲（Range）] を選択します。
- 月曜日から金曜日の 8am から 5pm まで（各日の夕方、夜、早朝を除く）など、複数の日の一部分を指定する場合は、[範囲タイプ（Range Type）] に [日次間隔（Daily Interval）] を選択します。
- 1 つのオブジェクトで最大 28 の期間を指定できます。
- 同じ曜日の複数の非連続時間、または異なる曜日の異なる時間を指定する場合は、繰り返し間隔を複数作成します。たとえば、標準の営業時間を除くすべての時間にポリシーを適用する場合は、次の 2 つの繰り返し間隔を持つ 1 つの時間範囲オブジェクトを作成します。

- 月曜日から金曜日の 5pm から 8am の [日次間隔（Daily Interval）]、および
- 金曜日の 5pm から月曜日の 8am までの [範囲（Range）] の繰り返し間隔。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

次のいずれかで時間範囲を設定します。

- アクセス コントロール ルール
- プレフィルタ ルール
- トンネル ルール
- VPN グループポリシー

VPN グループ ポリシー オブジェクトでは、[アクセス時間（Access Hours）] フィールドを使用して時間範囲オブジェクトを指定します。詳細については、グループ ポリシー オブジェクトの設定（1430 ページ）およびグループ ポリシーの詳細オプション（1438 ページ）を参照してください。

タイムゾーン

管理対象デバイスのローカルタイムゾーンを指定するには、タイムゾーンオブジェクトを作成し、デバイスに割り当てられたデバイスプラットフォーム設定ポリシーでそのオブジェクトを指定します。

このデバイスのローカルタイムは、アクセス制御、プレフィルタ、VPN グループポリシーなどの、時間範囲をサポートしているポリシーのルールで時間範囲を適用するためにのみ使用されます。デバイスにタイムゾーンを割り当てない場合、これらのポリシーで時間範囲を適用するときは、デフォルトでは UTC が使用されます。システムの他の機能では、タイムゾーンオブジェクトで指定されたタイムゾーンは使用されません。

タイムゾーンオブジェクトは、Firewall Threat Defense デバイスでのみサポートされています。

（注） 時間ベースの ACL は、Firewall Management Center 7.0 以降の Snort 3 でもサポートされています。

トンネル ゾーン

トンネル ゾーンとは、特別な分析のために明示的にタグ付けする特定のタイプのプレーン テキスト、パススルー トンネルを表します。トンネル ゾーンは、一部の設定でインターフェイスの制約として使用できますが、インターフェイス オブジェクトではありません。

詳細については、トンネル ゾーンおよびプレフィルタリング （1907 ページ）を参照してください。

URL

重要 セキュリティ インテリジェンス設定、およびアクセス コントロール ポリシーと QoS ポリシーの URL ルールにこのオプションおよび同様のオプションを使用する場合のベストプラクティスについては、手動 URL フィルタリングオプション （1834 ページ） を参照してください。

URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループ オブジェクトは複数の URL またはアドレスを定義できます。URL オブジェクトとグループは、アクセス コントロール ポリシーやイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。

URL オブジェクトを作成する場合は、次の点に注意してください。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。1 つ以上の / を含める場合、文字列の部分一致には URL 文字列全体が使用されます。次に、次のいずれかに該当する場合、URL は一致と見なされます。
  - 文字列が URL の先頭にある。
  - 文字列がドットの後に続く。
  - 文字列の先頭にドットが含まれている。
  - 文字列が :// 文字の後に続く。

  たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。

（注） サーバーは再構成でき、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部（つまり / 文字を含む URL 文字列）をブロックまたは許可するために手動の URL フィルタリングは使用しないことをお勧めします。

- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成するときに、プロトコルを指定する必要はありません。たとえば、http://example.com ではなく example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。また、システムはサブジェクト共通名に含まれるサブドメインを無視するので、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

  ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

URL オブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクト タイプのリストから [URL] を選択します。

ステップ 3 [URL の追加（Add URL）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 [URL] に、URL または IP アドレスを入力します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。

- このオブジェクトにオーバーライド値を追加する場合は、[Override]セクションを展開し、[Add]をクリックします（オブジェクトのオーバーライドの追加（1312ページ）を参照）。

ステップ8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開（172ページ）を参照してください。

変数セット

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーで変数を使用して、ルール抑制、adaptive profile updates、および動的（ダイナミック）ルール状態で IP アドレスを表すこともできます。

ヒント プリプロセッサルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。システム提供のデフォルトの変数セットを使用することも、独自のカスタムセットを作成することもできます。いずれのセット内でも、定義済みのデフォルト変数を変更したり、ユーザ定義変数を追加および変更したりできます。

システム提供の多くの共有オブジェクトルールと標準テキストルールでは、定義済みのデフォルト変数を使用してネットワークとポート番号が定義されます。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ルールがより効率的なのは、変数がユーザーのネットワーク環境をより正確に反映する場合です。少なくとも、デフォルトセットにあるデフォルト変数は変更する必要があります。`$HOME_NET` などの変数がネットワークを正しく定義し、`$HTTP_SERVERS` にネットワーク上のすべての Web サーバーが含まれていれば、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムがモニターされます。

変数を使用するには、変数セットをアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセス コントロール ポリシーによって使用されるすべての侵入ポリシーにリンクされています。

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。どの変数セット内でも、ユーザ定義変数を追加し、任意の変数の値をカスタマイズすることができます。

初めに、定義済みのデフォルト値で構成される単一のデフォルトの変数セットが提供されます。デフォルトセット内の各変数は、最初はそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値は Talos インテリジェンスグループ によって設定され、ルール更新で提供される値です。

定義済みのデフォルト変数は、そのデフォルト値に設定されたままにすることもできますが、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルトセットでのみ使用できますが、多くの場合、1つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の現在値によって、他のすべてのセットの変数のデフォルト値が決まることに注意してください。

[オブジェクト マネージャ（Object Manager）] ページで [変数セット（Variable Sets）] を選択した場合、オブジェクトマネージャには、デフォルトの変数セットと、作成したすべてのカスタム セットがリストされます。

新しくインストールされたシステムでは、デフォルトの変数セットは、Cisco で定義済みのデフォルト変数だけで構成されています。

各変数セットには、システムによって提供されるデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルトセットの名前を変更したり、削除したりすることはできないことに注意してください。

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

関連トピック

変数の管理 （1421 ページ）
変数セットの管理 （1419 ページ）

侵入ポリシー内の変数セット

Firepower システムは、デフォルトではアクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルトの変数セットをリンクします。侵入ポリシーを使用するアクセスコントロールポリシーを展開すると、その侵入ポリシー内で有効にした侵入ルールでは、リンクされた変数セットの変数値が使用されます。

アクセス コントロール ポリシー内の侵入ポリシーで使用されるカスタム変数セットを変更すると、システムの [アクセス コントロール ポリシー（Access Control Policy）] ページで、そのポリシーのステータスが「失効（out-of-date）」と表示されます。変数セットの変更内容を実装するには、アクセスコントロールポリシーを再度展開する必要があります。デフォルトセットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効（out-of-date）」と表示され、変更内容を実装するにはすべてのアクセス コントロール ポリシーを再度展開する必要があります。

変数

変数は、次のカテゴリのいずれかに属します。

デフォルト変数

Firepower システムから提供される変数。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。ただし、デフォルト変数のカスタマイズしたバージョンを作成できます。

カスタマイズされた変数

作成した変数。この変数には、次の変数があります。

- カスタマイズされたデフォルト変数

  デフォルト変数の値を編集すると、システムはその変数を [デフォルトの変数（Default Variables）] 領域から [カスタマイズされた変数（Customized Variables）] 領域に移動します。デフォルト セットの変数値によってカスタム セットの変数のデフォルト値が決まるため、デフォルトセットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

- ユーザー定義変数

  独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットすると、それは [カスタマイズされた変数（Customized Variables）] 領域に残ります。

  ユーザ定義変数は、次のいずれかのタイプにできます。

  - ネットワーク変数は、ネットワーク トラフィックのホストの IP アドレスを指定します。
  - ポート 変数は、ネットワーク トラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 `any` を指定することもできます。

たとえば、カスタム標準テキストルールを作成する場合、独自のユーザ定義変数を追加して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化したりすることもできます。また、「緩衝地帯」（つまり DMZ）でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリスト

される $DMZ という変数を作成することもできます。こうして、この地帯で作成された任意のルールで $DMZ 変数を使用できます。

拡張変数

特定の条件下で Firepower システムから提供される変数。この変数が含まれる展開は非常に限定的です。

定義済みデフォルト変数

デフォルトでは、Firepower System は、1 つのデフォルト変数セットを提供します。このセットは、定義済みのデフォルト変数から構成されています。Talos インテリジェンスグループ では、ルール更新を使用し、新しい侵入ルールや更新された侵入ルール、他の侵入ポリシーエレメント（デフォルト変数など）を提供します。

システムが提供する侵入ルールの多くが定義済みのデフォルト変数を使用していることから、これらの変数に関する適切な値を設定します。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更できます。

⚠

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

次の表では、システムによって提供される変数について説明し、通常、いずれの変数が変更されるかを示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートに問い合わせてください。

表 *69 :* システム提供変数

変数名	説明	変更しますか
$AIM_SERVERS	既知の AOL Instant Messenger（AIM）サーバを定義し、チャット ベースのルールおよび AIM エクスプロイトを検索するルールで使用されます。	不要。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバーに特に影響するルールを作成する場合、$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルールセットでは不要です。
$EXTERNAL_NET	Firepower System が非保護ネットワークとして表示されるネットワークを定義し、外部ネットワークを定義する多くのルールで使用されます。	はい。$HOME_NET を適切に定義してから、$EXTERNAL_NET の値として $HOME_NET を除外する必要があります。
$FILE_DATA_PORTS	ネットワーク ストリームでファイルを検出する侵入ルールで使用される、暗号化されていないポートを定義します。	不要。

変数名	説明	変更しますか
$FTP_PORTS	ネットワーク上の FTP サーバーのポートを定義し、FTP サーバーのエクスプロイト ルールに使用されます。	はい。FTP サーバーがデフォルト ポート以外のポートを使用する場合（web インターフェイスのデフォルト ポートを表示できます）。
$GTP_PORTS	パケット デコーダが GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）PDU 内部でペイロードを取得するデータ チャネル ポートを定義します。	不要。
$HOME_NET	関連した侵入ポリシーが監視するネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークの IP アドレスを指定する場合は変更します。
$HTTP_PORTS	ネットワーク上の Web サーバーのポートを定義し、Web サーバーのエクスプロイト ルールに使用されます。	はい。web サーバーがデフォルト ポート以外のポートを使用する場合（web インターフェイスのデフォルト ポートを表示できます）。
$HTTP_SERVERS	ネットワーク上の Web サーバを定義します。Web サーバのエクスプロイト ルールで使用されます。	HTTP サーバを実行する場合は変更します。
$ORACLE_PORTS	ネットワーク上で Oracle データベース サーバのポートを定義し、Oracle データベースでの攻撃をスキャンするルールで使用されます。	Oracle サーバを実行する場合は変更します。
$SHELLCODE_PORTS	システムにシェル コードのエクスプロイトをスキャンさせるポートを定義し、シェル コードを使用するエクスプロイトを検出するルールで使用されます。	不要。
$SIP_PORTS	ネットワーク上の SIP サーバのポートを定義し、SIP のエクスプロイト ルールに使用されます。	不要。
$SIP_SERVERS	ネットワーク上で SIP サーバを定義し、SIP をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SIP サーバーを実行している場合は、$HOME_NET を適切に定義してから、$SIP_SERVERS の値として $HOME_NET を含める必要があります。
$SMTP_SERVERS	ネットワーク上で SMTP サーバを定義し、メール サーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTP サーバを実行する場合は変更します。
$SNMP_SERVERS	ネットワーク上で SNMP サーバを定義し、SNMP サーバでの攻撃をスキャンするルールで使用されます。	SNMP サーバを実行する場合は変更します。

変数名	説明	変更しますか
$SNORT_BPF	その後バージョン5.3.0以降にアップグレードされるバージョン5.3.0 以前の Firepower System ソフトウェア リリースのシステム上に存在する場合のみに表示されるレガシー拡張変数を特定します。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
$SQL_SERVERS	ネットワーク上でデータベース サーバを定義し、データベースをターゲットとしたエクスプロイトを解決するルールで使用されます。	SQL サーバを実行する場合は変更します。
$SSH_PORTS	ネットワーク上の SSH サーバーのポートを定義し、SSH サーバーのエクスプロイト ルールに使用されます。	はい。デフォルト ポート以外の SSH サーバーのポートを使用する場合（web インターフェイスでのデフォルト ポートを表示できます）。
$SSH_SERVERS	ネットワーク上で SSH サーバを定義し、SSH をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SSH サーバーを実行している場合は、$HOME_NET を適切に定義してから、$SSH_SERVERS の値として $HOME_NET を含める必要があります。
$TELNET_SERVERS	ネットワーク上で既知の Telnet サーバを定義し、Telnet サーバをターゲットとしたエクスプロイトを解決するルールで使用されます。	Telnet サーバを実行する場合は変更します。
$USER_CONF	Web インターフェイスを介して利用可能できる場合を除き、1 つ以上の特徴を設定できる一般的なツールを提供します。 $USER_CONF の設定が競合または重複していると、システムは停止します。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

ネットワーク変数

ネットワーク変数で表される IP アドレスを、侵入ポリシーで有効にした侵入ルール、侵入ポリシー ルール抑制、動的ルール状態、およびadaptive profile updatesで使用することができます。ネットワーク変数とネットワーク オブジェクトおよびネットワーク オブジェクト グループとの相違点として、ネットワーク変数は侵入ポリシーおよび侵入ルールに固有のものです。一方、ネットワーク オブジェクトおよびグループを使用すると、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で IP アドレスを表すことができます。

次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール：侵入ルールの [送信元 IP（Source IPs）] および [宛先 IP（Destination IPs）] 見出しフィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。
- 抑制：送信元または宛先の侵入ルール抑制の [ネットワーク（Network）] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。
- 動的ルール状態：送信元または宛先の動的ルール状態の [ネットワーク（Network）] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサ ルールの一致数が多すぎる場合に、それを検出できます。
- adaptive profile updates：アダプティブ プロファイルの更新が有効にされている場合、アダプティブ プロファイルの [ネットワーク（Networks）] フィールドに、パッシブ展開でパケット フラグメントおよび TCP ストリームのリアセンブルを改善する必要があるホストが示されます。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセス コントロール ポリシーで処理されるネットワーク トラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ
- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のネットワーク オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）
- リテラルの単一 IP アドレスまたはアドレス ブロック

  それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は `any` で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は `none` です。これは「ネットワークなし」を意味します。また、リテラル値の中でアドレス `::` を指定すると、包含ネットワーク リストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレス ブロックが除外されます。つまり、除外された IP アドレスやアドレス ブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラル アドレス `192.168.1.1` を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、`2001:db8:ca2e::fa4c` を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラル ネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 `192.168.1.1` および `192.168.1.5` を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが含まれます。つまり、システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワーク リストに、値 `any` を持つ変数を追加することはできません。
- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレス ブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。

ポート変数

ポート変数は、侵入ポリシーで有効になった侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP や UDP 以外のプロトコル用にポート オブジェクトを作成して、ポート変数、アクセス コントロール ポリシー、ネットワーク検出ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。

侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドでポート変数を使用すると、パケット インスペクションを特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、アクセス コントロール ポリシーが展開されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

  使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。

- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のポート オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

  有効な変数値は TCP および UDP ポートのみです（どちらのタイプでも値 `any` を含む）。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効な

ポートオブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクトリストには表示されません。オブジェクトマネージャを使用して、変数で使われるポートオブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラルポート値とポート範囲

  ポート範囲はダッシュ（-）を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

  複数のリテラルポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わせることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は `any` で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は `none` で、これは「ポートなし」を示します。

ヒント　値 `any` を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 `any` を持つ変数を除外ポートリストに追加した場合、変数セットを保存することはできません。
- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が除外されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。

拡張変数

拡張変数を使用すると、他の方法では Web インターフェイスで設定できない機能を設定することができます。現在、システムで提供されている拡張変数は、USER_CONF 変数のみです。

USER_CONF

USER_CONF は、Web インターフェイスで通常設定できない 1 つ以上の機能を設定するための汎用ツールです。

注意 機能の説明またはサポート担当の指示に従う場合を除き、拡張変数USER_CONFを使用して侵入ポリシー機能を設定**しないで**ください。競合または重複する設定が存在すると、システムが停止します。

USER_CONFを編集するときには、1行に合計4096文字まで入力できます。行は自動的に折り返します。変数の最大長8192文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンドディレクティブでは、完全な引数の後にバックスラッシュ（\）行連結文字を使用します。

USER_CONFをリセットすると、空になります。

変数のリセット

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 *70*：変数のリセット値

リセットする変数のタイプ	それが含まれるセットタイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	any
デフォルトまたはユーザ定義	カスタム	現在のデフォルト セット値（変更/未変更にかかわらず）

カスタム セットの変数をリセットすると、単にデフォルト セット内のその変数の現在値にリセットされます。

逆に、デフォルト セットの変数の値をリセットまたは変更すると、すべてのカスタム セット内のその変数のデフォルト値が常に更新されます。リセットアイコンがグレー表示され、その変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタム セット内の変数の値をすでにカスタマイズした場合を除き、デフォルトセットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。

（注） デフォルトセット内の変数を変更するときには、その変更により、リンクされたカスタムセットの変数を使用する侵入ポリシーがどのような影響を受けるか評価するのが適切です（特に、カスタム セット内の変数値をカスタマイズしていない場合）。

変数セット内の**リセットアイコン**の上にポインタを置くと、リセット値を確認できます。カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタム セットまたはデフォルト セットの中で、値 any を持つ変数を追加した

- カスタムセットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

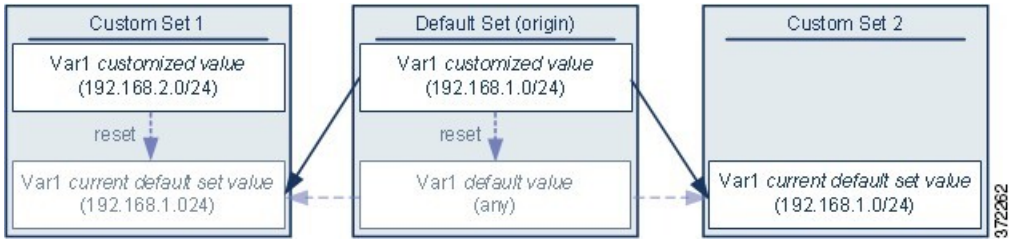
セットに変数を追加する

変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。カスタムセットから変数を追加する場合は、設定値をデフォルトセットのカスタマイズ値として使用するかどうかを選択する必要があります。

- **設定値を使用する場合**（たとえば、192.168.0.0/16）、変数は、デフォルト値 `any` を持つカスタマイズ値として設定値を使用するデフォルトセットに追加されます。デフォルトセットの現在の値によって他のセットのデフォルト値が決まるため、他のカスタムセットの初期のデフォルト値は設定値（この例では 192.168.0.0/16）になります。
- **設定値を使用しない場合**、変数はデフォルト値 `any` のみを使用してデフォルトセットに追加され、こうして、他のカスタムセットの初期のデフォルト値は `any` になります。

例：デフォルト セットへのユーザー定義変数の追加

次の図は、値が `192.168.1.0/24` のデフォルト セットにユーザ定義の変数 `Var1` を追加した場合のセットのインタラクションを示しています。



任意のセットで `Var1` の値をカスタマイズできます。`Var1` がカスタマイズされていない Custom Set 2 では、この値は `192.168.1.0/24` です。Custom Set 1 では、`Var1` のカスタマイズ値 `192.168.2.0/24` はデフォルト値をオーバーライドします。デフォルトセットのユーザ定義変数をリセットすると、すべてのセットのそのデフォルト値が `any` にリセットされます。

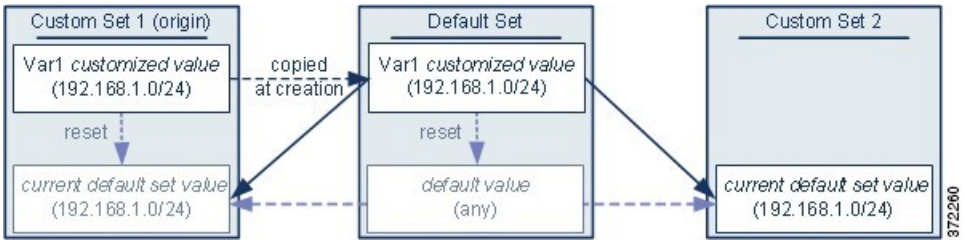
この例では、Custom Set 2 で `Var1` を更新しなかった場合、デフォルト セットで `Var1` をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 `Var1` が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間のインタラクションは、デフォルトセットのデフォルト変数をリセットすると現在のルール更新で Cisco によって設定された値に、そのデフォルト変数がリセットされること以外は、ユーザー定義変数およびデフォルト変数で同じであることに注意してください。

例：カスタム セットへのユーザー定義変数の追加

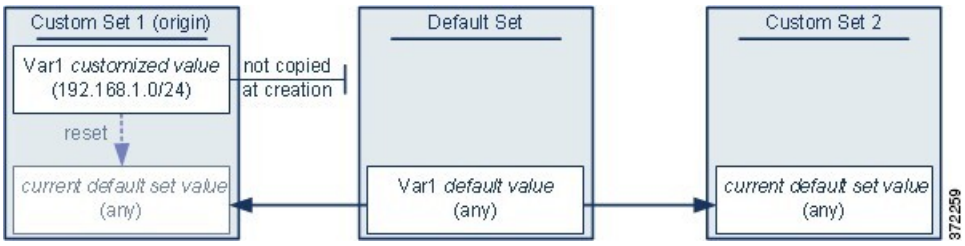
次の2つの例は、カスタムセットにユーザ定義変数を追加した場合の変数セットのインタラクションについて示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値

として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を**使用する**という選択がなされています。



Custom Set 1 からの `Var1` の発信元を除き、この例は `Var1` をデフォルト セットに追加した上述の例と同じであることに注意してください。`Var1` のカスタマイズ値 `192.168.1.0/24` を Custom Set 1 に追加すると、値はデフォルト値 `any` を持つカスタマイズ値としてデフォルト セットにコピーされます。その後、`Var1` の値とインタラクションは、`Var1` をデフォルト セットに追加した場合と同じになります。前述の例と同様、デフォルト セットで `Var1` をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 `Var1` が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の `Var1` を Custom Set 1 に追加しますが、`Var1` の設定値を他のセットのデフォルト値として**使用しない**ことを選択します。



このアプローチでは、`Var1` をデフォルト値 `any` を持つすべてのセットに追加します。`Var1` を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルト セットで `Var1` を最初にカスタマイズしないことによって、デフォルト セットの値をカスタマイズし、`Var1` をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

変数のネスト

循環したネストにならない限り、変数をネストすることができます。否定形の変数をネストすることはできません。

有効なネストされた変数

以下の例では、SMTP_SERVERS、HTTP_SERVERS、OTHER_SERVERS がネストしても有効な変数です。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザー定義	10.2.2.0/24	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

無効なネストされた変数

以下の例では、HOME_NET はネストすると無効な変数です。HOME_NET をネストすると、変数の循環になるためです。つまり、OTHER_SERVERS の定義には HOME_NET が含まれるため、HOME_NET はそれ自体でネストすることになります。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザー定義	10.2.2.0/24 HOME_NET	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

ネストでサポートされない否定形の変数

否定形の変数のネストはサポートされないため、以下の例に示されているように、保護ネットワークの外部にある IP アドレスを表す変数 NONCORE_NET を使用することはできません。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	カスタマイズされたデフォルト	—	HOME_NET
DMZ_NET	ユーザー定義	10.4.0.0/16	—
NOT_DMZ_NET	ユーザー定義	—	DMZ_NET
NONCORE_NET	ユーザー定義	EXTERNAL_NET NOT_DMZ_NET	—

ネストでサポートされない否定形の変数の代替手段

上記の例の代替手段として、以下に示す変数 NONCORE_NET を作成することで、保護ネットワークの外部にある IP アドレスを表すことができます。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	ユーザー定義	10.4.0.0/16	—
NONCORE_NET	ユーザー定義	—	HOME_NET DMZ_NET

変数セットの管理

変数セットを使用するには、IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 変数セットを管理します。

- 追加：カスタムの変数セットを追加するには、[変数セットの追加（Add Variable Set）] をクリックします。変数セットの作成 （1420 ページ）を参照してください。
- 削除：カスタムの変数セットを削除するには、変数セットの横にある[削除（Delete）]（）をクリックして、[はい（Yes）] をクリックします。デフォルトの変数セットまたは先祖ドメインに属している変数セットは削除できません。

  （注）
  削除する変数セットで作成された変数は、別のセットで削除されたり他の方法で影響を受けることはありません。

- 編集：変数セットを編集するには、変更する変数セットの横にある[編集（Edit）]（）をクリックします。オブジェクトの編集 （1306 ページ）を参照してください。
- フィルタ処理：変数セットを名前でフィルタリングするには、名前の入力を開始します。入力中にページが更新され、一致する名前が表示されます。名前のフィルタリングをクリアするには、フィルタフィールドにある[クリア（Clear）]（）をクリックします。
- 変数の管理：変数セットに含まれる変数を管理するには、変数の管理 （1421 ページ）を参照してください。

変数セットの作成

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 [変数セットの追加（Add Variable Set）] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 セット内の変数を管理します（変数の管理 （1421 ページ）を参照）。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

変数の管理

IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 編集する変数セットの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 変数を管理します。

- 表示：変数の完全な値を表示するには、変数の横の [値（Value）] 列内の値にポインタを重ねます。
- 追加：変数を追加するには、[追加（Add）]をクリックします。変数の追加 （1422 ページ）を参照してください。
- 削除：変数の横にある [削除（Delete）]（） をクリックします。変数の追加後に変数セットを保存した場合は、[はい（Yes）] をクリックして、変数の削除を確認します。

  次の変数は削除できません。

  - デフォルトの変数
  - 侵入ルールや別の変数で使用されているユーザー定義変数
  - 先祖ドメインに属している変数

- 編集：編集する変数の横にある [編集（Edit）]（） をクリックします。「変数の編集（1423 ページ）」を参照してください。
- リセット：変更した変数をデフォルト値にリセットするには、変更した変数の横にある [リセット（Reset）]をクリックします。[リセット（Reset）]がグレー表示になっている場合は、次のいずれかが当てはまります。

  - 現在の値がすでにデフォルト値になっている。
  - 設定が先祖ドメインに属している。

ヒント
アクティブな [リセット（Reset）] の上にポインタを移動して、デフォルト値を表示します。

ステップ 5 [保存（Save）]をクリックして変数セットを保存します。変数セットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。

デフォルト セットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルトセットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

変数の追加

IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 変数セット エディタで、[追加（Add）] をクリックします。

ステップ 2 [名前（Name）] に一意の変数名を入力します。

ステップ 3 [タイプ（Type）] ドロップダウン リストから、[ネットワーク（Network）] または [ポート（Port）] を選択します。

ステップ 4 変数の値を指定します。

- 使用可能ネットワークまたはポートのリストの項目を包含リストまたは除外リストに移動する場合は、1 つまたは複数の項目を選択してドラッグアンドドロップするか、[包含（Include）] または [除外（Exclude）] をクリックします。

  ヒント
  ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1 つのリテラル値を入力し、[追加（Add）]をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレスブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。
- 包含リストまたは除外リストから項目を削除するには、項目の横にある [削除（Delete）]（） をクリックします。

（注）
ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ 5 [保存（Save）] をクリックして変数を保存します。カスタムセットから新しい変数を追加する場合、次のオプションがあります。

- [Yes] をクリックすると、設定値を使用する変数がデフォルト セットのカスタマイズ値として追加され、結果として他のカスタム セットのデフォルト値として追加されます。
- [いいえ（No）] をクリックすると、変数はデフォルト セットのデフォルト値 `any` として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

ステップ 6 [保存（Save）] をクリックして変数セットを保存します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

変数の編集

IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

カスタム変数とデフォルト変数の両方を編集できます。

既存の変数の [名前（Name）] と [タイプ（Type）] の値は変更できません。

手順

ステップ 1 変数セットエディタで変更する変数の横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 2 変数を変更します。

- 利用可能なネットワークまたはポートのリストから、含める項目のリストまたは除外する項目のリストに項目を移動するには、1 つ以上の項目を選択してからドラッグ アンド ドロップするか、または [含める（Include）] か [除外（Exclude）] をクリックします。

  ヒント
  ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1 つのリテラル値を入力し、[追加（Add）] をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレスブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。

- 包含リストまたは除外リストから項目を削除するには、項目の横にある [削除（Delete）]（） をクリックします。

（注）
ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ 3 [保存（Save）] をクリックして変数を保存します。

ステップ 4 [保存（Save）]をクリックして変数セットを保存します。変数セットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

VLAN タグ

設定した個々のVLANタグオブジェクトは、1つのVLANタグまたはタグの範囲を表します。

複数の VLAN タグ オブジェクトをグループ化できます。グループは複数のオブジェクトを表します。つまり、1つのオブジェクトでVLANタグの範囲を使用することは、この意味ではグループとはみなされません。

VLANタグオブジェクトとグループは、ルールやイベント検索など、システムのWebインターフェイスのさまざまな場所で使用できます。たとえば、特定の VLAN だけに適用されるアクセス コントロール ルールを作成することができます。

VLAN タグ オブジェクトの作成

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクト タイプのリストから [VLAN タグ（VLAN Tag）] を選択します。

ステップ 3 [VLAN タグの追加（Add VLAN Tag）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドに値を入力します。VLAN タグの範囲を指定するには、ハイフンを使用します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （1312 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （1312 ページ）を参照）。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

VPN

Firewall Threat Defense デバイスでは、次の VPN オブジェクトを使用できます。これらのオブジェクトを使用するには、管理者権限が必要であり、スマート ライセンス アカウントが輸出規制を満たす必要があります。これらのオブジェクトは、リーフドメインでのみ設定できます。

証明書マップオブジェクト

証明書のマップ オブジェクトは、証明書一致ルールの名前付きセットです。これらのオブジェクトは、受信した証明書とリモート アクセス VPN 接続プロファイルとの関連付けを提供するために使用されます。接続プロファイルと証明書のマップ オブジェクトは両方とも、リモート アクセス VPN ポリシーの一部です。受信した証明書が証明書マップに含まれているルールと一致すると、接続は指定の接続プロファイルに「マッピングされている」か、関連付けられています。ルールは優先順位で整理され、UI に表示される順序で照合されます。照合は、証明書マップ オブジェクト内の最初のルールが一致したときに終了します。

ナビゲーション

[オブジェクト（Objects）] > [オブジェクトの管理（Object Management）] > [VPN] > [証明書のマップ（Certificate Map）]

フィールド

- [名前（Name）]：このオブジェクトを特定します。これにより、リモート アクセス VPN などの他の設定で参照できます。

- [マッピング条件（Mapping Criteria）]：評価する証明書の内容を指定します。証明書がこれらのルールの条件を満たしている場合、ユーザーはこのオブジェクトを含む接続プロファイルにマッピングされます。
  - [フィールド（Field）]：クライアント証明書の [件名（Subject）] または [発行元（Issuer）] に従って、一致ルールのフィールドを選択します。

    [フィールド（Field）] が [代替サブジェクト（Alternative Subject）] または [拡張キーの使用状況（Extended Key Usage）] に設定されている場合、コンポーネントは [フィールド全体（Whole Field）] として凍結されます。
  - [コンポーネント（Component）]：一致ルールに対して使用するクライアント証明書のコンポーネントを選択します。

（注） [SER（シリアル番号）コンポーネント（SER (Serial Number) component）]：[サブジェクト（Subject）] フィールドにシリアル番号を指定していることを確認します。証明書マップは、サブジェクト名内のシリアル番号属性とのみ一致します。

  - [演算子（Operator）]：一致ルールの演算子を次のうちから選択します。
    - [等しい（Equals）]：証明書コンポーネントは、入力された値と一致する必要があります。完全に一致しない場合、接続は拒否されます。
    - [含む（Contains）]：証明書コンポーネントには、入力された値が含まれている必要があります。コンポーネントにその値が含まれていない場合、接続は拒否されます。
    - [等しくない（Does Not Equal）]：証明書コンポーネントは、入力された値と等しくない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値が US と等しければ、接続が拒否されます。
    - [次を含まない（Does Not Contain）]：証明書コンポーネントには、入力された値が含まれていない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値に US が含まれていると、接続が拒否されます。
- [値（Value）]：一致ルールの値。入力された値は、選択されたコンポーネントおよび演算子と関連付けられています。

関連トピック

証明書マップの設定 （1615 ページ）

セキュアクライアント カスタム属性オブジェクト

カスタム属性は、セキュアクライアントが、Per App VPN、Allow or Defer Upgrade、および Dynamic Split Tunneling などの機能を設定するために使用します。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を 1 つ以上定義できます。Firewall Management Center を使用してセキュアクライアントカスタム属性オブジェクトを作成し、オブジェクトをグループポリシーに追加し、グループポリシーをリモートアクセス VPN に関連付けて、VPN クライアントの機能を有効にすることができます。

Firewall Threat Defense は、カスタム属性オブジェクトを使用して次の機能をサポートします。

- **Per App VPN**：Per App VPN 機能は、アプリを識別し、Firewall Threat Defense 管理者によって許可されたアプリケーションのみを VPN 経由でトンネリングするのに役立ちます。
- **Allow or Defer Upgrade**：セキュアクライアント ユーザーは、遅延アップグレードを使用して、セキュアクライアントアップグレードのダウンロードを遅らせることができます。クライアントアップデートが使用できる場合、セキュアクライアントで更新するかアップグレードを延期するかを尋ねるダイアログを開くための属性を設定できます。
- **Dynamic Split Tunneling**：Dynamic Split Tunneling を使用すると、VPN トンネルから IP アドレスまたはネットワークを含めたり除外したりするポリシーをプロビジョニングできます。ダイナミック スプリット トンネリングを設定するには、カスタム属性を作成し、グループ ポリシーに追加します。

セキュアクライアントカスタム属性を設定するための段階的な手順については、セキュアクライアントのカスタム属性オブジェクトの追加 （1427 ページ）および次を参照してください：

機能に対して設定する固有のカスタム属性の詳細については、使用しているセキュアクライアント リリースの『*Cisco Secure Client (including AnyConnect) Administrator Guide*』を参照してください。

関連トピック

グループポリシーの セキュアクライアントオプション （1434 ページ）

セキュアクライアントのカスタム属性オブジェクトの追加

始める前に

Per App VPN のカスタム属性オブジェクトを追加する前に、次のことを確認してください。

- Per App VPN が MDM 経由で適切に設定されていて、各デバイスが MDM サーバーに登録されている必要があります。
- Cisco セキュアクライアント企業アプリケーション セレクタ ツールを使用して、アプリケーションごとに Base64 エンコード文字列を作成します。

1. ここから Cisco セキュアクライアント企業アプリケーション セレクタ ツールをダウンロードします。

2. アプリケーション選択ツールを開き、左上にあるドロップダウンメニューからモバイルプラットフォームを選択します。
3. フレンドリ名とアプリケーション ID を入力してルールを追加します。残りのフィールドの指定は任意です。
4. メニューバーで、[Policy] をクリックします。エンコードされた Base65 ルールは、エンコードされた形式で表示されます。
5. ポリシー文字列を選択してコピーし、後で セキュアクライアント のカスタム属性オブジェクトを作成するときに使用するために保存します。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [カスタム属性（Custom Attributes）]** を選択します。

ステップ 2 **[Secure Clientカスタム属性の追加（Add Secure Client Custom Attribute）]** をクリックします。

ステップ 3 [Name] を入力し、任意で属性の [Description] を入力します。

ステップ 4 **[Secure Client属性（Secure Client Attribute）]** ドロップダウンリストから属性を選択します。

- [Per App VPN]：このオプションを選択し、[Attribute Value] ボックスに Base64 エンコード文字列を指定します。
- [延期更新を許可（Allow Defer Update）]：次のオプションのいずれかを選択し、セキュアクライアントの更新を許可または延期するために必要な情報を指定します。
  - [Show the prompt until user takes action]：VPN クライアントの更新を許可するか延期するかを選択するまで、VPN ユーザーにプロンプトを表示します。
  - [Show the prompt until times out]：指定した期間にプロンプトを表示し、[Timeout] ボックスで期間を指定するには、このオプションを選択します。
  - [Do not show the prompt and take automatic action]：VPN の更新を自動的に許可または延期するには、このオプションを選択します。
  - [Default Action]：ユーザーが応答しない場合、またはユーザーが介入しない自動アクションを設定する場合に実行するデフォルトアクションを選択します。セキュアクライアントを更新するか、更新を延期するかを選択できます。
  - [最小バージョン（Minimum Version）]：更新を許可または延期するために、クライアントシステムに存在する必要がある最小の Secure Client バージョンを指定します。
- [Dynamic Split Tunneling]：IP アドレスまたはネットワークを VPN トンネルに含めるか、または VPN トンネルから除外するには、このオプションを選択します。
  - [Include domains]：リモートアクセス VPN トンネルに含めるドメイン名を指定します。

- [Exclude domains]：リモートアクセス VPN トンネルから除外するドメイン名を指定します。

ステップ 5 [Allow Overrides] チェックボックスをオンにして、オブジェクトのオーバーライドを許可します。

ステップ 6 [保存（Save）] をクリックします。
カスタム属性オブジェクトがリストに追加されます。

次のタスク

カスタム属性をグループポリシーに関連付けます。グループポリシーへのカスタム属性の追加（1429 ページ）を参照してください。

グループポリシーへのカスタム属性の追加

グループポリシーをリモートアクセス VPN 接続に使用するには、Secure Client カスタム属性をグループポリシーに関連付ける必要があります。を

手順

ステップ 1 **[Objects]** > **[Object Management]** > **[VPN]** > **[Group Policy]** を選択します。

ステップ 2 新しいグループ ポリシーを追加するか、既存のグループ ポリシーを編集します。

ステップ 3 **[Secure Client]** > **[カスタム属性（Custom Attributes）]** の順にクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[Secure Client属性（Secure Client Attribute）]**（Per App VPN、Allow Defer Update、または Dynamic Split Tunneling）を選択します。

ステップ 6 リストから [Custom Attribute Object] を選択します。

（注）
[追加（Add）]（+）をクリックして、選択した Secure Client 属性の新しいカスタム属性オブジェクトを作成します。**[Objects]** > **[Object Management]** > **[VPN]** > **[Custom Attribute]** でカスタム属性オブジェクトを作成することもできます。「セキュアクライアントのカスタム属性オブジェクトの追加 （1427 ページ）」を参照してください。

ステップ 7 [Add] をクリックして属性をグループポリシーに保存し、[Save] をクリックしてグループポリシーへの変更を保存します。

関連トピック

グループポリシーの セキュアクライアントオプション （1434 ページ）

Firewall Threat Defense グループ ポリシー オブジェクト

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、リモート アクセス VPN のエクスペリエンスを定義します。たとえば、グループ ポリシー オブジェクトで、アドレス、プロトコル、接続設定などの一般的な属性を設定します。

ユーザーに適用されるグループ ポリシーは VPN トンネルが確立される際に決定されます。RADIUS 承認サーバーがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

（注） Firewall Threat Defense にグループポリシー属性の継承はありません。ユーザーについては、グループ ポリシー オブジェクトが全体として使用されます。ログイン時に AAA サーバーで特定されたグループ ポリシー オブジェクトが使用されるか、またはこれが指定されていない場合は、VPN 接続に対して設定されたデフォルトのグループ ポリシーが使用されます。指定されたデフォルトのグループポリシーはデフォルト値に設定できますが、これは、接続プロファイルに割り当てられ、他のグループ ポリシーがユーザーに対して特定されていない場合にのみ使用されます。

グループオブジェクトを使用するには、エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の セキュアクライアントライセンスのいずれかが必要です。

- Secure Client VPN のみ
- Secure Client Advantage
- Secure Client Premier

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）

グループ ポリシー オブジェクトの設定

Firewall Threat Defense グループ ポリシー オブジェクト （1430 ページ）を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]** を選択します。

以前に設定したポリシーがシステム デフォルトと共にリストされます。ユーザーのアクセス レベルに応じて、グループ ポリシーの編集、表示、または削除ができます。

ステップ 2 Click **Add Group Policy** or choose a current policy to edit.

ステップ 3 このポリシーの [名前（Name）] とオプションで [説明（Description）] を入力します。

名前には最大64文字の長さを使用でき、スペースも使用できます。説明には、最大1,024文字を使用できます。

ステップ4 グループ ポリシー一般オプション（1431ページ）の説明に従って、このグループ ポリシーの [General] パラメータを指定します。

ステップ5 グループポリシーのセキュアクライアントオプション（1434ページ）の説明に従って、このグループポリシーの **[Secure Client]** パラメータを指定します。

ステップ6 グループ ポリシーの詳細オプション（1438ページ）の説明に従って、このグループポリシーの [詳細（Advanced）] パラメータを指定します。

ステップ7 [保存（Save）] をクリックします。
新しいグループ ポリシーがリストに追加されます。

次のタスク

グループ ポリシー オブジェクトをリモート アクセス VPN 接続プロファイルに追加します。

グループ ポリシー一般オプション

ナビゲーション パス

[オブジェクト（Objects）] > **[オブジェクト管理（Object Management）]** > **[VPN]** > **[グループ ポリシー（Group Policy）]**、Click **Add Group Policy** or choose a current policy to edit. で、[全般（General）] タブを選択します。

VPN プロトコル フィールド

このグループ ポリシーを適用するときに使用できるリモート アクセス VPN トンネルのタイプを指定します。[SSL] または [IPsec IKEv2] です。

IP アドレス プール

リモート アクセス VPN のユーザ グループに固有のアドレス プールに基づいて適用される IPv4 アドレス割り当てを指定します。リモート アクセス VPN では、認証に RADIUS/ISE を使用して、識別されたユーザ グループの特定のアドレス プールから IP アドレスを割り当てることができます。特定のユーザ グループに対して、特定のグループ ポリシーを RADIUS 認証属性（GroupPolicy/Class）として設定することにより、非アイデンティティアウェア システム内のユーザまたはユーザ グループにポリシーの適用をシームレスに実行できます。たとえば、請負業者用に特定のアドレス プールを選択して、これらのアドレスを使用してポリシーの適用を行い、内部ネットワークへの制限付きのアクセスを許可する必要があります。

Firewall Threat Defense デバイスがクライアントに IPv4 アドレスプールを割り当てる優先順位：

1. IPv4 アドレス プールの RADIUS 属性
2. グループ ポリシーの RADIUS 属性
3. 接続プロファイルにマップされたグループ ポリシー内のアドレス プール

4. 接続プロファイル内の IPv4 アドレス プール

グループ ポリシーで IP アドレス プールを使用する際の制限事項の一部を以下に示します。

- IPv6 アドレス プールはサポートされていません。
- グループ ポリシーでは、最大で 6 つの IPv4 アドレス プールを設定できます。
- 使用中のアドレス プールが変更されると、展開が失敗します。アドレス プールを変更する前に、すべてのユーザをログオフする必要があります。
- アドレス プールの名前が変更されたり、重複するアドレス プールが設定されると、展開が失敗する可能性があります。変更を展開するには、古いアドレス プールを削除してから、変更されたアドレス プールを展開する必要があります。

  トラブルシューティング コマンドの一部を以下に示します。

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

バナー フィールド

ログイン時にユーザーに対して表示するバナーテキストを指定します。長さは最大491文字です。デフォルト値はありません。IPsec VPN クライアントではバナーに対してすべての HTML がサポートされますが、セキュアクライアント では 一部の HTML のみがサポートされます。バナーがリモート ユーザーに正しく表示されるようにするには、IPsec クライアントに /n タグ、SSL クライアントに
 タグを使用します。

DNS/WINS フィールド

Domain Naming System（DNS）サーバーおよび Windows Internet Naming System（WINS）サーバー。セキュアクライアント の名前解決に使用されます。

- [プライマリ DNS サーバー（Primary DNS Server）] および [セカンダリ DNS サーバー（Secondary DNS Server）]：このグループで使用する DNS サーバーの IPv4 または IPv6 アドレスを定義するネットワーク オブジェクトを選択または作成します。
- [プライマリ WINS サーバー（Primary WINS Server）] および [セカンダリ WINS サーバー（Secondary WINS Server）]：このグループで使用する WINS サーバーの IP アドレスを含むネットワーク オブジェクトを選択または作成します。
- [DHCPネットワークスコープ（DHCP Network Scope）]：目的のプールと同じサブネット上にあり、プール内にないルーティング可能なIPv4アドレスを含むネットワークオブジェクトを選択または作成します。DHCP サーバーは、この IP アドレスが属するサブネットを判別し、そのプールからのIPアドレスを割り当てます。適切に設定されていない場合、VPN ポリシーの展開は失敗します。

  接続プロファイルのアドレスプールにDHCPサーバーを設定した場合、DHCPスコープはこのグループのプールに使用するサブネットを識別します。DHCPサーバーには、そのス

コープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用するDHCPサーバーで定義されているアドレスプールのサブセットを選択できます。

ネットワーク スコープを定義しない場合、DHCPサーバはアドレス プールの設定順にプール内を探してIP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

ルーティングの目的で可能な場合は常に、インターフェイスのIP アドレスを使用することを推奨します。たとえば、プールが10.100.10.2 ～ 10.100.10.254 で、インターフェイスアドレスが10.100.10.1/24 の場合、DHCP スコープとして10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP はIPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

LINK-SELECTION（RFC 3527）およびSUBNET-SELECTION（RFC 3011）は現在サポートされていません。

- [デフォルト ドメイン（Default Domain）]：デフォルト ドメインの名前。最上位ドメイン（たとえば、example.com）を指定します。

スプリット トンネリング フィールド

スプリット トンネリングは、一部のネットワーク トラフィックをVPN トンネルに誘導して通過させ（暗号化）、残りのネットワーク トラフィックをVPN トンネルの外に誘導します（非暗号化、つまり「クリア テキストの状態」）。

- [IPv4 スプリット トンネリング/IPv6 スプリット トンネリング（IPv4 Split Tunneling/IPv6 Split Tunneling）]：デフォルトでは、スプリット トンネリングは無効です。IPv4 と IPv6 両方とも、[トンネル上ですべてのトラフィックを許可する（Allow all traffic over tunnel）]に設定されています。このままにした場合、エンドポイントからのすべてのトラフィックはVPN 接続経由で送信されます。

  スプリット トンネリングを設定するには、[次に指定されたトンネル ネットワーク（Tunnel networks specified below）] または [次に指定されたネットワークを除外（Exclude networks specified below）] を選択します。その後、そのポリシーのアクセス コントロール リストを設定します。

- [スプリット トンネル ネットワーク リスト タイプ（Split Tunnel Network List Type）]：使用するアクセス リストのタイプを選択します。[標準アクセス リスト（Standard Access List）] または [拡張アクセス リスト（Extended Access List）] を選択するか、作成します。詳細については、アクセスリスト （1319 ページ）を参照してください。

- [DNS 要求スプリット トンネリング（DNS Request Split Tunneling）]：スプリット DNS とも呼ばれます。ご使用の環境で期待されるDNS 動作を設定します。

  デフォルトでは、スプリットDNS は無効で、[スプリット トンネル ポリシーに従ってDNS 要求を送信する（Send DNS request as per split tunnel policy）] に設定されています。[DNS 要求を常にトンネル経由で送信する（Always send DNS request over tunnel）] を選択する

と、すべての DNS 要求は強制的にトンネル経由でプライベート ネットワークに送信されます。

スプリット DNS を設定するには、[指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）] を選択し、ドメイン名のリストを [ドメイン リスト（Domain List）] フィールドに入力します。これらの要求が、プライベート ネットワークにスプリット トンネルを介して解決されます。他のすべての名前は、パブリック DNS サーバーを使用して解決されます。ドメインのリストに最大 10 のエントリをカンマで区切って入力します。文字列全体は、255 文字以下である必要があります。

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）

グループポリシーの セキュアクライアントオプション

以下の仕様は、セキュアクライアント VPN の動作に適用されます。

ナビゲーション

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループポリシー（Group Policy）]。Click **Add Group Policy** or choose a current policy to edit.次に、**[Secure Client]** タブを選択します。

プロファイル フィールド

[プロファイル（Profile）]：Secure Client プロファイルを含むファイルオブジェクトを選択または作成します。オブジェクト作成の詳細については、ファイルオブジェクト （1446ページ）を参照してください。

Secure Client プロファイルは XML ファイルに格納された設定パラメータのグループです。セキュアクライアントソフトウェアは、クライアントのユーザーインターフェイスに表示される接続エントリを設定するためにこれを使用します。これらのパラメータ（XML タグ）では、追加の セキュアクライアント機能を有効にする設定も行われます。

Secure Client プロファイルを作成するには、独立した構成ツールである GUI ベースの Secure Client プロファイルエディタ を使用します。詳細については、『Cisco Secure Client (including AnyConnect) Administrator Guide』の該当するリリースの「*Secure Client* プロファイルエディタ」章を参照してください。

管理プロファイルのフィールド

管理 VPN トンネルは、エンドユーザーが VPN 経由で接続していない場合でも、エンドポイントの電源が投入されるたびに企業ネットワークへの接続を提供します。

[Management VPN Profile]：管理プロファイルファイルには、エンドポイントで管理 VPN トンネルを有効にして確立するための設定が含まれています。

スタンドアロン管理 VPN トンネル プロファイル エディタを使用して、新しいプロファイル ファイルを作成したり、既存のプロファイルファイルを変更したりできます。プロファイルエディタはシスコのソフトウェア ダウンロード センターからダウンロードできます。

プロファイルファイルの追加に関する詳細については、ファイルオブジェクト （1446ページ）を参照してください。

クライアントモジュールのフィールド

Cisco Secure Client VPN のみは、さまざまな組み込みモジュールによって、強化されたセキュリティを提供します。これらのモジュールは、Webセキュリティ、エンドポイントフローに対するネットワークの可視性、オフネットワークローミング保護などのサービスを提供します。各クライアントモジュールには、要件に応じたカスタム設定のグループを含むクライアントプロファイルが含まれています。

次の セキュアクライアント モジュールはオプションであり、VPN ユーザーが セキュアクライアントをダウンロードしたときにダウンロードされるようにこれらのモジュールを設定できます。

- **AMP イネーブラ**：エンドポイント向けの高度なマルウェア防御（AMP）を導入します。
- **DART**：トラブルシューティングのために CiscoTAC に送信できるシステムログおよびその他の診断情報のスナップショットをキャプチャします。
- **ISE ポスチャ**：OPSWAT ライブラリを使用してポスチャチェックを実行し、エンドポイントの適合性を評価します。
- **ネットワーク アクセス マネージャ**：有線とワイヤレスの両方のネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。
- **ネットワーク可視性**：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。
- **Start Before Login**：Windows のログインダイアログボックスが表示される前に セキュアクライアントを開始することにより、ユーザーを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。
- **Umbrella Roaming Security**：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。
- **Web セキュリティ**：定義されているセキュリティポリシーに基づいて、Web ページの要素を分析し、許容可能なコンテンツを許可し、悪意のあるコンテンツまたは許容できないコンテンツをブロックします。

[追加（Add）] をクリックし、クライアントモジュールごとに次を選択します。

- [クライアントモジュール（Client Module）]：リストから セキュアクライアントモジュールを選択します。
- [ダウンロードするプロファイル（Profile to download）]：Secure Client プロファイルを含むファイルオブジェクトを選択または作成します。オブジェクト作成の詳細については、ファイルオブジェクト （1446 ページ）を参照してください。
- [モジュールのダウンロードを有効化（Enable module download）]：オンにすると、エンドポイントがプロファイルとともにクライアントモジュールをダウンロードできるようにな

ります。オフの場合、エンドポイントはクライアントプロファイルだけをダウンロードできます。

各モジュールのクライアントプロファイルを作成するには、独立した設定ツールである GUI ベースの Secure Client プロファイルエディタ を使用します。Secure Client プロファイルエディタ はシスコのソフトウェア ダウンロード センターからダウンロードしてください。詳細については、『Cisco Secure Client (including AnyConnect)』の該当するリリースの「*Secure Client* プロファイルエディタ」の章を参照してください。

SSL 設定フィールド

- [SSL 圧縮（SSL Compression）]：データ圧縮を有効にするかどうか。有効にする場合は、使用するデータ圧縮の方法（[圧縮（Deflate）] または [LZS（LZS）]）。[SSL 圧縮（SSL Compression）] はデフォルトで無効になっています。

  データ圧縮は、伝送速度を上げますが、各ユーザ セッションのメモリ要件と CPU 使用率も高めます。そのため、セキュリティ アプライアンスの全体的なスループットが低下します。

- [DTLS 圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）の接続を圧縮するかどうか。[DTLS 圧縮（DTLS Compression）] はデフォルトで無効になっています。

- [MTUサイズ（MTU Size）]：Cisco Secure Client VPN のみによって確立された SSL VPN 接続の最大伝送ユニット（MTU）サイズ。デフォルトは 1406 バイト、有効な範囲は 576 ～ 1462 バイトです。

  - [DF ビットを無視（Ignore DF Bit）]：フラグメント化が必要なパケットの Don't Fragment（DF）ビットを無視するかどうか。DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。

接続設定フィールド

- **[Secure Client と VPN ゲートウェイ間のキープアライブメッセージの有効化（Enable Keepalive Messages between Secure Client and VPN gateway）]**。およびその [間隔（Interval）] 設定：トンネルでのデータ送受信にピアを使用できることを示すために、ピア間でキープアライブ メッセージを交換するかどうかを指定します。デフォルトでは有効です。キープアライブ メッセージは、設定された間隔で送信されます。有効にする場合は、リモート クライアントが IKE キープアライブ パケットの各送信間の待機時間の間隔を入力します（秒単位）。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。

- **[デッド ピア検出の有効化（Enable Dead Peer Detection on ...）]** . およびその [間隔（Interval）] 設定：デッド ピア検出（DPD）により、VPN セキュア ゲートウェイまたは VPN クライアントは、ピアが応答しなくなったこと、および接続に失敗したことを迅速に検出できます。デフォルトでは、ゲートウェイとクライアントの両方で有効です。DPD メッセージは、設定された間隔で送信されます。有効にする場合は、リモート クライアントが DPD メッセージの各送信間の待機時間の間隔を入力します（秒単位）。デフォルトの間隔は 30 秒、有効な範囲は 5 ～ 3600 秒です。

- [クライアント バイパス プロトコルを有効にする（Enable Client Bypass Protocol）]：セキュア ゲートウェイが IPv6 トラフィックだけを想定しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを想定しているときの IPv6 トラフィックの管理方法を設定することができます。

  セキュアクライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが セキュアクライアント 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合に、ヘッドエンドが IP アドレスを割り当てなかったネットワークトラフィックについて、クライアント プロトコルバイパスによってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できるようになりました。

  たとえば、セキュアゲートウェイが セキュアクライアント 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [SSL キー再生成（SSL rekey）]：クライアントが接続のキーを再生成できるようにして、暗号キーと初期化ベクターを再ネゴシエートし、接続のセキュリティを向上させます。これは、デフォルトでは無効になっています。有効にすると、再ネゴシエーションが指定された間隔で実行され、既存のトンネルのキーが再生成されるか、次のフィールドを設定して新しいトンネルが作成されます。

  - [方法（Method）]：SSL キー再生成が有効な場合に使用可能です。[新しいトンネル（New Tunnel）] を作成する（デフォルト）か、[既存のトンネル（Existing Tunnel）] の仕様を再ネゴシエーションします。

  - [間隔（Interval）]：SSL キー再生成が有効な場合に使用可能です。4 ～ 10080 分（1 週間）の範囲で 4 分のデフォルトに設定します。

- [クライアント ファイアウォール ルール（Client Firewall Rules）]：クライアント ファイアウォール ルールを使用して VPN クライアントのプラットフォームのファイアウォール設定を設定します。ルールは、送信元アドレス、宛先アドレス、プロトコルなどの条件に基づきます。拡張アクセス コントロール リスト構成要素オブジェクトを使用してトラフィックのフィルタ条件を定義します。このグループ ポリシーの拡張 ACL を選択するか、作成します。プライベート ネットワークに流れるデータを制御する [プライベート ネットワーク ルール（Private Network Rule）]、確立された VPN トンネルの外部に「クリア テキストで」流れるデータを制御する [パブリック ネットワーク ルール（Public Network Rule）]、または両方を定義します。

（注） ACL に TCP/UDP/ICMP/IP ポートのみが含まれていて、送信元ネットワークが any、any-IPv4、または any-IPv6 であることを確認します。

Microsoft Windows を実行している VPN クライアントだけが、これらのファイアウォール設定を使用できます。

カスタム属性フィールド

ここでは、セキュアクライアントが、アプリごとの VPN、アップグレードの許可または延期、およびダイナミック スプリット トンネリングなどの機能を設定するために使用する Secure Client カスタム属性を示します。[Add] をクリックして、カスタム属性をグループポリシーに追加します。

1. [Secure Client属性（Secure Client Attribute）]（[アプリごとのVPN（Per App VPN）]、[延期更新を許可（Allow Defer Update）]、または[ダイナミックスプリットトンネリング（Dynamic Split Tunneling）]）を選択します。
2. リストから [Custom Attribute Object] を選択します。

（注） [追加（Add）]（+）をクリックして、選択した Secure Client 属性の新しいカスタム属性オブジェクトを作成します。**[Objects]** > **[Object Management]** > **[VPN]** > **[Custom Attribute]** でカスタム属性オブジェクトを作成することもできます。「セキュアクライアントのカスタム属性オブジェクトの追加 （1427 ページ）」を参照してください。

3. [Add] をクリックして属性をグループポリシーに保存し、[Save] をクリックしてグループポリシーへの変更を保存します。

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）

グループ ポリシーの詳細オプション

ナビゲーション パス

[オブジェクト（Objects）] > **[オブジェクト管理（Object Management）]** > **[VPN]** > **[グループポリシー（Group Policy）]**、Click **Add Group Policy** or choose a current policy to edit.、[詳細設定（Advanced）] タブの順に選択します。

トラフィック フィルタ フィールド

- [アクセス リスト フィルタ（Access List Filter）]：フィルタは、VPN 接続を経由するトンネリングされたデータ パケットを許可するかブロックするかを決定するルールで構成され

ています。ルールは、送信元アドレス、宛先アドレス、プロトコルなどの条件に基づきます。VPN フィルタは初期接続にのみ適用されます。アプリケーション インスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。拡張アクセス コントロール リスト構成要素オブジェクトを使用してトラフィックのフィルタ条件を定義します。このグループ ポリシーの新しい拡張 ACL を選択または作成します。

- [VPN を VLAN に規制する（Restrict VPN to VLAN）]：「VLAN マッピング」とも呼ばれ、このパラメータにより、このグループ ポリシーが適用されるセッションの出力 VLAN インターフェイスが指定されます。ASA は、このグループからのすべてのトラフィックを指定された VLAN に転送します。

  この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウン リストには、デフォルト値（[無制限（Unrestricted）]）の他に、この ASA で設定されている VLAN だけが表示されます。可能な値の範囲は 1 ～ 4094 です。

セッション設定フィールド

- [アクセス時間（Access Hours）]：時間範囲オブジェクトを選択または作成します。このオブジェクトは、このグループ ポリシーがリモート アクセス ユーザに適用可能な時間範囲を指定します。詳細については、時間範囲 （1401 ページ）を参照してください。
- [ユーザーあたり同時ログイン（Simultaneous Logins Per User）]：ユーザーに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザー アクセスを禁止します。複数の同時接続を許可した場合、セキュリティの重大な問題が発生し、パフォーマンスに影響する可能性があります。
- [最大接続時間（Maximum Connection Time）]/[アラート間隔（Alert Interval）]：最大ユーザー接続時間（分単位）を指定します。ここで指定した時間が経過すると、システムは接続を停止します。最小値は 1 分です。[アラート間隔（Alert Interval）] では、最大接続時間に達してユーザーにメッセージを表示するまでの時間間隔を指定します。
- [アイドル タイムアウト（Idle Timeout）]/[アラート間隔（Alert Interval）]：このユーザーのアイドル タイムアウト期間（分単位）を指定します。この期間、ユーザ接続に通信アクティビティがなかった場合、システムは接続を停止します。最小値は 1 分です。デフォルトは 30 分です。[アラート間隔（Alert Interval）] では、アイドル時間に達してユーザーにメッセージを表示するまでの時間間隔を指定します。

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）

Firewall Threat Defense IPsec プロポーザル

IPsec プロポーザル（またはトランスフォーム セット）は VPN トポロジを設定するときに使用されます。ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエート中に、

特定のデータ フローを保護する特定のプロポーザルの使用に同意します。プロポーザルは、両方のピアで同じである必要があります。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPsec プロポーザル（またはトランスフォーム セット）オブジェクトを作成する場合、IPsec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成します。
- IKEv2 IPsec プロポーザル オブジェクトを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。IKEv2 ネゴシエーション中に、ピアは、それぞれでサポートされる最適なオプションを選択します。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 の両方の IPsec プロポーザルに使用されます。これは認証、暗号化、およびアンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

IKEv1 IPsec プロポーザル オブジェクトの設定

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IPsec IKev1 プロポーザル（IPsec IKev1 Proposal）]** を選択します。

前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを[編集（Edit）]（）、[表示（View）]（）、または [削除（Delete）]（） できます。

ステップ 2 **[IPsec IKEv1 プロポーザルの追加（Add IPsec IKEv1 Proposal）]** を選択して、新しいプロポーザルを作成します。

ステップ 3 このプロポーザルの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このプロポーザルの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [ESP 暗号化（ESP Encryption）] 方法を選択します。このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。

IKEv1 では、いずれかのオプションを選択します。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。オプションの詳しい説明については、使用する暗号化アルゴリズムの決定 （1475 ページ）を参照してください。

ステップ 6 [ESP ハッシュ（ESP Hash）] のオプションを選択します。

オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1476 ページ）を参照してください。

ステップ 7 [Save] をクリックします。
新しいプロポーザルがリストに追加されます。

IKEv2 IPsec プロポーザル オブジェクトの設定

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv2 IPsec プロポーザル（IKEv2 IPsec Proposal）]** を選択します。

前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを[編集（Edit）]（）、[表示（View）]（）、または [削除（Delete）]（） できます。

ステップ 2 **[IKEv2 IPsec プロポーザルを追加（Add IKEv2 IPsec Proposal）]** を選択し、新しいプロポーザルを作成します。

ステップ 3 このプロポーザルの **[名前（Name）]** を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このプロポーザルの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 **[ESPハッシュ（ESP Hash）]** 方法を選択して、ハッシュまたは整合性アルゴリズムを認証用プロポーザルに使用します。

（注）
Firewall Threat Defense は、NULL 暗号化を使用する IPSec トンネルをサポートしていません。IPSec IKEv2 プロポーザルには NULL 暗号化を選択しないでください。

IKEv2 では、[ESP ハッシュ（ESP Hash）] をサポートするオプションすべてを選択します。 オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1476 ページ）を参照してください。

ステップ 6 [ESP 暗号化（ESP Encryption）] 方法を選択します。このプロポーザルに Encapsulating Security Protocol（ESP）暗号化アルゴリズムを使用します。

IKEv2 では、[選択（Select）] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。オプションの詳しい説明については、使用する暗号化アルゴリズムの決定（1475 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。
新しいプロポーザルがリストに追加されます。

Firewall Threat Defense IKE ポリシー

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKEv1 では、IKE プロポーザルには、単一のアルゴリズム セットと係数グループが含まれています。複数のポリシーをプライオリティ付きで作成して、少なくとも 1 つのポリシーがリモート ピアのポリシーに一致するようにできます。IKEv1 とは異なり、IKEv2 プロポーザルでは、1 つのポリシーで複数のアルゴリズムとモジュラス グループを選択できます。フェーズ 1 のネゴシエーションでピアを選択するため、作成する IKE プロポーザルの数を 1 つにすることは可能ですが、複数の異なる IKE プロポーザルを作成して、最も望ましいオプションを高い優先順位に設定することも検討してください。IKEv2 では、ポリシー オブジェクトは認証の指定は行わず、他のポリシーで認証の要件を定義する必要があります。

サイト間 IPsec VPN を設定する際は、IKE ポリシーが必要です。詳細については、「VPN（1467 ページ）」を参照してください。

IKEv1 ポリシー オブジェクトの設定

IKEv1 ポリシー ページを使用して、IKEv1 ポリシー オブジェクトを作成、削除、または編集します。これらのポリシー オブジェクトには、IKEv1 ポリシーに必要なパラメータが含まれています。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv1 ポリシー（IKEv1 Policy）]** を選択します。

前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを [編集（Edit）]（）、[表示（View）]（）、または [削除（Delete）]（） できます。

ステップ 2 （任意）**[IKEv1 ポリシーの追加（Add IKEv1 Policy）]** を選択して、新しいポリシー オブジェクトを作成します。

ステップ 3 このポリシーの [名前（Name）] を入力します。最大 128 文字を使用できます。

ステップ 4 （任意） このプロポーザルの [説明（Description）] を入力します。最大 1,024 文字を使用できます。

ステップ 5 IKE ポリシーの [プライオリティ（Priority）] 値を入力します。

このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。有効な値の範囲は 1 ～ 65,535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。

ステップ 6 [暗号化（Encryption）] 方法を選択します。

IKEv1 ポリシーで使用する暗号化およびハッシュ アルゴリズムを決定する場合、ピア デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。IKEv1 では、いずれかのオプションを選択します。オプションの詳しい説明については、使用する暗号化アルゴリズムの決定 （1475 ページ）を参照してください。

ステップ 7 [ハッシュ（Hash）] アルゴリズムを選択して、メッセージの整合性の確保に使用されるメッセージ ダイジェストを作成します。

IKEv1 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。 オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1476 ページ）を参照してください。

ステップ 8 **[Diffie-hellman グループ（Diffie-Hellman Group）]** を設定します。

暗号化に使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があり

ます。VPN で許可するグループを選択します。 オプションの詳しい説明については、使用する Diffie-Hellman 係数グループの決定 （1477 ページ）を参照してください。

ステップ 9 セキュリティ アソシエーション（SA）の [ライフタイム（Lifetime）]（秒数）を設定します。120 ～ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。

このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

ステップ 10 2 つのピア間で使用する [認証方法（Authentication Method）] を設定します。

- [事前共有キー（Preshared Key）]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。参加ピアの 1 つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
- [証明書（Certificate）]：VPN 接続に認証方式として証明書を使用すると、ピアは PKI インフラストラクチャの CA サーバーからデジタル証明書を取得して、互いの認証で交換します。

（注）
IKEv1 をサポートする VPN トポロジでは、選択した IKEv1 ポリシー オブジェクトで指定した [認証方式（Authentication Method）] が、IKEv1 の [認証タイプ（Authentication Type）] 設定のデフォルトになります。これらの値は一致する必要があります。一致しないと設定がエラーになります。

ステップ 11 [Save] をクリックします。
新しい IKEv1 ポリシーがリストに追加されます。

IKEv2 ポリシー オブジェクトの設定

IKEv2 ポリシー ダイアログボックスを使用して、IKEv2 ポリシーオブジェクトを作成、削除、編集します。これらのポリシーオブジェクトには、IKEv2 ポリシーに必要なパラメータが含まれています。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv2 ポリシー（IKEv2 Policy）]** を選択します。

前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、ポリシーを[編集（Edit）]（）、[表示（View）]（）、または [削除（Delete）]（）することもできます。

ステップ 2 [IKEv2 ポリシーの追加（Add IKEv2 Policy）] を選択して、新しいポリシーを作成します。

ステップ 3 このポリシーの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このポリシーの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [プライオリティ（Priority）] を入力します。

IKEプロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティ ポリシーで定義されているパラメータの使用を試行します。有効な値の範囲は 1 ～ 65535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。

ステップ 6 セキュリティ アソシエーション（SA）の [ライフタイム（Lifetime）]（秒数）を設定します。120 ～ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。

このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティアソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

ステップ 7 IKE ポリシーで使用するハッシュ アルゴリズムの [整合性アルゴリズム（Integrity Algorithms）] 部分を選択します。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。

IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1476 ページ）を参照してください。

ステップ 8 フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される [暗号化アルゴリズム（Encryption Algorithm）] を選択します。

IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。 オプションの詳しい説明については、使用する暗号化アルゴリズムの決定 （1475 ページ）を参照してください。

ステップ 9 [PRF アルゴリズム（PRF Algorithm）] を選択します。

IKE ポリシーに使用されるハッシュ アルゴリズムの疑似乱数関数（PRF）部分です。IKEv1 では、整合性アルゴリズムと PRF アルゴリズムを分けることができません。ただし、IKEv2 では、これらのエレメントに対して異なるアルゴリズムを指定できます。VPN で許可するアルゴ

リズムすべてを選択します。 オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1476 ページ）を参照してください。

ステップ 10 暗号化には、**[Diffie-Hellman グループ（Diffie-Hellman Group）]** を選択します。

係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。VPN で許可するグループを選択します。 オプションの詳しい説明については、使用する Diffie-Hellman 係数グループの決定 （1477 ページ）を参照してください。

ステップ 11 [Save] をクリックします。
任意の有効な組み合わせが選択された場合、新しい IKEv2 ポリシーがリストに追加されます。選択されなかった場合、エラーが表示され、このポリシーを正常に保存するために、変更する必要があります。

ファイルオブジェクト

[ファイル オブジェクトの追加（Add File Object）] や [ファイル オブジェクトの編集（Edit File Object）] ダイアログボックスを使用して、ファイル オブジェクトを作成および編集します。ファイル オブジェクトは、通常はリモート アクセス VPN ポリシーの設定で使用するファイルを表します。これには、Secure Client プロファイル ファイルや Secure Client イメージ ファイルが含まれます。

また、プロファイルが各 AnyConnect および セキュアクライアント管理 VPN に対して、独立したプロファイルエディタを使用して作成され、Secure Client の一部としてエンドポイント上の管理者定義のエンドユーザー要件および認証ポリシーに展開されます。これにより、エンドユーザーは事前設定済みのネットワークプロファイルを使用できるようになります。

ファイル オブジェクトを作成すると、Firewall Management Center によってそのファイルのコピーがリポジトリに作成されます。これらのファイルは、データベースのバックアップを作成するたびにバックアップされ、データベースを復元すると復元されます。ファイルオブジェクトでの使用のためにファイルを Management Center プラットフォームにコピーするときは、ファイルをファイルリポジトリに直接コピーしないでください。

ファイルオブジェクトを指定する設定を展開すると、関連付けられているファイルが、デバイスの適切なディレクトリにダウンロードされます。

各ファイルに対して次のいずれかのオプションをクリックできます。

- [ダウンロード（Download）]：クリックして Secure Client ファイルをダウンロードします。
- [Edit]：ファイルオブジェクトの詳細を変更します。
- [削除（Delete）]：セキュアクライアント ファイル オブジェクトを削除します。ファイル オブジェクトを削除しても、関連付けられているファイルはファイル リポジトリから削除されず、オブジェクトのみが削除されます。

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [Secure Clientファイル]。

フィールド

- [Name]：ファイルオブジェクトを識別するファイルの名前を入力します。最大128文字まで追加できます。
- [File Name]：[Browse] をクリックしてファイルを選択します。ファイルを選択すると、ファイル名とファイルのフルパスが追加されます。
- [File Type]：選択したファイルに対応するファイルタイプを選択します。次のファイルタイプを使用できます。
  - **[Secure Clientイメージ（Secure Client Image）]**：シスコのソフトウェア ダウンロードセンターからダウンロードしたセキュアクライアントイメージを追加する場合は、このタイプを選択します。

    新規または追加のセキュアクライアントイメージを、リモートアクセスVPNポリシーに関連付けることができます。また、サポート対象外または期限切れで不要になったクライアント パッケージの関連付けを解除できます。
  - **[Secure Client VPNプロファイル（Secure Client VPN Profile）]**：Secure Client VPN プロファイルファイルにはこのタイプを選択します。

    プロファイルファイルは、独立した設定ツールであるGUIベースのSecure Client プロファイルエディタ を使用して作成されます。詳細については、『Cisco Secure Client (including AnyConnect) User Guide』の該当するリリースの「*Secure Client* プロファイルエディタ」の章を参照してください。
  - [Secure Client管理VPNプロファイル（Secure Client Management VPN Profile）]：Secure Client管理VPNトンネルのプロファイルファイルを追加する場合は、このタイプを選択します。

    シスコのソフトウェア ダウンロードセンターからSecure Client VPN Management Tunnel Standalone Profile Editor をまだダウンロードしていない場合はダウンロードして、 管理 Secure Client トンネルに必要な設定を使用してプロファイルを作成します。
  - [AMPイネーブラサービスプロファイル（AMP Enabler Service Profile）]：このプロファイルは Secure Client AMP イネーブラに使用されます。リモートアクセス VPN ユーザーが VPN に接続すると、AMP Enabler がこのプロファイルと共に Firewall Threat Defense からエンドポイントにプッシュされます。
  - [Feedback Profile]：カスタマーエクスペリエンス フィードバック プロファイルを追加し、このタイプを選択すると、顧客が有効にして使用している機能およびモジュールに関する情報を受信できます。
  - [ISEポスチャプロファイル（ISE Posture Profile）]：Secure Client ISE ポスチャモジュールのプロファイルファイルを追加する場合は、このオプションを選択します。

- [NAM Service Profile]：ネットワーク アクセス マネージャのプロファイルエディタを使用して、NAM プロファイルファイルを設定および追加します。
- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：Secure Client Network Visibility Module のプロファイルファイル。NVM プロファイルエディタを使用してプロファイルを作成できます。
- [Umbrella Roaming Security Profile]：プロファイルエディタを使用して作成された .json ファイルを使用して Umbrella ローミング セキュリティ モジュールを展開する場合は、このファイルタイプを選択する必要があります。
- [Web Security Service Profile]：Web セキュリティモジュールのプロファイルファイルを追加するときに、このファイルタイプを選択します。
- [Secure Firewall ポスチャパッケージ（ Package）]：Secure Firewall ポスチャ パッケージファイルを追加するときに、このファイルタイプを選択します。このファイルは、エンドポイントにインストールされているオペレーティングシステム、ウイルス対策、スパイウェア対策、およびファイアウォール ソフトウェアに関する情報を収集するために、ダイナミック アクセス ポリシー（DAP）を構成するときに使用されます。
- **[Secure Client外部ブラウザパッケージ（Secure Client External Browser Package）]**：このファイルタイプは、SAML シングルサインオン Web 認証用の外部ブラウザパッケージファイルを選択するためのものです。

  外部パッケージファイルの新しいバージョンが利用可能になったときに、パッケージファイルを追加できます。

  詳細については、「リモートアクセス VPN の AAA 設定（1588 ページ）」を参照してください。

- [Description]：説明を追加します（オプション）。

関連トピック

Cisco Secure Client イメージ （1611 ページ）
グループポリシーの セキュアクライアントオプション （1434 ページ）

オブジェクト管理の履歴

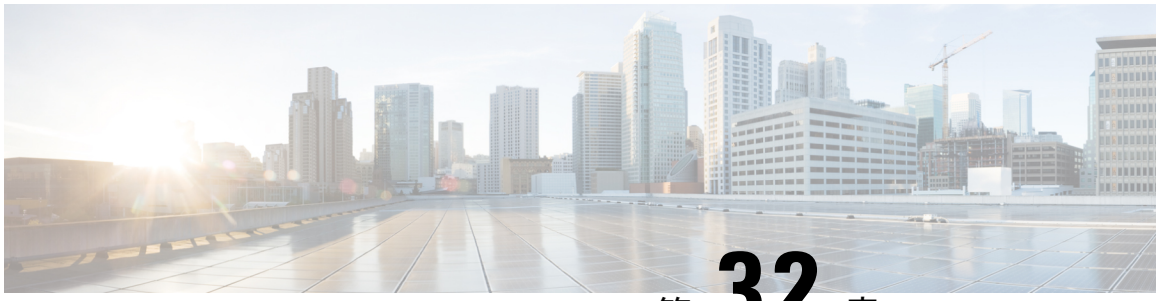
機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
DHCP IPv6 プール	任意（Any）	7.3	Firewall Threat Defense は、DHCPv6 プレフィックス委任クライアントを使用するときに、軽量の DHCPv6 ステートレスサーバーをサポートするようになりました。SLAAC クライアントが Firewall Threat Defense に情報要求（IR）パケットを送信すると、Firewall Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Firewall Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの追加/編集（Add/Edit Interfaces）] > [IPv6] > [DHCP]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [DHCP IPv6プール（DHCP IPv6 Pool）]** 新規/変更されたコマンド：**show ipv6 dhcp**
BFD テンプレート（BFD Template）	任意（Any）	7.3	以前のリリースでは、BFD は FlexConfig を介してのみ Threat Defense で設定可能でした。FlexConfig は、BFD 設定をサポートしなくなりました。Management Center の UI で Threat Defense の BFD ポリシーを設定できるようになりました。そのため、BFDテンプレートオブジェクトが導入されました。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BFD]**。 • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [BFDテンプレート（BFD Template）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ポリシーベースルーティング用の新しい [アプリケーション（Applications）] タブ	いずれか	7.1	直接インターネット アクセス ポリシー（ポリシーベースルーティング）を設定するためのアプリケーションを選択できる新しいタブが、拡張アクセスリストオブジェクトに導入されました。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）]**ページ。 サポートされているプラットフォーム： Secure Firewall Management Center
新しい拡張コミュニティ リスト オブジェクトおよび	いずれか	7.1	ポリシーリストおよびルートマップオブジェクトで使用するために、拡張コミュニティ リスト オブジェクトが導入されました。拡張コミュニティ リスト オブジェクトは、仮想ルータの BGP ルートリークサポートにおいて、ルートのインポートまたはエクスポートにのみ適用できます。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [コミュニティリスト（Community List）] > [拡張コミュニティ（Extended Community）]**ページ。 サポートされているプラットフォーム： Secure Firewall Management Center
ポリシーリストオブジェクトおよびルートマップオブジェクトの機能拡張	いずれか	7.1	ポリシーリストおよびルートマップで新しく導入された拡張コミュニティ リスト オブジェクトを選択するためのオプション。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ポリシーリスト（Policy List）] > [コミュニティルール（Community Rule）]**タブおよび **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ルートマップ（Route Map）] > [BGP] > [コミュニティ リスト（Community List）]**タブ。 サポートされているプラットフォーム： Secure Firewall Management Center
Snort 3 の時間ベース ACL のサポート	任意（Any）	7.0	アクセス コントロール ポリシーとプレフィルタポリシーの時間ベースのルールは、Snort 3 でもサポートされています。 サポートされているプラットフォーム： Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
証明書の登録用のEST	任意（Any）	7.0	証明書の登録用の Enrollment over Secure Transport のサポートが提供されました。 新規/変更された画面：**[オブジェクト（Objects）]** > **[PKI]** > **[証明書の登録（Cert Enrollment）]** > **[CA情報（CA Information）]**タブ。 サポートされているプラットフォーム： Secure Firewall Management Center
EdDSA証明書タイプのサポート	任意（Any）	7.0	新しい証明書キータイプ：EdDSA（キーサイズ 256）が追加されました。 新規/変更された画面：**[オブジェクト（Objects）]** > **[PKI]** > **[証明書の登録（Cert Enrollment）]** > **[キー（Key）]**。 サポートされているプラットフォーム： Secure Firewall Management Center
暗号とキーサイズの制限	任意（Any）	7.0	RSA 暗号化署名アルゴリズムを使用した SHA-1、および RSA キーサイズが 2048 ビット未満の SHA-1 を持つ証明書はサポートされていません。既存の証明書に対するこれらの制限をオーバーライドするには、Firewall Threat Defense で弱い暗号のオプションを有効にします。ただし、サイズが 2048 ビット未満の RSA キーは生成できません。 新規/変更された画面：**[デバイス（Devices）]** > **[証明書（Certificates）]** を設定するときの新しいトグルボタン。 サポートされているプラットフォーム： Secure Firewall Management Center
セキュリティインテリジェンスフィードのオプション	いずれか	6.7	カスタム セキュリティ インテリジェンス フィードの新しい更新頻度オプション（5 分と 15 分）。 更新頻度が 30 分未満の場合は、フィードが変更されていない場合に不要なダウンロードが行われないように、MD5 URL が必要です。 新規/変更された画面：**[セキュリティ インテリジェンス（Security Intelligence）]** > **[ネットワーク リストおよびフィード（Network Lists and Feeds）]**を設定するときの新しい頻度の選択肢。 サポートされているプラットフォーム： Secure Firewall Management Center

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
カンマ区切り値（csv）ファイルを使用したオブジェクトの一括アップロード	いずれか	6.7	オブジェクトは、カンマ区切り値ファイルからインポートできます。1 回の試行で最大 1000 個のオブジェクトをインポートできます。 新規/変更された画面：次のオブジェクトタイプについて、[[オブジェクトタイプ]の追加（Add [Object Type]）] ドロップダウンリストに、新しい [オブジェクトのインポート（Import Object）] オプションがあります。 • **[識別名（Distinguished Name）]** > **[個々のオブジェクト（Individual Objects）]** • **[ネットワーク オブジェクト（Network Object）]** • **ポート（Port）** • **URL** • **VLAN タグ** サポートされているプラットフォーム： Secure Firewall Management Center
インターフェイスオブジェクトが使用されているポリシーの表示	任意（Any）	6.6	インターフェイス オブジェクトが使用されているポリシーを表示します。 新規/変更された画面：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** の **[インターフェイス（Interface）]** オブジェクト ページには新しい **[検索（Find）]** ボタンがあります。 サポートされているプラットフォーム： Secure Firewall Management Center
タイムゾーンオブジェクトの導入	任意（Any）	6.6	時間ベースのポリシーを適用するときに使用するために、タイムゾーンを Firewall Threat Defense デバイスに割り当てることができます。 新規/変更された画面：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**の新しい**[タイムゾーンオブジェクト（Time Zone Object）]**。 サポートされているプラットフォーム： Secure Firewall Management Center

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
アクセスコントロールポリシーとプレフィルタポリシーで時間ベースのオブジェクトが使用可能に	任意（Any）	6.6	アクセス コントロール ポリシーとプレフィルタポリシーで時間ベースのルールを適用するために、時間範囲オブジェクトを新しいタイムゾーンオブジェクトと組み合わせて使用します。 適用するルールの絶対時間または反復時間、あるいは時間範囲を指定できます。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。
プレフィルタルールページからのオブジェクトの詳細の表示	任意（Any）	6.6	導入された機能：プレフィルタルールを表示するときに、オブジェクトまたはオブジェクトグループの詳細を表示するオプション。 新しいオプション：プレフィルタルールリストの次のいずれかの列の値を右クリックすると、オブジェクトの詳細を表示するオプションが提供されます：[送信元ネットワーク（Source Networks）]、[接続先ネットワーク（Destination Networks）]、[送信元ポート（Source Port）]、[接続先ポート（Destination Port）]、および[VLANタグ（VLAN Tag）]。 サポートされているプラットフォーム： Secure Firewall Management Center



第 32 章

証明書

- 証明書の要件と前提条件 （1455 ページ）
- Secure Firewall Threat Defense VPN 証明書の注意事項と制約事項 （1455 ページ）
- Firewall Threat Defense 証明書の管理 （1456 ページ）
- 自己署名登録を使用した証明書のインストール （1460 ページ）
- EST 登録を使用した証明書のインストール （1461 ページ）
- SCEP の登録を使用した証明書のインストール （1462 ページ）
- 手動登録を使用した証明書のインストール （1463 ページ）
- PKCS12 ファイルを使用した証明書のインストール （1464 ページ）
- Firewall Threat Defense 証明書のトラブルシューティング （1465 ページ）
- 証明書の履歴 （1466 ページ）

証明書の要件と前提条件

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

Secure Firewall Threat Defense VPN 証明書の注意事項と制約事項

- PKI 登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに、証明書の登録プロセスが開始されます。プロセスは、自己署名および SCEP 登録タイ

プの場合は自動的に行われます。管理者による追加のアクションは必要ありません。手動証明書登録では、管理者によるアクションが必要になります。

- 証明書の登録が完了すると、証明書の登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。VPN認証方式の設定でこのトラストポイントを使用します。
- Firewall Threat Defenseデバイスは、Microsoft Certificate Authority（CA）サービスと、Cisco適応型セキュリティアプライアンス（ASA）およびCisco IOSルータで提供されるCAサービスを使用した証明書の登録をサポートしています。
- Firewall Threat Defenseデバイスは、認証局（CA）として設定することはできません。

ドメインとデバイス間での証明書管理ガイドライン

- 証明書の登録は、子ドメインまたは親ドメインで行うことができます。
- 親ドメインからの登録が完了したら、証明書の登録オブジェクトも同じドメイン内に存在する必要があります。デバイスのトラストポイントが子ドメインで上書きされた場合、上書きされた値がデバイスに展開されます。
- リーフドメインのデバイスで証明書の登録が行われる場合、その登録は親ドメインまたは他の子ドメインに表示されます。また、証明書を追加することもできます。
- リーフドメインが削除されると、含まれているデバイス上の証明書の登録が自動的に削除されます。
- あるドメインに登録されている証明書を持つデバイスは、他のドメインに登録できます。他のドメインに証明書を追加できます。
- あるドメインから別のドメインにデバイスを移動すると、証明書もそれに応じて移動します。これらのデバイスの登録を削除するための警告が表示されます。

Firewall Threat Defense 証明書の管理

デジタル証明書の概要については、PKI インフラストラクチャとデジタル証明書 （1479 ページ）を参照してください。

管理対象デバイスの証明書を登録および取得するために使用するオブジェクトの説明については、証明書の登録オブジェクト （1363 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[証明書（Certificates）]** を選択します。

この画面には、リスト表示されるデバイスごとに次の列が表示されます。

- [名前（Name）]：すでにトラストポイントが関連付けられているデバイスがリスト表示されます。デバイスを展開して、関連付けられたトラストポイントのリストを確認します。

- [ドメイン（Domain）]：特定のドメインに登録された証明書が表示されます。
- [登録タイプ（Enrollment Type）]：トラストポイントに使用される登録のタイプが表示されます。
- [ステータス（Status）]：[CA 証明書（CA Certificate）] と [アイデンティティ証明書（Identity Certificate）] のステータスが表示されます。虫めがねをクリックすることで、証明書の内容を表示できます（`Available` の場合）。

  CA 証明書の情報を表示すると、CA 証明書を発行したすべての認証局の階層を確認できます。

  登録に失敗した場合は、ステータスをクリックして失敗メッセージを表示します。
- 証明書で弱い暗号の使用を有効にするには、右側の [Enable weak-crypto] をクリックします。トグルボタンをクリックすると、弱い暗号を有効にする前に確認のための警告が表示されます。[Yes] をクリックして、弱い暗号を有効にします。

  （注）
  弱い暗号の使用が原因で証明書の登録が失敗した場合は、弱い暗号を有効にすることを求めるメッセージが表示されます。弱い暗号化を使用する必要がある場合は、弱い暗号を有効にするができます。
- 追加の列には、次のタスクを実行するためのアイコンが一覧表示されます。
  - 証明書のエクスポート：クリックして、証明書のコピーをエクスポートおよびダウンロードします。PKCS12（完全な証明書チェーン）形式または PEM（アイデンティティ証明書のみ）形式のエクスポートを選択できます。

    PKCS12 証明書形式でエクスポートして後でファイルをインポートするには、パスフレーズを指定する必要があります。
  - 証明書の再登録：既存の証明書を再登録します。
  - 証明書ステータスの更新：証明書を更新して、Firepower Threat Defense デバイスの証明書ステータスを Firepower Management Center に同期させます。
  - 証明書の削除：トラストポイントに関連付けられているすべての証明書を削除します。

ステップ 2 [（+）追加（(+) Add）] を選択して、登録オブジェクトをデバイスに関連付けてインストールします。

証明書登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに、証明書登録プロセスが開始されます。プロセスは、自己署名および SCEP 登録タイプの場合は自動的に行われます。つまり、管理者による追加のアクションは必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。

（注）
デバイス上の証明書の登録ではユーザーインターフェイスがブロックされず、登録プロセスはバックグラウンドで実行され、ユーザーは他のデバイスで証明書の登録を並行して実行できま

す。これらの並列操作の進行状況は、同じユーザインターフェイスでモニタできます。それぞれのアイコンには、証明書の登録ステータスが表示されます。

関連トピック

自己署名登録を使用した証明書のインストール （1460 ページ）
SCEP の登録を使用した証明書のインストール （1462 ページ）
手動登録を使用した証明書のインストール （1463 ページ）
PKCS12 ファイルを使用した証明書のインストール （1464 ページ）

CA バンドルの自動更新

CLI コマンドを使用して CA 証明書を自動的に更新するように Management Center を設定できます。デフォルトでは、バージョン 7.0.5 をインストールまたは 7.0.5 にアップグレードすると、CA 証明書が自動的に更新されます。

（注） IPv6 のみの展開では、一部のシスコのサーバーが IPv6 をサポートしていないため、CA 証明書の自動更新が失敗することがあります。このような場合は、**configure cert-update run-now force** コマンドを使用して CA 証明書を強制的に更新します。

手順

ステップ 1 SSH を使用して FMC CLI にログインします。仮想の場合は VM コンソールを開きます。

ステップ 2 ローカルシステムの CA 証明書が最新の証明書であるか確認できます。

configure cert-update test

このコマンドは、ローカルシステムの CA バンドルを（シスコサーバーからの）最新の CA バンドルと比較します。CA バンドルが最新の場合、接続チェックは実行されず、以下の例のようなテスト結果が表示されます。

例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

CA バンドルが古い場合、ダウンロードされた CA バンドルに対して接続チェックが実行され、テスト結果が表示されます。

例：

接続チェックが失敗した場合：

```
> configure cert-update test
Test failed, not able to fully connect.
```

例：

接続チェックが成功した場合、または CA バンドルがすでに最新の場合：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

ステップ 3 （任意）CA バンドルをすぐに更新する場合：

configure cert-update run-now

例：

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

このコマンドを実行すると、（シスコサーバーからの）CA 証明書が SSL 接続に対して検証されます。シスコサーバーのうち 1 つでも SSL 接続チェックが失敗した場合、プロセスは終了します。

例：

```
> configure cert-update run-now
Certs failed some connection checks.
```

接続に失敗しても更新を続行するには、**force** キーワードを使用します。

例：

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

ステップ 4 CA バンドルが自動的に更新されないようにする場合は、構成を無効にします。

configure cert-update auto-update disable

例：

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

ステップ 5 CA バンドルの自動更新を再度有効にするには、次のコマンドを入力します。

configure cert-update auto-update enable

例：

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

CA 証明書の自動更新を有効にすると、更新プロセスはシステムで定義された時刻に毎日実行されます。

ステップ 6 （任意）CA 証明書の自動更新のステータスを表示します。

show cert-update

例：

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

自己署名登録を使用した証明書のインストール

手順

ステップ 1 [デバイス（Devices）] > [証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [Device] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [自己署名（Self-Signed）] の証明書登録オブジェクトを選択します。
- [(+)] をクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加 （1365 ページ） を参照してください。

ステップ 4 [追加（Add）] をクリックして、自己署名の自動登録プロセスを開始します。

自己署名登録タイプのトラストポイントの場合は、[CA 証明書（CA Certificate）] ステータスが常に表示されます。これは、管理対象デバイス自体が独自の CA として機能し、独自のアイデンティティ証明書を生成するために CA 証明書を必要としないためです。

[ID 証明書（Identity Certificate）] は、デバイスが独自の自己署名アイデンティティ証明書を作成すると、InProgress から Available に変化します。

ステップ 5 虫めがねをクリックして、このデバイスの自己署名アイデンティティ証明書を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

EST 登録を使用した証明書のインストール

始める前に

（注） EST 登録を使用すると、管理対象デバイスと CA サーバーとの間に直接接続が確立されます。したがって、登録プロセスを開始する前に、デバイスが CA サーバーに接続されていることを確認してください。

（注） 証明書の有効期限が切れたときにデバイスを自動登録する EST の機能はサポートされていません。

手順

ステップ 1 [Devices] > [Certificates] 画面で [Add] をクリックして、[Add New Certificate] ダイアログを開きます。

ステップ 2 [Device] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- [Cert Enrollment] ドロップダウンリストから EST 証明書登録オブジェクトを選択します。
- [(+)] をクリックして新しい 証明書の登録オブジェクト を追加します（証明書の登録オブジェクトの追加 （1365 ページ）を参照）。

ステップ 4 [Add] をクリックして、デバイスに証明書を登録します。

[Identity Certificate] は、デバイスが EST を使用したアイデンティティ証明書を指定の CA から取得すると、[InProgress] から [Available] に変化します。場合によっては、アイデンティティ証明書の取得には手動更新が必要になります。

ステップ 5 虫めがねをクリックして、このデバイスに作成してインストールしたアイデンティティ証明書を表示します。

SCEP の登録を使用した証明書のインストール

始める前に

（注） SCEP 登録を使用すると、管理対象デバイスと CA サーバーとの間に直接接続が確立されます。したがって、登録プロセスを開始する前に、デバイスが CA サーバーに接続されていることを確認してください。

手順

ステップ 1 [デバイス（Devices）] > [証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [Device] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [SCEP] の証明書登録オブジェクトを選択します。
- [(+)] をクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加 （1365 ページ） を参照してください。

ステップ 4 [追加（Add）] をクリックして、自動登録プロセスを開始します。

SCEP 登録タイプのトラストポイントの場合、[CA 証明書（CA Certificate）] ステータスは、CA サーバから CA 証明書が取得され、デバイスにインストールされると、InProgress から Available に遷移します。

[アイデンティティ証明書（Identity Certificate）] は、デバイスが SCEP を使用したアイデンティティ証明書を指定の CA から取得すると、`InProgress` から `Available` に変化します。場合によっては、アイデンティティ証明書の取得には手動更新が必要になります。

ステップ 5 虫めがねをクリックして、このデバイスに作成してインストールしたアイデンティティ証明書を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

手動登録を使用した証明書のインストール

手順

ステップ 1 [デバイス（Devices）] > [証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [Device] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [マニュアル（Manual）] の証明書登録オブジェクトを選択します。
- [(+)] をクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加 （1365 ページ） を参照してください。

ステップ 4 [追加（Add）] をクリックして、登録プロセスを開始します。

ステップ 5 アイデンティティ証明書を取得するための PKI CA サーバーに対する適切なアクティビティを実行します。

a) [アイデンティティ証明書（Identity Certificate）] の警告をクリックして、CSR を表示してコピーします。

b) この CSR を使用してアイデンティティ証明書を取得するための PKI CA サーバーに対する適切なアクティビティを実行します。

このアクティビティは、Secure Firewall Management Center または管理対象デバイスとは完全に無関係です。完了すると、管理対象デバイスのアイデンティティ証明書が生成されます。これをファイルに配置できます。

c) 手動プロセスを終了するには、取得したアイデンティティ証明書を管理対象デバイスにインストールします。

Secure Firewall Management Center ダイアログに戻って、[アイデンティティ証明書の参照（Browse Identity Certificate）] を選択して、アイデンティティ証明書ファイルを選択します。

（注）
バイナリ証明書（PKCS12、DER など）ファイルは Firewall Threat Defense でサポートされていないため、選択しないでください。

ステップ 6 [インポート（Import）] を選択して、アイデンティティ証明書をインポートします。

[アイデンティティ証明書（Identity Certificate）] のステータスは、インポートが完了すると `Available` になります。

ステップ 7 虫めがねをクリックして、このデバイスの [アイデンティティ証明書（Identity Certificate）] を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

PKCS12 ファイルを使用した証明書のインストール

手順

ステップ 1 [デバイス（Devices）] > [証明書（Certificates）] 画面の順に移動し、[追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウンリストから、事前設定された管理対象デバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウン リストから PKCS タイプの 証明書の登録オブジェクト を選択します。
- [(+)] をクリックして新しい 証明書の登録オブジェクト を追加します（証明書の登録オブジェクトの追加 （1365 ページ）を参照）。

ステップ 4 [ツイカ（Add）] を押します。

[CA証明書（CA Certificate）] および [アイデンティティ証明書（Identity Certificate）] のステータスは、デバイスに PKCS12 ファイルがインストールされるときに `In Progress` から `Available` に変化します。

（注）
初めて PKCS12 ファイルをアップロードすると、ファイルが CertEnrollment オブジェクトの一部として Firewall Management Center に格納されます。不正なパスフレーズや展開の失敗が原因で登録できなかった場合は、ファイルをアップロードせずに PKCS12 証明書の登録を再試行します。また、登録を成功させるには、オーバーライドを許可するように証明書の登録オブジェクトを変更するたびに、証明書の [パスフレーズ（Passphrase）] を更新する必要があります。PKCS12 ファイル サイズは 24 K を超えてはなりません。

ステップ 5 `Available` になったら、虫めがねをクリックして、このデバイスのアイデンティティ証明書を表示します。

次のタスク

管理対象デバイスの証明書（トラストポイント）には、PKCS#12 ファイルと同じ名前が付けられます。この証明書は、VPN 認証設定で使用します。

Firewall Threat Defense 証明書のトラブルシューティング

Secure Firewall Threat Defense VPN 証明書の注意事項と制約事項（1455 ページ）を参照して、証明書の登録環境のバリエーションが原因で問題が発生しているかどうかを判断してください。その後、次の点を確認します。

- デバイスから CA サーバへのルートがあることを確認します。

  CA サーバのホスト名が登録オブジェクトで指定されている場合、Flex コンフィギュレーションを使用して、サーバに到達できるように DNS を適切に設定します。あるいは、CA サーバの IP アドレスを使用することもできます。

- Microsoft 2012 CA サーバを使用している場合、デフォルトの IPsec テンプレートは管理対象デバイスで受け入れられないため、これを変更する必要があります。

  作業テンプレートを設定するには、MS CA のドキュメントを参照しながら次の手順に従います。

  1. IPsec（オフライン要求）テンプレートを複製します。
  2. [拡張子（Extensions）]>[アプリケーションポリシー（Application policies）] で、[*IP*セキュリティ*IKE*中間（*IP security IKE intermediate*）] ではなく、[*IP*セキュリティ末端システム（*IP security end system*）] を選択します。
  3. アクセス許可とテンプレート名を設定します。
  4. 新しいテンプレートを追加し、レジストリ設定を変更して新しいテンプレート名を反映させます。

- Firewall Management Center で、Firewall Threat Defense デバイスに関連する次のヘルスアラートが表示される場合があります。

  ```
  Code - F0853; Description - default Keyring's certificate is invalid, reason: expired
  ```

  （コード：F0853。説明：デフォルトのキーリングの証明書が無効です。理由：期限切れ。）

  解決策：このような場合は、CLISH CLI で、次のコマンドを使用してデフォルトの証明書を再生成します。

  ```
  > system support regenerate-security-keyring default
  ```

- CA 証明書のステータスに赤いバツ印が表示され、次のエラーが発生します。

  ```
  CA 証明書の設定に失敗する
  ```

  解決策：FMC での証明書エラーのトラブルシュートを参照してください。

- .pfx ファイル内の証明書のリストを確認するには、`certutil` や `openssl` などのツールを使用します。ID 証明書、SubCA 証明書、および CA 証明書（存在する場合）を含むチェーン全体を確認できます。
  - `certutil -dump cert.pfx`
  - `openssl pkcs12 -info -in cert.pfx`
- 次のエラーが表示されます。

  `ID 証明書のインポートが必要`

  解決策：FMC の「アイデンティティ証明書のインポートが必要」証明書エラーのトラブルシュートを参照してください。

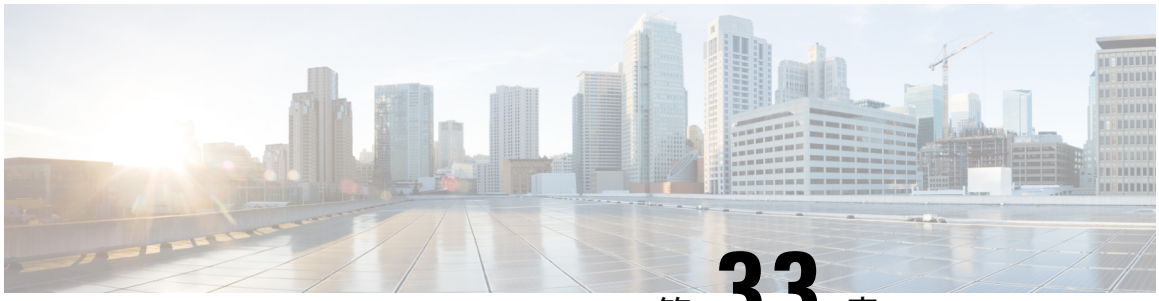
証明書の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
手動登録の拡張機能	6.7	いずれか	アイデンティティ証明書なしで、CA 証明書のみを作成できるようになりました。CA 証明書がなくても CSR を生成し、CA からアイデンティティ証明書を取得することができます。
PKCS CA チェーン	6.7	いずれか	証明書を発行する認証局（CA）のチェーンを表示および管理できるようになりました。証明書のコピーをエクスポートすることもできます。

第 VI 部

VPN

- VPN の概要 （1469 ページ）
- サイト間 VPN （1485 ページ）
- リモート アクセス VPN （1557 ページ）
- ダイナミック アクセス ポリシー （1683 ページ）
- VPN のモニタリングとトラブルシューティング （1699 ページ）



第 33 章

VPN の概要

バーチャルプライベートネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介してエンドポイント間の安全なトンネルを確立します。

この章は、Secure Firewall Threat Defense デバイス上のリモート アクセスおよびサイト間 VPN に適用されます。サイト間およびリモート アクセス VPN の構築に使用される Internet Protocol Security（IPsec）、Internet Security Association and Key Management Protocol（ISAKMP、または IKE）および SSL 規格について説明します。

- VPN タイプ （1469 ページ）
- VPN の基本 （1470 ページ）
- VPN パケット フロー （1473 ページ）
- IPsec フローのオフロード （1473 ページ）
- VPN ライセンス （1474 ページ）
- VPN 接続をセキュアにする方法 （1475 ページ）
- 削除または廃止されたハッシュアルゴリズム、暗号化アルゴリズム、およびDiffie-Hellman モジュラスグループ （1480 ページ）
- VPN トポロジ オプション （1481 ページ）

VPN タイプ

Firewall Management Center は次のタイプの VPN 接続をサポートします。

- Firewall Threat Defense デバイス上のリモート アクセス VPN。

  リモート アクセス VPN は、リモート ユーザと会社のプライベート ネットワーク間のセキュアな暗号化接続、またはトンネルです。接続は、社内のプライベート ネットワークのエッジにある、VPN クライアント機能を備えたワークステーションやモバイル デバイスである VPN エンドポイント デバイス、VPN ヘッドエンド デバイス、またはセキュア ゲートウェイで構成されます。

  Secure Firewall Threat Defense デバイスは SSL 経由のリモート アクセス VPN または Firewall Management Center による IPsec IKEv2 をサポートするように設定できます。このデバイスは、この容量でセキュアなゲートウェイとして機能して、リモート ユーザを認証し、アクセスを許可し、データを暗号化してネットワークへのセキュアな接続を提供します。Firewall

Management Center によって管理されるその他のタイプのアプライアンスは、リモート アクセス VPN 接続をサポートしていません。

Secure Firewall Threat Defense セキュア ゲートウェイは、Secure Client の完全なトンネル クライアントをサポートしています。このクライアントは、リモート ユーザにセキュアな SSL IPsec IKEv2 接続を提供するために必要です。接続時にクライアント プラットフォームに展開できるため、このクライアントにより、ネットワーク管理者がリモートコンピュータにクライアントをインストールして設定しなくても、リモートユーザはクライアントを活用できます。これは、エンドポイントデバイスでサポートされている唯一のクライアントです。

- Firewall Threat Defense デバイス上のサイト間 VPN。

  サイト間 VPN は、地理的に異なる場所にあるネットワークを接続します。管理対象デバイス間、および管理対象デバイスと関連するすべての規格に準拠するその他のシスコまたはサードパーティのピアとの間で、サイト間IPsec接続を作成できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコル スイートと IKEv1 または IKEv2 を使用して構築されます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。

VPN の基本

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモートユーザと企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

IPsec ベースの VPN テクノロジーは、Internet Security Association and Key Management Protocol（ISAKMP または IKE）と IPsec トンネリング標準を使用して、トンネルの構築と管理を行います。ISAKMP と IPsec は、次の処理を実行できます。

- トンネル パラメータのネゴシエーション。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネル経由のデータ転送の管理。
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理。

VPN内のデバイスは、双方向のトンネルエンドポイントとして機能します。プライベートネットワークからプレーンパケットを受信してカプセル化し、トンネルを作成して、カプセル化したパケットをトンネルのもう一方の終端に送信します。トンネルの終端では、パケットのカプ

セル化が解除されて最終的な宛先に送信されます。また、カプセル化されたパケットをパブリック ネットワークから受信してカプセル化を解除し、プライベート ネットワーク上の最終的な宛先に送信します。

サイト間 VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストが、セキュアな VPN トンネルを介してリモート ゲートウェイの背後にあるホストに接続します。接続は、2 つのゲートウェイの IP アドレスとホスト名、それらの背後のサブネット、2 つのゲートウェイが相互認証に使用する方式で構成されます。

ハブ：1 つ以上のリモートブランチデバイスまたはスポークとの間でセキュアな VPN 接続を可能にするデバイスです。ハブは、スポーク同士が相互通信するためのゲートウェイとしても機能します。

スポーク：VPN を介してハブに接続し、ハブの背後にある企業リソースにセキュアにアクセスするデバイスです。スポーク同士は、ハブを介して相互に通信します。

Internet Key Exchange（IKE）

インターネット キー交換（IKE）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、およびセキュリティ アソシエーション（SAs）の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE ポリシーは、2 つのピア間の IKE ネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、どのセキュリティ パラメータが後続の IKE ネゴシエーションを保護するかを規定します。IKE バージョン 1（IKEv1）では、IKE ポリシーに、単一のアルゴリズムのセットと係数グループが含まれています。IKEv1 とは異なり、IKEv2 ポリシーでは、フェーズ 1 ネゴシエーション中にピアがその中から選択できるように、複数のアルゴリズムとモジュラス グループを選択できます。単一の IKE ポリシーを作成できますが、最も必要なオプションにより高い優先順位をつけるために異なるポリシーが必要となる場合もあります。サイト間 VPN の場合は、単一の IKE ポリシーを作成できます。IKEv1 と IKEv2 はどちらも、最大 20 個の IKE ポリシーをサポートしますが、値のセットはそれぞれ異なります。作成するポリシーのそれぞれに、固有のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

IKE ポリシーを定義するには、次を指定します。

- 一意の優先順位（1 ～ 65,543、1 が最高優先順位）。
- データを保護して、プライバシーを確保するための IKE ネゴシエーション用の暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証するハッシュ メッセージ 認証コード（HMAC）方式（IKEv2 では整合性アルゴリズムと呼ばれます）。

- IKEv2 では、別個の疑似乱数関数（PRF）をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していました。オプションは、ハッシュ アルゴリズムに使用されるものと同じです。
- 暗号キー決定アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号キーとハッシュ キーを導き出します。
- ピアの ID を保証するための認証方式。
- デバイスが暗号化キーを交換するまでに使用できる時間制限。

IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。暗号化、ハッシュ（IKEv2 の場合、整合性と PRF）、認証、および Diffie-Hellman 値が同じで、SA ライフタイムが、送信されたポリシーのライフタイム以下の場合に、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、リモート ピア ポリシーから取得した短い方のライフタイムが適用されます。デフォルトでは、Secure Firewall Management Center は、正常なネゴシエーションを確保するために、すべての VPN エンドポイントに対して IKEv1 ポリシーを最低優先順位で展開します。

IPsec

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2 つのピア間のセキュアで論理的な通信パスです。IPSec トンネルを通過するトラフィックは、セキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。

IPsec プロポーザル ポリシーは、IPsec トンネルに必要な設定を定義します。IPsec プロポーザルとは、デバイスの VPN インターフェイスに適用される 1 つ以上の暗号マップの集合です。暗号マップには、IPsec セキュリティ アソシエーションを設定するために必要なすべてのコンポーネントが組み合わされています。これらのコンポーネントには以下のものがあります。

- プロポーザル（またはトランスフォーム セット）とは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルおよびアルゴリズムの組み合わせです。IPsec セキュリティ アソシエーション（SA）ネゴシエーション中に、ピアでは、両方のピアに共通するプロポーザルが検索されます。そのようなプロポーザルが検出されると、そのプロポーザルを適用して、その暗号マップのアクセス リストでデータ フローを保護する SA が作成され、VPN でトラフィックが保護されます。IKEv1 と IKEv2 には別個の IPsec プロポーザルがあります。IKEv1 プロポーザル（トランスフォーム セット）では、パラメータごとに 1 つの値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに複数の暗号化アルゴリズムと統合アルゴリズムを設定できます。
- 暗号マップには、IPsec ルール、プロポーザル、リモート ピア、IPsec SA を定義するために必要なその他のパラメータを含む、IPsec セキュリティ アソシエーション（SA）を設定するために必要なすべてのコンポーネントが組み合わされています。2 つのピアが SA を

確立しようとする場合は、それぞれに少なくとも1つの互換暗号マップエントリが必要です。

不明なリモート ピアがローカル ハブとの間の IPsec セキュリティ アソシエーションの開始を試みた場合、ダイナミック暗号マップ ポリシーがサイト間 VPN で使用されます。ハブは、セキュリティ アソシエーション ネゴシエーションを開始できません。ダイナミック暗号ポリシーを使用することによって、ハブがリモートピアのアイデンティティを把握していない場合でも、リモートピアはローカルハブとの間でIPsecトラフィックを交換できます。実質的には、ダイナミック暗号マップポリシーによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモート ピアの要件に合うようにあとで動的に設定されます。

ダイナミック暗号マップ ポリシーは、ハブアンドスポークとポイントツーポイント VPN トポロジの両方に適用されます。ダイナミック暗号マップポリシーを適用するには、トポロジ内のピアの 1 つにダイナミック IP アドレスを指定し、このトポロジでダイナミック暗号マップが有効になっていることを確認します。フル メッシュ VPN トポロジでは、スタティック クリプト マップ ポリシーのみを適用できます。

（注） Firepower Threat Defense（FTD）でのリモートアクセス VPN とサイト間 VPN の両方の同じインターフェイスでは、同時 IKEv2 ダイナミッククリプトマップはサポートされていません。

VPN パケット フロー

Firewall Threat Defense デバイスでは、デフォルトでは、明示的な許可なしにいずれのトラフィックもアクセス コントロールを通過できません。VPN トンネル トラフィックも、Snort を通過するまでは、エンドポイントにリレーされません。着信トンネル パケットは復号されてから、Snort プロセスへ送信されます。Snort は、暗号化の前に発信パケットを処理します。

VPN トンネルのエンドポイント ノードごとに保護されたネットワークを識別するアクセス制御は、どのトラフィックが Firewall Threat Defense デバイスをパス スルーしてエンドポイントに到達できるかを決定します。リモート アクセス VPN トラフィックでは、グループ ポリシー フィルタまたはアクセス制御ルールを、VPN トラフィック フローを許可するように設定する必要があります。

さらに、システムは、トンネルがダウンしている場合は、トンネル トラフィックをパブリックなソースに送信しません。

IPsec フローのオフロード

IPsec フローのオフロードを使用するように、サポートするデバイスモデルを設定できます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期

設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。

オフロード操作は、特に、入力の事前復号および復号処理と出力の事前暗号化および暗号化処理に関連しています。システムソフトウェアは、セキュリティポリシーを適用するための内部フローを処理します。

IPsec フローのオフロードはデフォルトで有効になっており、次のデバイスタイプに適用されます。

- Cisco Secure Firewall 3100

IPsec フローのオフロードに関する制約事項

次の IPsec フローはオフロードされません。

- IKEv1 トンネル。IKEv2 トンネルのみがオフロードされます。IKEv2 は、より強力な暗号をサポートしています。
- ボリュームベースのキー再生成が設定されているフロー。
- 圧縮が設定されているフロー。
- トランスポートモードのフロー。トンネルモードのフローのみがオフロードされます。
- AH 形式。ESP/NAT-T 形式のみがサポートされます。
- ポストフラグメンテーションが設定されているフロー。
- 64 ビット以外のアンチリプレイ ウィンドウ サイズを持ち、アンチリプレイが無効になっていないフロー。
- ファイアウォールフィルタが有効になっているフロー。
- マルチインスタンス モード。

IPsec フローのオフロードの設定

IPsec フローのオフロードは、この機能をサポートするハードウェア プラットフォームではデフォルトで有効になっています。設定を変更するには、FlexConfig を使用して **flow-offload-ipsec** コマンドを実装します。このコマンドの詳細については、ASA コマンドリファレンスを参照してください。

VPN ライセンス

Secure Firewall Threat Defense VPN を有効にするための特別なライセンスはありません。デフォルトで利用可能です。

Firewall Management Center は、スマートライセンスサーバーから提供される属性に基づいて、Firewall Threat Defense デバイスで強力な暗号の使用を許可するかブロックするかを決定します。

これは、Cisco Smart License Manager に登録するときにデバイス上で輸出管理機能を許可するオプションを選択しているかどうかによって制御されます。評価ライセンスを使用している場合、または輸出管理機能を有効にしていない場合は、強力な暗号化を使用できません。

評価ライセンスを使用して VPN 構成を作成し、ライセンスを評価版から輸出規制により機能が限定されたスマートライセンスにアップグレードした場合は、暗号化アルゴリズムを確認および更新して暗号化を強化し、VPN が適切に機能するようにしてください。DES ベースの暗号化はサポートされなくなりました。

VPN 接続をセキュアにする方法

通常、VPN トンネルはインターネットなどのパブリック ネットワークを通過するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーザルの使用を適用するために、暗号化とその他のセキュリティ テクニックを定義します。

デバイスライセンスで強力な暗号化の適用が可能な場合は、さまざまな暗号化アルゴリズム、ハッシュ アルゴリズム、Diffie-Hellman グループから選択することができます。ただし、一般的なルールとして、トンネルに適用する暗号化が強力なほど、システムパフォーマンスは低下します。効率を犠牲にすることなく十分な保護を提供するようにセキュリティとパフォーマンスのバランスを取る必要があります。

オプションの選択肢に関する特定のガイダンスを示すことはできませんが、大規模な企業や組織で運用する場合は、すでに標準が定義されていることがあります。そうでない場合は、時間をかけてオプションを検討してください。

ここでは、使用可能なオプションについて説明します。

セキュリティ証明書要件の遵守

多数の VPN 設定には、さまざまなセキュリティ認証規格に準拠するためのオプションがあります。認定要件と使用可能なオプションを確認して、VPN 構成を計画します。

使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルで使用する暗号化アルゴリズムを決定する場合は、選択肢が VPN 内のデバイスによってサポートされているアルゴリズムに限られます。

IKEv2 の場合は、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものの順に並べ、その順序を使用してピアとのネゴシエーションを行います。IKEv1 の場合は、1 つのオプションしか選択できません。

IPsec プロポーザルの場合、このアルゴリズムはカプセル化セキュリティ プロトコル（ESP）で使用されます。これは、認証サービス、暗号化サービス、アンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の先頭に ESP- が付けられます。

デバイスライセンスが強力な暗号化に対応している場合は、次の暗号化アルゴリズムの中から選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

（注） 強力な暗号化の対象である場合、評価ライセンスをスマートライセンスにアップグレードする前に、暗号化アルゴリズムを確認および更新して暗号化を強化し、VPN設定が適切に機能するようにしてください。AESベースのアルゴリズムを選択します。強力な暗号化をサポートするアカウントを使用して登録されている場合、DES はサポートされません。登録後は、DES の使用対象をすべて削除するまで変更を展開できません。

- AES-GCM—（IKEv2 のみ）ガロア/カウンタ モードの Advanced Encryption Standard は、機密性とデータ発信元認証を提供するブロック暗号モードの操作であり、AES より優れたセキュリティを実現します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCM は NSA Suite B をサポートするために必要な AES のモードです。NSA Suite B は暗号強度に関する連邦規格を満たすためにデバイスがサポートすべき暗号化アルゴリズムのセットです。。
- AES：Advanced Encryption Standard は、DES よりも優れたセキュリティを提供し、3DES よりも効率的に計算する対称暗号アルゴリズムです。AESには、128ビット、192ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。
- DES：56 ビットのキーを使用して暗号化するデータ暗号化規格（Data Encryption Standard）は、対称秘密キー ブロック アルゴリズムです。ライセンスアカウントが輸出規制の要件を満たしていない場合、これは唯一のオプションです。
- NULL、ESP-NULL：使用しないでください。NULL 暗号化アルゴリズムは、暗号化を使用しない認証を提供します。通常はテスト目的にのみ使用されます。ただし、仮想および Firepower 2100 を含む多くのプラットフォームではまったく動作しません。

使用するハッシュ アルゴリズムの決定

IKEポリシーでは、ハッシュアルゴリズムがメッセージダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプション（整合性アルゴリズム用に 1 つと Pseudo-Random Function（PRF; 疑似乱数関数）用に 1 つ）に分かれています。

IPsec プロポーザルでは、ハッシュ アルゴリズムが、認証用のカプセル化セキュリティ プロトコル（ESP）で用されます。IKEv2 IPsec プロポーザルでは、これが整合性ハッシュと呼ばれています。IKEv1 IPsec プロポーザルでは、アルゴリズム名の先頭に ESP- が付けられ、末尾に -HMAC（「ハッシュ法認証コード」を意味する）が付けられます。

IKEv2 の場合は、複数のハッシュ アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものの順に並べ、その順序を使用してピアとのネゴシエーションを行います。IKEv1 の場合は、1 つのオプションしか選択できません。

次のハッシュ アルゴリズムから選択できます。

- [SHA (Secure Hash Algorithm)]：標準の SHA（SHA1）は、160 ビットのダイジェストを生成します。

  よりセキュアな次の SHA-2 オプションを IKEv2 設定に使用できます。NSA Suite B 暗号化仕様を実装する場合は、次のいずれかを選択します。

  - SHA256：256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA384：384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA512：512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

- ヌルまたはなし（NULL、ESP-NONE）：（IPsec プロポーザルのみ）。ヌル ハッシュ アルゴリズムは、通常、テスト目的にのみ使用されます。しかし、暗号化オプションとしていずれかの AES-GCM オプションを選択した場合は、NULL 整合性アルゴリズムを選択する必要があります。ヌル以外のオプションを選択した場合でも、これらの暗号化標準では整合性ハッシュは無視されます。

使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec セキュリティ アソシエーション（SA）キーを生成することができます。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択した場合は、AES に必要な大きいキー サイズをサポートするために、Diffie-Hellman（DH）グループ 5 以上を使用する必要があります。IKEv1 ポリシーは、以下に示すすべてのグループをサポートしているわけではありません。

NSA Suite B 暗号化仕様を実装するには、IKEv2 を使用し、楕円曲線 Diffie-Hellman（ECDH）オプション（19、20、または21）のいずれかを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものの順に並べ、その順序を使用してピアとのネゴシエーションを行います。IKEv1 の場合は、1 つのオプションしか選択できません。

- 14：Diffie-Hellman グループ 14（2048 ビット Modular Exponential（MODP）グループ）。192 ビットのキーでは十分な保護レベルです。
- 15：Diffie-Hellman グループ 15（3072 ビット MODP グループ）。
- 16：Diffie-Hellman グループ 16（4096 ビット MODP グループ）。

- 19：Diffie-Hellman グループ 19（国立標準技術研究所（NIST）256 ビット楕円曲線モジュロプライム（ECP）グループ）。
- 20：Diffie-Hellman グループ 20（NIST 384 ビット ECP グループ）。
- 21：Diffie-Hellman グループ 21（NIST 521 ビット ECP グループ）。
- 31：Diffie-Hellman グループ 31（Curve25519 256 ビット EC グループ）。

使用する認証方式の決定

事前共有キーとデジタル証明書は、VPN で使用可能な認証方法です。

サイト間、IKEv1 および IKEv2 VPN 接続では、両方のオプションを使用できます。

SSL および IPsec IKEv2 のみを使用するリモート アクセスでは、デジタル証明書認証だけがサポートされます。

事前共有キーを使用すると、秘密鍵を 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていない場合は、IKE SA を確立できません。

デジタル証明書は IKE キー管理メッセージの署名や暗号化に RSA キー ペアを使用します。証明書によって、2 つのピア間の通信の否認防止を実施します。つまり、実際に通信が行われたことを証明できます。この認証方式を使用する場合、ピアが証明機関（CA）からデジタル証明書を取得できるように Public Key Infrastructure（PKI）を定義する必要があります。CA は参加するネットワークデバイスの証明書要求を管理し、証明書を発行することで、すべての参加デバイスの Centralized Key Management を行います。

事前共有キーの拡張性は高くありませんが、CA を使用することによって IPsec ネットワークの管理性や拡張性が高まります。CA を使用する場合は、すべての暗号化デバイス間でキーを設定する必要がありません。代わりに、参加する各デバイスは CA に登録され、CA に対して証明書を要求します。自身の証明書と CA の公開キーを持つ各デバイスは、その CA のドメイン内にある他のすべてのデバイスを認証できます。

事前共有キー

事前共有キーを使用すると、2 つのピア間で秘密キーを共有できます。IKE は、このキーを認証フェーズで使用します。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていない場合は、IKE SA を確立できません。

事前共有キーを設定するには、手動または自動生成されたキーを使用するかどうかを選択し、IKEv1/IKEv2 オプションでキーを指定します。これにより、設定の展開時に、トポロジ内のすべてのデバイス上に共有キーが設定されます。

PKI インフラストラクチャとデジタル証明書

公開キー インフラストラクチャ

PKI では、参加ネットワーク デバイスのキーを一元管理できます。PKI は、一般にデジタル証明書 と呼ばれる公開キー証明書 を生成、検証、失効することで公開キー暗号化 をサポートするポリシー、プロシージャ、権限の定義済みセットです。

公開キー暗号化では、接続の各エンドポイントが公開キーと秘密キーの両方からなるキー ペアを保持します。キー ペアは、VPN エンドポイントがメッセージに署名して暗号化するために使用します。これらのキーは相互に補完し合い、一方のキーで暗号化されたものはもう一方のキーでしか復号できません。この仕組みにより、接続で送受信されるデータを保護します。

署名と暗号化の両方に使用される汎用RSA、ECDSA、またはEDDSAキーペアを生成するか、署名と暗号化用に別々のキーペアを生成します。署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。SSLは署名用ではなく暗号化用にキーを使用しますが、IKEは暗号化ではなく署名にキーを使用します。キーを用途別に分けることで、キーの公開頻度が最小化されます。

デジタル証明書またはアイデンティティ証明書

デジタル証明書を VPN 接続の認方式として使用する場合、ピアはデジタル証明書を認証局（CA）から取得するように設定されます。CAは、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。

CA サーバは公開 CA 証明書要求を管理し、参加ネットワーク デバイスに公開キー インフラストラクチャ（PKI）の一部として証明書を発行します。このアクティビティは、証明書の登録と呼ばれます。これらのデジタル証明書は、アイデンティティ証明書とも呼ばれています。デジタル証明書の内容は以下のとおりです。

- 認証のための所有者のデジタル識別（名前、シリアル番号、会社、部署、IP アドレスなど）。
- 証明書所有者に対して暗号化データを送受信するために必要な公開キー。
- CA のセキュアなデジタル署名。

また、証明書によって、2 つのピア間の通信の否認が防止されます。つまり、実際に通信が行われたことを証明できます。

証明書の登録

PKIを使用すると、すべての暗号化デバイス間で事前に共有するキーを設定する必要がなくなるため、VPNをもっと容易に管理できるようになり、スケーラビリティが高まります。代わりに、参加する各デバイスを CA サーバーに個別に登録します。CA サーバーは、アイデンティティを検証し、デバイスのアイデンティティ証明書を作成することを明示的に信任されています。登録が完了すると、参加する各ピアは、もう一方の参加するピアにアイデンティティ証明書を送信し、証明書に含まれる公開キーでそのアイデンティティを検証して、暗号化セッショ

ンを確立できるようにします。Firewall Threat Defense デバイスの登録の詳細については、証明書の登録オブジェクト （1363 ページ）を参照してください。

認証局証明書

ピアの証明書を検証するには、参加デバイスのそれぞれが CA の証明書をサーバから取得する必要があります。CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。この証明書に含まれる CA の公開キーを使用して、CA のデジタル署名および受信したピアの証明書の内容を復号して検証します。CA 証明書は次の方法で取得可能です。

- Simple Certificate Enrollment Protocol（SCEP）または Enrollment over Secure Transport（EST）を使用して、CA サーバーから CA の証明書を取得します。
- 別の参加デバイスから CA の証明書を手動でコピーします。

トラストポイント

登録が完了すると、管理対象デバイス上にトラストポイントが作成されます。トラストポイントは、CA および関連する証明書を表すオブジェクトです。トラストポイントには、CA の ID、CA 固有のパラメータ、単一の登録済みアイデンティティ証明書とのアソシエーションが含まれています。

PKCS#12 ファイル

PKCS#12（PFX）ファイルとは、サーバー証明書、中間証明書、秘密キーのすべてを暗号化して保持するファイルです。このタイプのファイルをデバイスに直接インポートして、トラストポイントを作成できます。

失効チェック

さらに CA は、ネットワークに参加しなくなったピアの証明書を無効にすることもできます。失効した証明書は、オンライン証明書ステータス プロトコル（OCSP）サーバによって管理されるか、LDAP サーバに格納されている証明書失効リスト（CRL）に含まれます。ピアは、別のピアからの証明書を受け入れる前に、これらを検査できます。

削除または廃止されたハッシュアルゴリズム、暗号化アルゴリズム、および Diffie-Hellman モジュラスグループ

安全性の低い暗号のサポートが削除されました。VPN が正しく機能するように、Firewall Threat Defense 6.70 にアップグレードする前に、サポートされる DH および暗号化アルゴリズムに VPN 設定を更新することを推奨します。

Firewall Threat Defense 6.70 でサポートされているものと一致するように IKE プロポーザルと IPSec ポリシーを更新してから、設定の変更を展開します。

次の安全性の低い暗号は、Firewall Threat Defense 6.70 以降では削除または廃止されました。

- **Diffie-Hellman グループ 5** は IKEv1 および IKEv2 では廃止されました。
- Diffie-Hellman グループ 2 および 24 は削除されました。
- **暗号化アルゴリズム**：3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256 は削除されました。

（注） **DES** は、評価モードで、または強力な暗号化の輸出規制を満たさないユーザーのために引き続きサポートされます。

NULL は IKEv2 ポリシーでは削除されますが、IKEv1 と IKEv2 両方の IPsec トランスフォームセットでサポートされます。

VPN トポロジ オプション

新しいVPNトポロジを作成するには、最低でも、固有の名前をつけ、トポロジの型を特定し、IKE バージョンを選択する必要があります。それぞれが VPN トンネル グループを含む 3 つの型のトポロジから選択できます。

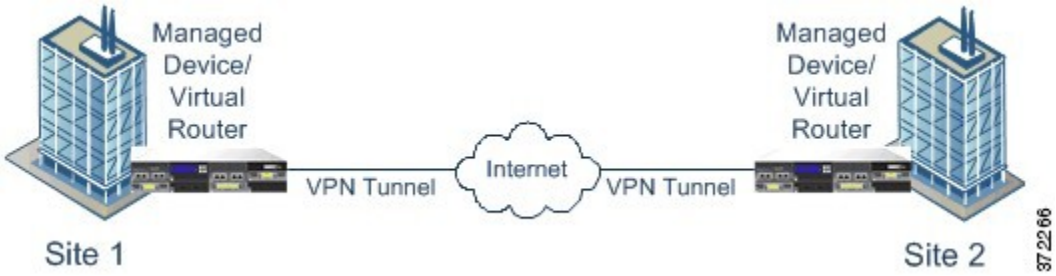
- ポイントツーポイント（PTP）トポロジでは、2 つのエンドポイント間に VPN トンネルを確立します。
- ハブおよびスポーク トポロジは、ハブ エンドポイントをスポーク エンドポイントのグループに接続する VPN トンネル グループを確立します。
- フル メッシュのトポロジは、エンドポイントのセットの間で VPN トンネルのグループを確立します。

VPN認証の事前共有キーを手動または自動で定義します。デフォルトのキーはありません。自動を選択すると、Secure Firewall Management Center は事前共有キーを生成して、そのキーをトポロジ内のすべてのノードに割り当てます。

ポイントツーポイントの VPN トポロジ

ポイントツーポイントのVPNトポロジでは、2つのエンドポイントが相互に直接通信します。2つのエンドポイントをピア デバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。

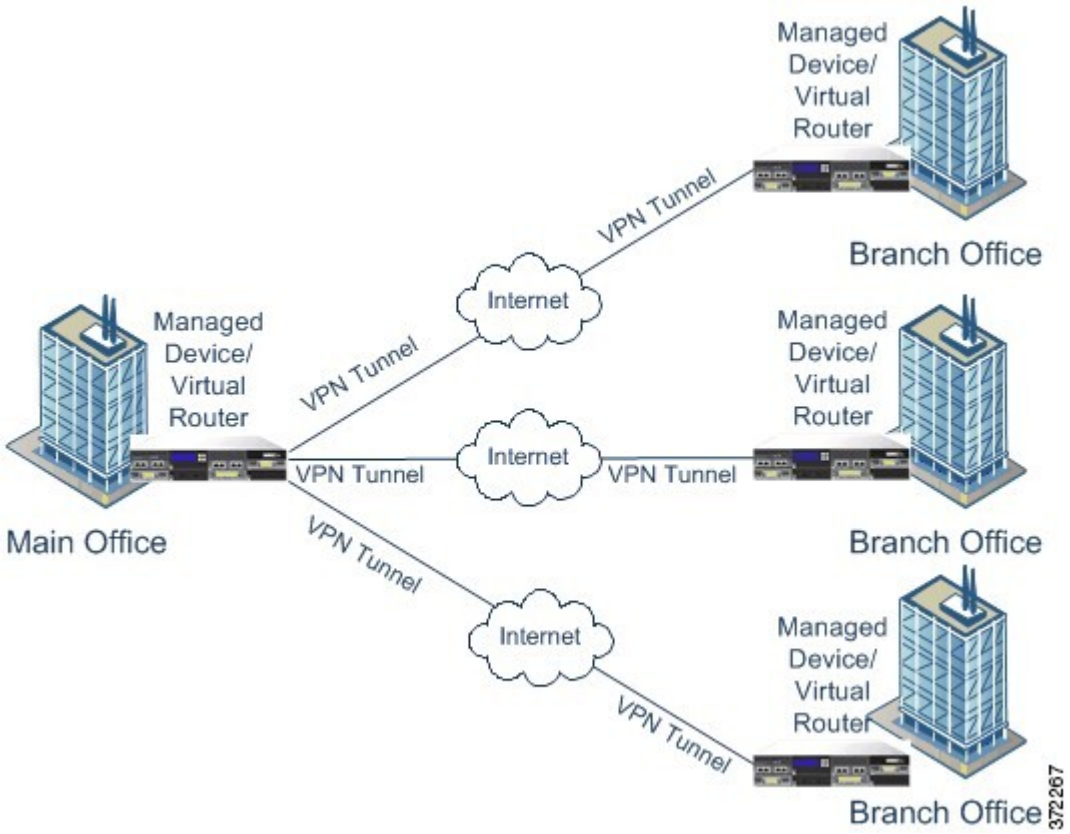


ハブ アンド スポーク VPN トポロジ

ハブ アンド スポーク VPN トポロジでは、中央のエンドポイント（ハブ ノード）が複数のエンドポイント（スポーク ノード）と接続します。ハブ ノードと個々のスポーク エンドポイント間のそれぞれの接続は、別の VPN トンネルです。いずれかのスポーク ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

ハブ アンド スポーク トポロジは一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本社とブランチ オフィスを接続する VPN を表します。これらの展開は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。一般的に、ハブ ノードは本社に配置します。スポーク ノードはブランチ オフィスに配置し、大半のトラフィックはここから開始されます。

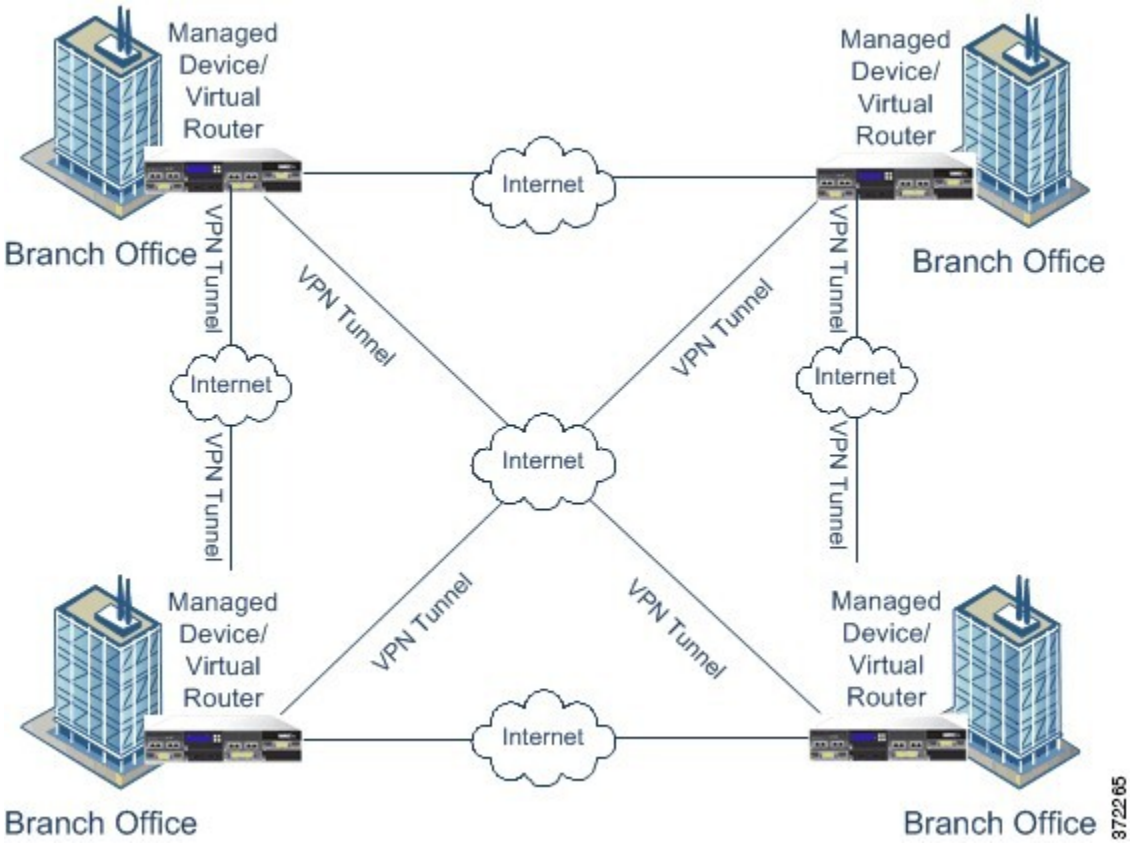
次の図は、一般的なハブ アンド スポーク VPN トポロジを示しています。



フル メッシュ VPN トポロジ

フル メッシュ VPN トポロジでは、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。このトポロジにより、あるエンドポイントで障害が発生しても、残りのエンドポイントの相互通信は維持されるように冗長性が提供されます。これは、一般的に分散したブランチ オフィスが配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。

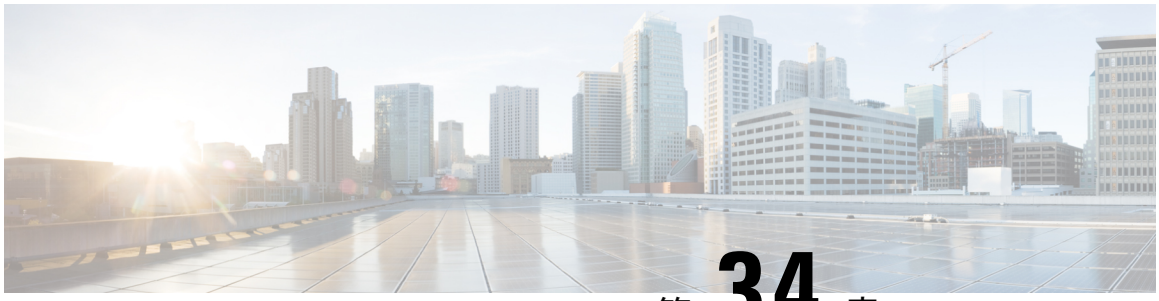
次の図は、一般的なフル メッシュ VPN トポロジを示しています。



暗黙的トポロジ

3つの主要なVPNトポロジに加えて、これらのトポロジを組み合わせた他のより複雑なトポロジを作成することもできます。具体的には以下のとおりです。

- 部分メッシュ：このネットワークでは、一部のデバイスはフル メッシュ トポロジに編成され、その他のデバイスは、フル メッシュ構成のデバイスのうちのいくつかとのハブアンドスポーク接続またはポイントツーポイント接続を形成します。部分メッシュには、フル メッシュ トポロジほどの冗長性はありませんが、導入コストがより低くなります。部分メッシュ トポロジは、フル メッシュ構成のバックボーンに接続するペリフェラル ネットワークで使用されます。
- 階層型ハブアンドスポーク：このネットワークでは、あるデバイスが、1 つ以上のトポロジでハブとして動作し、他のトポロジではスパイクとして動作できます。スポーク グループからそれらの直近のハブへのトラフィックが許可されます。
- 結合ハブアンドスポーク：接続して 1 つのポイントツーポイント トンネルを形成する、2 つのトポロジ（ハブアンドスポーク、ポイントツーポイント、またはフル メッシュ）の組み合わせです。たとえば、2 つのハブアンドスポーク トポロジから構成され、それぞれのハブがポイントツーポイント トポロジのピア デバイスとして動作する結合ハブアンドスポーク トポロジを作成できます。



第 34 章

サイト間 VPN

- サイト間 VPN について （1485 ページ）
- サイト間 VPN トポロジのタイプ （1488 ページ）
- サイト間 VPN の要件と前提条件 （1489 ページ）
- サイト間 VPN の管理 （1489 ページ）
- ポリシーベースのサイト間 VPN の設定 （1491 ページ）
- 仮想トンネル インターフェイスについて （1507 ページ）
- 仮想トンネルインターフェイスのガイドラインと制限事項 （1512 ページ）
- VTI インターフェイスの追加 （1516 ページ）
- ルートベースのサイト間 VPN の作成 （1518 ページ）
- バックアップ VTI トンネルを介したトラフィックのルーティング （1532 ページ）
- ルートベースのサイト間 VPN のダイナミック VTI の設定 （1534 ページ）
- VTI のルーティングおよび AC ポリシーの設定 （1534 ページ）
- Umbrella に SASE トンネルを展開する （1538 ページ）
- Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項 （1540 ページ）
- Cisco Umbrella に SASE トンネルを展開する方法 （1541 ページ）
- サイト間 VPN のモニタリング （1547 ページ）
- サイト間 VPN の履歴 （1553 ページ）

サイト間 VPN について

Secure Firewall Threat Defense サイト間 VPN では、次の機能がサポートされています。

- IPsec IKEv1 および IKEv2 プロトコルの両方。
- 証明書および自動または手動の事前共有認証キー。
- IPv4 および IPv6。内部、外部のすべての組み合わせをサポート。
- IPsec IKEv2 サイト間 VPN トポロジにより、セキュリティ認定に準拠するための設定を提供。
- スタティック インターフェイスおよびダイナミック インターフェイス。

- Firewall Management Center と Firewall Threat Defense の両方の HA 環境。
- トンネルがダウンした際の VPN アラート。
- Firewall Threat Defense 統合 CLI により利用可能なトンネル統計。
- ポイントツーポイント エクストラネット VPN およびハブアンドスポーク VPN の IKEv1 および IKEv2 バックアップピア設定。
- 「ハブアンドスポーク」展開でのハブとしてのエクストラネットデバイス。
- 「ポイントツーポイント」展開でのエクストラネットデバイスを使用した管理対象エンドポイントペアリングのダイナミック IP アドレス。
- エンドポイントとしてのエクストラネットデバイスのダイナミック IP アドレス。
- 「ハブアンドスポーク」展開でのエクストラネットとしてハブ。

VPN トポロジ

新しいサイト間VPNトポロジを作成するには、一意の名前を付け、トポロジタイプを指定し、IPsec IKEv1 または IKEv2 あるいはその両方に使用される IKE バージョンと認証方式を選択する必要があります。また、認証方法を決定します。設定したら、Firewall Threat Defense デバイスにトポロジを展開します。Secure Firewall Management Center は、Firewall Threat Defense デバイスのサイト間 VPN のみ設定します。

次の 3 つのタイプのトポロジから選択することができます。トポロジには、VPN トンネルが 1 つ以上含まれています。

- ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。
- ハブ アンド スポーク型の展開は、VPN トンネルのグループを確立し、ハブ エンドポイントをスポーク ノードのグループに接続します。
- フル メッシュ型の展開は、エンドポイントのセット内で VPN トンネルのグループを確立します。

IPsec と IKE

Secure Firewall Management Center では、サイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよび IPsec プロポーザルに基づいて設定されます。ポリシーとプロポーザルはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシー タイプが必要となる場合があります。

認証

VPN接続の認証には、トポロジ内で事前共有キー、または各デバイスでトラストポイントを設定します。事前共有キーにより、IKE 認証フェーズで使用する秘密鍵を 2 つのピア間で共有で

きます。トラストポイントには、CA の ID、CA 固有のパラメータ、登録されている単一の ID 証明書とのアソシエーションが含まれています。

エクストラネット デバイス

各トポロジタイプには、Firewall Management Center で管理しないデバイスである、エクストラネットデバイスが含まれる可能性があります。次のようなものがあります。

- Secure Firewall Management Center ではサポートされているが、ユーザーの部門が担当していないシスコデバイス。たとえば、社内の他の部門が管理するネットワーク内のスポークや、サービス プロバイダーやパートナー ネットワークへの接続などです。
- シスコ製以外のデバイス。Secure Firewall Management Center を使用して、シスコ製以外のデバイスに対する設定を作成したり、展開したりすることはできません。

シスコ以外のデバイス、または Secure Firewall Management Center で管理されていないシスコデバイスを VPN トポロジに「エクストラネット」デバイスとして追加します。また、各リモート デバイスの IP アドレスも指定します。

Secure Firewall Threat Defense サイト間 VPN ガイドラインと制約事項

- ECMP ゾーンインターフェイスは、サイト間 VPN でサポートされます。
- 暗号 ACL または保護されたネットワークのいずれかを使用して、トポロジ内のすべてのノードを設定する必要があります。あるノードでは暗号 ACL を使用し、別のノードでは保護されたネットワークを使用するトポロジを設定することはできません。
- 現在のドメイン内ではないエンドポイント用のエクストラネットピアを使用して、ドメイン間の VPN 接続を設定できます。
- Firewall Management Center バックアップを使用して Firewall Threat Defense VPN をバックアップできます。
- IKEv1 は、CC/UCAPL 準拠のデバイスをサポートしていません。これらのデバイスには IKEv2 を使用することをお勧めします。
- VPN トポロジをドメイン間で移動させることはできません。
- VPN は、「範囲」オプションのあるネットワークオブジェクトをサポートしていません。
- Firewall Threat Defense VPN では、現在、PDF のエクスポートおよびポリシーの比較をサポートしていません。
- Firewall Threat Defense VPN ではトンネル単位またはデバイス単位の編集オプションはありません。トポロジ全体のみ編集できます。
- 暗号 ACL を選択した場合、Firewall Management Center は、トランスポートモードのデバイス インターフェイス アドレスの検証を行いません。
- 自動ミラー ACE 生成はサポートされません。ピアのミラー ACE 生成は、どちらの側でも手動プロセスです。

- 暗号 ACL では、Firewall Management Center はポイントツーポイント VPN のみをサポートし、トンネルヘルスイベントはサポートしません。
- IKE ポート 500/4500 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、サイト間 VPN を同じポートに設定することはできません。
- Firewall Management Center では、トンネルの状態はリアルタイムではなく、5 分間隔でアップロードされます。
- 文字「"」（二重引用符）は事前共有キーの一部として使用できません。事前共有キーで「"」を使用した場合は、文字必ずを変更してください。
- 2 つのデバイスが同じ Firewall Management Center によって管理されているサイト間 VPN 設定では、デバイスをバックアップピアとして設定できません。トポロジ内のピアデバイスの 1 つをエクストラネットデバイスとして設定する必要があります。
- すべての VPN トポロジのすべてのトンネルで一意のローカル IKE アイデンティティを設定します。

サイト間 VPN トポロジのタイプ

サイト間 VPN トポロジ	説明	詳細情報
ルートベース VPN	仮想トンネルインターフェイス（VTI）を介したルーティングに基づいて、セキュアなネットワーク内のピア間のトラフィックを動的に設定します。	ルートベースのサイト間 VPN の作成 （1518 ページ）
ポリシーベース VPN	保護されたネットワークを使用し、静的ポリシーに基づいて、ネットワーク内のピア間のセキュアなトラフィックを設定します。	ポリシーベースのサイト間 VPN の設定 （1491 ページ）
SASE トポロジ	Threat Defense デバイスから Umbrella Secure Internet Gateway（SIG）への IPsec IKEv2 トンネルを設定します。このトンネルは、インターネットに向かうすべてのトラフィックを、検査とフィルタリングのために Cisco Umbrella SIG に転送します。	Cisco Umbrella 用の SASE トンネルの設定 （1544 ページ）

サイト間 VPN の要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

リーフ

ユーザの役割

管理者

サポートされるインターフェイス

トポロジタイプ	インターフェイス タイプ

ポリシーベース	• 物理インターフェイス
	  • 非管理
	  • インターフェイスモードは「ルーテッド」または「なし」のいずれかにする必要があります
	• サブインターフェイス インターフェイス
	• 冗長インターフェイス
	• EtherChannel インターフェイス
	• VLAN インターフェイス

ルートベース	スタティック仮想トンネル インターフェイス

サイト間 VPN の管理

[サイト間VPN（Site-to-Site VPN）]ページには、サイト間 VPN トンネルのスナップショットが表示されます。トンネルのステータスを表示し、デバイス、トポロジ、またはトンネルタイプに基づいてトンネルをフィルタ処理できます。このページには、ページごとに 20 のトポロジが一覧表示され、ページ間を移動してトポロジの詳細を表示できます。個々の VPN トポロジをクリックして展開し、エンドポイントの詳細を表示できます。

始める前に

サイト間VPNの証明書認証の場合は、証明書（1455ページ）の説明に従い、トラストポイントを割り当ててデバイスを準備する必要があります。

手順

[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択して、Firewall Threat Defense のサイト間 VPN の設定と展開を管理します。

このページには、サイト間 VPN トポロジが一覧表示され、色コードを使用してトンネルのステータスが示されます。

- [アクティブ（Active）]（緑）：アクティブな IPsec トンネルがあります。
- [不明（Unknown）]（オレンジ）：デバイスからトンネル確立イベントをまだ受信していません。
- [ダウン（Down）]（赤）：アクティブな IPsec トンネルがありません。
- [展開保留中（Deployment Pending）]：トポロジはまだデバイスに展開されていません。

次のオプションから選択します。

- [更新（Refresh）]：VPN の更新されたステータスが表示されます。
- [追加（Add）]：新しいポリシーベースまたはルートベースのサイト間 VPN を作成します。
- [編集（Edit）]：既存の VPN トポロジの設定を変更します。

  （注）
  トポロジ タイプは、最初の保存後に編集することはできません。トポロジ タイプを変更するには、トポロジを削除してから新しいものを作成します。

  2 人のユーザーで同じトポロジを同時に編集しないでください。ただし、Web インターフェイスでは同時編集できます。

- [削除（Delete）]：VPN の展開を削除するには、[削除（Delete）]（🗑）をクリックします。
- [展開（Deploy）]：**[展開（Deploy）] > [展開（Deployment）]** をクリックします（設定変更の展開 （172 ページ） を参照）。

  （注）
  一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

ポリシーベースのサイト間 VPN の設定

手順

ステップ 1 [デバイス（Devices）] > [サイト間（Site To Site）]。その後、[+サイト間VPN（+ Site To Site VPN）] をクリックするか、リストされている VPN トポロジを編集します。 を選択します。

ステップ 2 一意のトポロジ名を入力します。トポロジには、Firewall Threat Defense VPN であることとトポロジ タイプを示す名前を付けることをお勧めします。

ステップ 3 **[ポリシー ベース（クリプト マップ）（Policy Based (Crypto Map)）]** ラジオ ボタンをクリックします。

ステップ 4 この VPN のネットワーク トポロジを選択します。

ステップ 5 IKE ネゴシエーション中に使用する IKE バージョンとして、**[IKEv1]** または **[IKEv2]** チェックボックスをオンにします。

デフォルトは [IKEv2] です。必要に応じて、いずれかまたは両方のオプションを選択します。トポロジ内のデバイスが IKEv2 をサポートしていない場合は、[IKEv1] を選択します。

ポイントツーポイント エクストラネット VPN のバックアップピアも設定できます。詳細については、Firewall Threat Defense VPN エンドポイント オプション （1492 ページ）を参照してください。

ステップ 6 必須: トポロジの各ノードの [追加（Add）] (+) をクリックして、この VPN 展開のためのエンドポイントを追加します。

Firewall Threat Defense VPN エンドポイント オプション （1492 ページ）の説明に従って各エンドポイント フィールドを設定します。

- ポイントツーポイントの場合は、ノード A とノード B を設定します。
- ハブ アンド スポークの場合は、ハブ ノードとスポーク ノードを設定します。
- フル メッシュの場合は、複数のノードを設定します

ステップ 7 （任意） 次の説明に従って、この展開のデフォルト以外の IKE オプションを指定しますFirewall Threat Defense VPN IKE オプション （1497 ページ）

ステップ 8 （任意） 次の説明に従って、この展開のデフォルト以外の IPsec オプションを指定しますFirewall Threat Defense VPN IPsec オプション （1500 ページ）

ステップ 9 （任意） Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （1503 ページ）の説明に従って、この展開のデフォルト以外の詳細オプションを指定します。

ステップ 10 [保存（Save）] をクリックします。
エンドポイントが構成に追加されます。

次のタスク

設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

（注） 一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

VPN セッションが稼働しているのに VPN トンネルが非アクティブであるというアラートを受け取った場合は、VPN のトラブルシューティング手順に従って、VPN がアクティブであることを確認します。詳細については、VPNのモニタリングとトラブルシューティング （1699ページ）およびVPN のトラブルシューティング （1703 ページ）を参照してください。

Firewall Threat Defense VPN エンドポイント オプション

ナビゲーション パス

[デバイス（Devices）] > [サイト間（Site To Site）]。その後、[+サイト間VPN（+ Site To Site VPN）] をクリックするか、リストされている VPN トポロジを編集します。[エンドポイント（Endpoints）] タブをクリックします。

フィールド

Device

展開するエンドポイント ノードを選択します。

- この Firewall Management Center で管理する Firewall Threat Defense デバイス。
- この Firewall Threat Defense で管理する Firewall Management Center ハイ アベイラビリティ コンテナ。
- [エクストラネット（Extranet）] デバイス。この Firewall Management Center の管理対象ではない任意のデバイス（シスコまたはサードパーティ）。

デバイス名（Device Name）

エクストラネットデバイスの場合のみ、このデバイスの名前を入力します。シスコでは、管理対象ではないデバイスとして識別できるような名前を付けることを推奨します。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択した場合は、その管理対象デバイスのインターフェイスを選択します。

「ポイントツーポイント」展開の場合、ダイナミック インターフェイスを使用してエンドポイントを設定することもできます。ダイナミック インターフェイスを使用したエンドポイントはエクストラネットデバイスとのみペアリングできます。管理対象デバイスを持つエンドポイントとはペアリングできません。

[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの追加/編集（Add/Edit device）] > [インターフェイス（Interfaces）] でデバイスのインターフェイスを設定できます。

IP アドレス（IP Address）

- Firewall Management Center の管理対象デバイス**ではない**エクストラネットデバイスを選択した場合は、エンドポイントの IP アドレスを指定します。

  エクストラネット デバイスの場合は、[スタティック（Static）] を選択して IP アドレスを指定するか、または [ダイナミック（Dynamic）] を選択してダイナミック エクストラネット デバイスを許可します。

- エンドポイントとして管理対象デバイスを選択した場合は、ドロップダウンリストから 1 つの IPv4 アドレスまたは複数の IPv6 アドレスを選択します。これらはすでにこの管理対象デバイスのインターフェイスに割り当てられている IP アドレスです。
- トポロジ内のすべてのエンドポイントは、同じ IP アドレッシング方式でなければなりません。IPv4 トンネルは IPv6 トラフィックを伝送でき、逆もまた同様です。保護ネットワークでは、トンネルするトラフィックで使用するアドレッシング方式が定義されます。
- 管理対象デバイスがハイ アベイラビリティ コンテナである場合は、インターフェイスのリストから選択します。

この IP はプライベートです（This IP is Private）

エンドポイントが、ネットワーク アドレス変換（NAT）を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

（注） このオプションは、ピアが同じ Firewall Management Center によって管理されている場合にのみ使用します。ピアがエクストラネットデバイスである場合は、このオプションは使用しません。

パブリック IP アドレス（Public IP address）

[この IP はプライベートです（This IP is Private）] チェックボックスがオンの場合は、ファイアウォールのパブリック IP アドレスを指定します。エンドポイントがレスポンダの場合は、この値を指定します。

接続タイプ（Connection Type）

許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。接続タイプのサポートされる組み合わせは次のとおりです。

表 *71* : 接続タイプのサポートされる組み合わせ

リモート ノード	中央ノード
Originate-Only	Answer-Only

リモート ノード	中央ノード
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

証明書マップ

事前設定された証明書マップオブジェクトを選択するか、[追加（Add）] (+) をクリックして証明書マップオブジェクトを追加します。証明書マップは、VPN接続で有効になるには受信したクライアント証明書でどのような情報が必要かを定義します。詳細については、「証明書マップオブジェクト （1425 ページ）」を参照してください。

保護されたネットワーク（Protected Networks）

⚠

注意 ハブアンドスポークトポロジ：ダイナミッククリプトマップでトラフィックのドロップを避けるために、両方のエンドポイントで保護されたネットワークに *any* を選択しないでください。

保護されたネットワークが両方のエンドポイントで *any* として設定されている場合、トンネルで機能する暗号 ACL が生成されません。

この VPN エンドポイントによって保護されるネットワークを定義します。このエンドポイントによって保護されるネットワークを定義するサブネット/IP アドレスのリストを選択することで、ネットワークを選択することができます。[追加（Add）] (+)をクリックして、使用可能なネットワークオブジェクトから選択するか、新しいネットワークオブジェクトを追加します。ネットワーク オブジェクトの作成（1351 ページ）を参照してください。アクセスコントロールリストは、ここで選択されたものから生成されます。

- [サブネット/IPアドレス（ネットワーク）（Subnet/IP Address (Network)）]：VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできません。エンドポイントの保護されたネットワークに IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っている必要があります。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。（IPv4 については/32 CIDR アドレスを使用し、IPv6 については/128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

（注） Firewall Management Center では、デフォルトで**リバース ルート インジェクションが有効になっています**。

[サブネット/IPアドレス（ネットワーク）（Subnet/IP Address (Network)）] はデフォルトの選択のままにします。

[保護されたネットワーク（Protected Networks）] を [任意（Any）] として選択し、デフォルトのルートトラフィックがドロップされることを確認した場合は、リバース ルート インジェクションを無効にします。[VPN] > [サイト間（Site to Site）] > [VPNの編集（edit a VPN）] > [IPsec] > [リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] を選択します。設定変更を展開して、暗号マップ設定から set reverse-route（リバース ルート インジェクション）を削除し、リバース トンネル トラフィックのドロップを引き起こす NVP でアドバタイズされたリバースルートを削除します。

- [アクセス リスト（拡張）（Access List (Extended)）]：拡張アクセスリストは、GRE トラフィックや OSPF トラフィックなどの、このエンドポイントによって受け入れられるトラフィックのタイプを制御する機能を提供します。トラフィックは、アドレスまたはポートにより制限できます。[追加（Add）] (＋)をクリックして、アクセス コントロール リスト オブジェクトを追加します。

（注） アクセス コントロール リストは、ポイントツーポイント トポロジでのみサポートされています。

詳細設定（Advanced Settings）

[ダイナミック リバース ルート インジェクションを有効にする（Enable Dynamic Reverse Route Injection）]：リバース ルート インジェクション（RRI）では、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティングプロセスに、ルートを自動的に組み込むことができます。ダイナミック RRI ルートは IPsec セキュリティ アソシエーション（SA）の確立成功時にのみ作成されます

（注）

- ダイナミック RRI は IKEv2 でのみサポートされ、IKEv1 または IKEv1 + IKEv2 ではサポートされません。
- ダイナミック RRI は、発信のみのピア、フルメッシュトポロジ、およびエクストラネットピアではサポートされていません。
- ポイントツーポイントでは、1 つのピアでのみダイナミック RRI を有効にすることができます。
- ハブとスポークの間では、1 つのエンドポイントでのみダイナミック RRI を有効にすることができます。
- ダイナミック RRI は、ダイナミッククリプトマップと組み合わせることはできません。

[ピアへのローカルIDの送信（Send Local Identity to Peers）]：ローカル ID 情報をピアデバイスに送信するには、このオプションを選択します。リストから次のいずれかの [ローカルID構成（Local Identity Configuration）] を選択し、ローカル ID を設定します。

- [IPアドレス（IP address）]：ID にインターフェイスの IP アドレスを使用します。
- [自動（Auto）]：事前共有キーにはIPアドレスを使用し、証明書ベースの接続には証明書 DN を使用します。
- [電子メールID（Email ID）]：IDに使用する電子メールIDを指定します。電子メール ID は最大 127 文字です。
- [ホスト名（Hostname）]：完全修飾ホスト名を使用します。
- [キーID（Key ID）]：ID に使用するキー ID を指定します。キー ID は 65 文字未満にする必要があります。

ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。一意の ID を設定すると、Cisco Umbrella Secure Internet Gateway（SIG）に接続するために、Firewall Threat Defense が NAT の背後に複数の IPsec トンネルを持つことができます。

Cisco Umbrella での一意のトンネル ID の設定については、**Cisco Umbrella SIG ユーザーガイド** [英語] を参照してください。

[VPNフィルタ（VPN Filter）]：リストから拡張アクセスリストを選択するか、[追加（Add）] をクリックして新しい拡張アクセスリストオブジェクトを作成し、サイト間 VPN トラフィックをフィルタリングします。

VPN フィルタはセキュリティを強化し、拡張アクセスリストを使用してサイト間VPNデータをフィルタリングします。VPN フィルタ用に選択された拡張アクセスリストオブジェクトを使用すると、VPN トンネルに入る前に事前暗号化されたトラフィックと、VPN トンネルを出る復号されたトラフィックをフィルタリングできます。**sysopt permit-vpn** オプションを有効にすると、VPN トンネルからのトラフィックのアクセス コントロール ポリ

シールールがバイパスされます。**sysopt permit-vpn** オプションが有効になっている場合、VPN フィルタは、サイト間 VPN トラフィックの識別とフィルタリングに役立ちます。

（注） VPN フィルタは、ポイントツーポイントトポロジおよびハブアンドスポークトポロジでのみサポートされます。メッシュトポロジではサポートされていません。

ハブアンドスポークトポロジの場合、特定のトンネルで別の VPN フィルタを有効にする必要がある場合に備えて、スポークエンドポイントでハブ VPN フィルタをオーバーライドすることを選択できます。

スポークのハブ VPN フィルタを無効にするには、[ハブでのVPNフィルタのオーバーライド（Override VPN Filter on the Hub）] オプションを選択します。[リモートVPNフィルタ（Remote VPN Filter）] 拡張アクセスリストオブジェクトを選択するか、上書きするアクセスリストを作成します。

（注） エクストラネットデバイスをスポークとして使用する場合、[ハブでのVPNフィルタのオーバーライド（Override VPN Filter on the Hub）] オプションのみを使用できます。

sysopt permit-VPN の詳細については、Firewall Threat Defense のサイト間 VPN トンネルの詳細オプション （1506 ページ）を参照してください。

NAT トラバーサル（NAT-T）

NAT トラバーサルにより、ピア Firewall Threat Defense デバイス間に NAT デバイスがある場合、これらのデバイス間のシームレス コミュニケーションが可能になります。Firewall Management Center UI を使用して、VPN ごとに NAT トラバーサル（NAT-T）を無効にすることはできません。このオプションは、バージョン 7.4.1 から利用できます。FlexConfig を使用して、NAT-T を無効にできます。 FlexConfig オブジェクトに **crypto map** *map-name seq-num* **set nat-t-disable** コマンドを追加できます。たとえば、 **crypt map CSM_outside_map 1 set nat-t-disable** などです。

（注） 展開を「EveryTime」、タイプを「Append」として FlexConfig オブジェクトを作成する必要があります。この設定により、コマンドが削除されますが、展開ごとにまた追加されます。展開を「1回」に設定すると、コマンドは次の展開で削除されます。このコマンドで FlexConfig オブジェクトを設定する場合は注意する必要があります。Firewall Management Center によってシーケンス番号が変更されると、導入に失敗します。

Firewall Threat Defense VPN IKE オプション

このトポロジに選択した IKE のバージョンの場合は、[IKEv1/IKEv2 設定（IKEv1/IKEv2 Settings）] を指定します。

（注） このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

ナビゲーション パス

[デバイス（Devices）] > [サイト間（Site To Site）]。その後、[+サイト間VPN（+ Site To Site VPN）] をクリックするか、リストされている VPN トポロジを編集します。[IKE] タブをクリックします。

フィールド

ポリシー（Policy）

事前定義リストから必要な IKEv1 または IKEv2 ポリシーオブジェクトを選択するか、または使用する新しいポリシーオブジェクトを作成します。複数の IKEv1 および IKEv2 ポリシーを選択できます。IKEv1 と IKEv2 は、最大 20 個の IKE ポリシーをサポートしますが、値のセットはそれぞれ異なります。作成するポリシーのそれぞれに、固有のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

10、20 などの値は使用しないことを推奨します。リモート アクセス VPN のデフォルト IKEv2 ポリシーにプライオリティ値としてこれらの値を設定している場合があるからです。展開前に、IKE ポリシー（サイト間およびリモートアクセス VPN）のプライオリティ値が競合しないことを確認してください。

詳細については、Firewall Threat Defense IKE ポリシー （1442 ページ）を参照してください。

認証タイプ（Authentication Type）

サイト間 VPN では、事前共有キーと証明書の 2 つの認証方式がサポートされています。2 つの方式の説明については、使用する認証方式の決定 （1478 ページ）を参照してください。

（注） IKEv1 をサポートする VPN トポロジでは、選択した IKEv1 ポリシー オブジェクトで指定した [認証方式（Authentication Method）] が、IKEv1 の [認証タイプ（Authentication Type）] 設定のデフォルトになります。これらの値は一致する必要があります。一致しないと設定がエラーになります。

- [事前共有自動キー（Pre-shared Automatic Key）]：Firewall Management Center により、この VPN の事前共有キーが自動的に定義されます。[事前共有キー長（Pre-shared Key Length）] を指定します。キーの文字数は 1 ～ 27 文字です。

  文字 "（二重引用符）は事前共有キーの一部としてサポートされていません。事前共有キーで " を使用した場合は、Secure Firewall Threat Defense 6.30 以降にアップグレードした後に必ず文字を変更してください。

- [事前共有手動キー（Pre-shared Manual Key）]：この VPN の事前共有キーを手動で割り当てます。[キー（Key）] を指定して、[キーの確認（Confirm Key）] に同じキーを再入力します。

IKEv2 に対してこのオプションを選択すると、[16進数ベースの事前共有キーのみを適用する（Enforce hex-based pre-shared key only）] チェックボックスが表示されるので、必要に応じてオンにします。適用する場合は、キーの有効な 16 数値を、数字 0 ～ 9 または A ～ F を使用して、2 ～ 256 文字の偶数で入力する必要があります。

- [証明書（Certificate）]：VPN 接続の認証方法として証明書を使用する場合、ピアは PKI インフラストラクチャ内の CA サーバーからデジタル証明書を取得し、相互に認証するためにトレードします。

  [証明書（Certificate）] フィールドで、事前設定された証明書登録オブジェクトを選択します。この登録オブジェクトにより、管理対象デバイス上で同じ名前のトラストポイントが生成使用されます。証明書登録オブジェクトが関連付けられ、デバイスにインストールされ、登録プロセスが完了してから、トラストポイントが作成されます。

  トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

  このオプションを選択する前に、次の点に注意してください。

  - トポロジ内のすべてのエンドポイントに証明書登録オブジェクトが登録されていることを確認します。証明書登録オブジェクトには、証明書署名要求（CSR）を作成し、指定された認証局（CA）からアイデンティティ証明書を取得するために必要な CA サーバー情報と登録パラメータが含まれています。証明書登録オブジェクトは、管理対象デバイスを PKI インフラストラクチャに登録し、VPN 接続をサポートするデバイス上にトラストポイント（CA オブジェクト）を作成するために使用されます。証明書登録オブジェクトの作成手順については、証明書の登録オブジェクトの追加（1365 ページ）を参照してください。エンドポイントにオブジェクトを登録する手順については、次のいずれかを参照してください。
    - 自己署名登録を使用した証明書のインストール （1460 ページ）
    - EST 登録を使用した証明書のインストール （1461 ページ）
    - SCEP の登録を使用した証明書のインストール （1462 ページ）
    - 手動登録を使用した証明書のインストール （1463 ページ）
    - PKCS12 ファイルを使用した証明書のインストール （1464 ページ）

（注） サイト間 VPN トポロジの場合、同じ証明書登録オブジェクトがトポロジ内のすべてのエンドポイントに登録されていることを確認します。詳細については、次の表を参照してください。

  - さまざまなシナリオの登録要件については、次の表を参照してください。一部のシナリオでは、特定のデバイスの証明書登録オブジェクトを上書きする必要があります。オブジェクトの上書き方法については、オブジェクト オーバーライドの管理 （1311 ページ）を参照してください。

証明書の登録タイプ	すべてのエンドポイントのデバイス ID 証明書の CA が同じ		すべてのエンドポイントのデバイス ID 証明書の CA が異なる
	デバイス固有のパラメータが証明書登録オブジェクトで指定されていない	デバイス固有のパラメータが証明書登録オブジェクトで指定されている	
手動	上書きは不要	上書きが必要	上書きが必要
EST	上書きは不要	上書きが必要	上書きが必要
SCEP	上書きは不要	上書きが必要	上書きが必要
PKCS	上書きが必要	上書きが必要	上書きが必要
自己署名	N/A	N/A	N/A

- Secure Firewall Threat Defense VPN 証明書の注意事項と制約事項 （1455 ページ）記載されている VPN 証明書の制限事項を確認。

（注） Windows認証局（CA）を使用する場合、デフォルトのアプリケーションポリシー拡張は**IP セキュリティ IKE 中間**です。このデフォルト設定を使用している場合は、選択したオブジェクトの [PKI証明書登録（PKI Certificate Enrollment）] ダイアログボックスの [キー（Key）] タブにある [詳細設定（Advanced Settings）] セクションで [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）] オプションを選択する必要があります。それ以外の場合、エンドポイントでサイト間 VPN 接続を完了できません。

Firewall Threat Defense VPN IPsec オプション

（注） このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

ポイントツーポイント トポロジのエンドポイントの設定の説明に従って、ルートベース VPN のポイントツーポイントトポロジの基本パラメータを設定し、**[IPsec]** タブをクリックします。

クリプト マップ タイプ（Crypto-Map Type）
クリプトマップには、IPsec Security Association（SA; セキュリティ アソシエーション）を設定するために必要なすべてのコンポーネントが組み合わされています。2つのピアが SA

を確立しようとする場合は、それぞれに少なくとも 1 つの互換クリプト マップ エントリが必要です。IPsec セキュリティ ネゴシエーションでは、クリプトマップエントリに定義されたプロポーザルを使用して、そのクリプトマップの IPsec ルールによって指定されたデータフローが保護されます。この展開のクリプト マップにスタティックまたはダイナミックを選択します。

- [スタティック（Static）]：スタティック クリプト マップは、ポイントツーポイントまたは完全メッシュ VPN トポロジで使用します。
- [ダイナミック（Dynamic）]：実質的に、ダイナミック暗号マップによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモート ピアの要件に合うようにあとで動的に設定されます。

  ダイナミック暗号マップ ポリシーは、ハブアンドスポークとポイントツーポイント VPN トポロジの両方に適用されます。これらのポリシーを適用するには、トポロジ内のピアの 1 つにダイナミック IP アドレスを指定し、このトポロジでダイナミック暗号マップが有効になっていることを確認します。フルメッシュ VPN トポロジでは、スタティック暗号マップポリシーのみを適用できます。

IKEv2 モード（IKEv2 Mode）

IPsec IKEv2 の場合のみ、カプセル化モードはトンネルに ESP 暗号化と認証を適用するために指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

- [トンネルモード（Tunnel mode）]：（デフォルト）カプセル化モードがトンネル モードに設定されます。トンネル モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、最終的な送信元アドレスと宛先アドレスが非表示になり、新しい IP パケットでペイロードになります。

  トンネルモードの主な利点は、エンドシステムを変更しなくても IPsec を利用できることです。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。また、トラフィック分析から保護することもできます。トンネルモードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- [転送優先（Transport preferred）]：ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きの転送モードに設定されます。トランスポートモードでは、IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。したがって、管理者は、VPN インターフェイスの IP アドレスと一致する保護されたネットワークを選択する必要があります。

  このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。転送モードでは、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッ

ダーの情報に基づいて実行できるようになります。ただし、レイヤ4ヘッダーが暗号化されるため、パケットの検査が制限されます。

- [転送必須（Transport required）]：カプセル化モードは転送モードのみに設定され、トンネルモードにフォールバックできます。転送モードをサポートしていない1つのエンドポイントがあるせいで、エンドポイントが転送モードを正常にネゴシエートできない場合、VPN 接続は行われません。

プロポーザル（Proposals）

選択した IKEv1 または IKEv2 メソッドのプロポーザルを指定するには、[編集（Edit）]（✎）をクリックします。利用可能な [IKEv1 IPsecプロポーザル（IKEv1 IPsec Proposals）] または [IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposals）] オブジェクトから選択するか、または新しいプロポーザルを作成して選択します。詳細については、「IKEv1 IPsec プロポーザル オブジェクトの設定 （1440ページ）」および「IKEv2 IPsec プロポーザル オブジェクトの設定 （1441 ページ）」を参照してください。

セキュリティ アソシエーション（SA）の強度適用の有効化（Enable Security Association (SA) Strength Enforcement）

このオプションを有効にすると、子 IPsec SA で使用される暗号化アルゴリズムが、親 IKE SA よりも強くなることはありません（キー内のビット数の観点から）。

リバース ルート インジェクションを有効にする（Enable Reverse Route Injection）

リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。

Perfect Forward Secrecy の有効化（Enable Perfect Forward Secrecy）

暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイントデバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。

係数グループ（Modulus Group）

2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。 オプションの詳しい説明については、使用する Diffie-Hellman 係数グループの決定 （1477 ページ）を参照してください。

ライフタイム期間

セキュリティ アソシエーションが期限切れになる前に存続できる秒数。デフォルトは 28,800 秒です。

ライフタイム サイズ

特定のセキュリティ アソシエーションが期限切れになる前にそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。デフォルトは 4,608,000 KB です。無制限のデータは許可されていません。

ESPv3 設定（ESPv3 Settings）

着信 ICMP のエラーメッセージを検証（Validate incoming ICMP error messages）
IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先の ICMP エラー メッセージを検証するかどうかを選択します。

「フラグメント禁止」ポリシーを有効にする（Enable 'Do Not Fragment' Policy）
IP ヘッダーに Do-Not-Fragment（DF）ビット セットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。

ポリシー

- [DF ビッドのコピー（Copy DF bit）]：DF ビットを維持します。
- [DF ビッドのクリア（Clear DF bit）]：DF ビットを無視します。
- [DF ビットの設定（Set DF bit）]：DF ビットを設定して使用します。

トラフィック フロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）
トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。[バースト（Burst）]、[ペイロードサイズ（Payload Size）]、および [タイムアウト（Timeout）] パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

（注） IPSec セキュリティ アソシエーション（SA）における、ランダムな長さおよび間隔のダミーのトラフィックフローの機密性（TFC）パケットを有効にできます。TFC をイネーブルにするには、IKEv2 IPsec プロポーザルが設定されている必要があります。

TFC パケットを有効にすると、VPN トンネルがアイドル状態になることが防止されます。そのため、TFC パケットを有効にすると、グループポリシーで設定された VPN アイドル タイムアウトが期待どおりに機能しません。

Firewall Threat Defense のサイト間 VPN 展開の詳細オプション

ここでは、サイト間 VPN の展開で指定できる詳細オプションについて説明します。それらの設定は、トポロジ全体、すべてのトンネル、およびすべての管理対象デバイスに適用されます。

Firewall Threat Defense VPN の IKE 詳細オプション

[詳細設定（Advanced）] > [IKE] > [ISAKAMP 設定（ISAKAMP Settings）]

IKE キープアライブ（IKE Keepalive）

IKE キープアライブを有効または無効にします。このオプションを [永続的に有効にする（EnableInfinite）] に設定して、デバイス自体がキープアライブモニタリングを開始しないようにできます。

しきい値（Threshold）

IKEキープアライブの信頼間隔を指定します。この間隔は、キープアライブモニタリングを開始するまでにピアに許可されるアイドル時間（秒）です。最小およびデフォルトの間隔は 10 秒で、最大の間隔は 3,600 秒です。

再試行間隔（Retry Interval）

IKEキープアライブの再試行から再試行までの待機秒数を指定します。デフォルトは 2 秒で、最大値は 10 秒です。

ピアに送信される ID:（Identity Sent to Peers:）

IKE ネゴシエーションでピアが自身の識別に使用する ID を選択します。

- [autoOrDN]（デフォルト）：接続タイプによって IKE ネゴシエーションを判別します。事前共有キーの IP アドレスまたは証明書認証の証明書 DN（未サポート）を使用します。
- [IPアドレス（ipAddress）]：ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
- [ホスト名（hostname）]：ISAKMP 識別情報を交換するホストの完全修飾ドメイン名を使用します。この名前は、ホスト名とドメイン名で構成されます。

（注） すべての VPN 接続のこのオプションを有効または無効にします。

ピアIDの確認

IKEトンネルの確立中に、ピアはそのアイデンティティ（IPアドレス、完全修飾ドメイン名（FQDN）、または識別名（DN）のいずれかを提供します。また、証明書も提示します。これらのフィールドをまったく含まない、一部を含む、またはすべてを含むのいずれかです。

IKE ピア アイデンティティの検証がイネーブルの場合、 Firewall Threat Defense はピアのアイデンティティ証明書の対応するフィールドと比較して、情報が一致するかどうかを確認します。情報が一致すると、ピアのアイデンティティが検証され、Firewall Threat Defense はトンネルを確立します。情報が一致していない場合、トンネルは確立されません。

- **[確認しない（Do not check）]**：Firewall Threat Defense はピアのアイデンティティを検証しません。
- **[必須（Required）]**：Firewall Threat Defense はピアのアイデンティティを検証します。
- **[証明書でサポートされている場合（If supported by cert）]**：Firewall Threat Defense はピアが証明書を提供する場合にのみピアのアイデンティティを検証します。

アグレッシブ モードの有効化（Enable Aggressive Mode）

IP アドレスが不明で、デバイスで DNS 解決を使用できない可能性がある場合は、このネゴシエーション方式を選択してキー情報を交換します。ホスト名およびドメイン名に基づいてネゴシエーションが行われます。

トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect）
管理者は、SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にすることができます。この通知はデフォルトで無効になっています。

[詳細設定（Advanced）]>[IKE]>[IVEv2 セキュリティ アソシエーション（SA）設定（IVEv2 Security Association (SA) Settings）]

IKE v2 について、オープン SA の数を制限するさらに詳細なセッション制御を使用することができます。デフォルトでは、オープン SA の数に制限はありません。

クッキー チャレンジ（Cookie Challenge）
SA 開始パケットの応答としてピア デバイスにクッキー チャレンジを送信するかどうかを指定します。これは、サービス妨害（DoS）攻撃の防止に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキー チャレンジを使用します。次のオプションのいずれか 1 つを選択します。

- カスタム（Custom）
- しない（Never）（デフォルト）
- 常に（Always）

着信クッキー チャレンジのしきい値（Threshold to Challenge Incoming Cookies）
許可されるネゴシエーション中の SA の総数の割合。この設定を指定すると、以降の SA ネゴシエーションに対してクッキー チャレンジがトリガーされます。範囲は 0 ～ 100 % です。

許可されるネゴシエーション中の SA の数（Number of SAs Allowed in Negotiation）
一時点でネゴシエーション中にできる SA の最大数を制限します。クッキー チャレンジと共に使用する場合は、有効なクロスチェックが実行されるようにするため、クッキーチャレンジのしきい値をこの制限値よりも低くしてください。

許可される SA の最大数（Maximum number of SAs Allowed）
許可される IKEv2 接続の数を制限します。デフォルトでは無制限です。

トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect）
管理者は、SA で受信された着信パケットがその SA のトラフィックセレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にできます。デフォルトでは、[この通知を送信する（Sending this notification）] は無効になっています。

Firewall Threat Defense VPN の IPsec 詳細オプション

[詳細設定（Advanced）] > [IPsec] > [IPsec 設定（IPsec Settings）]

暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）
このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。

パスの最大伝送ユニットのエージング（Path Maximum Transmission Unit Aging）
オンにすると、パス最大伝送ユニット（PMTU）のエージング、つまり、セキュリティアソシエーション（SA）の PMTU がリセットされるまでの時間が有効になります。

値のリセット間隔（Value Reset Interval）
SA の PMTU 値が元の値にリセットされるまでの時間（分）を入力します。有効範囲は 10 ～ 30 分です。デフォルトは無制限です。

Firewall Threat Defense のサイト間 VPN トンネルの詳細オプション

ナビゲーション パス

[デバイス（Devices）] > [サイト間（Site To Site）]。その後、[+サイト間VPN（+ Site To Site VPN）] をクリックするか、リストされている VPN トポロジを編集します。[詳細設定（Advanced）] タブをクリックし、ナビゲーションペインで [トンネル（Tunnel）] を選択します。

[詳細（Advanced）] > [トンネル（Tunnel）]。

トンネル オプション

ハブ アンド スポークおよびフル メッシュ トポロジでのみ使用できます。このセクションはポイントツーポイント構成の場合は表示されません。

- [ハブを介したスポークツースポーク接続を有効にする（Enable Spoke to Spoke Connectivity through Hub）] : デフォルトでは無効になっています。このフィールドを選択すると、スポークの両端にあるデバイスは、ハブ ノードを介して他のデバイスへの接続を拡張できます。

NAT 設定

- [キープアライブ メッセージ トラバーサル（Keepalive Messages Traversal）] : デフォルトで有効です。このパラメータは、トポロジ内のすべてのエンドポイントに対して NAT -T を有効にするグローバル設定です。NAT トラバーサルのキープアライブメッセージを有効にするには、このチェックボックスをオンにします。VPN接続ハブアンドスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブメッセージを転送するために NAT トラバーサルキープアライブを使用します。このデバイスでは、IPsec フローで NAT が実行されます。

  NAT トラバーサルにより、ピア Firewall Threat Defense デバイス間に NAT デバイスがある場合、これらのデバイス間のシームレスコミュニケーションが可能になります。ハブアンドスポークトポロジの場合、このオプションはスポークでのみ使用できます。

  このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス間でキープアライブ信号が送信される**間隔**（秒）を設定します。値は、5 ～ 3600 秒の範囲で指定します。デフォルトは 20 秒です。

VPN トラフィックのアクセス制御

[復号されたトラフィック（sysopt permit-vpn）に対するバイパスアクセスコントロールポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：Firewall Threat Defense デフォルトでは、アクセス コントロール ポリシーの検査は復号されたトラフィックに適用されます。ACL 検査をバイパスするには、このオプションを有効にします。Firewall Threat Defense では、AAA サーバーからダウンロードされた VPN フィルタ ACL および認証 ACL は引き続き VPN トラフィックに適用されます。

すべての VPN 接続のオプションを有効または無効にします。このオプションを無効にする場合は、トラフィックがアクセス コントロール ポリシーまたはプレフィルタポリシーによって許可されていることを確認してください。

（注） ルートベースの VPN の場合、**sysopt permit-vpn** は機能しません。ルートベースの VPN トラフィックを許可するには、アクセス制御ルールを設定する必要があります。

証明書マップの設定

- [エンドポイントで設定された証明書マップを使用してトンネルを判別する（Use the certificate map configured in the Endpoints to determine the tunnel）]：このオプションを有効にする（オンにする）と、受信した証明書の内容をエンドポイントノードに設定されている証明書マップオブジェクトと照合することによってトンネルが判別されます。
- [証明書のOUフィールドを使用してトンネルを判別する（Use the certificate OU field to determine the tunnel）]：選択した場合、設定されたマッピング（上記のオプション）に基づいてノードが判別されない場合は、受信した証明書のサブジェクト識別名（DN）の組織単位（OU）の値を使用してトンネルを判別することを示します。
- [IKE IDを使用してトンネルを判別する（Use the IKE identity to determine the tunnel）]：選択した場合、OU（上記のオプション）と一致するルールまたは OU から取得されたルールに基づいてノードが判別されない場合は、証明書ベースの IKE セッションが、フェーズ 1 IKE ID の内容に基づいてトンネルにマッピングされることを示します。
- [ピアIPアドレスを使用してトンネルを判別する（Use the peer IP address to determine the tunnel）]：選択した場合、トンネルが OU または IKE ID 方式と一致するルールまたはその方式から取得されたルールに基づいて判別されない場合は、確立されたピア IP アドレスを使用することを示します。

仮想トンネル インターフェイスについて

Firewall Management Center は、仮想トンネルインターフェイス（VTI）と呼ばれるルーティング可能な論理インターフェイスをサポートします。VTI では、IPsec セッションから物理インターフェイスへのスタティックマッピングは不要です。IPsec トンネルエンドポイントは仮想

インターフェイスに関連付けられます。仮想インターフェイスを他のインターフェイスと同様に使用して、スタティックおよびダイナミック ルーティング ポリシーを適用できます。

ポリシーベースの VPN の代わりに、VTI を使用してピア間に VPN トンネルを作成できます。VTI は、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。VTI ではスタティックまたはダイナミックルートが使用されます。デバイスは、トンネルインターフェイスとの間のトラフィックを暗号化または復号し、ルーティングテーブルに従って転送します。展開が用意になり、ダイナミック ルーティング プロトコルのルートベースの VPN をサポートする VTI があると、仮想プライベートクラウドの多くの要件も満たせます。Firewall Management Center を使用すると、暗号マップベースの VPN の設定を VTI ベースの VPN に簡単に移行できます

サイト間 VPN ウィザードを使用して、静的またはダイナミック VTI でルートベース VPN を構成できます。トラフィックは、スタティックルート、BGP、OSPFv2/v3、または EIGRP を使用して暗号化されます。

ルーテッド セキュリティ ゾーンを作成し、そこに VTI インターフェイスを追加し、VTI トンネルを介して復号されたトラフィック制御のアクセス制御ルールを定義できます。

VTI ベースの VPN は、次の間で作成できます。

- 2 つの Firewall Threat Defense デバイス。
- Firewall Threat Defense とパブリッククラウド。
- サービスプロバイダーの冗長性を備えた Firewall Threat Defense と別の Firewall Threat Defense
- VTI インターフェイスが設定されている Firewall Threat Defense およびその他のデバイス
- ポリシーベースの VPN 構成を持つ Firewall Threat Defense およびその他のデバイス

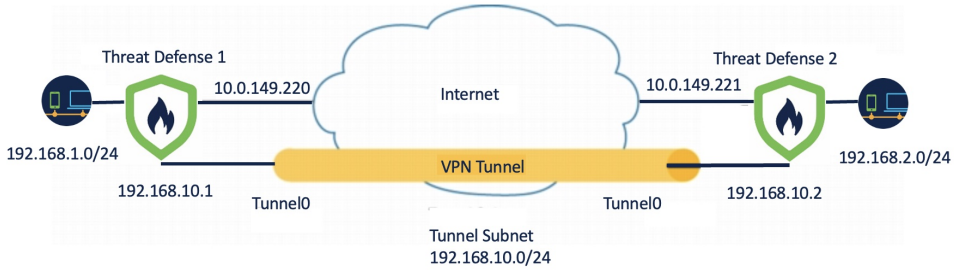
スタティック VTI とダイナミック VTI という 2 つのタイプの VTI インターフェイスが存在します。

詳細については、スタティック VTI （1508 ページ）および Dynamic VTI （1510 ページ）を参照してください。

スタティック VTI

スタティック VTI は、トンネルインターフェイスを使用して、2 つのサイト間で常時接続のトンネルを作成します。スタティック VTI のトンネル送信元として、物理インターフェイスを定義する必要があります。デバイスごとに最大 1024 の VTI を関連づけることができます。Management Center でスタティック VTI インターフェイスを作成する場合は、VTI インターフェイスの追加 （1516 ページ）を参照してください。

以下の図に、スタティック VTI を使用した VPN トポロジを示します。



Threat Defense 1 の場合：

- スタティック VTI の IP アドレス：192.168.10.1
- トンネルの送信元：10.0.149.220
- トンネルの宛先：10.0.149.221

Threat Defense 2 の場合：

- スタティック VTI の IP アドレス：192.168.10.2
- トンネルの送信元：10.0.149.221
- トンネルの宛先：10.0.149.220

利点

- 設定を最小限に抑えて簡素化します。

  クリプト マップ アクセス リストのすべてのリモートサブネットを追跡し、複雑なアクセスリストまたはクリプトマップを設定する必要はありません。

- ルーティング可能なインターフェイスを提供します。

  BGP、EIGRP、OSPFv2/v3 などの IP ルーティングプロトコルと、スタティックルートをサポートします。

- バックアップ VPN トンネルのサポート
- ECMP を使用したロード バランシングをサポートします。
- 仮想ルータをサポートします。
- VPN トラフィックに差別化したアクセス制御を提供します。

  セキュリティゾーンを使用して VTI を設定し、AC ポリシーで使用できます。この設定は以下を可能にします。

  - VPN トラフィックをクリアテキストトラフィックから分類および差別化し、VPN トラフィックを選択的に許可できます。
  - 異なる VPN トンネル間の VPN トラフィックに差別化したアクセス制御を提供します。

Dynamic VTI

ダイナミックVTIでは、IPsecインターフェイスの動的なインスタンス化および管理のために、仮想テンプレートが使用されます。仮想テンプレートは、VPNセッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。

利点

- 設定を最小限に抑えて簡素化します。

  複雑なアクセスリストやクリプトマップを設定する必要はありません。

- 管理を簡素化します。
  - 大規模な企業のハブアンドスポーク展開で、ピア設定を容易に管理できます。
  - スポークごとに 1 つの静的 VTI を設定するのではなく、複数のスポークに 1 つのダイナミック VTI のみを使用します。

- ルーティング可能なインターフェイスを提供します。

  BGP、EIGRP、OSPFv2/v3 などの IP ルーティングプロトコルと、 スタティックルートをサポートします。

- スケーリングの簡素化

  新しいスポークを追加しても、ハブで追加の VPN 設定を行う必要はありません。設定によっては、NAT およびルーティングの設定の更新が必要になる場合があります。

- バックアップ VPN トンネルをサポートします。
- ダイナミックスポークをサポートします。

  スポークの DHCP IP アドレス変更のためにハブ設定を更新する必要はありません。

- IP アドレスを節約します。
  - IP のアンナンバード インターフェイス機能を使用して、別の物理インターフェイスまたはループバック インターフェイスから IP アドレスを借用します。
  - ダイナミックVTIに関連付けられているすべての仮想アクセスインターフェイスは、同じ IP アドレスを使用します。

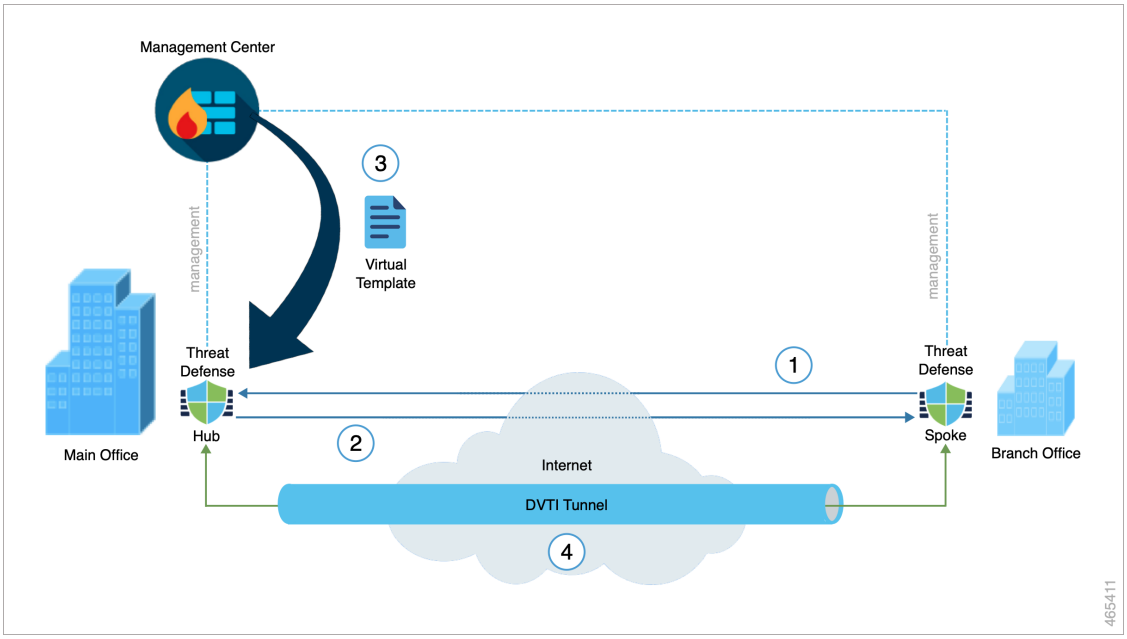
- VPN トラフィックに差別化したアクセス制御を提供します。

  セキュリティゾーンを使用して VTI を設定し、AC ポリシーで使用できます。この設定は以下を可能にします。

  - VPN トラフィックをクリアテキストトラフィックから分類および差別化し、VPN トラフィックを選択的に許可できます。

- 異なる VPN トンネル間の VPN トラフィックに差別化したアクセス制御を提供します。

Firewall Management Center による VPN セッションのダイナミック VTI トンネルの作成方法



スポークがハブとのトンネル要求を開始する場合

1. スポークが VPN 接続のためにハブとの IKE 交換を開始します。
2. ハブがスポークを認証します。
3. Firewall Management Center がスポークのハブにダイナミック仮想テンプレートを割り当てます。

   仮想テンプレートにより、ハブの仮想アクセスインターフェイスが動的に生成されます。このインターフェイスは、スポークとの VPN セッションに固有です。
4. ハブが仮想アクセスインターフェイスを使用して、スポークとのダイナミック VTI トンネルを確立します。
   1. ハブアンドスポークでは、以下を使用して、トンネルを介してトラフィックが交換されます。
      - IKE 交換を介してスポークによって提案された特定のトラフィック。
      - IPsec 経由の BGP/OSPF/EIRGP プロトコル。
   2. VPN セッションが終了すると、トンネルは切断され、ハブは対応する仮想アクセスインターフェイスを削除します。

Firewall Management Center でダイナミック VTI インターフェイスを作成するには、VTI インターフェイスの追加 （1516 ページ）を参照してください。

ダイナミック VTI を使用してルートベースのサイト間 VPN を設定するには、ルートベースのサイト間 VPN のダイナミック VTI の設定 （1534 ページ）を参照してください。

仮想トンネルインターフェイスのガイドラインと制限事項

IPv6 のサポート

- VTI は IPv6 をサポートしています。
- トンネル送信元インターフェイスに IPv6 アドレスを使用でき、同じアドレスをトンネルエンドポイントとして使用できます。
- Firewall Management Center は、パブリック IP バージョンを介した VTI IP（または内部ネットワーク IP バージョン）の次の組み合わせをサポートしています。
  - IPv6 over IPv6
  - IPv4 over IPv6
  - IPv4 over IPv4
  - IPv6 over IPv4
- VTI は、トンネルの送信元および宛先として静的および動的 IPv6 アドレスをサポートしています。
- トンネル送信元インターフェイスには IPv6 アドレスを設定でき、トンネルエンド ポイント アドレスを指定できます。このアドレスを指定しない場合、デフォルトでは、Firewall Threat Defense はリスト内の最初の IPv6 グローバルアドレスをトンネルエンドポイントとして使用します。

BGP IPv6 のサポート

VTI は IPv6 BGP をサポートしています。

EIGRP IPv4 のサポート

VTI は IPv4 EIGRP をサポートしています。

OSPFv2 および OSPFv3 IPv6/IPv4 のサポート

VTI は、IPv4 および IPv6 OSPF をサポートしています。

ECMP サポート

- アプリケーション トラフィックのロード バランシングを行うために、ECMP ゾーンでスポークのスタティック VTI を設定します。ECMP ゾーンを設定しない場合、残りのパスは、プライマリパスがダウンしたときにバックアップパスとして機能します。

マルチインスタンスおよびクラスタリング

- VTI は複数のインスタンスでサポートされています。
- VTI はクラスタリングではサポートされていません。

ファイアウォールモード

VTI はルーテッドモードのみでサポートされています。

スタティック VTI の制限事項

- 20 個の一意の IPSec プロファイルのみがサポートされます。
- ルートベースのルーティングでは、VTI を出力インターフェイスとしてのみ設定できます。

ダイナミック VTI の制限事項

- ダイナミック VTI は以下をサポートしていません。
  - ECMP と VRF
  - クラスタリング
  - IKEv1
  - QoS
- スポークに動的 IP アドレスがあり、ハブに NAT の背後のダイナミック VTI がある場合、トンネルステータスは不明になります。
- ダイナミックエクストラネットの場合、複数のスポークが接続を確立すると、サイト間監視ダッシュボードに個々のトンネルが表示されません。
- ダイナミックスポークのある NAT の背後にダイナミック VTI を使用してハブを設定すると、VPN モニタリングデータが不正確になります。

スタティックおよびダイナミック VTI の設定時の一般的な注意事項

- サイト間 VPN でダイナミッククリプトマップとダイナミック VTI を使用する場合は、ダイナミック VTI トンネルのみが起動します。この動作は、クリプトマップとダイナミック VTI の両方がデフォルトのトンネルグループを使用しようとするために発生します。

  次のいずれかを実行することを推奨します。

- サイト間 VPN をダイナミック VTI に移行します。
- 独自のトンネルグループを持つ静的クリプトマップを使用します。

- VTI は IPsec モードのみで設定可能です。
- Management Center では、ダイナミック VTI はハブアンドスポークトポロジのみをサポートします。
- ダイナミック VTI は、バージョン 7.3 以降の Threat Defense デバイスのみをサポートしています。
- ルートベースのハブアンドスポークトポロジには、1 つのハブだけを設定することをお勧めします。一組のスポークに対して複数のハブを持ち、1 つのハブをバックアップハブとして使用するトポロジを設定するには、単一のハブと同じ一組のスポークを持つ複数のトポロジを設定します。詳細については、ルートベースの VPN での複数ハブの設定 （1527 ページ）を参照してください。
- トンネルインターフェイスを使用するトラフィックには、静的、BGP、EIGRP IPv4、OSPFv2/v3 ルートを使用できます。
- ダイナミックルーティングを使用した HA 構成では、これらのトンネルはアクティブな IP アドレスを使用して作成されるため、スタンバイデバイスは VTI トンネルを介して既知のサブネットにアクセスできません。
- デバイスには最大 1024 のスタティックおよびダイナミック VTI を設定できます。VTI 数を計算する際は、次の点を考慮してください。
  - nameif サブインターフェイスを含めて、デバイスに設定できる VTI の総数を導き出します。
  - ポートチャネルのメンバーインターフェイスに nameif を設定することはできません。したがって、トンネル数は実際のメイン ポートチャネル インターフェイスの数だけ減少し、そのメンバーインターフェイスの数は減少しません。
  - プラットフォームでの VTI の数は、そのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、Firepower 1120 は 512 個の VLAN をサポートしているため、トンネル数は 512 から設定された物理インターフェイスの数を引いた数になります。
- 高可用性設定でデバイスに 400 個を超える VTI を設定する場合は、Firewall Threat Defense HA のユニットの保留時間として 45 秒を設定する必要があります。
- VTI の MTU は、基盤となる物理インターフェイスに応じて自動的に設定されます。
- ダイナミック VTI の場合、仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスから MTU を継承します。トンネル送信元インターフェイスを指定しない場合、仮想アクセスインターフェイスは、Threat Defense が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。

- スタティック VTI は IKE のバージョン v1 および v2 をサポートしており、トンネルの送信元と宛先の間でのデータ送受信に IPsec を使用します。
- ダイナミック VTI は IKE のバージョン v2 をサポートしており、トンネルの送信元と宛先の間でのデータ送受信に IPsec を使用します。
- スタティックおよびダイナミック VTI の場合は、借用 IP インターフェイスを VTI インターフェイスのトンネルソース IP アドレスとして使用しないでください。
- スタティックまたはダイナミック VTI インターフェイスを使用してルートベースのサイト間 VPN を設定する際に、 BGP を使用している場合は、TTL ホップの値が 2 以上であることを確認してください。
- NAT を適用する必要がある場合、IKE および ESP パケットは、UDP ヘッダーにカプセル化されます。
- IKE および IPsec のセキュリティ アソシエーションには、トンネル内のデータ トラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。
- トンネルグループ名は、ピアが自身の IKEv1 または IKEv2 識別情報として送信するものと一致する必要があります。
- LAN-to-LAN トンネルグループの IKEv1 では、トンネルの認証方式がデジタル証明書である場合、かつ/またはピアがアグレッシブモードを使用するように設定されている場合、IP アドレス以外の名前を使用できます。
- 暗号マップに設定されるピアアドレスと VTI のトンネル宛先が異なる場合、VTI 設定と暗号マップの設定を同じ物理インターフェイスに共存させることができます。
- デフォルトでは、VTI を経由して送信されるすべてのトラフィックは暗号化されます。
- VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセスルールを適用することができます。
- VTI インターフェイスを ECMP ゾーンに関連付け、ECMP スタティックルートを設定して、次のことを実現できます。
  - ロードバランシング（アクティブ-アクティブ VTI）：任意の並列 VTI トンネルを介して接続を送ることができます。
  - シームレスな接続移行：VTI トンネルが到達不能になると、フローは同じゾーンで設定されている別の VTI インターフェイスにシームレスに移行されます。
  - 非対称ルーティング：ある VTI インターフェイスを介したトラフィックフローを転送し、別の VTI インターフェイスを介したリバーストラフィックフローを設定します。

ECMP の設定については、等コストスタティックルートの設定（1156 ページ）を参照してください。

- ルートベースの VPN の場合、復号されたトラフィックのバイパス アクセス コントロール ポリシー（**sysopt connection permit-vpn**）は機能しません。ルートベースの VPN トラフィックを許可するには、アクセス制御ルールを設定する必要があります。

バックアップ VTI の注意事項と制約事項

- トンネルフェールオーバー全体のフローの復元力はサポートされていません。たとえば、トンネルフェールオーバー後にクリアテキストの TCP 接続が失われ、フェールオーバー中に行われた FTP 転送を再開始する必要があります。
- バックアップ VTI では、証明書認証はサポートされていません。

関連トピック

ループバック インターフェイスのガイドラインと制限事項 （687 ページ）
ルートベースのサイト間 VPN の作成 （1518 ページ）

VTI インターフェイスの追加

ルートベースのサイト間VPNを設定するには、VTIトンネルの両方のノードでデバイスにVTIインターフェイスを作成する必要があります。

トンネルタイプを「ダイナミック」として指定し、関連パラメータを設定すると、Firewall Management Centerはダイナミック仮想テンプレートを生成します。仮想テンプレートは、VPNセッションごとに固有の仮想アクセスインターフェイスを動的に生成します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 VTI インターフェイスを作成するデバイスの横にある**編集**アイコンをクリックします。

ステップ 3 [インターフェイスの追加（Add Interfaces）] > [仮想トンネルインターフェイス（Virtual Tunnel Interface）] を選択します。

ステップ 4 [トンネルタイプ（Tunnel Type）] として [スタティック（Static）] または [ダイナミック（Dynamic）] を選択します。

ステップ 5 インターフェイスの名前と説明を入力します。デフォルトでは、インターフェイスはイネーブルになっています。

28 文字以下の名前を指定してください。

ステップ 6 （任意）[セキュリティゾーン（Security Zone）] ドロップダウンメニューからセキュリティゾーンを選択して、そのゾーンにスタティック VTI インターフェイスまたはダイナミック VTI インターフェイスを追加します。

セキュリティゾーンに基づいてトラフィック検査を実行する場合は、VTIをセキュリティゾーンに追加し、アクセスコントロール（AC）ルールを設定します。トンネルを介したVPNトラ

フィックを許可するには、このセキュリティゾーンをソースゾーンとして使用する AC ルールを追加する必要があります。

ステップ 7 **[優先順位（Priority）]** フィールドに、複数の VTI 間でトラフィックのロードバランシングを行うための優先順位を入力します。

指定できる範囲は 0 ～ 65535 です。最も小さい番号が最も高い優先順位になります。このオプションは、ダイナミック VTI には適用されません。

ステップ 8 トンネルタイプに応じて、次のいずれかを実行します。

- ダイナミック VTI の場合は、[テンプレートID（Template ID）] フィールドに 1 ～ 10413 の範囲で一意の ID を入力します。
- スタティック VTI の場合は、[トンネル ID（Tunnel ID）] フィールドに 1 ～ 10413 の範囲で一意のトンネル ID を入力します。

ステップ 9 （ダイナミック VTI の場合は任意）[トンネル送信元（Tunnel Source）] ドロップダウンリストからトンネル送信元インターフェイスを選択します。

VPN トンネルは、このインターフェイス（物理インターフェイスまたはループバック インターフェイス）で終端します。ドロップダウンリストからインターフェイスの IP アドレスを選択します。IPSec トンネルモードに関係なく IP アドレスを選択できます。IPv6 アドレスが複数ある場合は、トンネルエンドポイントとして使用するアドレスを選択します。

ステップ 10 [IPSecトンネルモード（IPSec Tunnel Mode）] で、[IPv4] または [IPv6] オプションボタンをクリックして、IPSec トンネルを通過するトラフィックのタイプを指定します。

ステップ 11 [IPアドレス（IP Address）] で、次の手順を実行します。

- [IPの設定（Configure IP）]：スタティック VTI インターフェイスの IPv4 アドレスまたは IPv6 アドレスを入力します。ダイナミック VTI インターフェイスの IP アドレスは設定できません。ダイナミック VTI インターフェイスについては、[IP の借用（Borrow IP）] フィールドを使用します。
- [IPの借用（IP アンナンバード）（Borrow IP (IP unnumbered)）]：ドロップダウンリストから物理インターフェイスまたはループバック インターフェイスを選択します。VTI インターフェイスはこの IP アドレスを継承します。

  トンネル送信元 IP アドレスとは異なる IP アドレスを使用していることを確認してください。このオプションは、スタティック VTI インターフェイスまたはダイナミック VTI インターフェイスに使用できます。

  [追加（Add）] ＋をクリックしてループバック インターフェイスを設定します。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。

ステップ 12 [OK] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

ルートベースのサイト間 VPN の作成

次の 2 つのトポロジに対してルートベースのサイト間 VPN を設定できます。

- [ポイントツーポイント（Point to Point）]：トンネルの両方のノードで VTI を設定し、ウィザードを使用して VPN を設定します。
- [ハブおよびスポーク（Hub and Spoke）]：ハブとスポークで VTI を設定します。ハブをダイナミック VTI で設定し、スポークを静的 VTI で設定します。

エクストラネットデバイスをハブとして設定し、管理対象デバイスをスポークとして設定することができます。複数のハブとスポークを設定でき、バックアップのハブとスポークも設定できます。

- エクストラネットのハブとスポークの場合、複数の IP をバックアップとして設定できます。
- 管理対象スポークの場合、プライマリ VTI インターフェイスとともにバックアップのスタティック VTI インターフェイスを設定できます。

VTI の詳細については、仮想トンネルインターフェイスについて （1507 ページ）を参照してください

（注） VTI へのすべての言及は、明記されていないかぎり、スタティック VTI とダイナミック VTI を表します。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [サイト間（Site to Site）]**を選択します。

ステップ 2 [+サイト間VPN（+ Site To Site VPN）] をクリックします。

ステップ 3 [トポロジ名（Topology Name）] フィールドに、VPN トポロジの名前を入力します。

ステップ 4 [ルートベース（VTI）（Route Based (VTI)）] を選択し、次のいずれかを実行します。

- ネットワークトポロジとして [ポイントツーポイント（Point to Point）] を選択します。ルートベースの「ポイントツーポイント」トポロジのエンドポイントを設定するには、ポイントツーポイント トポロジのエンドポイントの設定 （1519 ページ）を参照してください。
- ネットワークトポロジとして [ハブアンドスポーク（Hub and Spoke）] を選択します。ルートベースの「ハブアンドスポーク」トポロジのエンドポイントを設定するには、ハブアンドスポークトポロジのエンドポイントの設定 （1522 ページ）を参照してください。

ステップ 5 （任意） Firewall Threat Defense VPN IKE オプション （1497 ページ）の説明に従って、展開の [IKE] オプションを指定します。

ステップ 6 （任意） Firewall Threat Defense VPN IPsec オプション （1500 ページ）の説明に従って、展開の [IPsec] オプションを指定します。

ステップ 7 （任意） Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （1503 ページ）の説明に従って、展開の [詳細（Advanced）] オプションを指定します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

両方のデバイスで VTI インターフェイスと VTI トンネルを設定したら、次のものを設定する必要があります。

- VTI トンネルを介してデバイス間で VTI トラフィックをルーティングするルーティングポリシー。詳細については、VTI のルーティングおよび AC ポリシーの設定 （1534 ページ）を参照してください。
- 暗号化されたトラフィックを許可するアクセスコントロールルール。[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

ポイントツーポイント トポロジのエンドポイントの設定

ポイントツーポイント トポロジ ノードのルートベースのサイト間 VPN のエンドポイントを設定するには、次のパラメータを設定します。

始める前に

ルートベースのサイト間 VPN の作成 （1518 ページ）の説明に従って、ルートベース VPN のポイントツーポイント トポロジの基本パラメータを設定し、[エンドポイント（Endpoints）] タブをクリックします。

手順

ステップ 1 [ノードA（Node A）] の [デバイス（Device）] ドロップダウンメニューで、VTI トンネルの最初のエンドポイントとして使用する登録済みデバイス（Firewall Threat Defense）またはエクストラネットの名前を選択します。

エクストラネットピアの場合は、次のパラメータを指定します。

1. デバイスの名前を指定します。
2. [エンドポイントのIPアドレス（Endpoint IP address）] フィールドに、プライマリ IP アドレスを入力します。バックアップ VTI を設定している場合は、カンマを追加して、バックアップ IP アドレスを指定します。

3. [OK] をクリックします。

エクストラネットハブに対する前述のパラメータを設定後、[IKE] タブでエクストラネットの事前共有キーを指定します。

（注）
AWS VPC には、デフォルトのポリシーとして **AES-GCM-NULL-SHA-LATEST** があります。リモートピアが AWS VPC に接続する場合は、[ポリシー（Policy）] ドロップダウンリストから [AES-GCM-NULL-SHA-LATEST] を選択して、AWS のデフォルト値を変更せずに VPN 接続を確立します。

ステップ 2 登録済みデバイスの場合、[仮想トンネルインターフェイス（Virtual Tunnel Interface）] ドロップダウンリストからノード A の VTI インターフェイスを指定できます。

選択したトンネルインターフェイスはノード A の送信元インターフェイスであり、ノード B のトンネルの宛先です。

ノード A に新しいインターフェイスを作成する場合は、[追加（Add）] ＋アイコンをクリックして、VTIインターフェイスの追加（1516ページ）の説明に従ってフィールドを設定します。

既存の VTI の設定を編集する場合は、[仮想トンネルインターフェイス（Virtual Tunnel Interface）] ドロップダウンフィールドで VTI を選択し、[VTIの編集（Edit VTI）] をクリックします。

ステップ 3 ノード A デバイスが NAT デバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェックボックスをオンにします。[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドに、トンネル送信元のパブリック IP アドレスを入力します。

ステップ 4 [ピアへのローカルIDの送信（Send Local Identity to Peers）]：ローカル ID 情報をピアデバイスに送信するには、このオプションを選択します。リストから次のいずれかの [ローカルID構成（Local Identity Configuration）] を選択し、ローカル ID を設定します。

- [IPアドレス（IP address）]：ID にインターフェイスの IP アドレスを使用します。
- [自動（Auto）]：事前共有キーにはIPアドレスを使用し、証明書ベースの接続には証明書 DN を使用します。
- [電子メールID（Email ID）]：ID に使用する電子メール ID を指定します。電子メール ID は最大 127 文字です。
- [ホスト名（Hostname）]：完全修飾ホスト名を使用します。
- [キーID（Key ID）]：ID に使用するキー ID を指定します。キー ID は 65 文字未満にする必要があります。

ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。一意の ID を指定すると、Cisco Umbrella Secure Internet Gateway（SIG）に接続するために、Firewall Threat Defense が NAT の背後に複数の IPsec トンネルを持つことができます。

Cisco Umbrella での一意のトンネル ID の設定については、**Cisco Umbrella SIG ユーザーガイド** [英語] を参照してください。

ステップ 5 （任意）[バックアップVTIの追加（Add Backup VTI）] をクリックして、追加の VTI をバックアップ インターフェイスとして指定し、パラメータを設定します。

（注）
トポロジの両方のピアで、バックアップVTIに対して同じトンネル送信元が設定されていないことを確認します。デバイスに、同じトンネル送信元とトンネル宛先を持つ2つのVTIは設定できないため、一意のトンネル送信元とトンネル宛先の組み合わせを設定します。

仮想トンネルインターフェイスはバックアップVTIで指定されますが、どちらのトンネルがプライマリまたはバックアップとして使用されるかは、ルーティング設定によって決まります。

ステップ 6 [追加の設定（Additional Configuration）] で、次の手順を実行します。

- [ルーティングポリシー（Routing Policy）] をクリックします。Firewall Management Center で**[デバイス（Devices）]** > **[ルーティング（Routing）]** ページが表示されます。

  VPN トラフィックのスタティックルーティング、BGP、OSPF v2/v3、または EIGRP ルーティングを設定できます。

- VPN トラフィックを許可するには、[ACポリシー（AC Policy）] をクリックします。Firewall Management Center でデバイスのアクセス コントロール ポリシー ページが表示されます。VTI のセキュリティゾーンを指定する、許可/ブロックルールの追加に進みます。バックアップ VTI を設定している場合は、プライマリ VTI と同じセキュリティゾーンへのバックアップトンネルが含まれていることを確認します。AC ポリシーページのバックアップ VTI に特定の設定は必要ありません。

ステップ 7 [詳細設定（Advance Settings）] を展開して、デバイスの追加構成を設定します。詳細については、ルートベース VPN のポイントツーポイント トポロジの詳細設定 （1522 ページ）を参照してください。

ステップ 8 ノード B に対して上記の手順を繰り返します。

ステップ 9 [OK] をクリックします。

次のタスク

- （任意）Firewall Threat Defense VPN IKE オプション （1497 ページ）の説明に従って、展開の [IKE] オプションを指定します。
- （任意）Firewall Threat Defense VPN IPsec オプション （1500 ページ）の説明に従って、展開の [IPsec] オプションを指定します。
- （任意）Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （1503 ページ）の説明に従って、展開の [詳細（Advanced）] オプションを指定します。
- [保存（Save）] をクリックします。
- トラフィックを VTI にルーティングするには、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、Threat Defense デバイスを編集して、[ルーティング（Routing）] タブをクリックします。

VPN トラフィックのルーティングには、スタティックルートを設定したり、BGP、OSPF v2/v3、または EIGRP を使用したりできます。

- VPN トラフィックを許可するには、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。 。VTI のセキュリティゾーンを指定するルールを追加します。バックアップ VTI の場合は、プライマリ VTI と同じセキュリティゾーンにバックアップ VTI が含まれていることを確認します。

ルートベース VPN のポイントツーポイント トポロジの詳細設定

ルートベース VPN のポイントツーポイント トポロジに対して、次の詳細な設定を設定します。

始める前に

ポイントツーポイント トポロジのエンドポイントの設定（1519ページ）の説明に従って、ルートベースの VPN でポイントツーポイント トポロジの基本パラメータを設定し、[詳細設定（Advance Settings）] を展開します。

手順

ステップ 1 [ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにして、VTI IP アドレスをピアデバイスに送信します。

ステップ 2 [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、スポークおよびピアからの着信 IKEv2 ルートを許可します。

ステップ 3 [接続タイプ（Connection Type）] ドロップダウンリストから、次のいずれかを選択します。

[応答のみ （Answer Only）] : デバイスは、ピアデバイスが接続を開始したときにのみ応答でき、接続は開始できません。

[双方向（Bidirectional）] : デバイスは接続を開始または応答できます。これがデフォルトのオプションです。

ハブアンドスポークトポロジのエンドポイントの設定

ダイナミック VTI を使用して、ハブアンドスポークトポロジ専用のルートベースのサイト間 VPN を作成できます。ハブはダイナミック VTI のみを使用でき、スポークはスタティック VTI インターフェイスのみを使用できます。エクストラネットデバイスをハブとして構成することもできます。

ハブ アンド スポーク トポロジ ノードのルートベースのサイト間 VPN のエンドポイントを設定するには、次のパラメータを設定します。

始める前に

ルートベースのサイト間VPNの作成（1518ページ）の説明に従って、ルートベースVPNのハブアンドスポークトポロジの基本パラメータを設定し、[エンドポイント（Endpoints）]タブをクリックします。

手順

ステップ1 [ハブノード（Hub Nodes）]の下で、次の手順を実行します。

a) [追加（Add）]＋をクリックして、**[エンドポイントの追加（Add Endpoint）]** ダイアログボックスでハブ ノードを設定します。

b) [デバイス（Device）] ドロップダウンリストからハブを選択します。

エクストラネットハブの場合は、次のパラメータを指定します。

1. デバイスの名前を入力します。
2. プライマリIPアドレスを入力します。バックアップVTIを設定している場合は、カンマを追加して、バックアップIPアドレスを指定します。
3. [OK] をクリックします。

エクストラネットハブに対する前述のパラメータを設定後、[IKE] タブでエクストラネットの事前共有キーを指定します。

（注）
AWS VPCには、デフォルトのポリシーとして **AES-GCM-NULL-SHA-LATEST** があります。リモートピアがAWS VPCに接続する場合は、[ポリシー（Policy）] ドロップダウンリストから [AES-GCM-NULL-SHA-LATEST] を選択して、AWSのデフォルト値を変更せずにVPN接続を確立します。

c) [ダイナミック仮想トンネルインターフェイス（Dynamic Virtual Tunnel Interface）] ドロップダウンリストからダイナミックVTIを選択します。

ダイナミックVTIにはトンネルソースの設定が必須です。これは、Management Centerではスポークのトンネル宛先を決定するためにこの情報を必要になるためです。

[追加（Add）]＋をクリックして、新しいダイナミックVTIを追加します。ループバックインターフェイスから動的インターフェイスの借用IPを設定することをお勧めします。

既存のダイナミックVTIを編集する場合は、インターフェイスを選択して、[VTIの編集（Edit VTI）] をクリックします。

d) （オプション）エンドポイントデバイスがNATデバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェック ボックスをオンにして、[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドでトンネル送信元のIPアドレスを設定します。

e) [ルーティングポリシー（Routing Policy）] をクリックして、ハブのルーティングポリシーを設定します。

f) [ACポリシー（AC Policy）] をクリックして、アクセス コントロール ポリシーを設定します。

g) [詳細設定（Advance Settings）] を展開して、ハブの追加構成を設定します。詳細については、ルートベースのVPNのハブアンドスポークに対する詳細設定（1526ページ）を参照してください。

h) [OK] をクリックします。

ステップ2 [スポークノード（Spoke Nodes）] の下で、次の手順を実行します。

a) [追加（Add）] ＋をクリックして、**[エンドポイントの追加（Add Endpoint）]** ダイアログボックスでスポークを設定します。

b) [デバイス（Device）] ドロップダウンリストからスポークを選択します。

エクストラネットスポークの場合は、次のパラメータを指定します。

1. デバイスの名前を入力します。
2. [エンドポイントIPアドレス（Endpoint IP Address）] で、次のいずれかを選択します。
   - [静的（Static）]：デバイスのIPアドレスと、必要に応じてバックアップIPアドレスを入力します。
   - [動的（Dynamic）]：エクストラネットスポークのIPアドレスを動的に割り当てるには、このオプションを選択します。
3. [OK] をクリックします。

c) [スタティック仮想トンネルインターフェイス（Static Virtual Tunnel Interface）] ドロップダウンリストからスタティック VTI を選択します。

[追加（Add）] ＋をクリックして、新しいスタティック VTI を追加します。スタティック VTI のトンネル IP は自動入力されます。この IP アドレスがスポークに対して一意であることを確認してください。

既存のスタティック VTI を編集する場合は、インターフェイスを選択して、[VTIの編集（Edit VTI）] をクリックします。

d) （オプション）エンドポイントデバイスが NAT デバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェックボックスをオンにします。Management Center では、スポークにトンネル宛先 IP アドレスを設定するために、トンネルの送信元インターフェイスアドレスが必要です。[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドに、トンネル送信元のパブリック IP アドレスを入力します。

e) （オプション）[ピアへのローカルIDの送信（Send Local Identity to Peers）]：ローカル ID 情報をピアデバイスに送信するには、このチェックボックスをオンにします。[ローカルID設定（Local Identity Configuration）] ドロップダウンリストから次のいずれかのパラメータを選択し、ローカル ID を設定します。

- [IPアドレス（IP address）]：ID にインターフェイスの IP アドレスを使用します。

- [自動（Auto）]：事前共有キーには IP アドレスを使用し、証明書ベースの接続には証明書 DN を使用します。
- [電子メールID（Email ID）]：ID に使用する電子メール ID を指定します。電子メール ID は最大 127 文字です。
- [ホスト名（Hostname）]：完全修飾ホスト名を使用します。
- [キーID（Key ID）]：ID に使用するキー ID を指定します。キー ID は 65 文字未満にする必要があります。

ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。一意の ID を設定すると、Cisco Umbrella Secure Internet Gateway（SIG）に接続するために、Firewall Threat Defense が NAT の背後に複数の IPsec トンネルを持つことができます。

Cisco Umbrella での一意のトンネル ID の設定については、*Cisco Umbrella SIG* ユーザーガイド [英語] を参照してください。

f) （オプション）[バックアップVTIの追加（Add Backup VTI）] をクリックして、追加の VTI インターフェイスをバックアップ インターフェイスとして指定します。

（注）
トポロジの両方のピアで、同じトンネル送信元にバックアップ VTI が設定されていないことを確認します。たとえば、ピア A で 1 つのトンネル送信元インターフェイス（10.10.10.1/30 など）を使用して 2 つの VTI（プライマリとバックアップ）が設定されている場合は、ピア B でも 1 つのトンネル送信元 IP（20.20.20.1/30 など）を使用して 2 つの VTI を設定することはできません。

仮想トンネルインターフェイスはバックアップ VTI で指定されますが、どちらのトンネルがプライマリまたはバックアップとして使用されるかは、ルーティング設定によって決まります。

g) [ルーティングポリシー（Routing Policy）] をクリックして、スポークのルーティングポリシーを設定します。

h) [ACポリシー（AC Policy）] をクリックして、アクセス コントロール ポリシーを設定します。

i) [詳細設定（Advance Settings）] を展開して、スポークの追加構成を設定します。詳細については、ルートベースの VPN のハブアンドスポークに対する詳細設定 （1526 ページ）を参照してください。

j) [OK] をクリックします。

次のタスク

- （任意）Firewall Threat Defense VPN IKE オプション （1497 ページ）の説明に従って、展開の [IKE] オプションを指定します。

- （任意）Firewall Threat Defense VPN IPsec オプション （1500 ページ）の説明に従って、展開の [IPsec] オプションを指定します。
- （任意）Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （1503 ページ）の説明に従って、展開の [詳細（Advanced）] オプションを指定します。
- [保存（Save）] をクリックします。

ルートベースの VPN のハブアンドスポークに対する詳細設定

ルートベースの VPN のハブアンドスポークに対して、次の詳細設定を構成します。

始める前に

ハブアンドスポークトポロジのエンドポイントの設定 （1522 ページ）の説明に従って、ルートベースの VPN でハブアンドスポークの基本パラメータを設定し、[詳細設定（Advance Settings）] を展開します。

手順

ステップ 1 [ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにして、VTI IP アドレスをピアデバイスに送信します。

ハブの場合、ルーティングプロトコルとして BGP を使用する場合は、このチェックボックスをオンにする必要があります。この構成により、ループバック IP アドレスが BGP ルーティングテーブルで共有されます。

スポークの場合、このオプションはデフォルトで有効になっています。

ステップ 2 [保護されたネットワーク（Protected Networks）] を追加して、VPN エンドポイントによって保護されるネットワークを定義します。[追加（Add）] ＋をクリックして、保護されたネットワークを選択します。

ハブの場合、ハブの背後にある保護されたネットワークを設定します。この情報とスポークの保護されたネットワークにより、スポークアクセスリストが生成されます。

ダイナミック VTI を使用したハブの仮想アクセスインターフェイスのスタティックルートは作成できません。これらのインターフェイスは、トンネルの確立および終了時にハブで動的に作成および削除されます。

スポークの場合、スポークの保護されたネットワークを設定します。

スポークのスタティックルーティングを有効にするには、トポロジのエンドポイントを設定後、[IPsec] タブをクリックし、[リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] チェックボックスをオンにします。

BGP、OSPF、または EIGRP を使用する場合、このオプションは不要です。

ステップ 3 [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、スポークおよびピアからの着信 IKEv2 ルートを許可します。

ハブの場合：IKE交換中、ハブは動的に作成された仮想アクセスインターフェイスをスポークにアドバタイズし、スポークはその VTI IP アドレスをハブにアドバタイズします。

スポークの場合：このオプションはデフォルトで有効になっています。

ステップ 4 [接続タイプ（Connection Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。

[応答のみ （Answer Only）]：デバイスは、ピアデバイスが接続を開始したときにのみ応答でき、接続は開始できません。

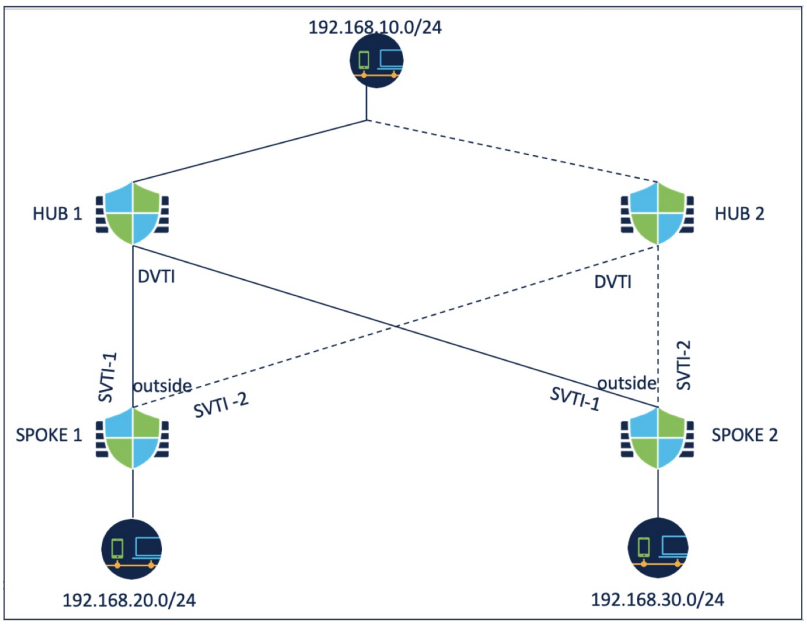
[双方向（Bidirectional）]：デバイスは接続を開始または応答できます。これがデフォルトのオプションです。

ルートベースの VPN での複数ハブの設定

一組のスポークに対して複数のハブを使用するトポロジを設定できます。1 つのハブをバックアップハブとした場合、単独のハブと同じ一組のスポークを持つ複数のトポロジを設定できます。

次の例では、2 つのハブが同じ一組のスポークに接続されています。ハブ 1 はプライマリハブで、ハブ 2 はセカンダリハブです。Firewall Management Center でこのネットワークを設定するには、ルートベースのハブ アンド スポーク トポロジを 2 つ設定する必要があります。

- トポロジ 1：ハブ 1 がスポーク 1 とスポーク 2 に接続されている。
- トポロジ 2：ハブ 2 がスポーク 1 とスポーク 2 に接続されている。



トポロジ 1 を設定するには、次の手順を実行します。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site to Site）]**を選択します。

ステップ 2 [+サイト間VPN（+ Site To Site VPN）] をクリックします。

ステップ 3 [トポロジ名（Topology Name）] フィールドに、VPN トポロジの名前を入力します。

ステップ 4 [ルートベース（VTI）（Route Based (VTI)）] を選択し、次のいずれかを実行します。

- ネットワークトポロジとして[ポイントツーポイント（Point to Point）] を選択します。ルートベースの「ポイントツーポイント」トポロジのエンドポイントを設定するには、ポイントツーポイント トポロジのエンドポイントの設定 （1519 ページ）を参照してください。
- ネットワークトポロジとして[ハブアンドスポーク（Hub and Spoke）] を選択します。ルートベースの「ハブアンドスポーク」トポロジのエンドポイントを設定するには、ハブアンドスポークトポロジのエンドポイントの設定 （1522 ページ）を参照してください。

ステップ 5 IKE バージョンを設定します。

ステップ 6 [エンドポイント（Endpoints）] タブをクリックします。

ステップ 7 [ハブノード（Hub Nodes）]の下で、次の手順を実行します。

a) [追加（Add）] ＋をクリックしてハブを追加します。

b) [デバイス（Device）] ドロップダウンリストからハブ 1 を選択します。

c) **[ダイナミック仮想トンネル インターフェイス（Dynamic Virtual Tunnel Interface）]** ドロップダウン リストからダイナミック VTI を設定するか、[追加（Add）] ＋をクリックして新しいダイナミック VTI を追加します。

ループバック インターフェイスから動的インターフェイスの借用 IP を設定することをお勧めします。

d) （オプション）エンドポイントデバイスが NAT デバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェック ボックスをオンにして、[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドでトンネル送信元の IP アドレスを設定します。

e) [ルーティングポリシー（Routing Policy）] をクリックして、ハブのルーティングポリシーを設定します。BGP を使用して動的ルーティングを設定できます。

f) [詳細設定（Advance Settings）] を展開します。ハブの次の詳細設定を構成して、動的ルーティングを使わない場合に使用できる IKEv2 ルーティングを有効にすることができます。

- （オプション）[ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにします。
- ハブの [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、スポークからのルートを許可し、ルーティングテーブルを更新します。
- [接続タイプ（Connection Type）] ではドロップダウンリストから [双方向（Bidirectional）] を選択します。

g) [OK] をクリックします。

ステップ 8 [スポークノード（Spoke Nodes）] の下で、次の手順を実行します。

a) [追加（Add）] ＋をクリックしてスポークを追加します。

b) [デバイス（Device）] ドロップダウンリストからスポーク 1 を選択します。

c) **[スタティック仮想トンネル インターフェイス（Static Virtual Tunnel Interface）]** ドロップダウンリストからスポークのスタティック VTI として SVTI-1 を選択するか、[追加（Add）] ＋をクリックして新しいスタティック VTI を追加します。

SVTI-1 のトンネル送信元として外部インターフェイスを選択します。SVTI-1 のトンネル IP は自動入力されます。この IP アドレスが、両方のトポロジのピア間でスポーク 1 に対して一意であることを確認してください。

d) [詳細設定（Advance Settings）] を展開します。動的ルーティングを使用しない場合は、これらの設定を行って、スポークの IKEv2 ルーティングを有効にすることができます。

- [ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにして、VTI IP アドレスをピアデバイスに送信します。
- [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、ピアからの着信 IKEv2 ルートを許可します。
- [接続タイプ（Connection Type）] ではドロップダウンリストから [双方向（Bidirectional）] を選択します。

e) [OK] をクリックします。

f) 手順 5a ～ 5e を繰り返して、スポーク 2 を追加します。SVTI-1 をスポーク 2 のスタティック VTI として設定します。

ステップ 9 必要に応じて IKE および IPSec パラメータを設定するか、デフォルト値を使用します。

次のタスク

1. ハブ 2、スポーク 1、およびスポーク 2 を使用してトポロジ 2 を設定します。

   SVTI-2 をスポーク 1 のスタティック VTI として設定し、SVTI-2 をスポーク 2 のスタティック VTI として設定します（上の図を参照）。SVTI-2 のトンネル送信元は同じ外部インターフェイスとしてください。

2. スポークごとに、ルーティングポリシーを設定します。詳細については、ルートベース VPN での複数ハブのルーティングの設定 （1530 ページ）を参照してください。

3. 設定とトンネルのステータスを確認します。詳細については、「ルートベースの VPN での複数ハブ構成の確認 （1531 ページ）」を参照してください。

ルートベース VPN での複数ハブのルーティングの設定

次の手順では、ハブとスポークでダイナミックルーティングを設定し、スポークでポリシーベースルーティングを設定する方法について説明します。

始める前に

ルートベースの VPN での複数ハブの設定（1527 ページ）で説明されているように、トポロジ 1 とトポロジ 2 を設定します。

手順

ステップ 1 BGP を使用してハブのダイナミックルーティングを設定します。

a) [デバイス（Device）]>[デバイス管理（Device Management）]>[ルーティング（Routing）] を選択します。
b) 左側のペインで、[一般設定（General Settings）] > [BGP] を選択します。
c) [BGPの有効化（Enable BGP）] チェックボックスをオンにして、**AS 番号**を入力します。

要件に応じて他のフィールドを設定できます。

d) [保存（Save）] をクリックします。
e) 左側のペインで、[BGP] > [IPv4] を選択します。
f) [IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。
g) [ネイバー（Neighbor）] タブをクリックし、[追加（Add）] をクリックして、パラメータを設定します。

1. [IPアドレス（IP Address）]：スポーク 1 のトンネルインターフェイス IP アドレスを入力します。
2. [リモートAS（Remote AS）]：スポーク 1 の AS 番号。
3. [アドレスの有効化（Enabled Address）] チェックボックスをオンにします。
4. [OK] をクリックします。

上記の手順を繰り返して、スポーク 2 をネイバーとして追加します。

h) [保存（Save）] をクリックします。
i) [ネットワーク（Networks）] タブをクリックし、[追加（Add）] をクリックして、ハブの背後にあるネットワークをピアにアドバタイズします。

ステップ 2 BGP を使用して、スポークのダイナミックルーティングを設定します。

スポークの BGP 設定は、次の相違点を除いてハブの BGP 設定と似ています。

- ハブ 1 とハブ 2 を両方のスポークのネイバーとして設定し、ハブのトンネルインターフェイス IP アドレスを使用します。
- ネットワークを設定するときは、各スポークの背後にあるネットワークを使用します。

ステップ 3 スポークでポリシーベースルーティングを設定します。

a) 左側のペインで、[ポリシーベースルーティング（Policy Based Routing）] を選択し、[追加（Add）] をクリックします。

b) ドロップダウンリストから [入力インターフェイス（Ingress Interface）] を選択します。

c) [追加（Add）] をクリックして、一致 ACL を設定します。

たとえば、スポーク 1 の場合、送信元ネットワークは 192.168.20.0/24 で、宛先ネットワークは 192.168.10.0/24 です。

d) [宛先（Send to）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。

e) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [順序（Order）] を選択します。

f) 出力インターフェイスとして SVTI-1 インターフェイスと SVTI-2 インターフェイスを選択します。

g) [保存（Save）] をクリックします。

ハブをロードバランシングペアとして使用する場合は、ECMP を設定する必要があります。

ステップ 4 ハブとスポークに設定を展開します。

次のタスク

設定とトンネルのステータスを確認します。詳細については、「ルートベースの VPN での複数ハブ構成の確認 （1531 ページ）」を参照してください。

ルートベースの VPN での複数ハブ構成の確認

複数ハブ構成とトンネルのステータスを確認するには、次の手順を実行します。

- 展開後、ダッシュボードでトンネルステータスを確認します。
- サイト間監視ダッシュボードからパケットトレーサを使用して、トラフィックの選択されたパス（ハブ 1 またはハブ 2）を確認します。
- エンドポイントごとに次の show コマンドを使用して、構成を確認します。
  - **show run route-map**
  - **show run access-list**
  - **show route-map**
  - **show route**

バックアップ VTI トンネルを介したトラフィックのルーティング

Secure Firewall Threat Defense は、ルートベース（VTI）VPN のバックアップトンネルの構成をサポートします。プライマリ VTI がトラフィックをルーティングできない場合、VPN 内のトラフィックはバックアップ VTI を介してトンネリングされます。

次のシナリオでバックアップ VTI トンネルを展開できます。

- 両方のピアにサービスプロバイダーの冗長性バックアップがある。

  この場合、2 つの物理インターフェイスがあり、ピアの 2 つの VTI のトンネルソースとして機能します。

- 一方のピアにのみ、サービスプロバイダーの冗長性バックアップがある。

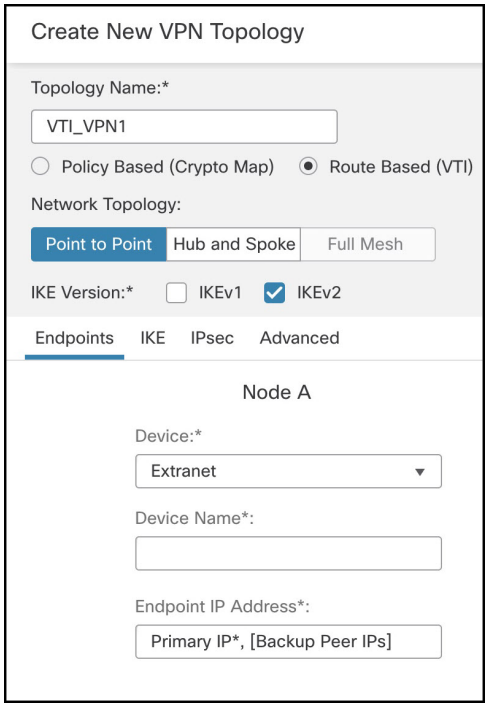
  この場合、ピアの一方の側だけにインターフェイスバックアップがあり、もう一方の端にはトンネル ソース インターフェイスが 1 つだけあります。

手順	操作手順	詳細
1	注意事項と制限事項を確認します。	仮想トンネルインターフェイスのガイドラインと制限事項 （1512 ページ）
2	VTIインターフェイスを作成します。	VTI インターフェイスの追加 （1516 ページ）
3	[新しいVPNトポロジの作成（Create New VPN Topology）] ウィザードの [エンドポイントの追加（Add Endpoint）] ダイアログボックスで、[バックアップVTIの追加（Add Backup VTI）] をクリックして、各ピアのそれぞれのバックアップ インターフェイスを構成します。	• ポイントツーポイント トポロジのエンドポイントの設定 （1519 ページ） • ハブアンドスポークトポロジのエンドポイントの設定 （1522 ページ）
4	ルーティングポリシーを設定します。	• [デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、Threat Defense デバイスを編集します。 • [ルーティング（Routing）] をクリックします。
5	アクセス コントロール ポリシーを設定します。	• [ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

バックアップ VTI トンネルを構成するためのガイドライン

- エクストラネットピアの場合、バックアップ インターフェイスのトンネルソース IP アドレスを指定し、管理対象ピアでトンネルの宛先 IP を構成できます。

  [新規VPNトポロジの作成（Create New VPN Topology）] ウィザードの [エンドポイントIPアドレス（Endpoint IP Address）] フィールドで、バックアップピアの IP アドレスを指定できます。



- バックアップインターフェイスを設定した後、ルーティングトラフィックのルーティングポリシーとアクセス コントロール ポリシーを設定します。

  プライマリ VTI とバックアップ VTI は常に使用可能ですが、トラフィックはルーティングポリシーで設定されたトンネルのみを通過します。詳細については、VTIのルーティングおよび AC ポリシーの設定 （1534 ページ）を参照してください。

- バックアップ VTI を設定している場合は、プライマリ VTI と同じセキュリティゾーンへのバックアップトンネルが含まれていることを確認します。AC ポリシーページのバックアップ VTI に特定の設定は必要ありません。

- バックアップトンネルにスタティックルートを設定する場合は、バックアップトンネルを介したトラフィックフローのフェールオーバーを処理するために、異なるメトリックでスタティックルートを設定します。

ルートベースのサイト間 VPN のダイナミック VTI の設定

Management Center でルートベースのサイト間 VPN のダイナミック VTI を設定するには、次の手順を実行します。

手順	操作手順	詳細情報
1	ハブにダイナミック VTI インターフェイスを作成します。	VTI インターフェイスの追加 （1516 ページ）
2	スポークにスタティック VTI インターフェイスを作成します。	VTI インターフェイスの追加 （1516 ページ）
3	ルートベースのサイト間 VPN を作成します。	ルートベースのサイト間 VPN の作成 （1518 ページ）
4	ルーティングポリシーとアクセス コントロール ポリシーを設定します。	ハブアンドスポークトポロジのエンドポイントの設定 （1522 ページ）

VTI のルーティングおよび AC ポリシーの設定

両方のデバイスで VTI インターフェイスと VTI トンネルを設定したら、次のものを設定する必要があります。

- VTI トンネルを介してデバイス間で VTI トラフィックをルーティングするルーティングポリシー。
- 暗号化されたトラフィックを許可するアクセスコントロールルール。

VTI のルーティング設定

VTI インターフェイスの場合、スタティックルートまたはルーティングプロトコル（BGP、EIGRP、OSPF/OSPFv3 など）を設定できます。

1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、Firewall Threat Defense デバイスを編集します。
2. [ルーティング（Routing）] をクリックします。
3. スタティックルート、または BGP、EIGRP、OSPF/OSPFv3 を設定します。

ルーティング	パラメータ	詳細情報
Static Route	• [インターフェイス（Interface）]：VTI インターフェイスを選択します。バックアップトンネルの場合は、バックアップ VTI インターフェイスを選択します。 • [選択したネットワーク（Selected Network）]：リモートピアの保護されたネットワーク。 • [ゲートウェイ（Gateway）]：リモートピアのトンネルインターフェイスの IP アドレス。バックアップトンネルの場合は、リモートピアのバックアップ トンネルインターフェイスの IP アドレスを選択します。 • [メトリック（Metrick）]：バックアップトンネルの場合は、異なるメトリックを設定して、バックアップトンネルを介したトラフィックフローのフェールオーバーを処理します。	スタティック ルートの追加 （1075 ページ）

ルーティング	パラメータ	詳細情報

BGP	• [一般設定（General Settings）] > [BGP] で、BGP を有効にし、ローカルデバイスの AS 番号を指定して、ルータ ID を追加します（[手動（Manual）] を選択した場合）。
	• [BGP] で、IPv4/IPv6 を有効にして、[ネイバー（Neighbor）] タブでネイバーを設定します。
	  • [IPアドレス（IP Address）]：リモートピアの VTI インターフェイス IP アドレス。バックアップトンネルの場合は、リモートピアのバックアップ VTI インターフェイスの IP アドレスを使用したネイバーを追加します。
	  • [リモートAS（Remote AS）]：リモートピアの AS 番号。
	• [再配布（Redistribution）] タブをクリックし、[ソースプロトコル（Source Protocol）] を [接続済み（Connected）] として選択し、接続済みルートの再配布を有効にします。
		BGP の設定 （1224 ページ）

ルーティング	パラメータ	詳細情報
EIGRP	• EIGRP を有効にし、ローカルデバイスの AS 番号を指定して、EIGRP ルーティングプロセスに参加するネットワークまたはホストを選択します。 • [ネイバー（Neighbors）] タブをクリックし、EIGRP プロセスの静的ネイバーを定義します。 • VTI インターフェイスからサマリーアドレスをアドバタイズするには、[サマリーアドバイス（Summary Address）] タブで、[インターフェイス（Interface）] ドロップダウンから VTI インターフェイスを選択します。[ネットワーク（Network）] ドロップダウンから、要約するネットワークを選択します。 • [インターフェイス（Interface）] タブをクリックして、VTI インターフェイスのインターフェイス固有 EIGRP ルーティングプロパティを設定します。 インターフェイスで EIGRP スプリットホライズンを有効にするには、[スプリットホライズン（Split Horizon）] チェックボックスをオンにします。EIGRP hello パケットでデバイスによってアドバタイズされる [ホールド時間（Hold Time）] を設定することもできます。	EIGRP の設定 （1208 ページ）

ルーティング	パラメータ	詳細情報
OSPF	• [プロセス 1（Process 1）] チェックボックスをオンにして、OSPF ロールを選択します。 • [インターフェイス（Interface）] タブをクリックし、VTI インターフェイスを選択します。	OSPFv2 の設定（1176 ページ）
OSPFv3	• [プロセス1（Process 1）] チェックボックスと [プロセス 1の有効化（Enable Process 1）] チェックボックスをオンにして、OSPFv3 ロールを選択します。 • [インターフェイス（Interface）] タブをクリックし、VTI インターフェイスを選択します。	OSPFv3 の設定（1192 ページ）

AC ポリシールール

デバイスのアクセス コントロール ポリシーにアクセスコントロールルールを追加して、次の設定を使用して VTI トンネル間の暗号化されたトラフィックを許可します。

1. 許可アクションを使用してルールを作成します。
2. ローカルデバイスの VTI セキュリティゾーンを送信元ゾーンとして選択し、リモートピアの VTI セキュリティゾーンを宛先ゾーンとして選択します。
3. リモートピアの VTI セキュリティゾーンを送信元ゾーンとして選択し、ローカルデバイスの VTI セキュリティゾーンを宛先ゾーンとして選択します。

アクセス制御ルールの設定の詳細については、アクセスコントロールルールの作成および編集（1788 ページ）を参照してください。

Umbrella に SASE トンネルを展開する

Cisco Umbrella は、シスコのクラウドベース Secure Internet Gateway（SIG）プラットフォームです。インターネットベースの脅威に対する防御を複数のレベルで提供します。Cisco Umbrella は、セキュア Web ゲートウェイ、DNS レイヤセキュリティ、およびクラウド アクセス セキュリティ ブローカ（CASB）機能を統合して、システムを脅威から保護します。

Management Center を使用すると、Threat Defense デバイスから Cisco Umbrella への IPsec IKEv2 トンネルを展開できます。このトンネルは、インターネットに向かうすべてのトラフィックを、検査とフィルタリングのために Cisco Umbrella SIG に転送します。このソリューションは、セキュリティの中央管理を実現するため、ネットワーク管理者は各ブランチのセキュリティ設定を個別に管理する必要がありません。

Threat Defense デバイスから Cisco Umbrella トンネルを直接設定して展開するには、シンプルなウィザードを使用して SASE トポロジを作成します。SASE トポロジは、次のものをサポートする新しいタイプのサイト間 VPN トポロジです。

- 静的 VTI ベースのサイト間 VPN。
- Cisco Umbrella がハブであり、管理対象の Threat Defense デバイスがスポークである、ハブアンドスポークトポロジ。
- 事前共有キーベースの認証。
- HA モードで展開された Firewall Threat Defense。
- マルチインスタンス：マルチインスタンス展開では、1 つの Cisco Umbrella アカウントのみを統合できます。

高可用性のために、Threat Defense デバイスからの 2 つのトンネルを設定し、2 つ目のトンネルをバックアップトンネルとして使用することができます。必ず、トンネルごとに異なるローカルトンネル ID を設定してください。

設定を容易にするために、Management Center はデフォルトの IPsec および IKEv2 ポリシーを設定します。

デフォルトの IKEv2 ポリシー設定：

- 整合性アルゴリズム：NULL
- 暗号化アルゴリズム：AES-GCM-256
- PRF アルゴリズム：SHA-256
- DH グループ：19、20

デフォルトの IKEv2 IPSec ポリシー設定：

- ESP ハッシュ：SHA-256
- ESP 暗号化：AES-GCM-256

関連トピック

Cisco Umbrella に SASE トンネルを展開する方法 （1541 ページ）

Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項

SASE トポロジでは以下の内容がサポートされます。

- PSK ベースの認証のみ
- IKEv2
- ハイ アベイラビリティ

一般的な設定時の注意事項

- Firewall Management Center は、Cisco Umbrella で直接作成されたトンネルや、他のアプリケーションによって作成されたトンネルを検出しません。
- Firewall Management Center によって管理されるデバイスのみを SASE トポロジのエンドポイントとして追加できます。エクストラネットデバイスは追加できません。

  高可用性ペアの場合、HA ペアの名前がエンドポイントリストに表示されます。
- Firewall Management Center からトンネルを削除し、そのトンネルを Cisco Umbrella から削除できない場合は、Cisco Umbrella にログインして手動でトンネルを削除する必要があります。
- Cisco Umbrella への展開が進行中の場合、SASE トポロジは編集または削除できません。トンネルの展開ステータスは、以下で確認できます。
  - ウィザードの [Cisco Umbrella設定（Cisco Umbrella Configuration）] ダイアログボックス
  - [展開（Deployments）] タブと [タスク（Tasks）] タブの [通知（Notifications）] ページ
  - サイト間 VPN 監視ダッシュボード
- ウィザードで [Threat Defenseノードに構成を展開する（Deploy configuration on threat defense nodes）] チェックボックスをオンにすると、トンネルが Cisco Umbrella に展開された後にのみ、Cisco Umbrella SASE トポロジ構成が Firewall Threat Defense に展開されます。

  Firewall Management Center で Firewall Threat Defense に Cisco Umbrella 設定を展開するには、ローカルトンネル ID が必要です。Firewall Management Center で Cisco Umbrella にトンネルが展開された後にのみ、Cisco Umbrella によって完全なトンネル ID（*<prefix>@<umbrella generated ID>*-umbrella.com）が生成されます。
- Firewall Management Center では、バージョン 7.3 より前でエクストラネットハブとして作成された Cisco Umbrella データセンターのトポロジは SASE トポロジとして認識されません。バージョン 7.3 で新しい SASE トポロジを作成し、既存のトポロジを削除する必要があります。

- Firewall Threat Defense HA スイッチオーバー後、SASE トポロジはサイト間監視/VPN サマリーダッシュボードには表示されません。**vpn-sessiondb logoff index** コマンドを使用してトンネルを停止し、パケットトレーサを使用してトンネルを起動することを推奨します。

制限事項

SASE トポロジでは以下の内容はサポートされていません。

- クラスタ
- 証明書ベースの認証
- IKEv1

Cisco Umbrella に SASE トンネルを展開する方法

このセクションでは、Firewall Management Center を使用して Firewall Threat Defense デバイスから Cisco Umbrella に SASE トンネルを展開する手順について説明します。

手順	操作手順	詳細
1	注意事項と制限事項を確認します。	Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項 （1540 ページ）
2	前提条件を満たしていることを確認します。	Cisco Umbrella SASE トンネルを設定するための前提条件 （1541 ページ）
3	Cisco Umbrella 接続設定を行います。	• [Cisco Umbrellaの接続設定（Cisco Umbrella Connection Setting）] の設定 • Management Center の Umbrella パラメータと Cisco Umbrella の API キーのマッピング （1542 ページ）
4	Cisco Umbrella で SASE トンネルを設定します。	Cisco Umbrella 用の SASE トンネルの設定 （1544 ページ）
5	SASE トンネルのステータスを表示します。	SASE トンネルステータスの表示 （1546 ページ）

Cisco Umbrella SASE トンネルを設定するための前提条件

- Cisco Umbrella Secure Internet Gateway（SIG）Essentials サブスクリプションが必要です。
- Firewall Management Center から Cisco Umbrella にトンネルを展開するには、輸出規制機能を使用してスマート ライセンス アカウントを有効にする必要があります。このライセン

スが有効になっていない場合は、SASE トポロジのみを作成できます。Cisco Umbrella にはトンネルを展開できません。

- https://umbrella.cisco.com で Cisco Umbrella のアカウントを確立し、http://login.umbrella.com で Cisco Umbrella にログインして、Cisco Umbrella への接続を確立するために必要な情報を取得する必要があります。
- Cisco Umbrella を Firewall Management Center に登録し、Cisco Umbrella の接続設定で管理キーと管理シークレットを設定する必要があります。Management Center で、Cisco Umbrella クラウドからデータセンターの詳細を取得するには、管理キーと管理シークレットが必要です。Cisco Umbrella の接続設定で、[組織ID（Organization ID）]、[ネットワークデバイスキー（Network Device Key）]、[ネットワークデバイスシークレット（Network Device Secret）]、および[レガシーネットワークデバイストークン（Legacy Network Device Token）]も設定する必要があります。[

  詳細については、以下を参照してください。

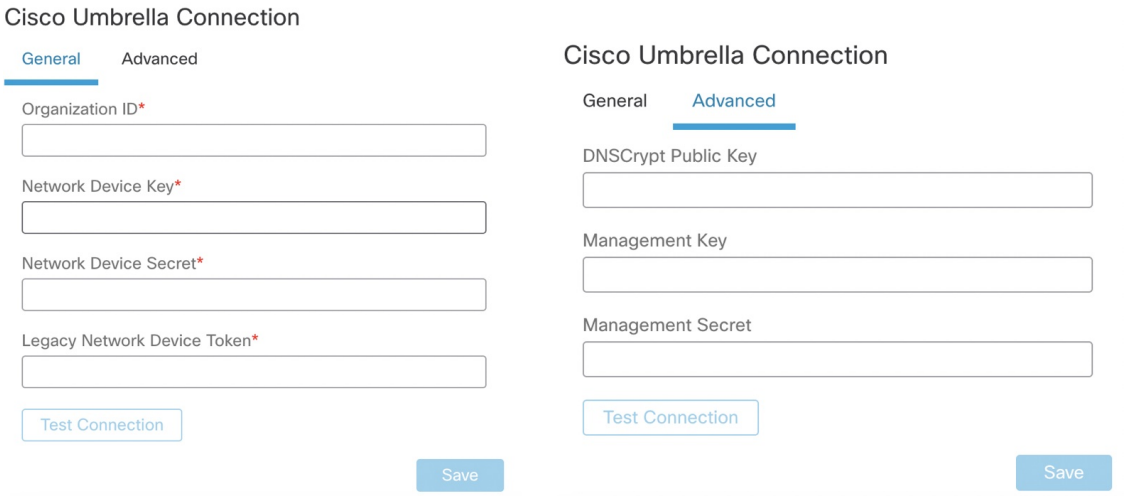
  - Cisco Umbrella の接続設定の設定
  - Management Center の Umbrella パラメータと Cisco Umbrella の API キーのマッピング（1542 ページ）
- Firewall Threat Defense から Cisco Umbrella データセンターに到達できることを確認します。
- Cisco Umbrella と Firewall Threat Defense バージョン 7.1.0 以降の間にのみトンネルを展開できます。

Management Center の Umbrella パラメータと Cisco Umbrella の API キーのマッピング

Firewall Management Center を使用して Cisco Umbrella を登録し、Firewall Management Center で Umbrella パラメータを設定するには、次の手順を実行する必要があります。

1. Cisco Umbrella にログインします。
2. [管理（Admin）]>[APIキー（API Keys）]>[レガシーキー（Legacy Keys）]を選択します。
3. 必要な API キーを生成してコピーします。
4. Firewall Management Center で API キーを使用して Cisco Umbrella 接続パラメータを設定します。

次の図は、Firewall Management Center の [Cisco Umbrella接続（Cisco Umbrella Connection）] で設定する必要があるパラメータを示しています。DNSCrypt 公開キーはオプションのパラメータです。



次の図は、Cisco Umbrella を Firewall Management Center に登録するために使用する必要がある Cisco Umbrella API キーを示しています。

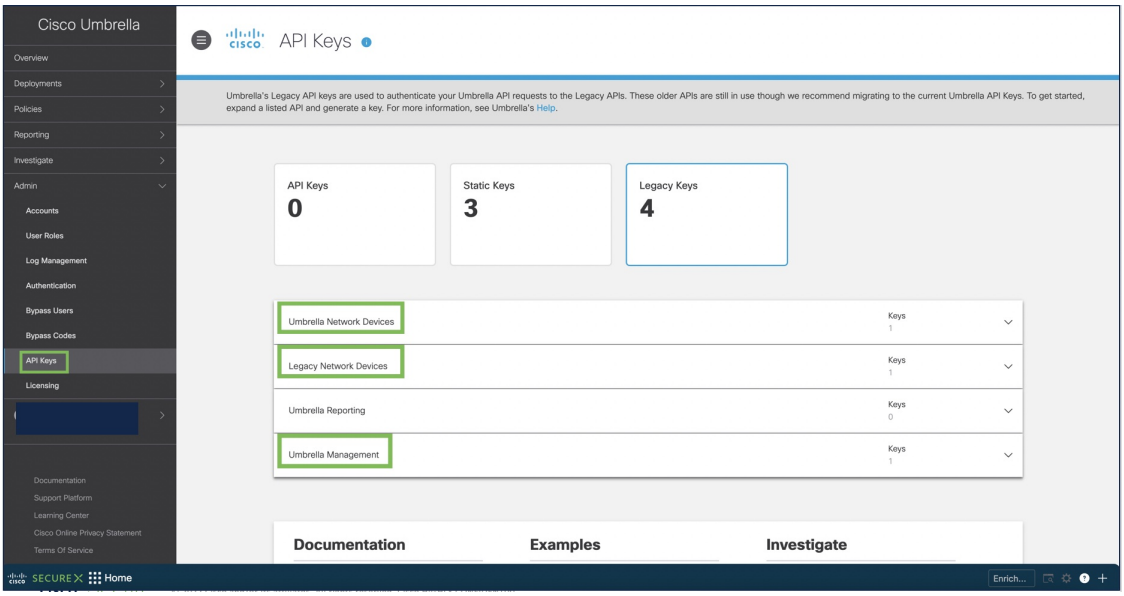


表 *72 : Firewall Management Center* の *Umbrella* パラメータと *Cisco Umbrella* の *API* キーのマッピング

Management Center のパラメータ	Cisco Umbrella の API キー
ネットワークデバイスキー ネットワーク デバイス シークレット	Umbrella ネットワークデバイス
レガシー ネットワーク デバイス トークン	レガシー ネットワーク デバイス
管理キー Management Secret	Umbrella 管理

Cisco Umbrella 用の SASE トンネルの設定

始める前に

Cisco Umbrella SASE トンネルを設定するための前提条件 （1541 ページ） および Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項 （1540 ページ） の前提条件とガイドラインを確認してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site to Site）]**を選択します。

ステップ 2 [+ SASEトポロジ（+ SASE Topology）] をクリックします。

ステップ 3 一意のトポロジ名を入力します。

ステップ 4 [事前共有キー（Pre-shared Key）]：このキーは、Umbrella PSK 要件に従って自動生成されます。単一トポロジの場合、事前共有キーはすべての Threat Defense スポークと Cisco Umbrella で共通です。

デバイスと Cisco Umbrella はこの秘密鍵を共有し、IKEv2 はそれを認証に使用します。このキーを構成する場合は、長さが 16 ～ 64 文字で、少なくとも 1 つの大文字、1 つの小文字、1 つの数字を使用する必要があります。特殊文字は使用できません。各トポロジには、一意の事前共有キーが必要です。トポロジに複数のトンネルがある場合、すべてのトンネルの事前共有キーは同じです。

ステップ 5 [Cisco Umbrellaデータセンター（Umbrella Data center）] ドロップダウンリストからデータセンターを選択します（Firewall Threat Defense からの Cisco Umbrella DC への到達可能性を確保するために、Firewall Threat Defense でルーティングを設定します）。

ステップ 6 [追加（Add）] をクリックして、Firewall Threat Defense ノードを追加します。

a) [デバイス（Device）] ドロップダウンリストから Firewall Threat Defense を選択します。

Firewall Management Center によって管理されているデバイスのみがリストに表示されます。高可用性ペアの場合、HA ペアの名前がエンドポイントリストに表示されます。

b) [VPNインターフェイス（VPN Interface）] ドロップダウンリストからスタティック VTI インターフェイスを選択します。

新しいスタティック VTI インターフェイスを作成するには、[追加（Add）] ＋をクリックします。[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスが表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] は static です。
- [名前（Name）] は *<tunnel_source interface logical name>*+ static_vti +*<tunnel ID>* です。たとえば、outside_static_vti_2 です。
- [トンネルID（Tunnel ID）] には、一意の ID が自動的に入力されます。

- [トンネル ソース インターフェイス（Tunnel Source Interface）] には、「outside」プレフィックスを持つインターフェイスが自動的に入力されます。
- IPsec トンネルモードは IPv4 です。
- IP アドレスは、169.254.xx/30 プライベート IP アドレスの範囲内です。

c) [ローカルトンネルID（Local Tunnel ID）] フィールドに、ローカルトンネル ID のプレフィックスを入力します。

プレフィックスは 8 文字以上で、100 文字を上限とします。管理センターで Cisco Umbrella にトンネルが展開された後、Cisco Umbrella によって完全なトンネル ID（*<prefix>@<umbrella generated ID>*-umbrella.com）が生成されます。次に、管理センターは完全なトンネル ID を取得して更新し、Threat Defense デバイスに展開します。各トンネルには、一意のローカルトンネル ID があります。

d) [保存（Save）] をクリックして、エンドポイントデバイスをトポロジに追加します。

SASE トポロジには複数のエンドポイントを追加できます。

ステップ 7 [次へ（Next）] をクリックして、Cisco Umbrella SASE トンネル設定の概要を確認します。

- [エンドポイント（Endpoints）] ペイン：設定されたエンドポイントの概要を表示します。
- [暗号化設定（Encryption Settings）] ペイン：トポロジのデフォルトの IKEv2 ポリシーと IKEv2 IPsec トランスフォームセットを表示します。

ステップ 8 [Threat Defense ノードに構成を展開する（Deploy configuration on threat defense nodes）] チェック ボックスをオンにすると、Threat Defense へのネットワークトンネルの展開がトリガーされます。この展開は、トンネルが Cisco Umbrella に展開された後に行われます。Threat Defense の展開には、ローカルトンネル ID が必要です。

ステップ 9 [保存（Save）] をクリックします。

このアクションは、次のように動作します。

1. トポロジを管理センターに保存します。
2. Cisco Umbrella へのネットワークトンネルの展開をトリガーします。
3. オプションが有効になっている場合、Threat Defense デバイスへのネットワークトンネルの展開をトリガーします。このアクションでは、デバイスでの最後の展開以降に更新されたすべての構成とポリシー（非 VPN ポリシーを含む）がコミットされて展開されます。
4. [Cisco Umbrella設定（Cisco Umbrella Configuration）] ウィンドウを開き、Cisco Umbrella でのトンネル展開のステータスを表示します。詳細については、SASE トンネルステータスの表示 （1546 ページ）を参照してください。

次のタスク

SASE トンネルを通過するように意図された対象のトラフィックについては、特定の一致基準を使用して PBR ポリシーを設定し、VTI インターフェイスを介してトラフィックを送信します。

SASE トポロジのエンドポイントごとに PBR ポリシーを設定してください。

SASE トンネルステータスの表示

手順

ステップ 1 [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。

ステップ 2 [+ SASEトポロジ（+ SASE Topology）] をクリックします。

ステップ 3 一意の **[トポロジ名（Topology Name）]**、**[事前共有キー（Pre-shared Key）]** を入力して、データセンターを選択し、デバイスを追加して、**[次へ（Next）]** をクリックします。

ステップ 4 Cisco Umbrella SASE トンネル設定の概要を表示し、[保存（Save）] をクリックします。[Cisco Umbrella設定（Cisco Umbrella Configuration）] ウィンドウが表示されます。

トンネル展開の名前、データセンター、データセンターの IP アドレス、開始時刻、終了時刻などのトポロジの詳細を確認できます。

Cisco Umbrella でトンネルの展開ステータスを確認できます。さまざまなトンネル展開ステータスは次のとおりです。

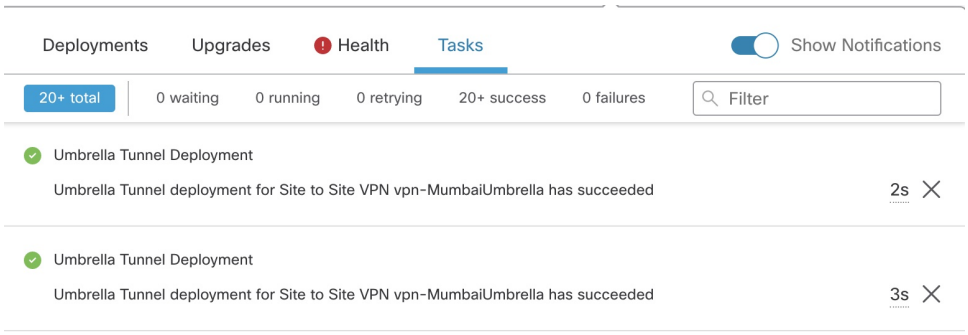
- 保留中：Management Center が構成を Cisco Umbrella にプッシュしていません。
- 成功：Management Center が Cisco Umbrella にトンネルを正常に設定しました。
- 進行中：Management Center が Cisco Umbrella にトンネルを展開しています。
- 失敗：Management Center が Cisco Umbrella でトンネルを設定できませんでした。

ステータスが保留中または失敗として表示される場合は、トランスクリプトを使用してトンネル作成のトラブルシューティングを行います。**[トランスクリプト（ transcript）]** ボタンをクリックして、API、リクエスト ペイロード、Cisco Umbrella から受信したレスポンスなど、トランスクリプトの詳細を表示します。

ステップ 5 [Cisco Umbrellaダッシュボード（Umbrella Dashboard）] をクリックして、Cisco Umbrella のネットワークトンネルを表示します。

ステップ 6 次の場所で Cisco Umbrella トンネルの展開ステータスを確認します。

- [展開（Deployments）] タブと [タスク（Tasks）] タブの [通知（Notifications）] ページ。



- **サイト間** VPN 監視ダッシュボード（**[概要（Overview）]** > **[ダッシュボード（Dashboards）]** > **[サイト間 VPN（Site to Site VPN）]**）。

  ダッシュボードには、Cisco Umbrella SASE トポロジを含むサイト間 VPN トポロジの概要が表示されます。ピアデバイス間のトンネルと各トンネルのステータスを確認できます。CLI コマンドとパケットトレーサを使用して、トンネルの展開に関する問題をトラブルシューティングすることもできます。

サイト間 VPN のモニタリング

Secure Firewall Management Center は、サイト間 VPN トンネルのステータスを判断するために、サイト間 VPN トンネル（SASE トポロジトンネルを含む）のスナップショットを提供します。ピアデバイス間のトンネルのリストと、各トンネルのステータス（[アクティブ（Active）]、[非アクティブ（Inactive）]、または [アクティブデータなし（No Active Data）]）を表示できます。トポロジ、デバイス、およびステータスでテーブル内のデータをフィルタ処理できます。監視ダッシュボードのテーブルにはライブデータが表示され、指定した間隔でデータが更新されるように設定できます。このテーブルは、暗号マップベースの VPN のピアツーピア、ハブアンドスポーク、およびフルメッシュトポロジを示しています。トンネル情報には、ルートベースの VPN または仮想トンネルインターフェイス（VTI）のデータも含まれます。

このデータを使用して、次のことができます。

- 問題のある VPN トンネルを特定し、トラブルシューティングを行います。
- サイト間 VPN ピアデバイス間の接続を確認します。
- VPN トンネルの正常性を監視して、サイト間の中断のない VPN 接続を提供します。

暗号マップベースのサイト間 VPN の設定については、ポリシーベースのサイト間 VPN の設定（1491 ページ）を参照してください。

VTI の詳細については、仮想トンネルインターフェイスについて（1507 ページ）を参照してください。

Firewall Threat Defense の VPN モニタリングおよびトラブルシューティングについては、VPN のモニタリングとトラブルシューティング（1699 ページ）を参照してください。

注意事項と制約事項

- テーブルには、展開されているサイト間（SASE トポロジを含む）VPN のリストが表示されます。作成されていても展開されていないトンネルは表示されません。
- テーブルには、ポリシーベースの VPN およびバックアップ VTI のバックアップトンネルに関する情報は表示されません。
- クラスタ展開の場合、テーブルには、ディレクタの変更はリアルタイムデータでは表示されません。VPN が展開されたときに存在していたディレクタ情報のみが表示されます。ディレクタ変更は、変更後にトンネル AM が再展開された後にのみテーブルに反映されます。

サイト間 VPN 監視ダッシュボード

[概要（Overview）] > **[ダッシュボード（Dashboards）]** > **[サイト間VPN（Site to Site VPN）]** を選択してサイト間監視ダッシュボードを開きます。

サイト間 VPN 監視ダッシュボードには、サイト間 VPN トンネルの次のウィジェットが表示されます。

- **トンネルステータス（Tunnel Status）**：Firewall Management Centerを使用して設定されたサイト間 VPN（Umbrella 用の SASE トンネルを含む）のトンネルステータスのリストが示されるテーブル。
- **トンネル要約（Tunnel Summary）**：トンネルステータスが集計されたドーナツグラフ。
- **トポロジ（Topology）**：トポロジ別に要約されたトンネルステータス。

VPN トンネルのステータス

サイト間監視ダッシュボードには、次の状態にある VPN トンネルのリストが表示されます。

- **非アクティブ（Inactive）**：すべての IPSec トンネルがダウンしている場合、ポリシーベース（暗号マップベース）の VPN トンネルは非アクティブです。トンネルで設定または接続に関する問題が発生した場合、VTI および SASE トポロジ VPN トンネルはダウンします。
- **アクティブ（Active）**：Firewall Management Center では、ポリシーベースのサイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよび IPsec プロポーザルに基づいて設定されます。展開後に Firewall Management Center がトンネルを通過する対象トラフィックを識別すると、ポリシーベースの VPN トンネルはアクティブ状態になります。IKE トンネルは、少なくとも 1 つの IPsec トンネルが稼働状態になった場合にのみ稼働状態になります。

  ルートベースの VPN（VTI）および SASE トポロジの VPN トンネルでは、対象トラフィックがアクティブ状態である必要はありません。それらは、エラーなしで設定および展開されると、アクティブ状態になります。
- **アクティブデータなし（No Active Data）**：ポリシーベースのトンネルおよび SASE トポロジ VPN トンネルは、トンネルを通過するトラフィックフローが初めて発生するまで、

アクティブデータなし状態のままになります。アクティブデータなし状態では、展開済みでエラーのあるポリシーベースおよびルートベース VPN のリストも表示されます。

Firewall Management Centerでのトンネルステータスに関する重要な注意事項

- Firewall Management Centerでの VPN ステータスはイベントベースです。Firewall Management Centerはステータスの更新を開始しません。そのため、ダッシュボードとFirewall Threat Defenseでトンネルステータスが一致しない場合があります。正しいステータスは、[トンネルステータス（Tunnel Status）] ウィジェットの [CLIの詳細（CLI Details）] タブで表示できます。
- Firewall Threat Defenseがセカンダリ Firewall Threat Defenseにスイッチオーバーすると、Firewall Management CenterとFirewall Threat Defenseで VPN トンネルのステータスに一致が発生します。デバイスがプライマリデバイスに戻ると、正しいトンネルステータスが表示されます。
- Firewall Management Centerは、デバイスの再起動後、7.3 より前のFirewall Threat Defenseデバイスのトンネルステータスを更新しません。**vpn-sessiondb logoff index** コマンドを使用してトンネルを停止し、パケットトレーサを使用してトンネルを起動することを推奨します。

Tunnel Status

このテーブルには、Firewall Management Centerを使用して設定されたサイト間 VPN（SASE トポロジ VPN を含む）のリストが示されます。トポロジにマウスのカーソルを合わせて [表示（View）]（👁） をクリックすると、トポロジに関する次の詳細情報が表示されます。

- [全般（General）]：IP アドレスやインターフェイス名など、ノードに関する詳細情報が表示されます。
- [CLIの詳細（CLI Details）]：次のコマンドの CLI 出力が表示されます。
  - **show crypto ipsec sa peer** <*node A/B_ip_address*>：ノード A とノード B の間に構築された IPSec SA が表示されます。
  - **show vpn-sessiondb l2l filter ipaddress** <*node A/B_ip_address*>：VPN セッションに関する情報が表示されます。

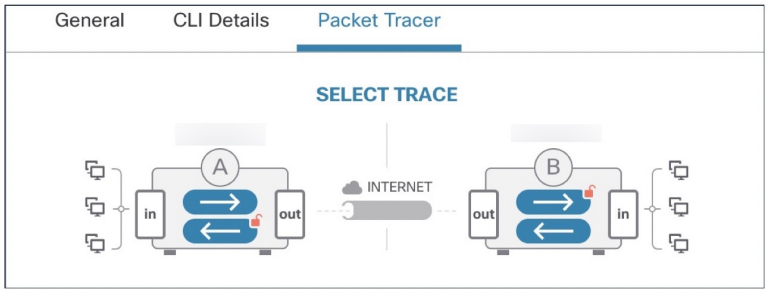
  エクストラネットデバイスの場合、コマンド出力は表示されません。
- [パケットトレーサ（Packet Tracer）]：パケットトレーサを使用して、脅威防御 VPN トンネルのトラブルシューティングを行います。

Packet Tracer

パケットトレーサを使用すると、2 つの Threat Defense デバイス間の VPN トンネルのトラブルシューティングを行うことができます。デバイス A とデバイス B の間の VPN 接続が稼働状態かどうかをチェックできます。このツールは、パケットをデバイスに挿入し、入力ポートから出力ポートへのパケットフローを追跡できます。このツールは、保護されるネットワークとと

もにデバイスの入力インターフェイスを設定した後、トラフィックをシミュレートします。パケットトレーサでは、フローおよびルーティングルックアップ、ACL、プロトコルインスペクション、NAT、QoS などのモジュールに照らしてパケットが評価されます。

図 *305 : Packet Tracer*



このツールは、デバイスごとに、暗号化トレースと復号トレースを実行します（パケットは復号された VPN トラフィックとして扱われます）。デバイスの入力ポートと出力ポートの間で4つの異なるトレースを実行できます。個別の暗号化オプションおよび復号オプションをクリックして、トレースを有効または無効にします。

トレースを実行すると、ツールは、次の順序で、トレースを順番に実行します。

1. A の暗号化トレース。
2. B の復号トレース。
3. B の暗号化トレース。
4. A の復号トレース。

トレースが完了したら、各モジュールの結果を含むトレースの出力を表示できます。

（注） ルートベース（VTI ベース）の VPN の復号トレースは実行できません。

パケットトレーサを実行するには、次の手順に従います。

1. [詳細設定を表示する（See Detailed Config）] をクリックして、VPN インターフェイス名、VPN インターフェイスの IP アドレス、VTI インターフェイス名、および VTI インターフェイスの IP アドレスを表示します。
2. （任意）[プロトコル（Protocol）] ドロップダウンリストからプロトコルを選択します。[ICMP/8/0]、[TCP]、または [UDP] を選択できます。

   [ICMP/8/0] がデフォルトのオプションです。[ICMP/8/0] を選択する場合は、8 がエコー要求の ICMP タイプを示し、0 が ICMP コードを示します。[TCP] または [UDP] を選択する場合は、[宛先ポート（Destination Port）] ドロップダウンリストから宛先ポートを選択します。指定できる範囲は 0 ～ 65535 です。

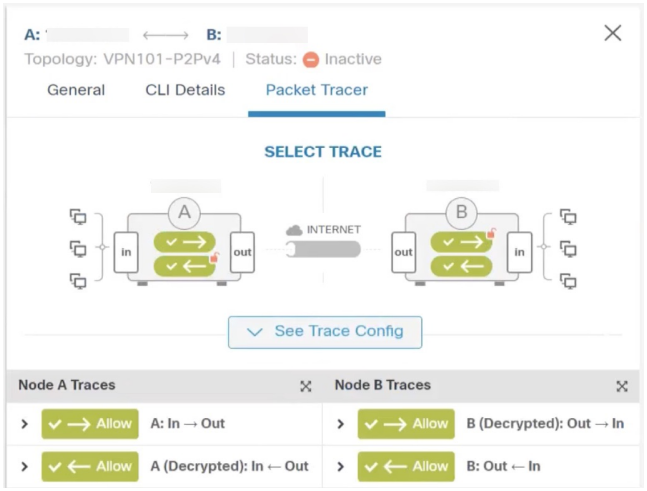
3. [入力インターフェイス（Ingress Interface）] ドロップダウンリストから、パケットをトレースする両方のデバイスの入力インターフェイスを選択します。パケットトレーサは、ループバック インターフェイスをサポートしていません。

4. [保護されたネットワークのIPアドレス（Protected Network IP Address）] フィールドに、入力インターフェイスと同じサブネットからの IP アドレスを入力します。

5. [今すぐトレース（Trace Now）] をクリックします。

   トレースを開始すると、モジュールごとにトレースが成功したかどうかを表示できます。トンネルがダウンしている場合、パスは赤色で表示されます。トンネルが稼働状態の場合、パスは緑色で表示されます。トンネルがダウンしている場合は、[再トレース（Re-trace）] をクリックしてツールを再実行します。暗号マップベースの VPN の場合、対象トラフィックがなく、トンネルが非アクティブのときは、最初のトレースが赤色になる可能性があります。[再トレース（Re-trace）] をクリックしてトレースを再実行してください。

図 *306* : トレースが成功した後のパケットトレーサ



エクストラネットノード：1つのノードをエクストラネットとして使用してVPNトンネルのパケットトレースを開始できます。エクストラネットノードの場合、入力インターフェイスを選択することはできません。パケットトレースの残りの手順は同じです。エクストラネット側でトレースを実行することはできません。

たとえば、ノード A が管理された脅威防御であり、ノード B がエクストラネットである場合は、次の手順に従います。

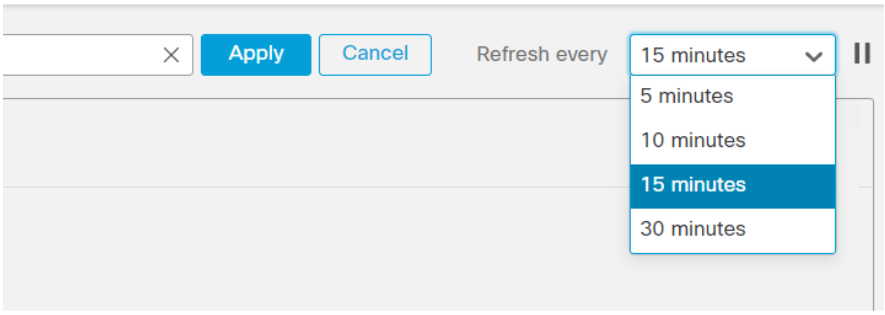
- ノード A の入力インターフェースを設定します。
- ノード A とノード B の保護されたネットワークを設定します。
- [今すぐトレース（Trace Now）] をクリックします。トレースは、ノードBではなく、ノードAについて表示されます。

自動データ更新

テーブル内のサイト間 VPN データは定期的に更新されます。VPN モニタリングデータの更新間隔を特定の間隔で設定するか、自動データ更新をオフにすることができます。

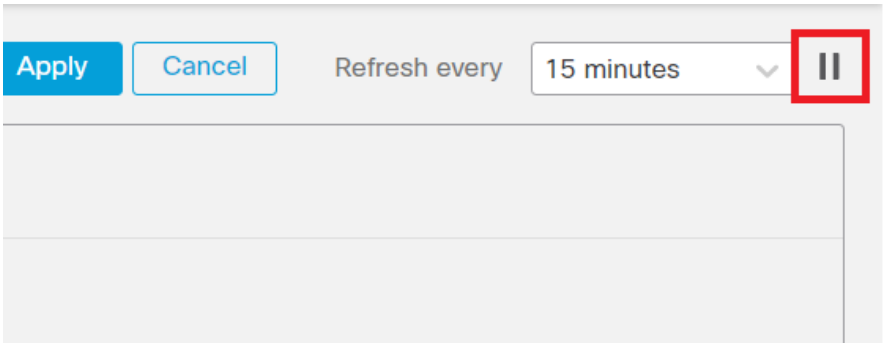
更新間隔のドロップダウンをクリックして、テーブル内のデータの更新に使用する間隔を選択します。

図 *307* : トンネルデータの更新



[一時停止（Pause）]をクリックすると、必要なだけ自動データ更新を停止できます。同じボタンをクリックすると、トンネルデータの更新を再開できます。

図 *308* : 定期的なデータ更新の一時停止



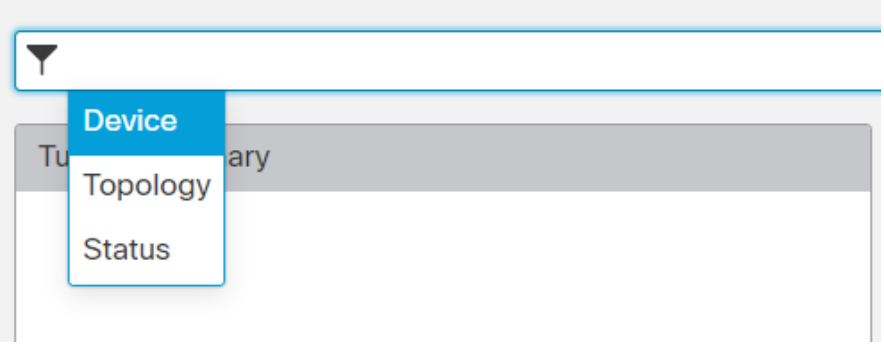
サイト間 VPN モニタリングデータのフィルタ処理およびソート

VPNモニタリングテーブルのデータを、トポロジ、デバイス、およびステータスでフィルタ処理して表示できます。

たとえば、特定のトポロジでダウン状態にあるトンネルを表示できます。

フィルタ処理ボックス内をクリックしてフィルタ条件を選択し、フィルタ処理する値を指定します。

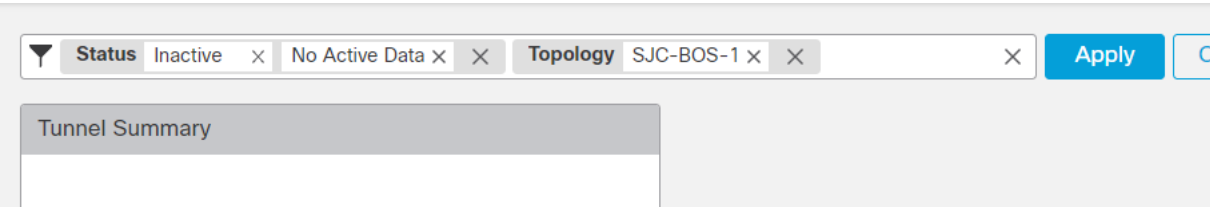
図 *309* : トンネルデータのフィルタ処理



複数のフィルタ処理基準により、要件に基づいてデータを表示できます。

たとえば、稼働状態とダウン状態のトンネルのみを表示し、不明状態のトンネルを無視するように選択できます。

図 *310* : 例 : トンネルデータのフィルタ処理



データのソート：列ごとにデータをソートするには、列の見出しをクリックします。

関連トピック

サイト間 VPN について （1485 ページ）
仮想トンネル インターフェイスについて （1507 ページ）

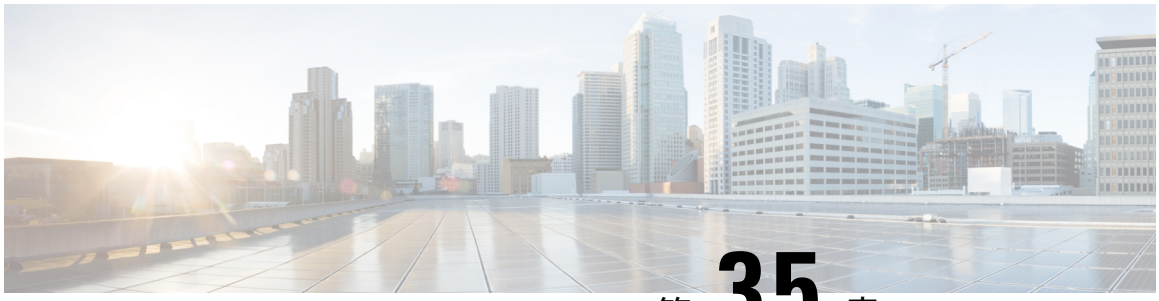
サイト間 VPN の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Umbrella SASE トポロジ	7.3	任意（Any）	Umbrella SASE トポロジを設定し、Threat Defense デバイスと Umbrella の間に IPsec IKEv2 トンネルを展開できます。このトンネルは、インターネットに向かうすべてのトラフィックを、検査とフィルタリングのために Umbrella Secure Internet Gateway（SIG）に転送します。
ダイナミック仮想トンネルインターフェイスのサポート	7.3	任意（Any）	ダイナミック VTI を作成し、それを使用して、ハブアンドスポークトポロジでルートベースのサイト間 VPN を設定できます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
VTI の EIGRP IPv4 サポート	7.3	任意（Any）	スタティックおよびダイナミック VTI インターフェイスは、EIGRP IPv4 ルーティングプロトコルをサポートしています。
VTI の OSPFv2/v3 IPv4/v6 サポート	7.3	任意（Any）	スタティックおよびダイナミック VTI インターフェイスは、OSPFv2/v3 IPv4/v6 ルーティングプロトコルをサポートしています。
サイト間 VPN 監視ダッシュボードのパケットトレーサ	7.3	任意（Any）	サイト間 VPN モニタリングダッシュボードのパケットトレーサツールを使用して、Threat Defense VPN トンネルのトラブルシューティングを行います。 新規/変更された画面： **[概要（Overview）] > [ダッシュボード（Dashboards）] > [拠点間 VPN（Site to Site VPN）]**
リモートアクセス VPN ダッシュボード	7.3	任意（Any）	リモートアクセス VPN ダッシュボードを使用して、デバイス上のアクティブなリモートアクセス VPN セッションからのリアルタイムデータをモニターします。 新規/変更された画面： **[概要（Overview）] > [ダッシュボード（Dashboards）] > [拠点間VPN（Site to Site VPN）][リモート アクセス VPN（Remote Access VPN）]**
IPSec フローのオフロード	7.2	任意（Any）	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
サイト間 VPN フィルタ	7.1	任意（Any）	アクセス コントロール ポリシーを使用してサイト間 VPN トラフィックを制御できます。
ローカルトンネル ID のサポート	7.1	任意（Any）	サイト間 VPN の各エンドポイントについて、ピアと共有する一意のトンネル ID を設定できます。
複数の IKE ポリシーのサポート	7.1	任意（Any）	エンドポイントごとに複数の IKEv1 および IKEv2 ポリシーオブジェクトを追加できます。
サイト間 VPN 監視ダッシュボード	7.1	任意（Any）	サイト間 VPN 監視ダッシュボードを使用して、サイト間 VPN トンネルのステータスを表示および監視します。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ルートベースのサイト間 VPN 向けバックアップ用仮想トンネルインターフェイス（VTI）。	7.0	任意（Any）	仮想トンネルインターフェイスを使用するサイト間 VPN を設定する場合、トンネルのバックアップ VTI を選択できます。バックアップ VTI を指定すると復元力が得られるため、プライマリ接続がダウンした場合でもバックアップ接続は継続して機能します。たとえば、プライマリ VTI をあるサービスプロバイダーのエンドポイントに接続し、バックアップ VTI を別のサービスプロバイダーのエンドポイントに接続できます。 ポイントツーポイント接続の VPN タイプとして [ルートベース（Route-Based）] を選択することで、サイト間 VPN ウィザードにバックアップ VTI を追加できます。
VTI の数をインターフェイスあたり 100 からデバイスあたり 1024 に強化	7.0	任意（Any）	VTI の最大数のサポートが、物理インターフェイスあたり 100 からデバイスあたり 1024 VTI に拡張されました。
IPv6 のサポート	7.0	任意（Any）	IPv6 アドレスが指定された VTI を設定できます。トンネルの送信元および接続先としてサポートされるのは、静的 IPv6 アドレスだけですが、VTI では IPv6 BGP はサポートされていません。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
弱い暗号の削除と廃止	6.7	いずれか	安全性の低い暗号のサポートが削除されました。VPN が正しく機能するように、Firewall Threat Defense 6.70 にアップグレードする前に、サポートされる DH および暗号化アルゴリズムに VPN 設定を更新することを推奨します。 Firewall Threat Defense 6.70 でサポートされているものと一致するように IKE プロポーザルと IPSec ポリシーを更新してから、設定の変更を展開します。 次の安全性の低い暗号は、Firewall Threat Defense 6.70 以降では削除または廃止されました。 • **Diffie-Hellman グループ 5** は IKEv1 では廃止され、IKEv2 では削除されました • Diffie-Hellman グループ 2 および 24 は削除されました。 • **暗号化アルゴリズム**：3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256 は削除されました。 （注） **DES** は、評価モードで、または強力な暗号化の輸出規制を満たさないユーザーのためにサポートされます。 **NULL** は IKEv2 ポリシーでは削除されますが、IKEv1 と IKEv2 両方の IPsec トランスフォームセットでサポートされます。
動的 RRI サポート	6.7	いずれか	ダイナミック リバース ルート インジェクションは、IKEv2 ベースの静的暗号マップでサポートされます。
サイト間 VPN のバックアップピア	6.6	任意（Any）	Firewall Management Center を使用して、サイト間 VPN 接続にバックアップピアを追加できます。たとえば、2 つの ISP がある場合は、最初の ISP への接続が使用できなくなった場合に、バックアップ ISP にフェールオーバーするように VPN 接続を設定できます。 新規/変更されたページ： **[デバイス（Devices）] > [VPN] > [サイト間（Site to Site）]**。ポイントツーポイントまたはハブアンドスポークの FTD VPN トポロジを追加または編集してエンドポイントを追加する場合、[IPアドレス（IP Address）] フィールドでカンマ区切りのバックアップピアがサポートされます。



第 35 章

リモート アクセス VPN

リモートアクセス仮想プライベートネットワーク（VPN）では、インターネットに接続されたコンピュータやその他のサポート対象デバイスを使用して、各ユーザーが離れた場所からネットワークに接続できます。これにより、モバイル ワーカーが各自のホーム ネットワークや公共の Wi-Fi ネットワークなどから接続できるようになります。

ここでは、ネットワークのリモート アクセス VPN を設定する方法について説明します。

- リモート アクセス VPN の概要 （1557 ページ）
- リモートアクセス VPN のライセンス要件 （1565 ページ）
- リモートアクセス VPN の要件と前提条件 （1565 ページ）
- リモート アクセス VPN のガイドラインと制限事項 （1566 ページ）
- 新規リモート アクセス VPN 接続の設定 （1570 ページ）
- 既存のリモートアクセス VPN ポリシーのコピーの作成 （1583 ページ）
- リモートアクセス VPN ポリシーのターゲットデバイスの設定 （1583 ページ）
- ローカルレルムとリモートアクセス VPN ポリシーの関連付け （1584 ページ）
- その他のリモートアクセス VPN の設定 （1585 ページ）
- リモート アクセス VPN の AAA の設定のカスタマイズ （1637 ページ）
- 拡張 セキュアクライアント 設定 （1662 ページ）
- リモート アクセス VPN の例 （1673 ページ）
- リモートアクセス VPN の履歴 （1679 ページ）

リモート アクセス VPN の概要

Secure Firewall Threat Defense は、リモート アクセス SSL と IPsec-IKEv2 VPN をサポートするセキュアなゲートウェイ機能を提供します。完全なトンネル クライアントである Secure Client は、セキュリティ ゲートウェイへのセキュアな SSL および IPsec-IKEv2 接続をリモート ユーザーに提供します。クライアントが Firewall Threat Defense と SSL VPN 接続をネゴシエートする際、Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）を使用して接続します。

Secure Client はエンドポイントデバイスでサポートされている唯一のクライアントで、Firewall Threat Defense デバイスへのリモート VPN 接続が可能です。このクライアントにより、ネット

ワーク管理者がリモートコンピュータにクライアントをインストールして設定しなくても、リモートユーザーはSSLまたはIPsec-IKEv2 VPNクライアントを活用できます。Windows、Mac、およびLinux用のSecure Clientは、接続時にセキュアゲートウェイから展開されます。Apple iOSデバイスおよびAndroidデバイス用のSecure Clientアプリは、当該プラットフォームのアプリ ストアからインストールされます。

[リモートアクセスVPNポリシー（Remote Access VPN Policy）] ウィザードを使用して、SSLとIPsec-IKEv2リモートアクセスVPNを基本機能も含めて設定します。次に、必要に応じてポリシー構成を強化し、Firewall Threat Defenseセキュア ゲートウェイ デバイスに展開します。

リモート アクセス VPN の機能

次の表では、Secure Firewall Threat Defenseのリモートアクセス VPNの機能について説明します。

表 *73 :* リモートアクセス *VPN* の機能

	説明
Secure Firewall Threat Defense リモートアクセス VPN の機能	• Secure Clientを使用したSSLおよびIPsec-IKEv2リモートアクセス。 • Secure Firewall Management Center IPv4トンネル上のIPv6など、すべての組み合わせがサポートされています。 • Firewall Management Center と Firewall Device Managerの両方での構成サポート。デバイス固有のオーバーライド。 • Secure Firewall Management CenterおよびFirewall Threat Defense両方のHA環境をサポート。 • 複数のインターフェイスと複数のAAAサーバーのサポート。 • Rapid Threat Containmentでは、RADIUS CoAまたはRADIUSダイナミック認証の使用がサポートされています。 • Cisco Secure Clientバージョン4.7以降でのDTLS v1.2プロトコルのサポート。 • セキュアクライアントモジュールは、リモートアクセスVPN接続用の追加のセキュリティサービスをサポートしています。 • VPNロードバランシング。

	説明
AAA 機能	• 自己署名または CA 署名のアイデンティティ証明書を使用したサーバー認証。 • RADIUS サーバー、LDAP、または AD を使用する AAA ユーザー名とパスワードベースのリモート認証。 • RADIUS グループとユーザー承認属性、および RADIUS アカウンティング。 • 二重認証では、セカンダリ認証での他の AAA サーバーの使用がサポートされています。 • VPN ID を使用した NGFW アクセス制御の統合。 • Secure Firewall Management Center の Web インターフェイスを使用した LDAP または AD 認可属性。 • SAML 2.0 を使用したシングルサインオンのサポート。 • 同じエンティティ ID に対して複数のアプリケーションを持つことができるが、ID 証明書は一意である、Microsoft Azure での複数の ID プロバイダートラストポイントのサポート。
VPN トンネリング機能	• アドレス割り当て。 • スプリットトンネリング。 • スプリット DNS。 • クライアント ファイアウォール ACL。 • 最大接続およびアイドル時間のセッションタイムアウト。

	説明
リモートアクセス VPN モニタリングの機能	• 期間、クライアント アプリケーションなどのさまざまな特性によって VPN ユーザーを表示する新しい VPN ダッシュボード ウィジェット。 • ユーザー名や OS プラットフォームなどの認証情報を含むリモートアクセス VPN イベント。 • Firewall Threat Defense 統合 CLI により利用可能なトンネル統計。

Secure Client のコンポーネント

Secure Client導入

リモートアクセス VPN ポリシーに、接続エンドポイントに配布するための Secure Client イメージ および Secure Client プロファイル を含めることができます。または、クライアント ソフトウェアを他の方法で配布できます。の「*Deploy AnyConnect*」の章Cisco Secure Client（AnyConnect を含む）管理者ガイド、リリース 5 [英語] の「*Deploy Cisco Secure Client*」の章を参照してください。

事前にクライアントがインストールされていない場合、リモート ユーザーは、SSL または IPsec-IKEv2 VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。セキュリティ アプライアンスが http:// 要求を https:// にリダイレクトするように設定されている場合を除いて、リモート ユーザーは https://*address* の形式で URL を入力する必要があります。URL を入力すると、ブラウザがそのインターフェイスに接続して、ログイン画面が表示されます。

ユーザー ログイン後、セキュア ゲートウェイは VPN クライアントを必要としているとユーザーを識別すると、リモート コンピュータのオペレーティング システムに一致するクライアントをダウンロードします。ダウンロード後、クライアントは自動的にインストールと設定を行い、セキュアな接続を確立します。接続の終了時には、（セキュリティ アプライアンスの設定に応じて）そのまま残るか、または自動的にアンインストールを実行します。以前にインストールされたクライアントの場合、ログイン後、Firewall Threat Defense セキュリティ ゲートウェイはクライアントのバージョンを検査し、必要に応じてアップグレードします。

Secure Client 操作

クライアントがセキュリティ アプライアンスとの接続をネゴシエートする場合、クライアントは、Transport Layer Security（TLS）、および任意で Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

IPsec-IKEv2 VPN クライアントがセキュア ゲートウェイへの接続を開始すると、インターネットキーエクスチェンジ（IKE）によるデバイスの認証と、続く IKE 拡張認証（Xauth）によるユーザ認証からなるネゴシエーションが行われます。グループ プロファイルが VPN クライアントにプッシュされ、IPsec セキュリティ アソシエーション（SA）が作成されて VPN が完了します。

Secure Client プロファイル およびエディタ

Secure Client プロファイル は、構成パラメータのグループで、動作や表示の設定に VPN クライアントで使用される XML ファイル内に保存されます。これらのパラメータ（XML タグ）には、ホストコンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

Secure Client プロファイルエディタ を使用してプロファイルを設定できます。このエディタは、Secure Client ソフトウェアパッケージの一部として利用できる便利な GUI ベースの設定ツールです。これは、Firewall Management Center の外部から実行する独立したプログラムです。

リモート アクセス VPN 認証

リモート アクセス VPN サーバー認証

Secure Firewall Threat Defense セキュア ゲートウェイは、VPN クライアントのエンドポイントに対して自身を特定し、認証するために必ず証明書を使用します。

リモートアクセス VPN ポリシーウィザードを使用しているときに、選択した証明書を対象の Firewall Threat Defense デバイスに登録できます。ウィザードの [アクセスおよび証明書（Access & Certificate）] フェーズで、[選択した証明書オブジェクトをターゲットデバイスに登録する（Enroll the selected certificate object on the target devices）] オプションを選択します。証明書の登録は、指定したデバイス上で自動的に開始されます。リモートアクセス VPN ポリシーの構成が完了すると、デバイス証明書のホームページで登録した証明書のステータスを確認できます。ステータスは、証明書の登録が成功したかどうかを明確に示します。これで、リモートアクセス VPN ポリシーの構成が完了し、展開の準備ができました。

PKI の登録とも呼ばれる、セキュア ゲートウェイの証明書の取得については、証明書 （1455 ページ）で説明しています。この章には、ゲートウェイ証明書の設定、登録、および管理の詳細な説明が含まれています。

リモート アクセス VPN のクライアント AAA

SSL と IPsec-IKEv2 の両方について、リモート ユーザー認証はユーザー名とパスワードのみ、証明書のみ、あるいはこの両方を使用して実行されます。

（注） 展開でクライアント証明書を使用している場合は、Secure Firewall Threat Defense または Secure Firewall Management Center に関係なく、クライアントのプラットフォームにこれらの証明書を追加する必要があります。クライアントに証明書を入力するために、SCEP や CA サービスなどの機能は提供されません。

AAA サーバーでは、セキュア ゲートウェイとして機能する管理対象デバイスが、ユーザーの身元（認証）、ユーザーが許可されていること（認可）、およびユーザーが行ったこと（アカウンティング）を確認できます。AAA サーバーの例としては、RADIUS、LDAP/AD、TACACS+、Kerberos などがあります。Firewall Threat Defense デバイス上のリモート アクセス VPN では、AD、LDAP、および RADIUS AAA サーバーが認証のためにサポートされています。

リモートアクセス VPN の認可の詳細については、「権限および属性のポリシー実施の概要」の項を参照してください。

リモートアクセス VPN ポリシーを追加または編集する前に、指定するレルムおよび RADIUS サーバーグループを設定する必要があります。詳細については、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）およびRADIUS サーバーグループの追加 （1314 ページ）を参照してください。

DNS が設定されていないと、デバイスは AAA サーバー名、名前付き URL、および FQDN またはホスト名を持つ CA サーバーを解決できません。解決できるのは IP アドレスのみです。

リモート ユーザーから提供されるログイン情報は、LDAP または AD レルムまたは RADIUS サーバー グループによって検証されます。これらのエンティティは、Secure Firewall Threat Defense セキュア ゲートウェイと統合されます。

（注） ユーザーが認証ソースとして Active Directory を使用してリモートアクセス VPN で認証を受ける場合、ユーザーは自分のユーザー名を使用してログインする必要があります。`domain\username` または `username@domain` 形式は失敗します。（Active Directory はこのユーザー名をログオン名、または場合によっては `sAMAccountName` と呼んでいます）。詳細については、MSDN でユーザーの命名属性 [英語] を参照してください。

認証に RADIUS を使用する場合、ユーザーは前述のどの形式でもログインできます。

VPN 接続経由で認証されると、リモート ユーザーには *VPN ID* が適用されます。この VPN ID は、そのリモート ユーザーに属しているネットワーク トラフィックを認識し、フィルタリングするために Secure Firewall Threat Defense のセキュア ゲートウェイ上のアイデンティティ ポリシーで使用されます。

アイデンティティ ポリシーはアクセス コントロール ポリシーと関連付けられ、これにより、誰がネットワーク リソースにアクセスできるかが決まります。リモート ユーザーがブロックされるか、またはネットワーク リソースにアクセスできるかはこのようにして決まります。

詳細については、アイデンティティ ポリシーについて （2553 ページ）およびアクセス制御ポリシー （1745 ページ）のセクションを参照してください。

関連トピック

リモートアクセス VPN の AAA 設定 （1588 ページ）

権限および属性のポリシー実施の概要

Secure Firewall Threat Defense デバイスは、外部認証サーバーおよび/または承認 AAA サーバー（RADIUS）から、あるいは Firewall Threat Defense デバイス上のグループ ポリシーから、ユーザー承認属性（ユーザーの権利または権限とも呼ばれる）を VPN 接続に適用することをサポートしています。Firewall Threat Defense デバイスがグループ ポリシーに設定されている属性と競合する外部 AAA サーバーから属性を受信した場合は、AAA サーバーからの属性が常に優先されます。

Firewall Threat Defense デバイスは次の順序で属性を適用します。

1. **外部 AAA サーバー上のユーザー属性**：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。
2. **Firepower Threat Defense デバイス上で設定されているグループ ポリシー**：RADIUS サーバーからユーザーの RADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場合は、Firewall Threat Defense デバイスはそのユーザーを同じ名前のグループ ポリシーに入れて、そのグループ ポリシーの属性のうち、サーバーから返されないものを適用します。
3. **接続プロファイル（トンネル グループと呼ばれる）で割り当てられたグループ ポリシー**：接続プロファイルには、接続の事前設定と、認証前にユーザーに適用されるデフォルトのグループ ポリシーが含まれています。

（注） Firewall Threat Defense デバイスは、デフォルトのグループ ポリシー *DfltGrpPolicy* から継承したシステムデフォルト属性をサポートしていません。前述のとおり、ユーザー属性または AAA サーバーのグループ ポリシーによって上書きされない場合、接続プロファイルに割り当てられたグループ ポリシーの属性がユーザー セッションに使用されます。

関連トピック

リモートアクセス VPN の AAA 設定 （1588 ページ）

AAA サーバー接続の概要

LDAP、AD、および RADIUS AAA サーバーは、ユーザー識別処理のみの場合、VPN 認証のみの場合、またはそれら両方の場合に、Firewall Threat Defense デバイスから到達できる必要があります。AAA サーバーは、次のアクティビティのためにリモートアクセス VPN で使用されます。

- **ユーザー識別処理**：サーバーは管理インターフェイスを介して到達できる必要があります。

  Firewall Threat Defense では、管理インターフェイスには VPN で使用される通常のインターフェイスとは別のルーティングプロセスと設定があります。

- **VPN 認証**：サーバーは通常のインターフェイス（診断インターフェイスまたはデータインターフェイス）のいずれかを介して到達できる必要があります。

  通常のインターフェイスでは、2 つのルーティング テーブルが使用されます。診断インターフェイス用および管理専用に設定されたその他のインターフェイス用の管理専用ルーティング テーブルと、データ インターフェイスに使用されるデータ ルーティング テーブルです。ルート ルックアップが完了すると、管理専用ルーティング テーブルが最初にチェックされ、次にデータ ルーティング テーブルがチェックされます。最初の照合は、AAA サーバーに到達するように選択されます。

（注） データ インターフェイスに AAA サーバーを配置する場合は、管理専用ルーティング ポリシーがデータ インターフェイス宛てのトラフィックと一致しないようにしてください。たとえば、診断インターフェイスを介するデフォルト ルートがある場合、トラフィックが決してデータ ルーティング テーブルにフォールバックしないように注意してください。**show route management-only** コマンドと **show route** コマンドを使用してルーティングの決定を確認します。

同じ AAA サーバー上の両方のアクティビティについて、ユーザー識別処理用の管理インターフェイスを介してサーバーに到達可能にすることに加え、次のいずれかを実行して、同じAAA サーバーへの VPN 認証アクセスを確保します。

- 管理インターフェイスと同じサブネット上の IP アドレスを使用して診断インターフェイスを有効にして設定し、インターフェイスを介した AAA サーバーへのルートを設定します。診断インターフェイスのアクセスは、VPNアクティビティ、識別処理のための管理インターフェイスのアクセスに使用されます。

（注） このように構成すると、診断インターフェイスおよび管理インターフェイスと同じサブネット上にデータインターフェイスを設定することもできません。管理インターフェイスとデータ インターフェイスが同じネットワーク上に必要な場合（たとえば、デバイス自体をゲートウェイとして使用する場合）でも、診断インターフェイスは無効のままでなければならないため、このソリューションを使用できません。

- AAA サーバーへのデータ インターフェイスを介してルートを設定します。データ インターフェイスのアクセスは、VPN アクティビティ、ユーザー識別処理のための管理インターフェイスのアクセスに使用されます。

さまざまなインターフェイスの詳細については、通常のファイアウォール インターフェイス（673 ページ）を参照してください。

展開後、次の CLI コマンドを使用して、Firewall Threat Defense デバイスからの AAA サーバー接続をモニターおよびトラブルシューティングします。

- **show aaa-server** AAA サーバーの統計情報を表示します。
- **show route management-only** 管理専用ルーティング テーブル エントリを表示します。
- **show network** と **show network-static-routes** は管理インターフェイスのデフォルトルートとスタティックルートを表示します。
- **show route** データ トラフィックのルーティング テーブル エントリを表示します。
- **ping system** と **traceroute system** は管理インターフェイスを介して AAA サーバーへのパスを確認します。
- **ping interface** *ifname* と **traceroute** *destination* は診断インターフェイスとデータインターフェイスを介して AAA サーバーへのパスを確認します。
- **test aaa-server authentication** と **test aaa-server authorization** は AAA サーバーでの認証と許可をテストします。
- **clear aaa-server statistics** *groupname* または **clear aaa-server statistics protocol** *protocol* はグループ別またはプロトコル別に AAA サーバーの統計情報をクリアします。
- **aaa-server** *groupname* **active host** *hostname* は障害が発生した AAA サーバーをアクティブ化します。または、 **aaa-server** *groupname* **fail host** *hostname* で AAA サーバーを不合格にします。
- **debug ldap level**、**debug aaa authentication**、 **debug aaa authorization**、**debug aaa accounting**。

リモートアクセス VPN のライセンス要件

Threat Defense ライセンス

Firewall Threat Defense リモートアクセス VPN には、高度暗号化、および セキュアクライアントの次のライセンスのいずれかが必要です。

- Secure Client Advantage
- Secure Client Premier
- Secure Client VPN のみ

リモートアクセス VPN の要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

リモート アクセス VPN のガイドラインと制限事項

リモート アクセス VPN ポリシーの設定

- 新しいリモートアクセスVPNポリシーは、ウィザードを使用してのみ追加できます。ウィザードのすべての手順を実行して新しいポリシーを作成する必要があります。ウィザードを完了する前にキャンセルすると、ポリシーは保存されません。
- 2 人のユーザーが同時にリモート アクセス VPN ポリシーを編集することは**できません**。ただし、Webインターフェイスでは同時編集が防止されません。これが発生した場合、最後に保存された設定が保持されます。
- リモートアクセス VPN ポリシーがそのデバイスに割り当てられている場合、あるドメインから別のドメインに Secure Firewall Threat Defense デバイスを移動することはできません。
- ECMP を使用している場合、リモートアクセス VPN は SSL をサポートしません。IPsec-IKEv2 を使用することをお勧めします。
- クラスタ モードの FirePOWER 9300 および 4100 シリーズは、リモート アクセス VPN の設定をサポートしていません。
- 誤って設定された Firewall Threat Defense NAT ルールがあると、リモートアクセス VPN 接続が失敗する可能性があります。
- DHCP を使用してクライアントに IP アドレスを提供しており、クライアントがアドレスを取得できない場合は、NAT ルールを確認します。RA VPN ネットワークに適用される NAT ルールには、ルート ルックアップ オプションが含まれている必要があります。ルートルックアップは、DHCP要求が適切なインターフェイスを介してDHCPサーバーに確実に送信されるようにするために役立つ場合があります。
- IKE ポート 500/4500 または SSL ポート 443 が使用されている場合や、アクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、Secure Client IPSec-IKEv2 または SSL リモートアクセス VPN を同じポートに設定することはできません。これらのポートは、リモートアクセス VPN ポリシーを設定する前に Firewall Threat Defense デバイスで使用しないようにする必要があります。
- ウィザードを使用してリモート アクセス VPN を設定しているときは、インライン証明書登録オブジェクトを作成できますが、それらを使用してアイデンティティ証明書をインストールすることはできません。証明書登録オブジェクトは、リモート アクセス VPN ゲー

トウェイとして設定されている Firewall Threat Defense デバイスでアイデンティティ証明書を生成するために使用されます。デバイスにリモートアクセス VPN 設定を展開する前に、デバイスにアイデンティティ証明書をインストールします。

証明書登録オブジェクトに基づいてアイデンティティ証明書をインストールする方法の詳細については、オブジェクト マネージャ （1303 ページ）を参照してください。

- ECMP ゾーンインターフェイスは、IPsec が有効なリモートアクセス VPN で使用できます。
- ECMP ゾーンインターフェイスは、SSL が有効なリモートアクセス VPN では使用できません。セキュリティゾーンまたはインターフェイスグループに属するすべてのリモートアクセス VPN インターフェイスが 1 つ以上の ECMP ゾーンにも属している場合、リモートアクセス VPN（SSL が有効）構成の展開は失敗します。ただし、セキュリティゾーンまたはインターフェイスグループに属するリモートアクセス VPN インターフェイスの一部のみが 1 つ以上の ECMP ゾーンにも属している場合は、それらのインターフェイスを除外してリモートアクセス VPN 構成を展開できます。
- リモート アクセス VPN ポリシーの設定を変更した後は、Firewall Threat Defense デバイスに変更を再展開します。設定変更の展開にかかる時間は、ポリシーとルールの複雑さ、デバイスに送信する設定のタイプと量、メモリとデバイスモデルなど、複数の要因によって異なります。リモート アクセス VPN ポリシーの変更を展開する前に、設定変更を展開するためのベストプラクティス （170 ページ）を確認してください。
- RA VPN ヘッドエンドなどに対する **curl** などのコマンドの実行は直接サポートされていないため、望ましい結果が得られない可能性があります。たとえば、ヘッドエンドは HTTP HEAD リクエストに応答しません。
- Firewall Threat Defense は、サードパーティ製クライアントが Null ユーザーエージェントを送信した場合、リモートアクセス VPN セッションを受け入れません。

同時 VPN セッションのキャパシティプランニング（Firewall Threat Defense Virtual モデル）

同時 VPN セッションの最大数は、インストールされている Firewall Threat Defense Virtual スマートライセンスの権限付与階層によって制御され、レートリミッタによって適用されます。ライセンスを取得したデバイスモデルに基づいて、1 台のデバイスで許可される同時リモートアクセス VPN セッション数に上限が設けられます。この限度は、システム パフォーマンスが許容できないレベルにまで低下することがないように設定されています。キャパシティプランニングの際は次の限度を考慮してください。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firewall Threat Defense Virtual5	50
Firewall Threat Defense Virtual10	250
Firewall Threat Defense Virtual20	250
Firewall Threat Defense Virtual30	250

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firewall Threat Defense Virtual50	750
Firewall Threat Defense Virtual100	10,000

同時 VPN セッションのキャパシティ プランニング（ハードウェア モデル）

同時 VPN セッションの最大数は、プラットフォーム固有の制限に準拠し、ライセンスには依存しません。デバイス モデルに基づいて、1 台のデバイスで許可される同時リモート アクセス VPN セッション数に上限が設けられます。この限度は、システム パフォーマンスが許容できないレベルにまで低下することがないように設定されています。キャパシティ プランニングの際は次の限度を考慮してください。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1,500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Secure Firewall 3110	3000
Secure Firewall 3120	6000
Secure Firewall 3130	15,000
Secure Firewall 3140	20,000
Firepower 4100、すべてのモデル	10,000
Firepower 9300 アプライアンス、すべてのモデル	20,000
ISA 3000	25

他のハードウェア モデルの容量については、セールス担当者にお問い合わせください。

（注） プラットフォームごとのセッション数の上限に達すると、Firewall Threat Defense デバイスが VPN 接続を拒否します。Syslog メッセージが示され、接続が拒否されます。Syslog メッセージ ガイドで Syslog メッセージ「%ASA-4-113029」と「and %ASA-4-113038」を参照してください。詳細については、「Cisco Secure Firewall ASA Series Syslog Messages」を参照してください。

VPN の暗号使用方法の制御

DES よりも高度な暗号方式を使用しないようにするため、Firewall Management Center の次の場所で、展開前チェックを使用することもできます。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [編集（Edit）] > [SSL]。

[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）] > [編集（Edit）] > [詳細（Advanced）] > [IPsec]。

SSL 設定と IPsec の詳細については、SSL （862 ページ）およびリモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定 （1628 ページ）を参照してください。

認証、認可、アカウンティング

リモートアクセス VPN を使用するには、トポロジ内の各デバイスで DNS を設定します。DNS がないと、デバイスは AAA サーバー名、名前付き URL、および FQDN またはホスト名を持つ CA サーバーを解決できません。解決できるのは IP アドレスのみです。

[プラットフォーム設定（Platform Settings）] を使用して DNS を設定できます。詳細については、DNS （828 ページ）およびDNS サーバ グループ （1335 ページ）を参照してください。

クライアント証明書

展開でクライアント証明書を使用している場合は、Secure Firewall Threat Defense または Secure Firewall Management Center に関係なく、クライアントのプラットフォームにこれらの証明書を追加する必要があります。クライアントに証明書を入力するために、SCEP や CA サービスなどの機能は提供されません。

Secure Client のサポートされない機能

サポートされている唯一の VPN クライアントは Cisco Secure Client です。それ以外のクライアントまたはネイティブ VPN はサポートされていません。クライアントレス VPN は、Web ブラウザを使用して セキュアクライアントの展開に使用されるだけで、VPN 接続としてはサポートされていません。

（注） Firewall Threat Defense デバイスで複数の Secure Client パッケージを使用すると、メモリ使用量が増加し、デバイスのパフォーマンスに影響を与える可能性があります。メモリの枯渇による継続的なリブートを回避するために、ローエンドの Threat Defense デバイスで複数の Secure Client パッケージを使用しないことを推奨します。

Firewall Threat Defense セキュアゲートウェイに接続する場合、次の Secure Client 機能はサポートされていません。

- Secure Client のカスタマイズとローカリゼーションのサポート。Firewall Threat Defense デバイスは、これらの機能用に Secure Client を設定するために必要なファイルを設定または展開しません。
- TACACS、Kerberos（KCD 認証および RSA SDI）、および SDI。
- ブラウザ プロキシ

新規リモート アクセス VPN 接続の設定

ここでは、VPN ゲートウェイとして Secure Firewall Threat Defense デバイス、VPN クライアントとして Cisco Secure Client を使用して、新しいリモートアクセス VPN ポリシーを設定する手順について説明します。

手順	操作手順	詳細
1	ガイドラインと前提条件を確認します。	リモート アクセス VPN のガイドラインと制限事項 （1566 ページ） リモート アクセス VPN を設定するための前提条件 （1571 ページ）
2	ウィザードを使用して新しいリモートアクセス VPN ポリシーを作成します。	新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）
3	デバイスに展開されているアクセス コントロール ポリシーを更新します。	Secure Firewall Threat Defense デバイスのアクセス コントロール ポリシーの更新 （1575 ページ）
4	（オプション）NAT がデバイスで設定されている場合は、NAT 免除ルールを設定します。	（任意）NAT 免除の設定 （1576 ページ）
5	DNS を設定します。	DNS の設定 （1578 ページ）
6	セキュアクライアント プロファイルを追加します。	Secure Client プロファイル XML ファイルの追加 （1578 ページ）

手順	操作手順	詳細
7	リモートアクセス VPN ポリシーを展開します。	設定変更の展開 （172 ページ）
8	（オプション）リモート アクセス VPN ポリシー設定を確認します。	設定の確認 （1582 ページ）

リモート アクセス VPN を設定するための前提条件

- Secure Firewall Threat Defense デバイスを展開し、Secure Firewall Management Center を設定して、輸出規制対象の機能を有効にした必要なライセンスを持つデバイスを管理します。詳細については、VPN ライセンス （1474 ページ）を参照してください。
- リモート アクセス VPN ゲートウェイとして機能する各 Firewall Threat Defense デバイスにアイデンティティ証明書を取得するために使用する証明書登録オブジェクトを設定します。
- リモートアクセス VPN ポリシーで使用されている AD または LDAP レルムを設定します。
- リモートアクセス VPN を使用した FTD の移行中に、リモートアクセス VPN を移行する前に、リモートアクセス VPN で使用されているレルム（LDAP、AD、またはローカルでも）を cdFMC で事前設定する必要があります。
- リモート アクセス VPN 設定が機能するように AAA サーバーに Firewall Threat Defense デバイスからアクセスできることを確認します。AAA サーバーへの接続を確実にするために、ルーティングを設定します（[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）]）。

  リモート アクセス VPN の二重認証の場合は、二重認証設定が機能するようにプライマリとセカンダリの両方の認証サーバーに Firewall Threat Defense デバイスからアクセスできることを確認します。
- Firewall Threat Defense のリモートアクセス VPN を有効にするため、Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ のうちいずれかの Cisco セキュアクライアントライセンスを購入します。
- シスコのソフトウェア ダウンロード センターから最新の セキュアクライアント イメージ ファイルをダウンロードします。

  Secure Firewall Management Center の Web インターフェイスで、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > **[Secure Clientファイル（Secure Client File）]** に移動し、新しい セキュアクライアント イメージ ファイルを追加します。
- ユーザーが VPN 接続のためにアクセスするネットワーク インターフェイスを含む、セキュリティゾーンまたはインターフェイスグループを作成します。インターフェイス（Interface）（1346 ページ） を参照してください。

- Secure Client プロファイルエディタをシスコのソフトウェア ダウンロードセンターからダウンロードし、Secure Client プロファイルを作成します。スタンドアロンプロファイルエディタを使用して、既存の Secure Client プロファイルを変更したり、新規に作成したりできます。

新しいリモート アクセス VPN ポリシーの作成

リモートアクセス VPN ポリシーウィザードは、基本的な機能を持つリモートアクセス VPN をすばやく、簡単にセットアップできるようにします。必要に応じて追加の属性を指定することでポリシー構成を強化して Secure Firewall Threat Defense のセキュア ゲートウェイ デバイスに展開できます。

始める前に

- リモート アクセス VPN を設定するための前提条件 （1571 ページ） に示されているすべての前提条件を満たしていることを確認します。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** を選択します。

ステップ 2 [追加（Add）] をクリックして、リモートアクセス VPN ポリシーウィザードを使用して、基本的なポリシー構成で新しいリモートアクセス VPN ポリシーを作成します。

ウィザードのすべての手順を実行して新しいポリシーを作成する必要があります。ウィザードを完了する前にキャンセルすると、ポリシーは保存されません。

ステップ 3 ターゲットデバイスとプロトコルを選択します。

ここで選択する Firewall Threat Defense デバイスは、VPN クライアントユーザーのリモートアクセス VPN ゲートウェイとして機能します。

新しいリモートアクセス VPN ポリシーを作成するときに Firewall Threat Defense デバイスを追加したり、後で変更したりできます。「リモートアクセス VPN ポリシーのターゲットデバイスの設定 （1583 ページ）」を参照してください。

SSL または **IPSec-IKEv2**、あるいはその両方の VPN プロトコルを選択できます。Firewall Threat Defense は、VPN トンネルを経由するパブリックネットワークを介してセキュアな接続を確立するために両方のプロトコルをサポートしています。

（注）
Firewall Threat Defense は、NULL 暗号化を使用する IPSec トンネルをサポートしていません。IPSec-IKEv2 を選択した場合は、IPSec IKEv2 プロポーザルに NULL 暗号化を選択しないでください。「IKEv2 IPsec プロポーザル オブジェクトの設定 （1441 ページ）」を参照してください。

SSL 設定については、SSL （862 ページ）を参照してください。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [接続プロファイル（Connection Profile）] および [グループポリシー（Group Policy）] 設定を設定します。

接続プロファイルでは、リモートユーザーが VPN デバイスに接続する方法を定義するパラメータ セットを指定します。パラメータには、認証、VPN クライアントへのアドレスの割り当てとグループ ポリシーの設定および属性が含まれています。Firewall Threat Defense デバイスは、リモート アクセス VPN ポリシーを設定する際の *DefaultWEBVPNGroup* というデフォルトの接続プロファイルを提供します。

詳細については、接続プロファイルの設定 （1585 ページ）を参照してください。

ステップ 6 [認証、認可、およびアカウンティング（Authentication, Authorization & Accounting）] の設定を指定します。

設定の詳細については、次を参照してください。

- AAA 設定： リモートアクセス VPN の AAA 設定 （1588 ページ）
- LDAP 属性マップ： LDAP 属性マッピングの設定 （1617 ページ）
- SAML 2.0 シングルサインオン認証： SAML シングルサインオン認証の設定 （1659 ページ）

ステップ 7 [クライアントアドレスの割り当て（Client Address Assignment）] の設定を指定します。

クライアントの IP アドレスは、AAA サーバー、DHCP サーバー、および IP アドレスプールから割り当てることができます。複数のオプションを選択した場合、IP アドレスの割り当ては、AAA サーバー、DHCP サーバー、IP アドレスプールの順に行われます。AAA サーバーからのクライアント IP アドレス割り当ては、レルムおよび RADIUS 認証についてのみサポートされています。レルムまたは RADIUS サーバーがクライアント IP アドレスを提供するように設定されていることを確認してください。

ステップ 8 [グループポリシー（Group Policy）] の設定を指定します。

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、VPN ユーザーに対してリモート アクセス VPN のエクスペリエンスを定義します。グループポリシーを使用して、ユーザー認証プロファイル、IP アドレス、Secure Client 設定、VLAN マッピング、およびユーザーセッション設定などの属性を設定します。RADIUS 承認サーバーがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。詳細については、グループ ポリシーの設定 （1616 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 VPN ユーザーがリモートアクセス VPN への接続に使用する **[Secure Clientイメージ（Secure Client Image）]** を選択します。

Secure Client は Secure Firewall Threat Defense デバイスへのセキュアな SSL 接続または IPSec（IKEv2）接続を提供し、これにより、リモートユーザーによる企業リソースへのフル VPN プロファイリングが可能となります。Firewall Threat Defense デバイスにリモートアクセス VPN ポリシーを展開したら、VPN ユーザーは設定したデバイスインターフェイスの IP アドレスを

ブラウザに入力し、セキュアクライアントをダウンロードしてインストールできるようになります。

クライアントプロファイルおよびクライアントモジュールの設定については、グループポリシーの セキュアクライアントオプション （1434 ページ）を参照してください。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [入力 VPN アクセスのネットワーク インターフェイス（Network Interface for Incoming VPN Access）] を設定します。

インターフェイス オブジェクトは、ネットワークをセグメント化してトラフィック フローを管理し、分類しやすくします。セキュリティ ゾーン オブジェクトはインターフェイスをグループ化します。これらのグループは複数のデバイスにまたがることがあります。また、単一のデバイスに複数のゾーンインターフェイス オブジェクトを設定することもできます。インターフェイス オブジェクトには次の 2 つのタイプがあります。

- セキュリティ ゾーン：インターフェイスは、1 つのセキュリティ ゾーンにのみ属することができます。
- インターフェイス グループ：インターフェイスは複数のインターフェイスグループ（および 1 つのセキュリティ ゾーン）に属することができます。

（任意）必要に応じて、[メンバーインターフェイスの DTLS の有効化（Enable DTLS on member interfaces）] チェックボックスをオンにします。DTLS は SSL プロトコルにのみ適用できます。

ステップ 13 [デバイス証明書（Device Certificates）] を設定します。

デバイス証明書（アイデンティティ証明書とも呼ばれる）により、リモート アクセス クライアントへの VPN ゲートウェイが識別されます。VPN ゲートウェイの認証に使用する証明書を選択します。**[証明書を登録（Certificate Enrollment）]** ドロップダウンリストで証明書を選択するか、**[+]** をクリックして証明書を追加して、VPN ゲートウェイを認証します。

ステップ 14 [VPN トラフィックのアクセス制御（Access Control for VPN Traffic）] を設定します。

デフォルトでは、VPN トンネルで復号されたトラフィックはすべて、アクセス コントロール ポリシーの対象となります。復号されたトラフィックをアクセス コントロール ポリシーからバイパスするには、[復号されたトラフィックでアクセス コントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] チェックボックスをオンにします。このオプションではアクセス コントロール ポリシー検査はバイパスされますが、AAA サーバーからダウンロードされた VPN フィルタ ACL および認可 ACL は引き続き VPN トラフィックに適用されます。

（注）
このオプションを選択した場合は、Secure Firewall Threat Defense デバイスのアクセス コントロール ポリシーの更新 （1575 ページ） で指定したリモート アクセス VPN のアクセス コントロール ポリシーを更新する必要はありません。

ステップ 15 [次へ（Next）] をクリックします。

ステップ 16 リモートアクセス VPN ポリシー構成の [概要（Summary）] を表示します。

[概要（Summary）] ページには、これまでに設定したすべてのリモート アクセス VPN 設定が表示され、選択したデバイスにリモート アクセス VPN ポリシーを展開する前に実行する必要がある追加設定へのリンクが示されます。

必要に応じて、[戻る（Back）] をクリックして設定に変更を加えます。

ステップ 17 リモートアクセス VPN ポリシーの基本設定を完了するには、[終了（Finish）] をクリックします。

リモートアクセス VPN ポリシーウィザードを完了すると、ポリシーリストページが表示されます。後で、DNS 構成をセットアップし、VPN ユーザーのアクセス制御を設定し、NAT の免除を有効にして（必要な場合）、基本的なリモートアクセス VPN ポリシー構成を完了します。

次のタスク

リモートアクセス VPN ダッシュボード（[概要（Overview）]>[ダッシュボード（Dashboards）]>[リモートアクセス VPN（Remote Access VPN）]）を使用して、デバイス上のアクティブなリモートアクセス VPN セッションからのリアルタイムデータをモニターします。ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。詳細については、リモートアクセス VPN ダッシュボード（1699 ページ）を参照してください。

Secure Firewall Threat Defense デバイスのアクセス コントロール ポリシーの更新

リモート アクセス VPN ポリシーを展開する前に、VPN トラフィックを許可するルールを使用してターゲットの Secure Firewall Threat Defense デバイス上でアクセス コントロール ポリシーを更新する必要があります。ルールは、定義済み VPN プール ネットワークの送信元と社内ネットワークの宛先を持つ外部インターフェイスを通過するすべてのトラフィックを許可する必要があります。

（注） [復号されたトラフィックのアクセス コントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択した場合は、リモート アクセス VPN のアクセス コントロール ポリシーを更新する必要はありません。

すべての VPN 接続のオプションを有効または無効にします。このオプションを無効にする場合は、トラフィックがアクセス コントロール ポリシーまたはプレフィルタポリシーによって許可されていることを確認してください。

詳細については、リモートアクセス VPN のアクセス インターフェイスの設定（1608 ページ）を参照してください。

始める前に

リモート アクセス VPN ポリシー ウィザードを使用してリモート アクセス VPN ポリシーの設定を実行します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

ステップ 2 更新するアクセス コントロール ポリシーで [編集（Edit）] をクリックします。

ステップ 3 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を指定し、[有効（Enabled）] を選択します。

ステップ 5 [アクション（Action）]、[許可（Allow）]、または [信頼（Allow）] を選択します。

ステップ 6 [ゾーン（Zones）] タブで次の項目を選択します。

a) [使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。

b) [使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

ステップ 7 [ネットワーク（Networks）] タブで次の項目を選択します。

a) 使用可能なネットワークから内部ネットワーク（内部インターフェイスまたは社内ネットワーク）を選択し、[宛先に追加（Add to Destination）] をクリックします。

b) **使用可能なネットワーク**から VPN アドレス プール ネットワークを選択し、[送信元ネットワークに追加（Add to Source Networks）] をクリックします。

ステップ 8 その他の必要なアクセス制御ルールを設定して [追加（Add）] をクリックします。

ステップ 9 ルールとアクセス コントロール ポリシーを保存します。

（任意）NAT 免除の設定

NAT 免除を使用すると、アドレスは変換から除外され、変換済みのホストとリモート ホストの両方が保護されたホストとの接続を開始できるようになります。アイデンティティ NAT と同様に、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では変換対象の実際のアドレスを決定するときに実際のアドレスおよび宛先アドレスを指定できます（ポリシー NAT と類似）。アクセス リストのポートを考慮するには、スタティック アイデンティティ NAT を使用します。

リモートアクセスまたはサイト間 VPN の静的アイデンティティ NAT を設定する場合は、ルートルックアップオプションを使用して NAT を設定する必要があります。ルートルックアップがない場合、Firewall Threat Defense は、ルーティング テーブルの内容に関係なく、NAT コマンドで指定されたインターフェイスからトラフィックを送信します。たとえば、Firewall Threat

Defense で DHCP スコープのトラフィックを誤ったインターフェイス経由で送信しないようにします。トラフィックがインターフェイスの IP アドレスに戻ることはありません。ルート ルックアップ オプションを使用すると、Firewall Threat Defense は、インターフェイスを介さずに、インターフェイスの IP アドレス上で直接トラフィックの送信および傍受が可能です。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルート ルックアップ オプションがあっても正しい出力インターフェイス（内部）になるため、通常のトラフィック フローは影響を受けません。

始める前に

リモート アクセス VPN ポリシーが展開されているターゲット デバイスに NAT が設定されているかどうかを確認します。NAT がターゲット デバイスで有効になっている場合、NAT ポリシーを定義して VPN トラフィックを対象外にする必要があります。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [NAT] をクリックします。

ステップ 2 更新する NAT ポリシーを選択するか、または [新しいポリシー（New Policy）]> [脅威対策NAT（Threat Defense NAT）] をクリックし、すべてのインターフェイスへの接続を許可する NAT ルールを含む NAT ポリシーを作成します。

ステップ 3 [ルールの追加（Add Rule）] をクリックして NAT ルールを追加します。

ステップ 4 [NAT ルールの追加（Add NAT Rule）] ウィンドウで、次を選択します。

a) [NAT ルール（NAT Rule）] に [手動 NAT ルール（Manual NAT Rule）] を選択します。

b) [タイプ（Type）] に [スタティック（Static）] を選択します。

c) [インターフェイス オブジェクト（Interface Objects）] をクリックし、送信元と宛先のインターフェイス オブジェクトを選択します。

（注）
このインターフェイス オブジェクトは、リモート アクセス VPN ポリシーで選択したインターフェイスと同じである必要があります。

詳細については、リモートアクセス VPN のアクセス インターフェイスの設定（1608 ページ）を参照してください。

a) [変換（Translation）] をクリックし、送信元と宛先のネットワークを選択します。

- [元の送信元（Original Source）] および [変換済み送信元（Translated Source）]
- [元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）]

ステップ 5 [詳細（Advanced）] タブで [宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination interface）] を選択します。

[宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッ

ピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。

ステップ 6 **[OK]** をクリックします。

DNS の設定

リモート アクセス VPN を使用するには、Firewall Threat Defense の各デバイスで DNS を設定します。DNS がないと、デバイスは AAA サーバー名、名前付き URL、FQDN またはホスト名を持つ CA サーバーを解決できません。IP アドレスのみを解決できます。

手順

ステップ 1 DNS サーバーの詳細とドメインルックアップ インターフェイスを [プラットフォーム設定（Platform Settings）] を使用して設定します。詳細については、DNS（828 ページ）および DNS サーバ グループ（1335 ページ）を参照してください。

ステップ 2 VNP ネットワーク経由で DNS サーバーに到達可能な場合は、リモート アクセス VPN トンネルを介して DNS トラフィックを許可するためのスプリット トンネルをグループ ポリシーに設定します。詳細については、「グループ ポリシー オブジェクトの設定（1430 ページ）」を参照してください。

Secure Client プロファイル XML ファイルの追加

Secure Client プロファイルは、構成パラメータのグループで、動作や表示の設定にクライアントで使用される XML ファイル内に保存されます。これらのパラメータ（XML タグ）には、ホスト コンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

Secure Client プロファイルは、Secure Client ソフトウェアパッケージの一部として提供される GUI ベースの設定ツールである Secure Client プロファイル エディタを使用して作成できます。これは、Firewall Management Center の外部から実行する独立したプログラムです。Secure Client プロファイル エディタの詳細については、Cisco Secure Client（AnyConnect を含む）管理者ガイド [英語] を参照してください。

始める前に

Secure Firewall Threat Defense リモートアクセス VPN ポリシーの場合、VPN クライアントに Secure Client プロファイル を割り当てる必要があります。クライアントプロファイルはグループポリシーに関連付けられます。

Secure Client プロファイル エディタは、シスコのソフトウェア ダウンロード センターからダウンロードします。

手順

ステップ 1 [デバイス（Devices）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 セキュアクライアント プロファイルを追加する接続プロファイルで [編集（Edit）] をクリックします。

ステップ 4 [グループポリシーの編集（Edit Group Policy）] をクリックします。新しいグループポリシーを追加する場合は、[追加（Add）] をクリックします。

ステップ 5 **[Secure Client]** > **[プロファイル（Profile）]**を選択します。

ステップ 6 [クライアントプロファイル（Client Profile）] ドロップダウンリストからプロファイルを選択します。新しいクライアントプロファイルを追加する場合は、[追加（Add）] をクリックして、次の手順を実行します。

a) プロファイルの [名前（Name）] を指定します。

b) [参照（Browse）] をクリックして Secure Client プロファイル XML ファイルを選択します。

（注）
二要素認証の場合、セキュアクライアント プロファイルのタイムアウト値は 60 秒以上に設定してください。

c) [保存（Save）] をクリックします。

ステップ 7 変更を保存します。

（任意）スプリット トンネリングの設定

スプリットトンネルではセキュアトンネル経由のリモートネットワークへの VPN 接続が可能ですが、VPN トンネル外のネットワークにも接続できます。VPN ユーザーがリモートアクセス VPN に接続されている間、外部ネットワークにアクセスできるようにするには、スプリットトンネリングを設定します。スプリットトンネル リストを設定するには、標準アクセス リストまたは拡張アクセス リストを作成する必要があります。

詳細については、グループ ポリシーの設定 （1616 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 2 スプリットトンネリングを設定するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 必要な接続プロファイルで [編集（Edit）] をクリックします。

ステップ 4 [追加（Add）] をクリックしてグループポリシーを追加するか、または [グループポリシーの編集（Edit Group Policy）] をクリックします。

ステップ 5 [全般（General）] > [スプリットトンネリング（Split Tunneling）] を選択します。

ステップ 6 [IPv4スプリットトンネリング（IPv4 Split Tunneling）] または [IPv6スプリットトンネリング（IPv6 Split Tunneling）] リストから、[次に指定されたネットワークを除外（Exclude networks specified below）] を選択し、VPN トラフィックから除外するネットワークを選択します。

デフォルト設定では、VPN トンネル経由のすべてのトラフィックが許可されます。

ステップ 7 [標準アクセスリスト（Standard Access List）] または [拡張アクセスリスト（Extended Access List）] をクリックし、ドロップダウンからアクセス リストを選択するか、新しいアクセス リストを追加します。

ステップ 8 新しい標準アクセスリストまたは拡張アクセスリストを追加する場合は、次の手順を実行します。

a) 新しいアクセス リストの [名前（Name）] を指定し、[追加（Add）] をクリックします。

b) [アクション（Action）] ドロップダウンから [許可（Allow）] を選択します。

c) VPN トンネル上で許可するネットワークトラフィックを選択し、[追加（Add）] をクリックします。

ステップ 9 変更を保存します。

関連トピック

アクセスリスト （1319 ページ）

（任意）ダイナミック スプリット トンネリングの設定

ダイナミック スプリット トンネリングにより、DNS ドメイン名に基づいてスプリットトンネリングを微調整できます。リモートアクセス VPN トンネルに含める、または除外する必要があるドメインを設定できます。除外されたドメインはブロックされません。代わりに、これらのドメインへのトラフィックは VPN トンネルの外部に保持されます。たとえば、パブリックインターネット上の Cisco WebEx にトラフィックを送信することで、保護されたネットワーク内のサーバーへのトラフィック用に VPN トンネル内の帯域幅を解放できます。この機能の設定に関する詳細については、「FMC で管理する FTD 上の AnyConnect ダイナミック スプリット トンネルの設定」を参照してください。

始める前に

バージョン 7.0 以降では、Firewall Management Center と Firewall Threat Defense を使用してこの機能を設定できます。Firewall Management Center の古いバージョンを使用している場合は、「FMC を使用した Firepower Threat Defense 用に向けた、高度な AnyConnect VPN の展開」の指示に従って、FlexConfig を使用して設定できます。

手順

ステップ 1 ダイナミック スプリット トンネルを使用するようにグループポリシーを設定します。

a) [デバイス（Devices）] > [リモートアクセス（Remote Access）] を選択します。
b) ダイナミック スプリット トンネリングを設定するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。
c) 必要な接続プロファイルで [編集（Edit）] をクリックします。
d) [グループポリシーの編集（Edit Group Policy）] をクリックします。

ステップ 2 [グループポリシーの追加/編集（Add/Edit Group Policy）] ダイアログボックスで Secure Client カスタム属性を設定します。

a) [Secure Client] タブをクリックします。
b) [カスタム属性（Custom Attributes）] をクリックし、[+] をクリックします。
c) Secure Client [属性（Attribute）] ドロップダウンリストから [ダイナミック スプリット トンネリング（Dynamic Split Tunneling）] を選択します。
d) [+] をクリックして、新しいカスタム属性オブジェクトを作成します。
e) カスタム属性オブジェクトの名前を入力します。
f) [Include domains]：リモートアクセス VPN トンネルに含めるドメイン名を指定します。

   IP アドレスに基づいて除外されるドメインをトンネルに含めることができます。

g) [Exclude domains]：リモートアクセス VPN から除外するドメイン名を指定します。

   除外されるドメインはブロックされず、これらのドメインへのトラフィックは VPN トンネルの外部に保持されます。

h) [Save（保存）] をクリックします。
i) **[追加（Add）]** をクリックします。

ステップ 3 設定されたカスタム属性を確認し、[保存（Save）] をクリックしてグループポリシーを保存します。

ステップ 4 [保存（Save）] をクリックして接続プロファイルを保存します。

ステップ 5 [保存（Save）] をクリックして、リモートアクセス VPN ポリシーを保存します。

次のタスク

1. Firewall Threat Defense に設定を展開します。

2. Firewall Threat Defense およびセキュアクライアント で設定されたダイナミック スプリット トンネルの設定を確認します。詳細については、「ダイナミック スプリット トンネリング設定の確認 （1582 ページ）」を参照してください。

ダイナミック スプリット トンネリング設定の確認

Firewall Threat Defense で以下を実行します。

ダイナミック スプリット トンネリング設定を確認するには、次のコマンドを使用します。

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** *<group-policy-name>*

セキュアクライアント で以下を実行します。

[統計（Statistics）]（ ）アイコンをクリックし、[VPN] > [統計（Statistics）] を選択します。[ダイナミックスプリットの除外/包含（Dynamic Split Exclusion/Inclusion）] カテゴリでドメインを確認できます。

設定の確認

手順

ステップ 1 外部ネットワークのマシンで Web ブラウザを開きます。

ステップ 2 Firewall Threat Defense のリモートアクセス VPN ゲートウェイデバイスの URL を入力します。

ステップ 3 プロンプトが表示されたらユーザー名とパスワードを入力し、[ログオン（Logon）] をクリックします。

（注）
Secure Client をシステムにインストールすると、VPN への接続が自動的に確立されます。

Secure Client がインストールされていない場合は、VPN から Secure Client をダウンロードするよう要求されます。

ステップ 4 インストールされていない場合は Secure Client をダウンロードし、VPN に接続します。Secure Client が自動的にインストールされます。認証が成功したら、Secure Firewall Threat Defense リモートアクセス VPN ゲートウェイへの接続を確立します。リモートアクセス VPN は、VPN ポリシー設定に従って、該当するアイデンティティポリシーまたは QoS ポリシーを適用します。

既存のリモートアクセス VPN ポリシーのコピーの作成

既存のリモートアクセス VPN ポリシーをコピーして、接続プロファイルやアクセスインターフェイスなど、すべての設定を含む新しいリモートアクセス VPN を作成できます。その後、デバイスを新しいポリシーに割り当て、必要に応じて、割り当てられたデバイスに VPN を展開できます。

（注） リモートアクセス VPN の読み取り専用権限を持つユーザーは、VPN のコピーを作成できません。ドメインで読み取り専用権限を持つユーザーは、リモートアクセス VPN をコピーできます。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。
ステップ 2 コピーするポリシーで [コピー（Copy）] をクリックします。
ステップ 3 新しいリモートアクセス VPN の [名前（Name）] を指定します。
ステップ 4 [OK] をクリックします。

次のタスク

デバイスを新しいポリシーに割り当てるには、リモートアクセス VPN ポリシーのターゲットデバイスの設定 （1583 ページ）を参照してください。

リモートアクセス VPN ポリシーのターゲットデバイスの設定

リモートアクセス VPN ポリシーを作成したら、そのポリシーを Threat Defense デバイスに割り当てることができます。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]** を選択します。
ステップ 2 編集するリモートアクセス VPN ポリシーの横にある [編集（Edit）]（✎）をクリックします。
ステップ 3 [ポリシー割り当て（Policy Assignments）] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、ハイアベイラビリティペア、またはデバイスグループをポリシーに割り当てるには、[Available Devices）] リストで選択し、[Add] をクリックします。表示されているデバイスをドラッグアンドドロップして選択することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス（Selected Device）] リストのデバイス、高可用性ペア、またはデバイスグループの横にある [削除（Delete）]（） をクリックします。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ローカルレルムとリモートアクセス VPN ポリシーの関連付け

ローカルレルムをリモートアクセス VPN ポリシーに関連付けて、ローカルユーザー認証を有効にすることができます。

レルムの作成と管理については、レルムの管理 （2486 ページ）を参照してください。

リモートアクセス VPN のローカルユーザー認証の設定については、リモートアクセス VPN の AAA 設定 （1588 ページ）を参照してください。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]** を選択します。

ステップ 2 編集するリモートアクセス VPN ポリシーの横にある [編集（Edit）]（） をクリックします。

ステップ 3 [ローカルレルム（Local Realm）] の横にあるリンクをクリックします。

ステップ 4 リストから [ローカルレルムサーバー（Local Realm Server）] を選択するか、[追加（Add）] をクリックして新しいローカルレルムを追加します。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

その他のリモートアクセス VPN の設定

接続プロファイルの設定

リモート アクセス VPN ポリシーには、特定のデバイスを対象とする接続プロファイルが含まれています。これらのポリシーはトンネル自体の作成に関連しています。たとえば AAA を行う方法、アドレス（DHCP やアドレス プール）を VPN クライアントに割り当てる方法などです。また、Firewall Threat Defense デバイスで設定された（または AAA サーバから得られる）グループ ポリシーで識別されるユーザ属性も、これらに含まれます。また、デバイスには *DefaultWEBVPNGroup* という名前のデフォルト接続プロファイルもあります。ウィザードを使って設定された接続プロファイルがリストに表示されます。

別のグループの VPN ユーザーに異なる権限を付与する場合は、各ユーザーグループの特定の接続プロファイルを追加し、リモートアクセス VPN ポリシーで複数の接続プロファイルを維持できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [接続プロファイル（Connection Profile）] を選択し、[編集（Edit）] をクリックします。

ステップ 4 （オプション）新しい接続プロファイルを追加する場合は、[追加（Add）]をクリックします。

ステップ 5 VPN クライアントの IP アドレスを設定します。
VPN クライアントの IP アドレスの設定 （1585 ページ）

ステップ 6 （任意）リモート アクセス VPN の AAA 設定を更新します。
リモートアクセス VPN の AAA 設定 （1588 ページ）

ステップ 7 （任意）エイリアスを作成または更新します。
接続プロファイルのエイリアスの作成または更新 （1607 ページ）

ステップ 8 変更を保存します。

VPN クライアントの IP アドレスの設定

クライアントアドレスの割り当てにより、リモートアクセス VPN ユーザー用の IP アドレスを割り当てることができます。

リモート VPN クライアントの IP アドレスは、ローカルの IP アドレスプール、DHCP サーバー、および AAA サーバーから割り当てることができます。最初に AAA サーバーが割り当てられ、その後で他のものが割り当てられます。[詳細（Advanced）] タブで [クライアントアドレスの割り当て（Client Address Assignment）] ポリシーを設定して、割り当て基準を定義します。こ

の接続プロファイルに関連付けられているグループポリシーやシステムのデフォルトグループポリシーである [DfltGrpPolicy] で定義された IP プールが存在しない場合、この接続プロファイルで定義されている IP プールのみが使用されます。

[IPv4 アドレス プール（IPv4 Address Pools）]：SSL VPN クライアントは、Firewall Threat Defense デバイスに接続したときに新しい IP アドレスを受け取ります。アドレスプールでは、リモートクライアントが受け取ることのできるアドレス範囲が定義されます。IPv4 および IPv6 アドレスそれぞれに最大 6 つのプールを追加できます。

（注） Firewall Management Center の既存の IP プールから IP アドレスを使用するか、または [追加（Add）] オプションを使用して新しいプールを作成できます。また、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）] パスを使用して、Firewall Management Center に IP プールを作成することもできます。詳細については、アドレス プール （1323 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [VP] > [リモート アクセス（Remote Access）] を選択します。
既存のリモート アクセス ポリシーがリストされます。

ステップ 2 リモートアクセス VPN ポリシーを選択し、編集アイコンをクリックします。

ステップ 3 更新する接続プロファイルを選択し、編集アイコンをクリックします。

ステップ 4 [クライアントアドレス割り当て（Client Address Assignment）] タブで、次の手順を実行します。

ステップ 5 [アドレスプール（Address Pools）] の横にある [+] をクリックします。

a) [アドレスプール（Address Pools）] の横にある [+] をクリックして IP アドレスを追加し、[IPv4] または [IPv6] を選択して対応するアドレスプールを追加します。[利用可能プール（Available Pools）] から IP アドレスプールを選択し、[追加（Add）] をクリックします。

（注）
複数の Secure Firewall Threat Defense デバイス間でリモート アクセス VPN ポリシーを共有する場合は、すべてのデバイスが同じアドレス プールを共有することに留意してください。ただし、デバイスレベルのオブジェクト オーバーライドを使用して、グローバル定義をデバイスごとの一意なアドレス プールに置き換える場合を除きます。NAT を使用していないデバイスでアドレスが重複しないようにするには、一意なアドレス プールが必要です。

b) [アドレスプール（Address Pools）] ウィンドウで [利用可能プール（Available Pools）] の横にある [+] をクリックして、新しい IPv4 または IPv6 アドレスプールを追加します。IPv4 プールを選択する場合は、開始と終了の IP アドレスを提供します。新しい IPv6 アドレス プールを含めることを選択する場合は、1 ～ 16384 の範囲の [アドレス数（Number of Addresses）] を入力します。オブジェクトが多数のデバイス間で共有される場合は、IP ア

ドレスの競合を回避するために、[オーバーライドを許可（Allow Overrides）] オプションを選択します。詳細については、アドレス プール （1323 ページ）を参照してください。

c) [OK] をクリックします。

IP アドレスプールを編集する場合は、メンテナンス期間中に次の手順を実行することを推奨します。

1. リモートアクセス VPN からデバイスの割り当てを解除します。
2. デバイスを選択して、[展開（Deploy）] をクリックします。

   この展開では、デバイスからすべてのリモートアクセス VPN 設定が削除され、リモートアクセス VPN セッションが終了します。セッションは再確立されません。
3. IP アドレスプールの横にある編集アイコンをクリックして編集し、必要に応じて Firewall Management Center で他のリモートアクセス VPN 設定を編集します。
4. 更新されたリモートアクセス VPN ポリシーにデバイスを割り当てます。
5. 設定をデバイスに展開します。

   リモートアクセス VPN クライアントは、メンテナンス期間の後、デバイスに接続できます。

ステップ 6 [DHCPサーバー（DHCP Servers）] の横にある [+] をクリックして、DHCP サーバーを追加します。

（注）
DHCP サーバー アドレスは、IPv4 アドレスでのみ設定可能です。

a) 名前と DHCP（Dynamic Host Configuration Protocol）のサーバー アドレスをネットワークオブジェクトとして指定します。[追加（Add）] をクリックして、オブジェクトリストからサーバーを選択します。DHCP サーバーを削除するには、[削除（Delete）] をクリックします。

b) 新しいネットワークオブジェクトを追加するには、[新しいオブジェクト（New Objects）] ページで [追加（Add）] をクリックします。新しいオブジェクト名、説明、ネットワークを入力し、必要に応じて [オーバーライドを許可（Allow Overrides）] オプションを選択します。詳細については、ネットワーク オブジェクトの作成（1351 ページ）およびオブジェクトのオーバーライドの許可 （1312 ページ）を参照してください。

c) [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

接続プロファイルの設定 （1585 ページ）

リモートアクセス VPN の AAA 設定

始める前に

- 必要なマシンとユーザーの証明書がエンドポイントに展開されていることを確認してください。Firewall Threat Defense の詳細については、「Firewall Threat Defense 証明書の管理（1456 ページ）」を参照してください。
- 必要な証明書を使用して Secure Client プロファイルを設定します。詳細については、『*Cisco Secure Client (including AnyConnect) Administrator Guide*』を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 AAA 設定が更新されるように接続プロファイルを選択し、**[編集（Edit）]** > **[AAA]** をクリックします。

ステップ 4 [認証（Authentication）] で次の項目を選択します。

- [認証方式（Authentication Method）]：ユーザーに対してネットワークとネットワークサービスへのアクセスを許可する前に、ユーザーの識別方法を決定します。有効なユーザー クレデンシャル（通常は、ユーザー名とパスワード）を要求することで、アクセスが制御されます。また、クライアントからの証明書も含まれます。サポートされている認証方式は、[AAA のみ（AAA only）]、[クライアント証明書のみ（Client Certificate only）]、および [AAA とクライアント証明書（AAA + Client Certificate）] です。

  [認証方式（Authentication Method）] の選択に応じて、次のようになります。

  - [AAA のみ（AAA only）]：[認証サーバー（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバーは同じ値になります。ドロップダウンリストから [アカウンティング サーバー（Accounting Server）] を選択します。[認証サーバー（Authentication Server）] ドロップダウンリストから [AD] および [LDAP] を選択する場合は、手動でそれぞれ [承認サーバー（Authorization Server）] と [アカウンティング サーバー（Accounting Server）] を選択する必要があります。
  - [SAML]：各ユーザーは SAML シングルサインオンサーバーを使用して認証されます。詳細については、「SAML 2.0 シングルサインオン認証（1657 ページ）」を参照してください。

    [IDプロバイダー証明書のオーバーライド（Override Identity Provider Certificate）]：選択すると、SAML プロバイダーのプライマリ ID プロバイダー証明書が、接続プロファイルまたは SAML アプリケーションに固有の IDP 証明書でオーバーライドされます。IdP 証明書をドロップダウンから選択します。

Microsoft Azure は、同じエンティティ ID に対して複数のアプリケーションをサポートできます。各アプリケーション（異なる接続プロファイルにマップされている）には、一意の証明書が必要です。現在の接続プロファイルのシングル サインオン オブジェクトの既存のエンティティ ID を保持し、別の IdP 証明書を使用する場合は、このオプションを選択できます。

これにより、Microsoft Azure SAML ID プロバイダーごとに複数の SAML アプリケーションがサポートされるようになります。

プライマリ ID 証明書は、シングル サインオン サーバー オブジェクトに構成されます。

シングル サインオン サーバー オブジェクトの構成の詳細については、シングルサインオンサーバーの追加 （1317 ページ）を参照してください。

[SAMLログインエクスペリエンス（SAML Login Experience）] を選択して、SAML Web 認証用のブラウザを構成します。

- [VPNクライアント組み込みブラウザ（VPN client embedded browser）]：Web 認証の場合に VPN クライアントに組み込まれているブラウザを使用するには、このオプションを選択します。認証は VPN 接続にのみ適用されます。
- [デフォルトOSブラウザ（Default OS Browser）]：WebAuthN（Web 認証の FIDO2 標準）をサポートするデフォルトまたはネイティブブラウザのオペレーティングシステムを構成するには、このオプションを選択します。このオプションは、生体認証などの Web 認証方法のシングルサインオン（SSO）サポートを有効にします。

  デフォルトのブラウザには、Web 認証用の外部ブラウザパッケージが必要です。Default-External-Browser-Package パッケージがデフォルトで構成されています。デフォルトの外部ブラウザパッケージを変更するには、リモートアクセス VPN ポリシーを編集し、**[詳細設定（Advanced）]** > **[Secure Clientイメージ（Secure Client Images）]** > **[パッケージファイル（Package File）]** でファイルを選択します。

  次を選択して、新しいパッケージファイルを追加することもできます。**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[VPN]** > **[Secure Clientファイル（Secure Client File）]** > **[Secure Clientファイルの追加（Add Secure Client File）]** の順に選択します。

- [クライアント証明書のみ（Client Certificate Only）]：各ユーザーはクライアント証明書を使用して認証されます。クライアント証明書は、VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザー名はクライアント証明書フィールド CN および OU から派生します。クライアント証明書の他のフィールドにユーザー名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

  マシン証明書とユーザー証明書を使用して VPN クライアントを認証するには、[Enable multiple certificate authentication] を選択します。

複数の証明書認証を有効にしている場合は、次のいずれかの証明書を選択してユーザー名をマッピングし、VPN ユーザーを認証できます。

- [最初の証明書（First Certificate）]：VPN クライアントから送信されたマシン証明書からユーザー名をマッピングするには、このオプションを選択します。
- [2番目の証明書（Second Certificate）]：クライアントから送信されたユーザー証明書からユーザー名をマッピングするには、このオプションを選択します。

（注）
複数の証明書認証を有効にしない場合、ユーザー証明書（2 番目の証明書）がデフォルトで認証に使用されます。

クライアント証明書のユーザー名が含まれる [マップ固有フィールド（Map Specific Field）] オプションを選択すると、[プライマリ（Primary）] および [セカンダリ（Secondary）] フィールドに [CN（一般名）（CN (Common Name)）] と [OU（組織ユニット）（OU (Organisational Unit)）] のデフォルト値がそれぞれ表示されます。[DN 全体をユーザー名として使用（Use entire DN as username）] オプションを選択した場合、ユーザー ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザーを接続プロファイルと照合するときに識別子として使用されます。DN ルールは、拡張証明書認証に使用されます。

[固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。

- C（国）
- CN（一般名）
- DNQ(DN修飾子)
- EA（電子メール アドレス）
- GENQ（世代識別子）
- GN（姓名の名）
- I（イニシャル）
- L（地名）
- N（名前）
- O（組織）
- OU（組織ユニット）
- SER（シリアル番号）
- SN（姓名の姓）
- SP（都道府県）

- T（タイトル）
- UID（ユーザー ID）
- UPN（ユーザー プリンシパル名）

- [クライアント証明書とAAA（Client Certificate & AAA）]：各ユーザーはクライアント証明書とAAAサーバーの両方を使用して認証されます。認証に必要な証明書と AAA 設定を選択します。

  どの認証方式を選択する場合にも、[ユーザーが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

- [クライアント証明書とSAML（Client Certificate & SAML）]：各ユーザーはクライアント証明書と SAML サーバーの両方を使用して認証されます。認証に必要な証明書と SAML の設定を選択します。
  - [証明書とSAMLのユーザー名が同じ場合にのみ接続を許可する（Allow connection only if username from certificate and SAML are the same）]：証明書のユーザー名が SAML シングルサインオンユーザー名と一致する場合にのみ VPN 接続を許可するときに選択します。
  - [認証用のクライアント証明書からユーザー名を使用する（Use username from client certificate for Authorization）]：認証のためにクライアント証明書からユーザー名を選択するオプションを選ぶ場合、クライアント証明書から選択するようにフィールドを設定する必要があります。

    特定のフィールドをユーザー名としてマップするか、認証に識別名（DN）全体を使用するかを選択できます。
    - [マップ固有フィールド（Map Specific Field）]：選択すると、クライアント証明書のユーザー名が含まれます。[プライマリ（Primary）] および [セカンダリ（Secondary）] フィールドに [CN（一般名）（CN (Common Name)）] と [OU（組織ユニット）（OU (Organisational Unit)）] のデフォルト値がそれぞれ表示されます。
    - [DN全体をユーザー名として使用（Use entire DN as username）]：承認用にユーザーアイデンティティが自動的に取得されます。

  ダイナミック アクセス ポリシー（DAP）を作成して、ユーザー固有の SAML アサーション属性またはユーザー名を DAP 証明書属性に一致させることもできます。DAP の AAA 基準設定を構成する （1687 ページ）を参照してください。

- [認証サーバー（Authentication Server）]：認証とは、ユーザーに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザーの識別を行う方法です。認証には、有効なユーザー クレデンシャル、証明書、またはその両方が必要です。認証は、単独で使用することも、認可およびアカウンティングとともに使用することもできます。

サーバーをすでに追加している場合は、リストから認証サーバーを選択します。あるいは、認証サーバーを作成します。

- [ローカル（LOCAL）]：Firewall Threat Defense のローカルデータベースがユーザー認証に使用されます。ローカル認証を設定するには、Firewall Threat Defense がバージョン 7.0 以降である必要があります。
  - [Local Realm]：ローカルレルムを選択するか、[Add] をクリックしてレルムを設定します。「LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）」を参照してください。
- [レルム（Realm）]：LDAP または AD レルムを設定します。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ） を参照してください。
- [RADIUS サーバーグループ（RADIUS Server Group）]：RADIUS サーバーグループオブジェクトを RADIUS サーバーとともに追加します。RADIUS サーバーグループの追加 （1314 ページ） を参照してください。
- [Single Sign-On Server]：SAML 認証用のシングル サインオン サーバー オブジェクトを作成します。「シングルサインオンサーバーの追加 （1317ページ）」を参照してください。

[Fallback to LOCAL Authentication]：ローカルデータベースが設定されていれば、ユーザーはローカルデータベースを使用して認証され、AAA サーバーグループが使用できない場合でも VPN トンネルを確立できます。

- [セカンダリ認証を使用（Use secondary authentication）]：VPN セッションのセキュリティを強化するため、プライマリ認証の他にセカンダリ認証を設定します。セカンダリ認証は、[AAA のみ（AAA only）] と [クライアント証明書と AAA（Client Certificate & AAA）] の認証方式にのみ適用されます。

  セカンダリ認証はオプションの機能であり、2 つのセットのユーザー名とパスワードを Secure Client ログイン画面に入力するには VPN ユーザーが必要です。認証サーバーまたはクライアント証明書からセカンダリ ユーザー名を事前入力するように設定することもできます。リモート アクセス VPN 認証は、プライマリとセカンダリの両方の認証が成功した場合にのみ許可されます。いずれの認証サーバーに到達できない場合、1 つの認証が失敗すると、VPN 認証が拒否されます。

  セカンダリ認証の設定前に、2つ目のユーザー名とパスワードのセカンダリ認証のサーバーグループ（AAA サーバー）を設定する必要があります。たとえば、プライマリ認証サーバーを LDAP または Active Directory レルムに、セカンダリ認証を RADIUS サーバーに設定できます。

  （注）
  デフォルトでは、セカンダリ認証は必要ありません。

  [認証サーバー（Authentication Server）]：VPN ユーザーのセカンダリ ユーザー名とパスワードを提供するセカンダリ認証サーバー。

- [Fallback to LOCAL Authentication]：ローカルデータベースが設定されていれば、ユーザーはローカルデータベースを使用して認証され、AAA サーバーグループが使用できない場合でも VPN トンネルを確立できます。

[セカンダリ認証のユーザー名（Username for secondary authentication）] で次の項目を選択します。

- [プロンプト（Prompt）]：VPN ゲートウェイへのログイン中にユーザー名とパスワードを入力するようユーザーに要求します。
- [プライマリ認証ユーザー名を使用（Use primary authentication username）]：プライマリとセカンダリの両方の認証にプライマリ認証サーバーからユーザー名が取得されます。パスワードは 2 つ入力する必要があります。
- [クライアント証明書からのユーザー名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザー名が事前に入力されます。

  複数の証明書認証を有効にしている場合は、次のいずれかの証明書を選択できます。

  - [First Certificate]：VPN クライアントから送信されたマシン証明書からユーザー名をマッピングするには、このオプションを選択します。
  - [Second Certificate]：クライアントから送信されたユーザー証明書からユーザー名をマッピングするには、このオプションを選択します。
  - クライアント証明書のユーザー名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN（識別名）全体をユーザー名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザー ID が自動的に取得されます。

    プライマリとセカンダリのフィールドのマッピングの詳細については、「**認証方式**」の説明を参照してください。
  - [ユーザーログインウィンドウに証明書からユーザー名を事前に入力（Prefill username from certificate on user login window）]：ユーザーが Secure Client クライアント経由で接続したときにクライアント証明書からセカンダリユーザー名を事前に入力します。
    - [ログイン ウィンドウでユーザー名を非表示にする（Hide username in login window）]：セカンダリ ユーザー名はクライアント証明書から事前に入力されますがユーザーには表示されず、ユーザーが事前に入力されたユーザー名を変更しないようにします。
- [VPN セッションのセカンダリ ユーザー名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザー アクティビティのレポートにセカンダリ ユーザー名を使用します。

ステップ 5 [認可（Authorization）] で次の項目を選択します。

- [認可（Authorization Server）]：認証の完了後、認可によって、認証済みの各ユーザーが使用できるサービスおよびコマンドが制御されます。認可は、ユーザーが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザーに対して同じアクセス権を提供します。認可には、認証が必要です。

  リモート アクセス VPN 認可の仕組みについては、権限および属性のポリシー実施の概要（1563 ページ）を参照してください。

  RADIUS サーバーが接続プロファイルのユーザー承認用に構成されている場合、リモートアクセス VPN システムの管理者は、ユーザーまたはユーザーグループに複数の承認属性を構成できます。RADIUS サーバーに構成される承認属性は、ユーザーまたはユーザーグループに固有にできます。ユーザーが認証されると、これらの特定の承認属性が Firewall Threat Defense デバイスにプッシュされます。

  （注）
  許可サーバーから所得した AAA サーバー属性は、グループ ポリシーまたは接続プロファイルで事前に設定されていた可能性がある属性値を上書きします。

- 必要な場合は、[ユーザーが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] をオンにします。

  有効にすると、システムは正常に接続するために、クライアントのユーザー名が承認データベース内に存在することを確認します。ユーザー名が承認データベース内に存在しない場合、接続が拒否されます。

- 許可サーバーとしてレルムを選択する場合は、LDAP 属性マップを設定する必要があります。認証と認可に単一のサーバーを選択することも別のサーバーを選択することもできます。[LDAP 属性マップの設定（Configure LDAP Attribute Map）] をクリックして、認可用の LDAP 属性マップを追加します。

  （注）
  Firewall Threat Defense は、認可サーバーとして SAML アイデンティティ プロバイダーをサポートしていません。SAML ID プロバイダーの背後にある Active Directory が Firewall Management Center および Firewall Threat Defense を介して到達可能な場合は、次の手順で認可を設定できます。

  - AD サーバーのレルムを追加します。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ） を参照してください。
  - リモートアクセス VPN 接続プロファイルで認可サーバーとしてレルムオブジェクトを選択します。
  - 選択したレルムの LDAP 属性マップを設定します。

  LDAP 属性マップの設定の詳細については、LDAP 属性マッピングの設定 （1617 ページ）を参照してください。

ステップ 6 [アカウンティング（Accounting）] で次の項目を選択します。

- [アカウンティングサーバー（Accounting Server）]：アカウンティングは、ユーザーがアクセスしているサービス、およびユーザーが消費しているネットワーク リソース量を追跡するために使用されます。AAA アカウンティングがアクティブになると、ネットワーク アクセス サーバーはユーザー アクティビティを RADIUS サーバーに報告します。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

  リモートアクセス VPN セッションを構成するために使用される RADIUS サーバー グループ オブジェクトを指定します。

ステップ 7 [詳細設定（Advanced Settings）] で次の項目を選択します。

- [ユーザー名からレルムを削除（Strip Realm from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からレルムを削除するには選択します。たとえば、このオプションを選択して、*domain\username* を指定した場合、ユーザー名からドメインが削除され、認証用の AAA サーバーに送信されます。デフォルトでは、このオプションはオフになっています。
- [ユーザー名からグループを削除（Strip Group from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からグループを削除するには選択します。デフォルトでは、このオプションはオフになっています。

  （注）
  レルムとは管理ドメインのことです。これらのオプションを有効にすると、ユーザー名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
- [パスワード管理（Password Management）]：リモートアクセス VPN ユーザーのパスワードを管理できるようにします。パスワードが期限切れになる前に通知するか、パスワードが期限切れになる日に通知するかを選択します。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

権限および属性のポリシー実施の概要 （1563 ページ）
レルムの管理 （2486 ページ）

Secure Firewall Threat Defense の RADIUS サーバー属性

Firewall Threat Defense デバイスは、リモート アクセス VPN ポリシーで認証および/または承認のために設定された外部 RADIUS サーバーから、VPN 接続にユーザー承認属性（ユーザーの権利または権限とも呼ばれる）を適用することをサポートしています。

（注） Secure Firewall Threat Defense デバイスはベンダー ID 3076 の属性をサポートしています。

次のユーザー認可属性が Firewall Threat Defense デバイスから RADIUS サーバーに送信されます。

- RADIUS 属性 146 および 150 は、認証および認可の要求の場合に Firewall Threat Defense デバイスから RADIUS サーバーに送信されます。
- 3 つの属性（146、150、151）はすべて、アカウンティングの開始、暫定更新、および停止要求のために、Firewall Threat Defense デバイスから RADIUS サーバーに送信されます。

表 *74 : Secure Firewall Threat Defense* から *RADIU* サーバーに送信される *RADIUS* 属性

属性	Attribute Number	シンタックス、タイプ	シングルまたはマルチ値	説明または値
接続プロファイル名またはトンネル グループ名。	146	文字列	シングル	1 ～ 253 文字
クライアント タイプ（Client Type）	150	整数	シングル	2＝セキュアクライアント SSL VPN、6＝セキュアクライアント IPsec VPN（IKEv2）
セッション タイプ	151	整数	シングル	1＝セキュアクライアント SSL VPN、2＝セキュアクライアント IPsec VPN（IKEv2）

表 *75 :* サポートされる *RADIUS* 認証属性

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	String	シングル	時間範囲の名前（Business-hours など）

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	Y	86	文字列	シングル	アクセス リスト属性の両方が、Firewall Defense デバイスで設定されている ACL 使用します。スマート CLI 拡張アクセス オブジェクトタイプを使用して、これら 作成します（[デバイス（Device）] > [詳（Advanced Configuration）] > [スマートC CLI）] > [オブジェクト（Object）] を選す）。 これらのACLは、着信(Firewall Threat De イスに入るトラフィック)または発信(Fire Defenseデバイスから出るトラフィック)ト フィックフローを制御します。
Access-List-Outbound	Y	87	文字列	シングル	
Address-Pools	Y	217	文字列	シングル	Firewall Threat Defense デバイスで定義さ トワークオブジェクトの名前。リモート VPN へのクライアント接続のアドレスプ て使用されるサブネットを識別します。 クト（Objects）]ページでネットワークオ トを定義し、次にネットワークオブジェ ループポリシーまたは接続プロファイル けます。
Allow-Network-Extension-Mode	Y	64	ブール	シングル	0 = 無効1 = 有効
Authenticated-User-Idle-Timeout	Y	50	整数	シングル	1 ～ 35791394 分
Authorization-DN-Field	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、 T、N、GN、SN、I、GENQ、DNQ、SER use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	対応	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモートアクセスセッション IKEv1、Secure Client SSL-TLS/DTLS/IKEv クライアントレス SSL）に対して表示され 文字列

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Banner2	Y	36	文字列	シングル	Cisco VPN リモートアクセスセッション（I IKEv1、Secure Client SSL-TLS/DTLS/IKEv2、クライアントレスSSL）に対して表示される 文字列Banner2 文字列は Banner1 文字列に連 ます（設定されている場合）。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効1 = 有効
Client Type	Y	150	整数	シングル	1 = Cisco VPN Client（IKEv1） 2 = セキュア アント SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 キュアクライアント IPsec VPN（IKEv2）
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	整数	シングル	0 = 無効1 = 有効
Framed-Interface-Id	Y	96	文字列	シングル	割り当てられた IPv6 インターフェイス ID。 割り当てられた IPv6 アドレスを作成するた Framed-IPv6-Prefix と組み合わせます。例： Framed-Interface-ID=1:1:1:1 と Framed-IPv6-Prefix=2001:0db8::/64 を組み合 と、IP アドレス 2001:0db8::1:1:1:1 が得られ
Framed-IPv6-Prefix	Y	97	文字列	シングル	割り当てられた IPv6 プレフィックスと長さ に割り当てられたIPv6アドレスを作成するた Framed-Interface-Id と組み合わせます。例： フィックス 2001:0db8::/64 と Framed-Interface-Id=1:1:1:1 を組み合わせると ドレス 2001:0db8::1:1:1:1 が得られます。こ を使用して、フレームインターフェイス Id せずに IP アドレスを割り当てることができ これには、プレフィックス長/128 を使用し なIPv6アドレスを割り当てます（たとえば、 ム化された IPv6 プレフィックス = 2001: 0db 1/128）。

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Group-Policy	Y	25	文字列	シングル	リモート アクセス VPN セッションのグリシーを設定します。次のいずれかの形できます。 • グループポリシー名 • OU=グループポリシー名 • OU=グループポリシー名。
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	文字列	シングル	改行（\n）区切りの DNS ドメインのリス
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検ンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	整数	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = 無効1 = 有効
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = 無効1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効1 = 有効
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP（認可のみドメイン 4 = SDI 5 = 内部 6 = RADIUS で認証 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバー アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	文字列	シングル	1 = クライアントが設定したリストを使用クライアント リストを無効化して消去すクアップ サーバー リストを使用する
IPsec-Client-Firewall-Filter-Name		57	文字列	シングル	クライアントにファイアウォール ポリシ配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルト ドメイ 1 つだけ指定します（1 ～ 255 文字）。
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場 チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There（A 定義されているポリシー 2 = Policy pushed C サーバーからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティ アソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリ ドメイ リストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリ ンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリット トンネルの包含リストを記述し トワークまたは ACL の名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビ 128 ビット 8 = ステートレスが必要 15 = 40/1 トで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = 無効1 = 有効

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： `Engineering, Sales` ダイナミック アクセス ポリシーで使用 属性。グループ ポリシーは設定されま
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL
NAC-Enable		89	整数	シングル	0 = いいえ 1 = はい
NAC-Revalidation-Timer		91	整数	シングル	300 ～ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = いいえ 1 = はい
PPTP-Encryption		20	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 128 ビット 8 = ステートレスが必要 15 = 4 トで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。
Required-Client- Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems（Cisco Integrated Client = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems（Cisco Intrusion Prevention Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Required-Client-Firewall-Product-Code	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent ま Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone Al 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Ag Sygate 製品： 1 = Personal Firewall 2 = Person Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = 無効1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 =クライアントレス 2 =クライアン クライアントのみ Session Subtype が適用されるのは、Session （151）属性の値が 1、2、3、または 4 の場 です。
Session Type	Y	151	整数	シングル	0 = なし 1 = セキュアクライアント SSL VPN キュアクライアント IPSec VPN（IKEv2） 3 イアントレス SSL VPN 4 = クライントレス電 ルプロキシ 5 = Cisco VPN Client（IKEv1） 6 = LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロー ンシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動ス
Smart-Tunnel-Auto-Signon-Enable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効1 = 有効

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
SVC-Ask	Y	131	文字列	シングル	0=ディセーブル 1=イネーブル 3=デフォ ビスをイネーブルにする 5 = デフォルト ントレスをイネーブルにする （2 と 4 は い）
SVC-Ask-Timeout	Y	132	整数	シングル	5 ～ 120 秒
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ、15 ～ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ～ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2 相互排他。0 ～ 11、16 ～ 27、32 ～ 43、 有効な値。
Use-Client-Address		17	ブール	シングル	0 = 無効1 = 有効
VLAN	Y	140	整数	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセス リスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効1 = 有効
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	予約済み
WebVPN-Citrix-Metaframe-Enable	Y	101	整数	シングル	0 = 無効1 = 有効

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Content-Filter-Parameters	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメ = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL（たとえば http://example-example.com）
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Browsing-Enable	Y	96	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Entry-Enable	Y	95	整数	シングル	0 = 無効1 = 有効
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	文字列	シングル	オプションのワイルドカード（*）を使用し マ区切りの DNS/IP（たとえば、*.cisco.com 192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	ブール	シングル	クライアントレス ホーム ページをスマート ル経由で表示する場合にイネーブルにしま
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ キー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	文字列	シングル	http= または https= プレフィックス付きの、 区切りの DNS/IP:ポート（例：http=10.10.10. https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	整数	シングル	0 = 無効1 = 有効

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」） このテキストでクライアントレス ポータ ページのデフォルト文字列「Application 置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN Smart-Card-Removal-Disconnect	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネ インオン リストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク 「a」のいずれか。ここで、ネットワーク マート トンネル ネットワークのリストの す。e はトンネルが除外されることを示 ンネルが指定されることを示し、a はすべ ネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Keep- Installation	Y	105	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Required	Y	104	整数	シングル	0 = 無効1 = 有効
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	整数	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	整数	シングル	0 = 無効1 = 有効

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ～ 10080 分、0=オフ
WebVPN-SVC-Rekey-Method	Y	111	整数	シングル	0（オフ）、1（SSL）、2（新しいトンネル
WebVPN-SVC-Compression	Y	112	整数	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザー ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = 無効1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

表 *76 :* 送信される *RADIUS* 属性 *Secure Firewall Threat Defense*

属性	Attribute Number	シンタックス、タイプ	シングルまたはマルチ値	説明または値
Address-Pools	217	文字列	シングル	Firewall Threat Defense デバイスで定義されたネットワークオブジェクトの名前。リモートアクセス VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[オブジェクト]ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザがログインしたときに表示されるバナー。
Banner2	36	文字列	シングル	ユーザがログインしたときに表示されるバナーの 2 番目の部分。Banner2 が Banner1 に追加されます。
Downloadable ACLs	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Cisco-AV-Pair 構成でサポートされます。

属性	Attribute Number	シンタックス、タイプ	シングルまたはマルチ値	説明または値
Filter ACLs	86、87	文字列	シングル	フィルタ ACL は、RADIUS サーバーで ACL 名で参照されます。ACL 設定が Firewall Threat Defense デバイス上にすでに存在していて、RADIUS 承認時に使用できるようにする必要があります。 86 = アクセスリスト-インバウンド 87 = アクセスリスト-アウトバウンド
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。リモートアクセス VPN の [グループポリシー（Group Policy）] ページでグループポリシーを作成する必要があります。次のいずれかの形式を使用できます。 • グループポリシー名 • OU=グループポリシー名 • OU=グループポリシー名。
Simultaneous-Logins	2	整数	シングル	ユーザが確立を許可されている個別の同時接続数。0 ～ 2147483647。
VLAN	140	整数	シングル	ユーザの接続を制限する VLAN。0 ～ 4094。Firewall Threat Defense デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

ISE から返される IE-Proxy-Server-Method 属性の値を次のいずれかに設定する必要があります。

- IE_PROXY_METHOD_PACFILE: 8
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_METHOD_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

上記の値のいずれかが IE-Proxy-Server-Method 属性に使用されている場合にのみ、Firewall Threat Defense はプロキシ設定を配信します。

接続プロファイルのエイリアスの作成または更新

エイリアスには、特定の接続プロファイルの代替名または URL が含まれます。リモートアクセス VPN 管理者は、エイリアス名とエイリアス URL を有効または無効にできます。VPN ユーザは、Secure Firewall Threat Defense デバイスに接続するときにエイリアス名を選択できます。このデバイスに設定されているすべての接続のエイリアス名の表示をオンまたはオフにできます。また、リモートアクセス VPN 接続の開始時にエンドポイントが選択できるエイリアス URL

のリストを設定することもできます。ユーザがエイリアス URL を使用して接続すると、システムはエイリアス URL と一致する接続プロファイルを使用して自動的にそのユーザをログに記録します。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 変更するポリシーの [編集（Edit）] をクリックします。

ステップ 3 エイリアスを作成または更新する接続プロファイルで [編集（Edit）] をクリックします。

ステップ 4 [エイリアス（Aliases）] をクリックします。

ステップ 5 エイリアス名を追加するには、次の手順を実行します。

a) [エイリアス名（Alias Names）] の [追加（Add）] をクリックします。
b) [エイリアス名（Alias Name）] を指定します。
c) エイリアスを有効にするには、各ウィンドウで [有効（Enabled）] チェックボックスをオンにします。
d) [OK] をクリックします。

ステップ 6 エイリアス URL を追加するには、次の手順を実行します。

a) [エイリアスURL（Alias URL）] の [追加（Add）] をクリックします。
b) リストから [エイリアスURL（Alias URL）] を選択するか、新しい URL オブジェクトを作成します。詳細については、URL オブジェクトの作成（1405 ページ）を参照してください。
c) エイリアスを有効にするには、各ウィンドウで [有効（Enabled）] チェックボックスをオンにします。
d) [OK] をクリックします。

ステップ 7 変更を保存します。

関連トピック

接続プロファイルの設定 （1585 ページ）

リモートアクセス VPN のアクセス インターフェイスの設定

[アクセス インターフェイス（Access Interface）] テーブルには、デバイス インターフェイスを含むインターフェイス グループとセキュリティ ゾーンが示されています。これらは、リモート アクセス SSL または IPsec IKEv2 VPN 接続用に設定されています。このテーブルには、各インターフェイス グループまたはセキュリティ ゾーン、インターフェイスで使用されるインターフェイス トラストポイント、および Datagram Transport Layer Security（DTLS）が有効かどうかが表示されます。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [アクセスインターフェイス（Access Interface）] タブをクリックします。

ステップ 4 アクセスインターフェイスを追加するには、[+] をクリックし、[アクセスインターフェイスの追加（Add Access Interface）] ダイアログボックスで以下に対する値を指定します。

a) [アクセスインターフェイス（Access Interface）]：インターフェイスが属するインターフェイス グループまたはセキュリティ ゾーンを選択します。

インターフェイス グループまたはセキュリティ ゾーンは、ルーテッド タイプでなければなりません。他のインターフェイスタイプは、リモートアクセス VPN 接続ではサポートされていません。

b) 次のオプションを選択して、アクセス インターフェイスに [プロトコル（Protocol）] オブジェクトを関連付けます。

- [IPSet-IKEv2の有効化（Enable IPSet-IKEv2）]：**IKEv2** 設定を有効にするには、このオプションを選択します。
- [SSL の有効化（Enable SSL）]：**SSL** 設定を有効にするには、このオプションを選択します。
  - [Datagram Transport Layer Security の有効化（Enable Datagram Transport Layer Security）] を選択します。

    選択すると、インターフェイスで Datagram Transport Layer Security（DTLS）が有効になり、Cisco Secure Client の AnyConnect VPN モジュールは 2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用して SSL VPN 接続を確立できます。

    DTLS を有効にすると、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

    SSL 設定と、TLS および DTLS バージョンを指定するには、SSL 設定について（863 ページ）を参照してください。

    Cisco Secure Client の AnyConnect VPN モジュールの SSL 設定の設定については、グループポリシーのセキュアクライアントオプション（1434 ページ）を参照してください。

  - [インターフェイス固有のアイデンティティ証明書を設定する（Configure Interface Specific Identity Certificate）] チェックボックスをオンにして、ドロップダウン リストから [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] を選択します。

    [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] を選択しないと、[トラストポイント（Trustpoint）] がデフォルトで使用されます。

[インターフェイスアイデンティティ証明書（Interface Identity Certificate）] または [トラストポイント（Trustpoint）] を選択しないと、[SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）] がデフォルトで使用されます。

c) [OK] をクリックして変更を保存します。

ステップ 5 [アクセス設定（Access Settings）] で次の項目を選択します。

- [ユーザーがログイン中に接続プロファイルを選択することを許可する（Allow Users to select connection profile while logging in）]：複数の接続プロファイルがある場合、このチェックボックスをオンにすると、ユーザーはログイン時に正しい接続プロファイルを選択できます。このオプションを **IPsec-IKEv2** VPN に選択する必要があります。
- [HTTP 専用 VPN クッキーの有効化（Enable HTTP-only VPN Cookies）]：HTTP 専用 VPN クッキーを有効にするには、このチェックボックスをオンにします。

ステップ 6 [SSL設定（SSL Settings）] で次のオプションを使用します。

- [Web アクセス ポート番号（Web Access Port Number）]：VPN セッションで使用するポート。デフォルト ポートは 443 です。
- [DTLS ポート番号（DTLS Port Number）]：DTLS 接続に使用する UDP ポート。デフォルト ポートは 443 です。
- [SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）]：[インターフェイス固有のアイデンティティ証明書（Interface Specific Identity Certificate）] が提供されていない場合、選択した [SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）] がすべての関連インターフェイスに使用されます。

ステップ 7 [IPsec-IKEv2設定（IPsec-IKEv2 Settings）] の場合、リストから [IKEv2アイデンティティ証明書（IKEv2 Identity Certificate）] を選択するか、アイデンティティ証明書を追加します。

ステップ 8 [VPNトラフィックのアクセスコントロール（Access Control for VPN Traffic）] セクションで、アクセス コントロール ポリシーをバイパスする場合に次のオプションを選択します。

- [復号されたトラフィック（sysopt permit-vpn）に対するバイパス アクセス コントロール ポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、復号されたトラフィックは、アクセス コントロール ポリシーのインスペクションの対象になります。復号されたトラフィック オプションに対してバイパス アクセス コントロール ポリシーを有効にすると、ACLインスペクションがバイパスされますが、AAA サーバーからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。

（注）
このオプションを選択した場合は、Secure Firewall Threat Defense デバイスのアクセス コントロール ポリシーの更新（1575 ページ） で指定したリモートアクセス VPN のアクセス コントロール ポリシーを更新する必要はありません。

ステップ 9 [保存（Save）] をクリックしてアクセス インターフェイスの変更を保存します。

関連トピック

インターフェイス（Interface） （1346 ページ）

リモートアクセス VPN の高度なオプションの設定

Cisco Secure Client イメージ

Secure Client イメージ

Secure Client は Firewall Threat Defense デバイスへのセキュアな SSL 接続または IPsec（IKEv2）接続を提供し、これにより、リモートユーザーによる企業リソースへのフル VPN プロファイリングが可能となります。インストール済みのクライアントがない場合、リモートユーザーは、クライアントレス VPN 接続を受け入れるように設定されたインターフェイスの IP アドレスをブラウザに入力し、セキュアクライアントをダウンロードしてインストールすることができます。Firewall Threat Defense デバイスは、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロード後に、クライアントがインストールされてセキュアな接続が確立されます。すでにクライアントがインストールされている場合は、ユーザーの認証時に Firewall Threat Defense デバイスがクライアントのバージョンを検査し、必要に応じてクライアントをアップグレードします。

リモートアクセス VPN 管理者は、新規または追加の セキュアクライアント イメージを VPN ポリシーに関連付けます。管理者は、サポート対象外または期限切れで不要になったクライアント パッケージの関連付けを解除できます。

Secure Firewall Management Center は、ファイル パッケージ名を使用してオペレーティング システムの種類を判別します。ユーザーがオペレーティング システム情報を示さずにファイルの名前を変更した場合は、有効なオペレーティング システム タイプをリスト ボックスから選択する必要があります。

シスコのソフトウェア ダウンロード センターを参照して セキュアクライアント イメージファイルをダウンロードします。

関連トピック

Secure Firewall Management Center への Secure Client イメージの追加 （1611 ページ）

Secure Firewall Management Center への Secure Client イメージの追加

[Secure Clientファイル（Secure Client File）] オブジェクトを使用して、Secure Client イメージを Secure Firewall Management Center にアップロードすることもできます。詳細については、ファイルオブジェクト （1446ページ）を参照してください。クライアントイメージの詳細については、Cisco Secure Client イメージ （1611 ページ） を参照してください。

手順

ステップ 1 [デバイス（Devices）]>[リモートアクセス（Remote Access）] で、リストされているリモートアクセスポリシーを選択および編集し、[詳細設定（Advanced）] タブを選択します。 を選択します。

ステップ 2 [追加（Image）] をクリックして、Secure Client イメージを追加します。

ステップ 3 [Secure Clientイメージ（Secure Client Images）] ダイアログの [使用可能なSecure Clientイメージ（Available Secure Client Images）] 部分で [追加（Add）] をクリックします。

ステップ 4 使用可能な Secure Client イメージの [名前（Name）] と [説明（Description）]（オプション）を入力します。

ステップ 5 [参照（Browse）]をクリックし、アップロードするクライアントイメージを見つけて選択します。

ステップ 6 [保存（Save）] をクリックしてイメージを Firewall Management Center にアップロードします。

クライアントイメージを Secure Firewall Management Center にアップロードすると、イメージのオペレーティングシステム情報が自動的に表示されます。

ステップ 7 クライアントイメージの順序を変更するには、[並べ替えボタンを表示（Show re-order buttons）] をクリックして、クライアントイメージを上下に移動します。

関連トピック

Cisco Secure Client イメージ （1611 ページ）

リモートアクセス VPN クライアントの Secure Client イメージ の更新

シスコのソフトウェア ダウンロードセンターで新しいSecure Client更新を入手できる場合は、そのパッケージを手動でダウンロードしてリモートアクセス VPN ポリシーに追加します。それにより、オペレーティングシステムに応じて VPN クライアントシステム上で新しいクライアントパッケージがアップグレードされます。

始める前に

この項の手順は、Secure Firewall Threat Defense VPN ゲートウェイに接続しているリモートアクセス VPN クライアントに新しい Secure Client イメージを更新するのに役立ちます。Secure Client のイメージを更新する前に、次の設定が完了していることを確認します。

- シスコのソフトウェア ダウンロード センターから最新の Secure Client イメージ ファイルをダウンロードします。
- Secure Firewall Management Center の Web インターフェイスで、**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]**>**VPN**>**[Secure Clientファイル（Secure Client File）]**に移動し、新しい [Secure Client] イメージファイルを追加します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 **[詳細（Advanced）]** > **[Secure Clientイメージ（Secure Client Image）]** > **[追加（Add）]**をクリックします。

ステップ 4 **[利用可能なSecure Clientイメージ（Available Secure Client Images）]** からクライアント イメージ ファイルを選択し、[追加（Add）] をクリックします。

必要なクライアントイメージが表示されていない場合は、[追加（Add）] をクリックして参照し、イメージをアップロードします。

ステップ 5 [OK] をクリックします。

ステップ 6 リモート アクセス VPN ポリシーを保存します。
リモートアクセス VPN ポリシーの変更が展開されると、リモートアクセス VPN ゲートウェイとして設定されている Secure Firewall Threat Defense デバイスで新しい Secure Client イメージが更新されます。新しい VPN ユーザーが VPN ゲートウェイに接続すると、クライアントイメージのオペレーティングシステムに応じて、新しいセキュアクライアントイメージがダウンロードされます。既存の VPN ユーザーの場合、セキュアクライアント イメージは次の VPN セッションで更新されます。

Secure Firewall Management Center への Cisco Secure Client 外部ブラウザパッケージの追加

ローカルディスクにすでに保存されている Secure Client 外部ブラウザパッケージのイメージがある場合は、この手順を使用して、それを Secure Firewall Management Center にアップロードします。外部ブラウザパッケージをアップロードしたら、リモートアクセス VPN 接続用に外部ブラウザパッケージを更新できます。

[Secure Clientファイル（Secure Client File）] オブジェクトを使用して、外部ブラウザパッケージファイルを Secure Firewall Management Center にアップロードできます。詳細については、ファイルオブジェクト （1446 ページ）を参照してください。

注意事項

- Firewall Threat Defense デバイスに追加できる外部ブラウザパッケージは 1 つだけです。
- 外部ブラウザパッケージが Firewall Management Center に追加された後、リモートアクセス VPN 構成で外部ブラウザが有効になった後にのみ、ブラウザが Firewall Threat Defense にプッシュされます。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[デバイス（Devices）] > [リモートアクセス（Remote Access）] で、リストされているリモートアクセスポリシーを選択および編集し、[詳細設定（Advanced）] タブを選択します。 を選択します

ステップ 2 **[Secure Clientイメージ（Secure Client Images）]** ページの **[Secure Client外部ブラウザパッケージ（Secure Client External Browser Package）]** の部分で、[追加（Add）] をクリックします。

ステップ 3 Secure Client パッケージの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 [参照（Browse）] をクリックしてアップロードする外部ブラウザパッケージを見つけます。

ステップ 5 [保存（Save）] をクリックしてイメージを Secure Firewall Management Center にアップロードします。

（注）
既存の外部ブラウザパッケージを使用してリモートアクセスVPN接続を更新する場合は、[パッケージファイル（Package File）] ドロップダウンからファイルを選択します。

ステップ 6 リモート アクセス VPN ポリシーを保存します。

関連トピック

Cisco Secure Client イメージ （1611 ページ）

リモート アクセス VPN のアドレス割り当てポリシー

Firewall Threat Defense デバイスは、IPv4 または IPv6 ポリシーを使用して、リモート アクセス VPN クライアントに IP アドレスを割り当てることができます。複数のアドレス割り当て方式を設定すると、Firewall Threat Defense デバイスは IP アドレスが見つかるまで各オプションを試行します。

IPv4 または IPv6 ポリシー

IPv4 または IPv6 ポリシーを使用すると、リモートアクセス VPN クライアントへの IP アドレスに対応できます。まず、IPv4 ポリシーを試してから、IPv6 ポリシーを試す必要があります。

- [承認サーバーを使用（Use Authorization Server）]：ユーザーごとに外部承認サーバーからアドレスを取得します。IP アドレスが設定された承認サーバを使用している場合は、この方式を使用することをお勧めします。アドレス割り当ては、RADIUS ベースの承認サーバでのみサポートされています。AD/LDAP ではサポートされていません。この方法は、IPv4 と IPv6 の両方の割り当てポリシーで使用できます。
- [DHCP を使用（Use DHCP）]：接続プロファイルに設定された DHCP サーバから IP アドレスを取得します。グループ ポリシーで DHCP ネットワーク範囲を設定することによって、DHCP サーバが使用できる IP アドレスの範囲を定義することもできます。DHCP を使用する場合は、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ネットワーク（Network）] ペインでサーバーを設定します。この方法は IPv4 の割り当てポリシーに使用できます。

DHCPネットワーク範囲の構成の詳細については、グループポリシー一般オプション（1431ページ）を参照してください。

- [内部アドレスプールを使用（Use an internal address pool）]：内部的に設定されたアドレスプールは、最も設定が簡単なアドレスプール割り当て方式です。この方式を使用する場合は、[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[アドレスプール（Address Pools）]ペインでIPアドレスプールを作成し、接続プロファイルで同じものを選択します。この方法は、IPv4とIPv6の両方の割り当てポリシーで使用できます。

- [IPアドレスが解放された後時間が経ってからIPアドレスを再利用することを許可（Allow reuse an IP address so many minutes after it is released）]：IPアドレスがアドレスプールに戻った後、IPアドレスの再使用を遅らせます。遅延時間を設けることにより、IPアドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、遅延はゼロに設定されています。遅延時間を延長する場合は、IPアドレスを再割り当てするまでの時間を0～480の範囲で指定します。この設定要素は、IPv4割り当てポリシーで使用できます。

関連トピック

接続プロファイルの設定（1585ページ）
リモートアクセスVPN認証（1561ページ）

証明書マップの設定

証明書マップを使用して、証明書フィールドの内容に基づいて接続プロファイルとユーザー証明書をマッチングするルールを定義できます。証明書マップにより、セキュアゲートウェイでの証明書認証が可能になります。

ルール、または証明書マップは、証明書マップオブジェクト（1425ページ）で定義されます。

手順

ステップ1 **[デバイス（Devices）]>[VPN]>[リモートアクセス（Remote Access）]**を選択します。

ステップ2 リストから既存のリモートアクセスVPNポリシーを選択し、対応する[編集（Edit）]アイコンをクリックします。

ステップ3 **[詳細（Advanced）]>[証明書マップ（Certificate Maps）]**を選択します。

ステップ4 [接続プロファイルマッピングの全般設定（General Settings for Connection Profile Mapping）]ペインから次のオプションを選択します。

選択肢は優先順位に基づいています。最初の選択肢が一致しない場合、オプションリストの次の選択肢が順番にマッチングされます。ルールが満たされたときにマッチングが完了します。ルールが満たされない場合、このページの下部に一覧表示されているデフォルトの接続プロファイルが接続に使用されます。次のいずれか、またはすべてのオプションを選択して、認証を確立し、クライアントにマッピングする必要がある接続プロファイル（トンネルグループ）を決定します。

- **グループ URL と証明書マップが異なる接続プロファイルと一致する場合、グループ URL を使用します**
- [設定したルールを使用して証明書を接続プロファイルと照合する（Use the configured rules to match a certificate to a Connection Profile）]：接続プロファイルマップで定義されているルールを使用するには、このオプションを有効にします。

（注）
証明書マッピングを設定することは、証明書に基づく認証を意味します。設定されている認証方法に関係なく、リモートユーザーはクライアント証明書を提供するよう求められます。

ステップ 5 [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Map）] セクションで、[マッピングの追加（Add Mapping）] をクリックし、このポリシーの証明書から接続プロファイルへのマッピングを作成します。

a) [証明書マップ名（Certificate Map Name）] オブジェクトを選択するか、作成します。
b) 証明書マップオブジェクトのルールが満たされた場合に使用する [接続プロファイル（Connection Profile）] を選択します。
c) [OK] をクリックして、マッピングを作成します。

ステップ 6 [保存（Save）] をクリックします。

グループ ポリシーの設定

グループポリシーはグループポリシーオブジェクト内に保存される属性と値の一連のペアで、リモートアクセス VPN のエクスペリエンスを定義します。たとえば、グループ ポリシー オブジェクトで、アドレス、プロトコル、接続設定などの一般的な属性を設定します。

ユーザーに適用されるグループ ポリシーは VPN トンネルが確立される際に決定されます。RADIUS 承認サーバーがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

（注） Firewall Threat Defense にグループポリシー属性の継承はありません。ユーザーについては、グループ ポリシー オブジェクトが全体として使用されます。ログイン時に AAA サーバーで特定されたグループ ポリシー オブジェクトが使用されるか、またはこれが指定されていない場合は、VPN 接続に対して設定されたデフォルトのグループ ポリシーが使用されます。指定されたデフォルトのグループポリシーはデフォルト値に設定できますが、これは、接続プロファイルに割り当てられ、他のグループポリシーがユーザーに対して特定されていない場合にのみ使用されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 **[詳細設定（Advanced）] > [グループポリシー（Group Policies）] > [追加（Add）]**を選択します。

ステップ 4 [使用可能なグループポリシー（Available Group Policy）] リストからグループポリシーを選択し、[追加（Add）] をクリックします。このリモートアクセス VPN ポリシーに関連付けるグループポリシーを 1 つ以上選択できます。

ステップ 5 [OK] をクリックして、グループ ポリシーの選択を完了します。

ステップ 6 変更を保存します。

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）

LDAP 属性マッピングの設定

LDAP 属性名により、LDAP ユーザーまたはグループの属性名が、シスコで理解される名前にマッピングされます。この属性マップにより、Active Directory（AD）または LDAP サーバーに存在する属性が、シスコの属性名と同一視されるようになります。任意の標準 LDAP 属性を既知のベンダー指定属性（VSA）にマッピングできます。1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングできます。リモートアクセス VPN 接続の確立中に AD または LDAP サーバーが Firewall Threat Defense デバイスに認証を返すと、Firewall Threat Defense デバイスは、その情報を使用して、セキュアクライアントが接続を完了する方法を調整できます。

VPN ユーザーにさまざまなアクセス許可や VPN コンテンツを提供する場合は、VPN サーバーでさまざまな VPN ポリシーを設定し、クレデンシャルに基づいてこれらのポリシーセットを各ユーザーに割り当てることができます。これを Firewall Threat Defense で実現するには、LDAP 属性マップを使用して LDAP 認可を設定します。LDAP を使用してグループポリシーをユーザーに割り当てるには、LDAP 属性をマッピングするマップを設定する必要があります。

LDAP 属性マップは、次の 3 つのコンポーネントで構成されます。

- [レルム（Realm）]：LDAP 属性マップの名前を指定します。名前は、選択したレルムに基づいて生成されます。
- [属性名マッピング（Attribute Name Mapping）]：LDAP ユーザーまたはグループの属性名を、シスコで理解される名前にマッピングします。
- [属性値マッピング（Attribute Value Mapping）]：LDAP ユーザーまたはグループの属性の値を、選択した名前マッピングのシスコ属性の値にマッピングします。

LDAP 属性マップで使用されるグループポリシーは、リモートアクセス VPN 構成のグループポリシーのリストに追加されます。リモートアクセス VPN 構成からグループポリシーを削除すると、関連付けられた LDAP 属性マッピングも削除されます。

バージョン 6.4 ～ 6.6 では、FlexConfig を使用してのみ LDAP 属性マップを設定できます。詳細については、「Configure AnyConnect Modules and Profiles Using FlexConfig」を参照してください。

バージョン 7.0 以降では、次の手順を使用できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 **[詳細設定（Advanced）]** > **[LDAP 属性マッピング（LDAP Attribute Mapping）]** をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [LDAP 属性マップの設定（Configure LDAP Attribute Map）] ページで、[レルム（Realm）] を選択して属性マップを設定します。

ステップ 6 [追加（Add）] をクリックします。

複数の属性マップを設定できます。各属性マップについて、名前マップと値マップを設定する必要があります。

（注）
LDAP 属性マップを作成する際は、次のガイドラインに従ってください。

- 1 つの LDAP 属性について少なくとも 1 つのマッピングを設定します。同じ LDAP 属性名を持つ複数のマッピングは許可されません。
- LDAP 属性マップを作成するには、少なくとも 1 つの名前マップを設定します。
- リモートアクセス VPN 構成の接続プロファイルに関連付けられていない LDAP 属性マップは削除できます。
- シスコと LDAP の**両方**の属性名および値について、LDAP 属性マップで正しいスペルと大文字/小文字を使用してください。

a) [LDAP 属性名（LDAP Attribute Name）] を指定し、リストから必要な [シスコ属性名（Cisco Attribute Name）] を選択します。
b) [値マップの追加（Add Value Map）] をクリックし、[LDAP 属性値（LDAP Attribute Value）] と [シスコ属性値（Cisco Attribute Value）] を指定します。

さらに値マップを追加するには、この手順を繰り返します。

ステップ 7 [OK] をクリックして LDAP 属性マップの設定を完了します。

ステップ 8 [保存（Save）] をクリックして LDAP 属性マッピングへの変更を保存します。

例

詳細な例については、「Configure RA VPN with LDAP Authentication and Authorization for FTD」を参照してください。

関連トピック

リモートアクセス VPN の AAA 設定 （1588 ページ）
権限および属性のポリシー実施の概要 （1563 ページ）

VPN ロード バランシングの設定

VPN ロードバランシングについて

Firewall Threat Defense の VPN ロードバランシングを使用すると、2 つ以上のデバイスを論理的にグループ化し、デバイス間でリモートアクセス VPN セッションを均等に分散できます。VPN ロードバランシングを使用すると、ロードバランシンググループ内のデバイス間でセキュアクライアント VPN セッションが共有されます。

VPN ロードバランシングは、スループットまたはその他の要因を考慮しない単純なトラフィックの分散に基づいています。VPN ロードバランシンググループは、2 つ以上の Firewall Threat Defense デバイスで構成されます。1 つのデバイスがディレクタとして機能し、その他のデバイスはメンバーデバイスとなります。グループのデバイスは、完全に同じタイプである必要はなく、同じソフトウェアバージョンや構成を使用する必要もありません。リモートアクセス VPN をサポートするすべての Firewall Threat Defense デバイスがロードバランシンググループに参加できます。Firewall Threat Defense は、Secure Client SAML 認証を使用した VPN ロードバランシングをサポートしています。

VPN ロードバランシンググループ内のすべてのアクティブなデバイスがセッションの負荷を伝送します。VPN ロードバランシングにより、トラフィックはグループ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

VPN ロードバランシングのコンポーネント

VPN ロードバランシングのコンポーネントは次のとおりです。

- **ロードバランシンググループ**：VPN セッションを共有するための 2 つ以上の Firewall Threat Defense デバイスの仮想グループ。

  VPN ロードバランシンググループは、同じリリースまたは混合リリースの Firewall Threat Defense デバイスで構成できますが、各デバイスでリモートアクセス VPN 構成がサポートされている必要があります。

  VPN ロードバランシングのグループ設定の構成（1621 ページ）およびロードバランシングの追加設定の構成 （1622 ページ）を参照してください。

- **ディレクタ**：グループの 1 つのデバイスがディレクタとして機能します。グループ内の他のメンバー間に負荷を分散させ、VPN セッションの提供に参加します。

ディレクタは、グループ内のすべてのデバイスをモニターし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。ディレクタの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在のディレクタで障害が発生すると、グループ内のメンバーデバイスの 1 つがその役割を引き継いで、すぐに新しいディレクタになります。

- **メンバー**：グループ内のディレクタ以外のデバイスは、メンバーと呼ばれます。ロードバランシングに参加し、リモートアクセス VPN 接続を共有します。

参加デバイスの設定の構成 （1622 ページ）。

VPN ロードバランシングの前提条件

- **証明書**：Firewall Threat Defense の証明書には、接続のリダイレクト先となるディレクタおよびメンバーの IP アドレスまたは FQDN が含まれている必要があります。そうしないと、証明書は信頼できないと見なされます。証明書ではサブジェクト代替名（SAN）またはワイルドカード証明書を使用する必要があります。
- [グループURL（Group URL）]：VPN ロードバランシンググループ IP アドレスのグループ URL を接続プロファイルに追加します。グループの URL を指定すると、ユーザーがログイン時にグループを選択する必要がなくなります。
- [IPアドレスプール（IP Address Pool）]：メンバーデバイスの一意の IP アドレスプールを選択し、メンバーデバイスごとに Firewall Management Center の IP アドレスプールをオーバーライドします。
- ネットワークアドレス変換（NAT）の背後にあるデバイスは、ロードバランシンググループに含めることもできます。

VPN ロード バランシングに関するガイドラインと制限事項

- VPN ロードバランシングはデフォルトでは無効になっています。VPN ロードバランシングは明示的にイネーブルにする必要があります。
- 同じ場所にある Firewall Threat Defense デバイスのみをロードバランシンググループに追加できます。
- ロードバランシンググループには、少なくとも 2 つの Firewall Threat Defense デバイスが必要です。
- Firewall Threat Defense 高可用性のデバイスは、ロードバランシンググループに参加できます。
- ネットワークアドレス変換（NAT）の背後にあるデバイスは、ロードバランシンググループに含めることもできます。
- メンバーまたはディレクタのデバイスがダウンすると、そのデバイスが提供するリモートアクセス VPN 接続が切断されます。VPN 接続を再度開始する必要があります。

- 各デバイスのアイデンティティ証明書には、サブジェクト代替名（SAN）またはワイルドカードが必要です。

VPN ロードバランシングのグループ設定の構成

VPN ロードバランシングを有効にし、ロードバランシンググループのすべてのメンバーに適用できるグループ設定を指定することができます。グループを作成するときに、ロードバランシングの参加設定を指定できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 **[詳細設定（Advanced）]** > **[ロードバランシング（Load Balancing）]** をクリックします。

ステップ 4 [メンバーデバイス間のロードバランシングを有効にする（Enable Load balancing between member devices）] トグルボタンをクリックして、ロードバランシングを有効にします。
[グループ設定の編集（Edit Group Configuration）] ページが開きます。グループパラメータは、ロードバランシンググループの下のすべてのデバイスに適用されます。

ステップ 5 必要に応じて、[グループIPv4アドレス（Group IPv4 Address）] と [グループIPv6アドレス（Group IPv6 Address）] を指定します。

ここで指定する IP アドレスはロードバランシンググループ全体で使用され、ディレクタは着信 VPN 接続用にこの IP アドレスを開きます。

ステップ 6 ロードバランシンググループの [通信インターフェイス（Communication Interface）] を選択します。[追加（Add）] をクリックして、インターフェイスグループまたはセキュリティゾーンを追加します。

通信インターフェイスは、ディレクタとメンバーが負荷に関する情報を共有するためのプライベート インターフェイスです。

ステップ 7 ディレクタとグループ内のメンバー間の通信に使用する [UDPポート（UDP Port）] を入力します。デフォルトのポートは 9023 です。

ステップ 8 [IPSec暗号化（IPsec Encryption）] トグルボタンをオンにして、ディレクタとメンバーの間の通信における IPsec 暗号化 を有効にします。

この暗号化を有効にすると、事前共有キーを使用して、ディレクタとメンバーの間に IPsec トンネルが確立されます。

[IPsec暗号化（IPsec Encryption）] オプションを有効にして Firewall Threat Defense デバイスをアップグレードまたはダウングレードする場合、展開の失敗を防ぐために、Firewall Management Center と Firewall Threat Defense の間に設定の不一致がないことを確認してください。

ステップ 9 IPSec 暗号化の [暗号化キー（Encryption Key）] を入力し、暗号化キーを確認します。

ステップ 10 **[OK]** をクリックします。

ロードバランシングの追加設定の構成

VPN ロードバランシングの追加設定には、FQDN および IKEv2 リダイレクトが含まれます。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 **[詳細設定（Advanced）]** > **[ロードバランシング（Load Balancing）]** をクリックします。

ステップ 4 まだ有効にしていない場合は、[メンバーデバイス間のロードバランシングを有効にする（Enable Load balancing between member devices）] トグルボタンをオンにして、ロードバランシングを有効にします。

ステップ 5 [設定（Settings）] をクリックします。

ステップ 6 完全修飾ドメイン名を使用したリダイレクトを有効にするには、[IPの代わりにFQDNをピアデバイスに送信する（Send FQDN to peer devices instead of IP）] トグルボタンをオンにします。

デフォルトでは、Firewall Threat Defense は VPN ロードバランシングのリダイレクトで IP アドレスだけをクライアントに送信します。

ステップ 7 [IKEv2リダイレクト（IKEv2 Redirect）] フェーズのいずれかを選択します。

- **[SA認証中のリダイレクト（Redirect during SA authentication）]**
- [SA初期化中のリダイレクト（Redirect during SA initialization）]

ステップ 8 [OK] をクリックします。

ステップ 9 変更を保存します。

参加デバイスの設定の構成

デバイスの参加設定では、デバイスが VPN ロードバランシングでどのように負荷を共有するかを決定します。デバイスでVPNロードバランシングを有効にし、デバイス固有のプロパティを定義することにより、参加するデバイスを設定します。これらの値はデバイスによって異なります。ロードバランシングに参加しているデバイスの優先順位番号を指定できます。優先順位番号が大きいほど、そのデバイスは、他のデバイスよりもディレクタになる可能性が高くなります。ただし、グループのディレクタになるデバイスを選択することはできません。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 変更するリモートアクセス VPN ポリシーの横にある [編集（Edit）] をクリックします。

ステップ 3 **[詳細設定（Advanced）]** > **[ロードバランシング（Load Balancing）]** をクリックします。

ステップ 4 まだ有効にしていない場合は、[メンバーデバイス間のロードバランシングを有効にする（Enable Load balancing between member devices）] トグルボタンをオンにして、ロードバランシングを有効にします。

ステップ 5 [デバイスの参加（Device Participation）] 設定を構成します。

[デバイスの参加（Device Participation）] セクションには、選択したリモートアクセス VPN 設定のすべてのターゲットデバイスが一覧表示されます。これらのデバイスは、着信 VPN セッションの負荷を共有するように設定できます。

a) [ロードバランシング（Load Balancing）] トグルボタンをオンにしてデバイスのロードバランシングを有効にし、[編集（Edit）] をクリックします。

b) デバイスの [優先順位（Priority）] を入力します。

デフォルトでは、デバイスの優先順位は 5 に設定されています。1 ～ 10 の番号を選択できます。

c) デバイスが NAT の背後にある場合は、VPN インターフェイスの IP アドレスに [IPv4 NAT] または [IPv6 NAT] アドレスを指定します。

d) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、リモートアクセス VPN ポリシー設定を保存します。

リモート アクセス VPN の IPsec の設定

IPsec 設定は、リモート アクセス VPN ポリシーを設定する際に、VPN プロトコルとして IPsec を選択した場合にのみ適用可能です。そうでない場合は、[アクセス インターフェイスの編集（Edit Access Interface）] ダイアログボックスを使用して、IKEv2 を有効にすることができます。詳細については、リモートアクセス VPN のアクセスインターフェイスの設定（1608 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] をクリックします。

IPsec 設定のリストは、画面左側のナビゲーション ウィンドウに表示されます。

ステップ 4 ナビゲーション ウィンドウを使用して、次の IPsec オプションを編集します。

a) 暗号マップ（Crypto Maps）：[暗号マップ（Crypto Maps）] ページには、IKEv2 プロトコルが有効になっているインターフェイス グループがリストされます。暗号マップは、IKEv2 プロトコルが有効になっているインターフェイス用に自動生成されます。暗号マップを編集するには、リモート アクセス VPN 暗号マップの設定（1624 ページ）を参照してください。[アクセスインターフェイス（Access Interface）] で、選択した VPN ポリシーのイン

ターフェイスグループを追加または削除できます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （1608 ページ）を参照してください。

b) [IKEポリシー（IKE Policy）]：[IKEポリシー（IKE Policy）] ページには、Secure Client エンドポイントが IPsec プロトコルを使用して接続している場合、選択した VPN ポリシーに適用可能なすべての IKE ポリシーオブジェクトが一覧表示されます。詳細については、リモート アクセス VPN での IKE ポリシー （1627 ページ）を参照してください。新しい IKE ポリシーを追加するには、IKEv2 ポリシー オブジェクトの設定 （1444 ページ）を参照してください。Firewall Threat Defense がサポートしているのは Secure Client IKEv2 クライアントのみです。サードパーティ標準の IKEv2 クライアントはサポートされていません。

c) [IPsec/IKEv2 パラメータ（IPsec/IKEv2 Parameters）]：[IPsec/IKEv2 パラメータ（IPsec/IKEv2 Parameters）] ページでは、IKEv2 セッション設定、IKEv2 セキュリティ アソシエーション設定、IPsec 設定、および NAT 透過設定を変更できます。詳細については、「リモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定 （1628 ページ）」を参照してください。

ステップ 5 [保存（Save）] をクリックします。

リモート アクセス VPN 暗号マップの設定

暗号マップは、IPsec-IKEv2 プロトコルが有効になっているインターフェイス用に自動生成されます。[アクセスインターフェイス（Access Interface）] で、選択した VPN ポリシーのインターフェイスグループを追加または削除できます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （1608 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [暗号マップ（Crypto Maps）] をクリックし、テーブルの行を選択し、[編集（Edit）] をクリックして暗号マップのオプションを編集します。

ステップ 4 [IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposals）] を選択し、トランスフォーム セットを選択して、トンネル内のトラフィックの保護に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。

ステップ 5 [リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] を選択し、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。

ステップ 6 [クライアントサービスの有効化（Enable Client Services）] を選択し、ポート番号を指定します。

クライアント サービス サーバーは、HTTPS（SSL）アクセスを提供します。これにより、Secure Client ダウンローダは、ソフトウェアアップグレード、プロファイル、ローカリゼーションおよびカスタマイゼーション ファイル、CSD、SCEP、およびクライアントが必要とするその他のファイルダウンロードを受信できます。このオプションを選択した場合は、クライアント

サービスのポート番号を指定します。クライアント サービス サーバーを有効にしない場合、ユーザーは、Secure Client が必要とする可能性があるこれらのファイルをダウンロードできません。

（注）
同じデバイスで実行する SSL VPN に対して同じポートを使用できます。SSL VPN を設定した場合でも、IPsec-IKEv2 クライアントで SSL を介してファイルをダウンロードするには、このオプションを選択する必要があります。

ステップ 7 [Perfect Forward Secrecyの有効化（Enable Perfect Forward Secrecy）] を選択し、[係数グループ（Modulus Group）] を選択します。

暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイントデバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。

係数グループは、2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループです。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。リモート アクセス VPN 設定を許可する係数グループを選択します。

- [1]：Diffie-Hellman グループ 1（768 ビット係数）。
- [2]：Diffie-Hellman グループ 2（1024 ビット係数）。
- [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。
- [14]：Diffie-Hellman グループ 14（2048 ビット係数。128 ビット キーの保護に推奨される）。
- [19]：Diffie-Hellman グループ 19（256 ビットの楕円曲線フィールド サイズ）。
- [20]：Diffie-Hellman グループ 20（384 ビットの楕円曲線フィールド サイズ）。
- [21]：Diffie-Hellman グループ 21（521 ビットの楕円曲線フィールド サイズ）。
- [24]：Diffie-Hellman グループ 24（2048 ビット係数および 256 ビット素数位数サブグループ）。

ステップ 8 [ライフタイム継続時間（秒数）（Lifetime Duration (seconds)）] を指定します。

セキュリティ アソシエーション（SA）のライフタイム（秒数）。このライフタイムを超えると、SAの期限が切れ、2つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKEネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

120 ～ 2147483647 秒の値を指定できます。デフォルトは 28800 秒です。

ステップ 9 [ライフタイムのサイズ（KB）（Lifetime Size (kbytes)）] を指定します。

特定のセキュリティ アソシエーションが期限切れになる前にそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。

10 ～ 2147483647 KB の値を指定できます。デフォルトは 4,608,000 KB です。無限のデータを指定することはできません。

ステップ 10 次の [ESPv3設定（ESPv3 Settings）] を選択します。

- [着信ICMPのエラーメッセージを検証（Validate incoming ICMP error messages）]：IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先の ICMP エラー メッセージを検証するかどうかを選択します。
- [「フラグメント禁止」ポリシーを有効にする（Enable 'Do Not Fragment' Policy）]：IP ヘッダーに Do-Not-Fragment（DF）ビット セットを使用する大量のパケットを IPsec サブシステムがどのように処理するかを定義し、[ポリシー（Policy）] リストからいずれかの項目を選択します。
  - コピー（Copy）：DF ビットを保持します。
  - クリア（Clear）：DF ビットを無視します。
  - 設定（Set）：DF ビットを設定して使用します。
- [トラフィックフロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）] を選択：トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。[バースト（Burst）]、[ペイロード サイズ（Payload Size）]、および[タイムアウト（Timeout）]パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

  （注）
  トラフィックフロー機密保持（TFC）パケットを有効にすると、VPN トンネルがアイドル状態になることが防止されます。そのため、TFC パケットを有効にすると、グループポリシーで設定された VPN アイドルタイムアウトが期待どおりに機能しません。グループ ポリシーの詳細オプション （1438 ページ）を参照してください。

  - バースト（Burst）：1 ～ 16 バイトの値を指定します。
  - ペイロード サイズ（Payload Size）：64 ～ 1024 バイトの値を指定します。
  - タイムアウト（Timeout）：10 ～ 60 秒の値を指定します。

ステップ 11 **[OK]** をクリックします。

関連トピック

インターフェイス（Interface） （1346 ページ）

リモート アクセス VPN での IKE ポリシー

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

（注） Firewall Threat Defense は、リモート アクセス VPN では IKEv2 のみサポートします。

IKEv1 とは異なり、IKEv2 プロポーザルでは、1 つのポリシーで複数のアルゴリズムとモジュラス グループを選択できます。フェーズ 1 のネゴシエーションでピアを選択するため、1 つの IKE プロポーザルを作成することもできますが、複数の異なるプロポーザルを作成して、最も望ましいオプションに高い優先順位を設定することも検討してください。IKEv2 では、ポリシー オブジェクトは認証の指定は行わず、他のポリシーで認証の要件を定義する必要があります。

リモート アクセス IPsec VPN を設定する際には IKE ポリシーが必要です。

リモート アクセス *VPN IKE* ポリシーの設定

IKE ポリシーテーブルには、IPsec プロトコルを使用して Secure Client のエンドポイントを接続する場合に、選択した VPN 設定で利用可能なすべての IKE ポリシーオブジェクトを記述します。詳細については、リモート アクセス VPN での IKE ポリシー（1627 ページ）を参照してください。

（注） Firewall Threat Defense では、リモート アクセス VPN の IKEv2 のみに対応しています。

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [IKEポリシー（IKE Policy）] をクリックします。

ステップ 4 [追加（Add）] をクリックして、利用可能な IKEv2 ポリシーから選択するか、新しい IKEv2 ポリシーを追加して、次の項目を指定します。

- [Name（名前）]：IKEv2 ポリシーの名前。
- [説明（Description）]：IKEv2 ポリシーの任意の説明
- [優先度（Priority）]：このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。
- [ライフタイム（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（秒数）。
- [整合性（Integrity）]：IKEv2 ポリシーで使用されるハッシュ アルゴリズムの整合性アルゴリズム部分です。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズムです。
- [PRFハッシュ（PRF Hash）]：IKE ポリシーに使用されるハッシュ アルゴリズムの疑似乱数関数（PRF）部分です。IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。
- [DHグループ（DH Group）]：暗号化に使用する Diffie-Hellman グループです。

ステップ 5 [保存（Save）] をクリックします。

リモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定

手順

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [IPsec] > [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] をクリックします。

ステップ 4 [IKEv2セッション設定（IKEv2 Session Settings）] で次の項目を選択します。

- [ピアに送信されるID（Identity Sent to Peers）]：IKE ネゴシエーションでピアが自身の識別に使用する ID を選択します。
  - [自動（Auto）]：接続タイプごとの IKE ネゴシエーションを決定します。事前共有キー用の IP アドレス、証明書認証のための Cert DN（非対応）。
  - [IPアドレス（IP address）]：ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
  - ホスト名（Hostname）：ISAKMP 識別情報を交換するホストの完全修飾ドメイン名（FQDN)）を使用します。この名前は、ホスト名とドメイン名で構成されます。

- [トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect]：管理者は、SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にすることができます。デフォルトでは、[この通知を送信する（Sending this notification）] は無効になっています。
- [すべてのセッションが終了するまでデバイスの再起動を許可しない（Do not allow device reboot until all sessions are terminated）]：オンにすると、すべてのアクティブなセッションが自主的に終了してからシステムが再起動されます。デフォルトでは、無効になっています。

ステップ 5 [IKEv2セキュリティアソシエーションIKEv（SA）の設定（IKEv2 Security Association (SA) Settings）] で次の項目を選択します。

- [クッキーチャレンジ（Cookie Challenge）]：SA 開始パケットに応答してピア デバイスにクッキーチャレンジを送信するかどうかを選択します。阻止サービス妨害（DoS）攻撃に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキーチャレンジを使用します。次のオプションのいずれか1つを選択します。
  - [カスタム（Custom）]：[着信クッキーチャレンジのしきい値（Threshold to Challenge Incoming Cookies）] を指定します。これは許可されるネゴシエーション中の SA の総数の割合です。この設定を指定すると、以降のSAネゴシエーションに対してクッキーチャレンジがトリガーされます。範囲は 0 ～ 100 % です。デフォルトは 50% です。
  - [常時（Always）]：ピア デバイスにクッキー チャレンジを常に送信します。
  - [不可（Never）]：ピア デバイスにクッキー チャレンジを送信しません。
- [許可されるネゴシエーション中のSAの数（Number of SAs Allowed in Negotiation）]：一時点でのネゴシエーション中 SA の総数を制限します。クッキー チャレンジと共に使用する場合は、有効なクロス チェックが実行されるようにするため、クッキー チャレンジのしきい値をこの制限値よりも低くしてください。デフォルトは 100 % です。
- [許可されるSAの最大数（Maximum number of SAs Allowed）]：許可される IKEv2 接続の数を制限します。

ステップ 6 [IPsec設定（IPsec Settings）] で次の項目を選択します。

- [暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）]：このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。
- [パスの最大伝送ユニットのエージング（Path Maximum Transmission Unit Aging）]：PMTU（パスの最大伝送ユニット）のエージング（SA（セキュリティ アソシエーション）のリセット PMTU までのインターバル）が可能であるかを確認します。

- [値のリセット間隔（Value Reset Interval）]：SA（セキュリティ アソシエーション）の PMTU 値が元の値にリセットされるまでの時間（分）を入力します。有効範囲は 10 ～ 30 分です。デフォルトは無制限です。

ステップ 7 [NAT設定（NAT Settings）] で次の項目を選択します。

- [キープアライブメッセージトラバーサル（Keepalive Messages Traversal）]：NAT キープアライブ メッセージ トラバーサルを有効にするかどうかを設定します。VPN 接続ハブとスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブ メッセージを転送するために NAT トラバーサル キープアライブを使用します。このデバイスでは、IPsec フローで NAT を実行します。このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス間でキープアライブ信号が送信される間隔（秒）を設定します。値は 10 ～ 3600 秒となります。デフォルトは 20 秒です。
- [間隔（Interval）]：NAT キープ アライブ間隔を 10 ～ 3600 秒に設定します。デフォルトは 20 秒です。

ステップ 8 [保存（Save）] をクリックします。

Secure Client 管理 VPN トンネルの設定

管理 VPN トンネルは、VPN ユーザーが VPN に接続しなくても、クライアントシステムの電源が入るたびに社内ネットワークへの接続を提供します。これにより、組織はソフトウェアのパッチと更新でエンドポイントを最新の状態に保つことができます。ユーザーが開始した VPN トンネルが確立されると、管理トンネルは切断されます。

このセクションでは、Firewall Threat Defense での Secure Client 管理 VPN トンネルの設定に関する情報を提供します。Firewall Management Center インターフェイスを使用して Firewall Threat Defense で Secure Client 管理トンネルを設定するには、次の設定が必要です。

- 証明書ベースの認証とグループ URL を使用する**接続プロファイル**。
- **Secure Client 管理 VPN プロファイルファイル**。必要に応じて、グループ URL およびバックアップサーバーを使用してサーバーを設定します。
- 管理 VPN プロファイル、明示的に含まれるネットワークによるスプリットトンネリング、およびクライアント バイパス プロトコルを使用し、バナーがなしの**グループポリシー**。

Secure Client 管理 VPN トンネルを設定する詳細な手順については、Firewall Threat Defense での Secure Client 管理 VPN トンネルの設定 （1632 ページ）を参照してください。

Secure Client 管理 VPN トンネルの要件と前提条件

ソフトウェア要件および設定要件

Firewall Management Center Web インターフェイスを使用する Firewall Threat Defense を使用して Secure Client 管理トンネルを設定する前に、次のものが揃っていることを確認します。

- Firewall Threat Defense および Firewall Management Center バージョン 6.7.0 以降を使用していることを確認します。
- Secure ClientSecure Client VPN Web 展開パッケージ 4.7 以降をダウンロードし、Firewall Threat Defense リモートアクセス VPN にアップロードします。
- 接続プロファイルで証明書認証が設定されていることを確認します。
- グループポリシーでバナーが設定されていないことを確認します。
- 管理トンネルグループポリシーのスプリットトンネリング設定を確認します。

証明書の要件

- Firewall Threat Defense にはリモートアクセス VPN の有効な ID 証明書が必要であり、ローカル認証局（CA）からのルート証明書が Firewall Threat Defense に存在する必要があります。
- 管理 VPN トンネルに接続するエンドポイントには、有効な ID 証明書が必要です。
- Firewall Threat Defense の ID 証明書の CA 証明書をエンドポイントにインストールし、エンドポイントの CA 証明書を Firewall Threat Defense にインストールする必要があります。
- 同じローカル CA によって発行された ID 証明書がマシンストア内に存在する必要があります。

  証明書ストア（Windows の場合）および/またはシステムキーチェーン（MacOS の場合）内です。

Secure Client 管理 VPN トンネルの制限事項

- Secure Client 管理 VPN トンネルは証明書認証のみをサポートし、AAA ベースの認証はサポートしていません。
- パブリックまたはプライベートのプロキシ設定はサポートされていません。
- 管理 VPN トンネルが接続されている場合、Secure Client のアップグレードと AnyConnect モジュールのダウンロードはサポートされません。

Firewall Threat Defense での Secure Client 管理 VPN トンネルの設定

手順

ステップ 1 ウィザードを使用してリモートアクセス VPN ポリシー構成を作成します。

リモートアクセス VPN の構成については、新規リモートアクセス VPN 接続の設定（1570 ページ）を参照してください。

ステップ 2 管理 VPN トンネルの接続プロファイル設定を構成します。

（注）
Secure Client 管理 VPN トンネルにのみ使用する新しい接続プロファイルを作成することをお勧めします。

a) 作成したリモートアクセス VPN ポリシーを編集します。
b) 管理 VPN トンネルに使用する接続プロファイルを選択して編集します。
c) [AAA] > [認証方式（Authentication Method）] をクリックし、[クライアント証明書のみ（Client Certificate Only）] をクリックします。必要に応じて、許可とアカウンティングの設定を構成します。
d) 接続プロファイルの [エイリアス（Aliases）] タブをクリックします。
e) [URLエイリアス（URL Aliases）] の下にある [追加（+）（Add (+)）] をクリックし、接続プロファイルの [URLエイリアス（URL Alias）] をクリックします。
f) [有効（Enabled）] をクリックして、URL を有効にします。
g) [OK] をクリックし、[保存（Save）] をクリックして接続プロファイル設定を保存します。

接続プロファイル設定の詳細については、接続プロファイルの設定（1585 ページ）を参照してください。

ステップ 3 Secure Client プロファイルエディタを使用して、管理トンネルプロファイルを作成します。

a) Cisco Software Download Center から Secure Client **VPN Management Tunnel Standalone Profile Editor** をまだダウンロードしていない場合はダウンロードします。
b) VPN ユーザーに必要な設定を使用して管理トンネルプロファイルを作成し、ファイルを保存します。
c) 接続プロファイルで構成したグループ URL を使用して、[サーバーリスト（Server List）] でサーバーを構成します。

プロファイルエディタを使用した管理プロファイルの作成方法の詳細については、*Cisco Secure Client（AnyConnect を含む）管理者ガイド* [英語] を参照してください。

ステップ 4 管理トンネルオブジェクトを作成します。

a) Secure Firewall Management Center Web インターフェイスで、**[オブジェクト（Object）]** > **[オブジェクト管理（Object Management）]** > **[VPN]** > **[Secure Client ファイル（Secure Client File）]** に移動します。
b) **[Secure Client ファイルの追加（Add Secure Client File）]** をクリックします。

c) Secure Client ファイルの [名前（Name）] を指定します。
d) [参照（Browse）] をクリックし、保存した管理トンネル プロファイル ファイルを選択します。
e) [ファイルタイプ（File Type）] ドロップダウンをクリックし、**[Secure Client管理VPNプロファイル（Secure Client Management VPN Profile）]** を選択します。
f) [保存（Save）] をクリックします。

（注）
グループポリシーの Secure Client 設定を作成または更新するときに、管理トンネルオブジェクトも作成します。グループポリシーのセキュアクライアントオプション（1434ページ）を参照してください。

ステップ 5 **管理プロファイルをグループポリシーに関連付け、グループポリシー設定を構成します。**

管理トンネル VPN 接続に使用する接続プロファイルに関連付けられているグループポリシーに管理 VPN プロファイルを追加する必要があります。ユーザーが接続すると、グループポリシーにすでにマッピングされているユーザー VPN トンネルとともに管理 VPN プロファイルがダウンロードされ、管理 VPN トンネル機能が有効になります。

注意
[バナーなし（No Banner）]：グループポリシー設定でバナーが設定されていないことを確認します。バナー設定は、**[グループポリシー（Group Policy）]** > **[一般設定（General Settings）]** > **[バナー（Banner）]** で確認できます。

a) 管理 VPN トンネル用に作成した接続プロファイルを編集します。
b) **[グループポリシーの編集（Edit Group Policy）]** > **[Secure Client]** > **[管理プロファイル（Management Profile）]**をクリックします。
c) [管理VPNプロファイル（Management VPN Profile）] ドロップダウンをクリックし、作成した管理プロファイル ファイル オブジェクトを選択します。

（注）
[+] をクリックして、新しい Secure Client 管理 VPN プロファイルオブジェクトを追加することもできます。

d) [保存（Save）] をクリックします。

ステップ 6 **グループポリシーにスプリットトンネリングを設定します。**

a) **[グループポリシーの編集（Edit Group Policy）]** > **[全般（General）]** > **[スプリットトンネリング（Split Tunneling）]** をクリックします。
b) [IPv4スプリットトンネリング（IPv4 Split Tunneling）] または [IPv6スプリットトンネリング（IPv6 Split Tunneling）] ドロップダウンから [以下に指定したネットワークをトンネリングする（Tunnel networks specified below）] を選択します。
c) スプリット トンネル ネットワーク リスト タイプとして [標準アクセスリスト（Standard Access List）] または [拡張アクセスリスト（Extended Access List）] を選択し、管理 VPN トンネル経由のトラフィックを許可するために必要なアクセスリストを選択します。
d) [保存（Save）] をクリックして、スプリットトンネリング設定を保存します。

[Secure Client][カスタム属性（Custom Attribute）]

Secure Client 管理 VPN トンネルには、デフォルトでスプリット インクルード トンネリング構成が必要です。スプリットトンネリングを使用してすべてをトンネリングする管理 VPN トンネルを展開するようにグループポリシーで Secure Client カスタム属性を設定する場合、Firewall Management Center 6.7 Web インターフェイスは Secure Client カスタム属性をサポートしていないため、FlexConfig を使用して設定できます。

次に、Secure Client カスタム属性のコマンド例を示します。

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

ステップ 7　リモートアクセス VPN ポリシーを展開、検証、およびモニターします。

a) 管理 VPN トンネル構成を Firewall Threat Defense に展開します。

（注）
クライアントシステムは、Firewall Threat Defense リモートアクセス VPN に 1 回接続して、管理トンネル VPN プロファイルをクライアントマシンにダウンロードする必要があります。

b) **[Secure Mobility Client]** > **[VPN]** > **[統計（Statistics）]**で Secure Client 管理 VPN トンネルを確認できます。

show vpn-sessiondb anyconnect コマンドを使用して、Firewall Threat Defense コマンドプロンプトで管理 VPN セッションの詳細を確認することもできます。

c) Firewall Management Center Web インターフェイスで、[分析（Analysis）] をクリックして、管理トンネルセッション情報を表示します。

関連トピック

接続プロファイルの設定 （1585 ページ）
Firewall Threat Defense グループ ポリシー オブジェクト （1430 ページ）

複数証明書認証

複数証明書ベースの認証を使用すると、Firewall Threat Defense で SSL または IKEv2 EAP フェーズで セキュアクライアント を使用して VPN アクセスを許可するためにユーザーのアイデンティティ証明書を認証することに加えて、マシンまたはデバイス証明書を検証して、デバイスが会社支給のデバイスであることを確認できます。

複数証明書オプションを使用すると、証明書を通じたマシンとユーザー両方の証明書認証が可能になります。このオプションを使用しない場合は、マシンまたはユーザーのいずれかの証明書認証のみを実行できます。両方は実行できません。

複数証明書認証のガイドラインと制限事項

（注） 複数の証明書認証を設定する場合は、Cisco セキュアクライアントのプロファイル設定で **AutomaticCertSelection** の値を true に設定してください。

- 複数証明書認証では、現在、証明書の数が 2 に制限されています。
- セキュアクライアントで、複数証明書認証のサポートが示されている必要があります。そうでない場合、ゲートウェイで従来の認証方法のいずれかが使用されるか、接続に失敗します。Secure Client バージョン 4.4.04030 以降では、複数証明書ベースの認証がサポートされています。
- Secure Client では、RSA ベースの証明書のみがサポートされています。
- Secure Client 集約認証の間は、SHA256、SHA384、および SHA512 ベースの証明書のみがサポートされています。
- 証明書認証を SAML 認証と組み合わせることはできません。

複数証明書認証の設定

始める前に

複数証明書認証を設定する前に、各 Firewall Threat Defense デバイスの ID 証明書を取得するために使用される証明書登録オブジェクトが設定されていることを確認します。詳細については、証明書マップオブジェクト （1425 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** を選択します。

ステップ 2 リモートアクセス VPN ポリシーを選択し、[編集（Edit）] をクリックします。

（注）
リモートアクセス VPN を設定していない場合は、[追加（Add）] をクリックして新しいリモートアクセス VPN ポリシーを作成します。

ステップ 3 複数証明書認証を設定するには、接続プロファイルを選択して [編集（Edit）] します。

ステップ 4 [AAA] 設定をクリックし、[認証方式（Authentication Method）] > [クライアント証明書のみ（Client Certificate Only）] または [クライアント証明書と AAA（Client Certificate & AAA）] を選択します。

（注）

[クライアント証明書とAAA（Client Certificate & AAA）] の認証方式を選択した場合は、[認証サーバー（Authentication Server）] を選択します

ステップ 5 [複数の証明書認証を有効にする（Enable multiple certificate authentication）] チェックボックスを選択します。

ステップ 6 [クライアント証明書からのユーザー名のマッピング（Map username from client certificate）] に 1 つの証明書を選択します。

- [First Certificate]：VPN クライアントから送信されたマシン証明書からユーザー名をマッピングするには、このオプションを選択します。
- [Second Certificate]：クライアントから送信されたユーザー証明書からユーザー名をマッピングするには、このオプションを選択します。

証明書のみの認証が有効になっている場合は、クライアントから送信されたユーザー名が、VPN セッションのユーザー名として使用されます。AAA と証明書の認証が有効になっている場合は、VPN セッションのユーザー名は事前入力オプションに基づいています。

（注）
クライアント証明書のユーザー名が含まれる [マップ固有フィールド（Map Specific Field）] オプションを選択すると、[プライマリ（Primary）] および [セカンダリ（Secondary）] フィールドに [CN（一般名）（CN (Common Name)）] と [OU（組織ユニット）（OU (Organisational Unit)）] のデフォルト値がそれぞれ表示されます。

[DN（識別名）全体をユーザー名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザー ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザーを拡張証明書認証に使用される接続プロファイル DN ルールと照合するときに識別子として使用できます。

[クライアント証明書とAAA（Client Certificate & AAA）] の認証を選択した場合、[ユーザーログインウィンドウに証明書からユーザー名を事前に入力（Prefill username from certificate on user login window）] オプションを選択すると、ユーザーが Cisco Secure Client の AnyConnect VPN モジュール経由で接続したときにクライアント証明書からセカンダリユーザー名を事前に入力されます。

- [ログイン ウィンドウでユーザー名を非表示にする（Hide username in login window）]：セカンダリユーザー名はクライアント証明書から事前に入力されますがユーザーには表示されず、ユーザーが事前に入力されたユーザー名を変更しないようにします。

ステップ 7 リモートアクセス VPN に必要な AAA 設定と接続プロファイル設定を設定します。

ステップ 8 接続プロファイルとリモートアクセス VPN の設定を保存し、Firewall Threat Defense デバイスに展開します。

関連トピック

リモートアクセス VPN の AAA 設定 （1588 ページ）

リモート アクセス VPN の AAA の設定のカスタマイズ

ここでは、リモート アクセス VPN の AAA プリファレンスのカスタマイズについて説明します。詳細については、「リモートアクセス VPN の AAA 設定（1588 ページ）」を参照してください。

クライアント証明書を使用した VPN ユーザーの認証

ウィザードを使用するか、またはポリシーを後で編集することによって新しいリモートアクセス VPN ポリシーを作成するときに、クライアント証明書を使用してリモートアクセス VPN 認証を設定できます。

始める前に

VPN ゲートウェイとして機能する各 Firewall Threat Defense デバイスにアイデンティティ証明書を取得するために使用する証明書登録オブジェクトを設定します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）]をクリックします。または、[追加（Add）] をクリックして、新しいリモートアクセス VPN ポリシーを作成します。

ステップ 3 新しいリモートアクセス VPN ポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアントプロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 **[AAA] > [認証方式（Authentication Method）] > [クライアント証明書のみ（Client Certificate Only）]** をクリックします。

この認証方式では、ユーザーはクライアント証明書を使用して認証されます。VPN クライアントエンドポイントで設定する必要があります。デフォルトでは、ユーザー名はクライアント証明書フィールド CN および OU からそれぞれ派生します。クライアント証明書の他のフィールドにユーザー名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

クライアント証明書のユーザー名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、それぞれのデフォルト値である [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] が表示されます。[DN全体をユーザー名として使用（Use entire DN as username）] オプションを選択した場合、ユーザー ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザーを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

- [固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれます。
  - C（国）
  - CN（一般名）
  - DNQ（DN 修飾子
  - EA（電子メール アドレス）
  - GENQ（世代識別子）
  - GN（姓名の名）
  - I（イニシャル）
  - L（地名）
  - N（名前）
  - O（組織）
  - OU（組織ユニット）
  - SER（シリアル番号）
  - SN（姓名の姓）
  - SP（都道府県）
  - T（タイトル）
  - UID（ユーザー ID）
  - UPN（ユーザー プリンシパル名）
- どの認証方式を選択する場合にも、[ユーザーが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

詳細については、リモートアクセス VPN の AAA 設定 （1588 ページ）を参照してください。

ステップ 5 変更を保存します。

関連トピック

接続プロファイルの設定 （1585 ページ）
証明書の登録オブジェクトの追加 （1365 ページ）

クライアント証明書と AAA サーバー経由での VPN ユーザー認証の設定

クライアント証明書と認証サーバーの両方を使用するようにリモートアクセス VPN 認証を設定する場合、VPN クライアント認証は、クライアント証明書の検証と AAA サーバーの両方を使用して実行されます。

始める前に

- VPN ゲートウェイとして機能する各 Firewall Threat Defense デバイスのアイデンティティ証明書を取得するために使用する証明書登録オブジェクトを設定します。
- RADIUS サーバー グループ オブジェクトと、このリモートアクセス VPN ポリシー設定で使用する AD または LDAP レルムを設定します。
- リモートアクセス VPN 設定が機能するように AAA サーバーに Secure Firewall Threat Defense デバイスからアクセスできることを確認します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）]>[リモートアクセス（Remote Access）] を選択します。

ステップ 2 認証を更新するリモートアクセス VPN ポリシーの [編集（Edit）] をクリックするか、[追加（Add）] をクリックして新しいポリシーを作成します。

ステップ 3 新しいリモートアクセス VPN ポリシーを作成する場合は、接続プロファイル設定の選択時に認証を設定します。既存の設定の場合は、クライアントプロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] に移動し、[認証方式（Authentication Method）] ドロップダウンから、[クライアント証明書とAAA（Client Certificate & AAA）] を選択します。

- [認証方式（Authentication Method）] の選択に応じて、次のようになります。

  [クライアント認証と AAA（Client Certificate & AAA）]：両方のタイプの認証が実行されます。

  - [AAA]：[認証サーバー（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバーは同じ値になります。ドロップダウン リストから [アカウンティング サーバー（Accounting Server）] を選択します。認証サーバー ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[許可サーバー（Authorization Server）] と [アカウンティング サーバー（Accounting Server）] をそれぞれ手動で選択する必要があります。
  - [クライアント証明書（Client Certificate）]：クライアント証明書を使用してユーザーを認証します。VPN クライアントエンドポイントでクライアント証明書を設定する必要があります。デフォルトでは、ユーザー名はクライアント証明書フィールドの CN

およびOUからそれぞれ取得されます。クライアントプロファイルの他のフィールドを使用してユーザー名を指定する場合は、[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

クライアント証明書のユーザー名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN全体をユーザー名として使用（Use entire DN as username）] オプションを選択した場合、ユーザー ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザーを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

[固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。

- C（国）
- CN（一般名）
- DNQ（DN 修飾子
- EA（電子メール アドレス）
- GENQ（世代識別子）
- GN（姓名の名）
- I（イニシャル）
- L（地名）
- N（名前）
- O（組織）
- OU（組織ユニット）
- SER（シリアル番号）
- SN（姓名の姓）
- SP（都道府県）
- T（タイトル）
- UID（ユーザー ID）
- UPN（ユーザー プリンシパル名）

- どの認証方式を選択する場合にも、[ユーザーが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

詳細については、リモートアクセス VPN の AAA 設定 （1588 ページ）を参照してください。

ステップ 5 変更を保存します。

関連トピック

接続プロファイルの設定 （1585 ページ）
証明書の登録オブジェクトの追加 （1365 ページ）

VPN セッションでのパスワード変更の管理

パスワードの管理では、リモートアクセス VPN ポリシー管理者がリモートアクセス VPN ユーザーのパスワード期限切れの通知を設定できます。パスワード管理は、 AAA のみとクライアント証明書と AAA の認証設定の AAA 設定で使用できます。詳細については、リモートアクセス VPN の AAA 設定 （1588 ページ）を参照してください。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）]>[リモートアクセス（Remote Access）] を選択します。

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 AAA の設定が含まれている接続プロファイルの [編集（Edit）] をクリックします。

ステップ 4 [AAA] > [詳細設定（Advanced Settings）] > を選択します。

ステップ 5 [パスワード管理の有効化（Enable Password Management）] チェックボックスをオンにして、次のいずれかを選択します。

- [ユーザー通知（Notify User）] : パスワードの有効期限が切れる何日前にユーザーに通知するのか、その日数をボックスで指定します。
- [パスワードの有効期限の日にユーザーに通知（Notify user on the day of password expiration）]

ステップ 6 変更を保存します。

関連トピック

接続プロファイルの設定 （1585 ページ）

RADIUS サーバーへのアカウンティング レコードの送信

リモートアクセス VPN のアカウンティングレコードは、ユーザーがアクセスしたサービスやユーザーが使用したネットワークリソースの量を VPN 管理者が追跡するのに役立ちます。アカウンティング情報には、ユーザーセッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれます。

アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。AAA アカウンティングをアクティブ化すると、ネットワーク アクセス サーバーは設定されたアカウンティングサーバーにユーザーアクティビティをレポートします。RADIUS サーバーはアカウンティングサーバーとして設定できるため、すべてのユーザーアクティビティ情報が Firewall Management Center から RADIUS サーバーに送信されます。

（注） リモート アクセス VPN AAA の設定では、認証、許可、およびアカウンティング用に同じ RADIUS サーバーまたは個別の RADIUS サーバーを使用できます。

始める前に

- 認証要求またはアカウンティングレコードを受診する RADIUS サーバーで RADIUS グループオブジェクトを設定します。詳細については、RADIUS サーバー グループのオプション（1314 ページ）を参照してください。
- RADIUS サーバーが Firewall Threat Defense デバイスから到達可能であることを確認します。[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）] > [ルーティング（Routing）] で Secure Firewall Management Center のルーティングを設定し、RADIUS へのサーバーへの接続を確保します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）]>[リモートアクセス（Remote Access）] を選択します。

ステップ 2 RADIUS サーバーを設定するリモートアクセスポリシーで [編集（Edit）] をクリックするか、新しいリモートアクセス VPN ポリシーを作成します。

ステップ 3 AAA の設定が含まれている接続プロファイルの [編集（Edit）] をクリックして、[AAAA] を選択します。

ステップ 4 [アカウンティングサーバー（Accounting Server）] ドロップダウンから RADIUS サーバーを選択します。

ステップ 5 変更を保存します。

関連トピック

接続プロファイルの設定 （1585 ページ）
リモートアクセス VPN の AAA 設定 （1588 ページ）

認証サーバーへのグループ ポリシーの選択の委任

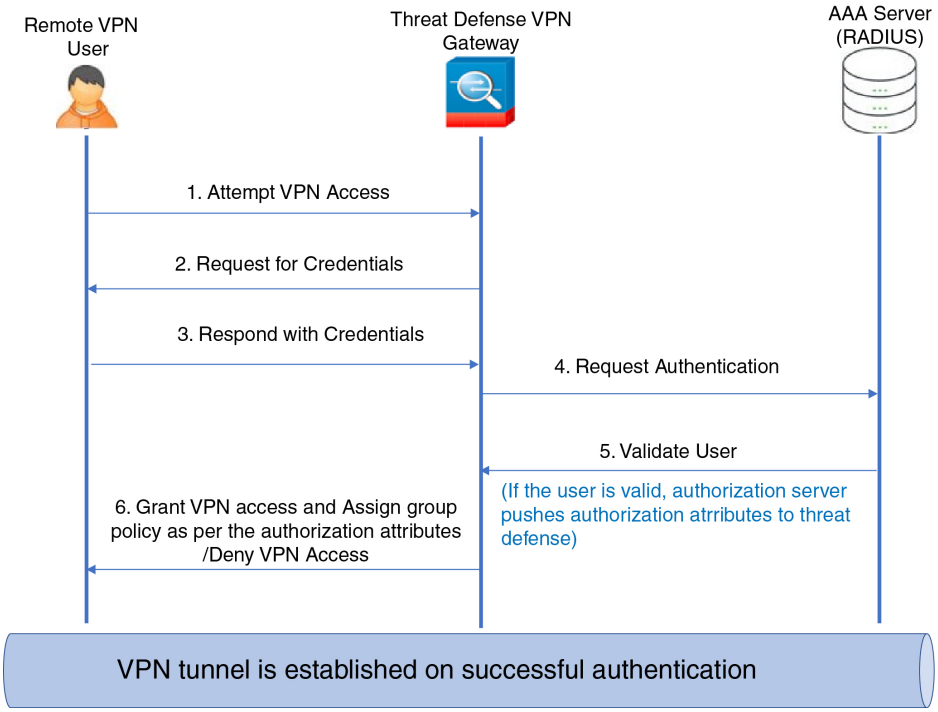
ユーザーに適用されるグループ ポリシーは VPN トンネルが確立される際に決定されます。ウィザードを使用してリモートアクセス VPN ポリシーを作成するときに接続プロファイルのグルー

プポリシーを選択するか、または後で接続プロファイルの接続ポリシーを更新することができます。ただし、グループ ポリシーを割り当てるように AAA（RADIUS）サーバーを設定するか、または現在の接続プロファイルから取得されます。Firewall Threat Defense デバイスが、接続プロファイルで設定されている属性と競合する外部 AAA サーバーから属性を受信した場合は、AAA サーバーからの属性が常に優先されます。

IETF RADIUS サーバ属性 25 を送信してユーザ/ユーザ グループの許可プロファイルを設定し、対応するグループ ポリシー名にマップするように、ISE または RADIUS サーバを構成します。ユーザーまたはユーザー グループに特定のグループ ポリシーを設定すると、ダウンロード可能な ACL をプッシュし、バナーを設定し、VLAN を制限し、セッションに SGT を適用する高度なオプションを設定できます。これらの属性は、VPN 接続が確立した時点でそのグループに含まれているすべてのユーザーに適用されます。

詳細については、『Cisco Identity Services Engine Administrator Guide』の「Configure Standard Authorization Policies」の項およびSecure Firewall Threat Defense の RADIUS サーバー属性 （1595 ページ）を参照してください。

図 *311 : AAA* サーバーによるリモート アクセス *VPN* グループ ポリシーの選択



関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）
接続プロファイルの設定 （1585 ページ）

許可サーバーによるグループ ポリシーまたはその他の属性の選択のオーバーライド

リモート アクセス VPN ユーザーが VPN に接続すると、接続プロファイル内に設定されているグループ ポリシーとその他の属性がそのユーザーに割り当てられます。ただし、リモート ア

クセス VPN システムの管理者は、ユーザーまたはユーザー グループの許可プロファイルを設定するように ISE または RADIUS サーバーを設定することによって、グループ ポリシーとその他の属性の選択を認証サーバーに委任できます。ユーザーが認証されると、これらの特定の承認属性が Firewall Threat Defense デバイスにプッシュされます。

始める前に

許可サーバーとして RADIUS を使用したリモート アクセス VPN ポリシーが設定されていることを確認します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3 まだ設定されていない場合は、認証サーバーとして RADIUS または ISE を選択します。

ステップ 4 [詳細（Advanced）] > [グループ ポリシー（Group Policies）] を選択し、必要なグループ ポリシーを追加します。グループ ポリシー オブジェクトの詳細については、グループ ポリシー オブジェクトの設定 （1430 ページ）を参照してください。

1 つのグループ ポリシーのみを 1 つの接続プロファイルにマップすることができますが、1 つのリモート アクセス VPN ポリシーには複数のグループ ポリシーを作成できます。これらのグループポリシーは、ISE または RADIUS サーバーで参照でき、許可サーバーの許可属性を割り当てることによって接続プロファイル内に設定されているグループポリシーをオーバーライドするように設定できます。

ステップ 5 ターゲットの Firewall Threat Defense デバイス上に設定を展開します。

ステップ 6 許可サーバーで、IP アドレスとダウンロード可能な ACL の RADIUS 属性を持つ許可プロファイルを作成します。

リモート アクセスで選択した許可サーバーにグループ ポリシーを設定すると、そのグループポリシーは、ユーザーが認証された後にリモート アクセス VPN ユーザーの接続プロファイルに設定されているグループ ポリシーをオーバーライドします。

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）

ユーザー グループへの VPN アクセスの拒否

VPN を使用可能な認証済みのユーザーまたはユーザー グループが不要な場合は、VPN アクセスを拒否するグループ ポリシーを設定できます。リモート アクセス VPN ポリシー内にグループポリシーを作成し、許可を行うため、ISE または RADIUS サーバーの設定でそれを参照します。

始める前に

リモートアクセスポリシーウィザードを使用してリモートアクセスVPNが設定されており、リモート アクセス VPN ポリシーに認証の設定が行われていることを確認します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3 [詳細（Advanced）] > [グループ ポリシー（Group Policies）] をクリックします。

ステップ 4 グループポリシーを選択して [編集（Edit）] をクリックするか、新しいグループポリシーを追加します。

ステップ 5 [詳細（Advanced）] > [セッション設定（Session Settings）] を選択し、[ユーザーごとの同時ログイン（Simultaneous Login Per User）] を 0（ゼロ）に設定します。
これにより、ユーザーまたはユーザー グループは VPN への接続を完全に停止します。

ステップ 6 [保存（Save）] をクリックしてグループ ポリシーを保存した後、リモート アクセス VPN 設定を保存します。

ステップ 7 IETF RADIUS サーバー 属性 25 を送信し、対応するグループ ポリシー名にマップするようにユーザー/ユーザー グループの許可プロファイルを設定して、ISE またはRADIUS サーバー サーバーを設定します。

ステップ 8 リモート アクセス VPN ポリシーでは、ISE または RADIUS サーバーを承認サーバーとして構成できます。

ステップ 9 リモート アクセス VPN ポリシーを保存および展開します。

関連トピック

接続プロファイルの設定 （1585 ページ）

ユーザー グループに対する接続プロファイルの選択の制限

1 つの接続プロファイルをユーザーまたはユーザーグループに適用する場合、接続プロファイルを無効にすることで、Cisco Secure Client の AnyConnect VPN モジュールを使用して接続するときに選択するユーザーのグループエイリアスや URL が表示されないようにできます。

たとえば、モバイル ユーザー、会社支給のラップトップのユーザー、個人のラップトップのユーザーなど、異なる VPN ユーザー グループに組織が特定の設定を使用する場合は、それらの各ユーザー グループに固有の接続プロファイルを設定し、ユーザーが VPN に接続したときに適切に接続プロファイルを適用することができます。

Cisco Secure Client の AnyConnect VPN モジュールのデフォルトでは、Firewall Management Center に設定されていて、Firewall Threat Defense に展開されている接続プロファイル（接続プロファイル名別、エイリアス別、またはエイリアス URL 別）のリストが表示されます。カスタム接続プロファイルが設定されていない場合、Cisco Secure Client の AnyConnect VPN モジュールに

はDefaultWEBVPNGroup接続プロファイルが表示されます。次の手順を使用して、1つの接続プロファイルをユーザー グループに適用します。

始める前に

- Secure Firewall Management Center の Web インターフェイスで、リモート アクセス VPN ポリシー ウィザードを使用し、[認証方式（Authentication Method）] を [クライアント証明書のみ（Client Certificate Only）] または [クライアント証明書と AAA（Client Certificate + AAA）] に設定してリモートアクセスVPNを設定します。証明書からユーザー名のフィールドを選択します。
- 認証のためのISEまたはRADIUSのサーバーを設定し、グループポリシーを認証サーバーに関連付けます。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3 [アクセスインターフェイス（Access Interfaces）] を選択し、[ログイン時にユーザーによる接続プロファイルの選択を許可（Allow users to select the connection profile while logging in）] を無効にします。

ステップ 4 [詳細（Advanced）]> [証明書マップ（Certificate Maps）] をクリックします。

ステップ 5 [設定したルールを使用して証明書を接続プロファイルと照合する（Use the configured rules to match a certificate to a Connection Profile）] をオンにします。

ステップ 6 [証明書マップ名（Certificate Map Name）] を選択するか、または [追加（Add）] アイコンをクリックして証明書ルールを追加します。

ステップ 7 [接続プロファイル（Connection Profile）] を選択し、[OK] をクリックします。
この設定では、Cisco Secure Client の AnyConnect VPN モジュールから接続するユーザーには、マップされた接続プロファイルが提供され、VPN を使用するように認証されます。

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）
接続プロファイルの設定 （1585 ページ）

リモートアクセス VPN クライアントの セキュアクライアント プロファイルの更新

セキュアクライアント プロファイルは、Secure Client の一部として VPN クライアントシステムに展開される管理者定義のエンドユーザー要件および認証ポリシーを含む XML ファイルです。これでエンドユーザーが事前設定されたネットワーク プロファイルを使用できるようになります。

プロファイルを作成するには、独立した構成ツールである GUI ベースの Secure Client プロファイルエディタ を使用できます。スタンドアロン プロファイル エディタを使用して、Secure Client プロファイルを新規作成したり、既存のプロファイルを変更したりできます。プロファイル エディタはシスコのソフトウェア ダウンロード センターからダウンロードできます。

詳細については、Cisco Secure Client（AnyConnect を含む）管理者ガイド [英語] の該当するリリースの「Secure Client プロファイルエディタ」の章を参照してください。

始める前に

- リモート アクセス ポリシー ウィザードを使用してリモート アクセス VPN が設定されており、設定が Firewall Threat Defense デバイスに展開されていることを確認します。新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）を参照してください。
- Secure Firewall Management Center の Web インターフェイスで、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > **[Secure Clientファイル（Secure Client File）]** に移動し、新しい セキュアクライアント イメージを追加します。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リモートアクセス VPN ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3 クライアント プロファイルに含まれている編集すべき接続プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 4 [グループポリシーの編集（Edit Group Policy）] > **[Secure Client]** > [プロファイル（Profiles）] をクリックします。

ステップ 5 リストからクライアントプロファイルの XML ファイルを選択するか、または [追加（Add）] をクリックして新しいクライアントプロファイルを追加します。

ステップ 6 グループ ポリシーと接続プロファイルを保存し、その後にリモート アクセス VPN ポリシーを保存します。

ステップ 7 変更を展開します。
クライアント プロファイルに加えた変更は、リモート アクセス VPN ゲートウェイに接続したときに VPN クライアント上で更新されます。

関連トピック

グループ ポリシー オブジェクトの設定 （1430 ページ）

RADIUS ダイナミック認証

Secure Firewall Threat Defense は、RADIUS サーバーを使用して、ダイナミック アクセス コントロール リスト（ACL）またはユーザーごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザー許可を実行できます。ダ

イナミック認証または RADIUS 認可変更（RADIUS CoA）のダイナミック ACL を実装するには、RADIUS サーバーをサポートするように設定する必要があります。ユーザーが認証を試みる場合、RADIUS サーバーによってダウンロード可能 ACL、または ACL 名が Firewall Threat Defense に送信されます。特定のサービスへのアクセスは ACL によって許可されるか拒否されるかのいずれかです。Secure Firewall Threat Defense は認証セッションの期限が切れると ACL を削除します。

関連トピック

RADIUS サーバーグループの追加 （1314 ページ）
インターフェイス（Interface） （1346 ページ）
RADIUS ダイナミック認証の設定 （1648 ページ）
Secure Firewall Threat Defense の RADIUS サーバー属性 （1595 ページ）

RADIUS ダイナミック認証の設定

始める前に：

- RADIUS サーバーで参照されている場合、セキュリティゾーンやインターフェイスグループには 1 つのインターフェイスのみ設定できます。
- ダイナミック認証が有効になっている RADIUS サーバーでダイナミック認証を機能させるためには、Secure Firewall Threat Defense 6.3 以降が必要です。
- Secure Firewall Threat Defense 6.2.3 以前のバージョンでは、RADIUS サーバーでのインターフェイスの選択はサポートされていません。展開中、インターフェイス オプションは無視されます。
- Firewall Threat Defense ポスチャ VPN は、ダイナミック認証または RADIUS 認可変更（CoA）によるグループポリシーの変更をサポートしていません。

表 77：手順

	操作手順	詳細
ステップ 1	Secure Firewall Management Center Web インターフェイスにログインします。	
ステップ 2	ダイナミック認証を使用して、RADIUS サーバー オブジェクトを設定します。	RADIUS サーバー グループのオプション （1314 ページ）

	操作手順	詳細
ステップ 3	認可変更（CoA）が有効になっているインターフェイスを介してISEサーバーへのルートを設定し、ルーティングまたは特定のインターフェイスを介して Firewall Threat Defense から RADIUS サーバーへの接続を確立します。	RADIUS サーバー グループのオプション （1314 ページ）
ステップ 4	リモートアクセスVPNポリシーを設定し、ダイナミック認証を使用して作成したRADIUSサーバグループオブジェクトを選択します。	新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）
ステップ 5	DNS サーバーの詳細とドメインルックアップインターフェイスを[プラットフォーム設定（Platform Settings）]を使用して設定します。	DNS の設定 （1578 ページ） DNS サーバ グループ （1335 ページ）
ステップ 6	VNP ネットワーク経由で DNS サーバーに到達可能な場合は、リモートアクセスVPNトンネルを介してDNSトラフィックを許可するためのスプリットトンネルをグループポリシーに設定します。	グループポリシーオブジェクトの設定 （1430ページ）
ステップ 7	設定変更を展開します。	設定変更の展開 （172 ページ）

二要素認証

リモート アクセス VPN に対してニ要素認証を設定することができます。二要素認証を使用する場合、ユーザーはユーザー名とスタティック パスワードに加えて、RSA トークンやパスコードなどの追加項目を指定する必要があります。二要素認証が2番目の認証ソースを使用することと異なるのは、1 つの認証ソースで 2 つの要素が設定され、RSA サーバーとの関係がプライマリ認証ソースに関連付けられている点です。

Secure Firewall Threat Defense は、2 番目の要素のために RSA トークンと Duo Mobile への Duo Push 認証要求を、二要素認証プロセスの最初の要素としての RADIUS または AD サーバーとの組み合わせでサポートします。

RSA 二要素認証の設定

このタスクの概要：

RADIUS サーバーまたは AD サーバーを RSA サーバーの認証エージェントとして設定し、サーバーをリモートアクセス VPN のプライマリ認証ソースとして Secure Firewall Management Center で使用することができます。

この方法を使用する場合、ユーザーは RADIUS または AD サーバーで設定されているユーザー名を使用して認証し、パスワードと 1 回限りの一時的な RSA トークンを連結し、パスワードとトークンをコンマで区切る必要があります（*password*,*token*）。

この設定では、認証サービスを提供するために（Cisco ISE で供給されるような)個別の RADIUS サーバを使用することが一般的です。2 番目の RADIUS サーバを認証サーバとして設定し、必要に応じてアカウンティングサーバを設定します。

始める前に：

Secure Firewall Threat Defense に RADIUS 二要素認証を設定する前に、次の設定が完了していることを確認します。

RSA サーバー上で以下の操作を実行します。

- RADIUS または Active Directory サーバーを認証エージェントとして設定します。
- 設定（*sdconf.rec*）ファイルを生成してダウンロードします。
- トークンプロファイルを作成してトークンをユーザーに割り当て、トークンをユーザーに配布します。トークンをダウンロードして、リモート アクセス VPN クライアント システムにインストールします。

詳細については、RSA SecureID スイートのドキュメントを参照してください。

ISE サーバー上で以下の操作を実行します。

- RSA サーバで生成した設定（*sdconf.rec*）ファイルをインポートします。
- 外部アイデンティティ ソースとして RSA サーバーを追加して、共有秘密を指定します。

表 *78 :* 手順

	操作手順	詳細
ステップ 1	Secure Firewall Management Center Web インターフェイスにログインします。	
ステップ 2	RADIUS サーバー グループを作成します。	RADIUS サーバー グループのオプション （1314 ページ）

	操作手順	詳細
ステップ 3	RADIUS または AD サーバをホストとして指定して、新しい RADIUS サーバ グループ内に RADIUS サーバ オブジェクトを作成します。タイムアウトの時間は 60 秒以上に設定します。	RADIUS サーバー グループのオプション （1314 ページ） （注） RADIUS または AD サーバーは、RSA サーバーで認証エージェントとして設定されているサーバーと同じである必要があります。 二要素認証の場合は、Secure Client プロファイル XML ファイルでもタイムアウトが 60 秒以上に更新されていることを確認してください。
ステップ 4	ウィザードを使用して新しいリモートアクセス VPN ポリシーを設定するか、既存のリモートアクセス VPN ポリシーを編集します。	新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）
ステップ 5	認証サーバとして RADIUS を選択し、新しく作成した RADIUS サーバ グループを認証サーバとして選択します。	リモートアクセス VPN の AAA 設定 （1588 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開 （172 ページ）

Duo 二要素認証の設定

このタスクの概要：

Duo RADIUS サーバはプライマリ認証ソースとして設定できます。このアプローチでは、Duo RADIUS 認証プロキシを使用します。（LDAPS 経由での Duo クラウド サービスとの直接接続は使用できません）。

Duo の設定に関する詳細手順については、https://duo.com/docs/cisco-firepower を参照してください。

その後、最初の認証要素として別の RADIUS サーバー（または AD サーバー）を使用し、2 番目の要素として Duo クラウド サービスを使用するため、プロキシ サーバー宛の認証要求を転送するように Duo を設定します。

このアプローチを使用する場合、Duo クラウドまたは web サーバーと、関連付けられている RADIUS サーバーの両方で設定されたユーザー名を使用してユーザーを認証する必要があります。ユーザは、RADIUS サーバに設定されたパスワードと、その後に次のいずれかの Duo コードを入力する必要があります。

- **Duo パスコード**。*my-password*,123456 など。

- **push**。my-password,pushなど。push は、ユーザーによるインストールと登録が完了している Duo モバイル アプリに認証をプッシュ送信するように Duo に指示する場合に使用します。
- **sms**。my-password,smsなど。smsを使用して、新しいパスコードのバッチを含むSMSメッセージをユーザのモバイルデバイスに送信するようにDuoに指示します。**sms** を使用すると、ユーザの認証試行は失敗します。その後、ユーザは再認証し、2 番目の認証ファクタとして新しいパスコードを入力する必要があります。
- phone。my-password,phoneなど。電話機のコールバックを使用して認証するには、**phone** を使用します。

例を含むログインオプションの詳細については、https://guide.duo.com/anyconnect を参照してください。

始める前に：

Firewall Threat Defense で Duo 認証プロキシを使用する RADIUS 二要素認証を設定する前に、次の設定が完了していることを確認します。

- リモートアクセスVPNユーザーに対して実行中のプライマリ認証（RADIUSまたはAD）を設定してから、Duo の展開を開始します。
- ネットワーク内の Windows または Linux マシンに Duo プロキシ サービスをインストールして、Duo と Secure Firewall Threat Defense リモート アクセス VPN を統合します。また、この Duo プロキシ サーバーは RADIUS サーバーとしても機能します。

  次の場所から最新の Duo 認証プロキシをダウンロードしてインストールします。

  - **Windows**：https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**：https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - https://duo.com/docs/checksums#duo-authentication-proxy でチェックサムを確認します。

- Duo 認証ファイル `authproxy.cfg` を設定します。https://duo.com/docs/cisco-firepower#configure-the-proxy ページの指示に従って、認証設定を構成します。

  `authproxy.cfg` 設定ファイルには、RADIUS または ISE サーバーの詳細、Firewall Threat Defense デバイス、Duo プロキシ サーバーの詳細、統合鍵、秘密鍵、API ホストの詳細を含める必要があります。

- `authproxy.cfg` ファイルに正しい API ホスト情報が含まれていることを確認します。
- [Duoセキュリティ設定（Duo Security Server）] > [Duo管理者パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [CISCO RADIUS VPN] で、新しくインストールされた Duo プロキシ サーバーのセカンダリ認証ファクタなど、その他の必要な設定を指定します。

表 79 : 手順

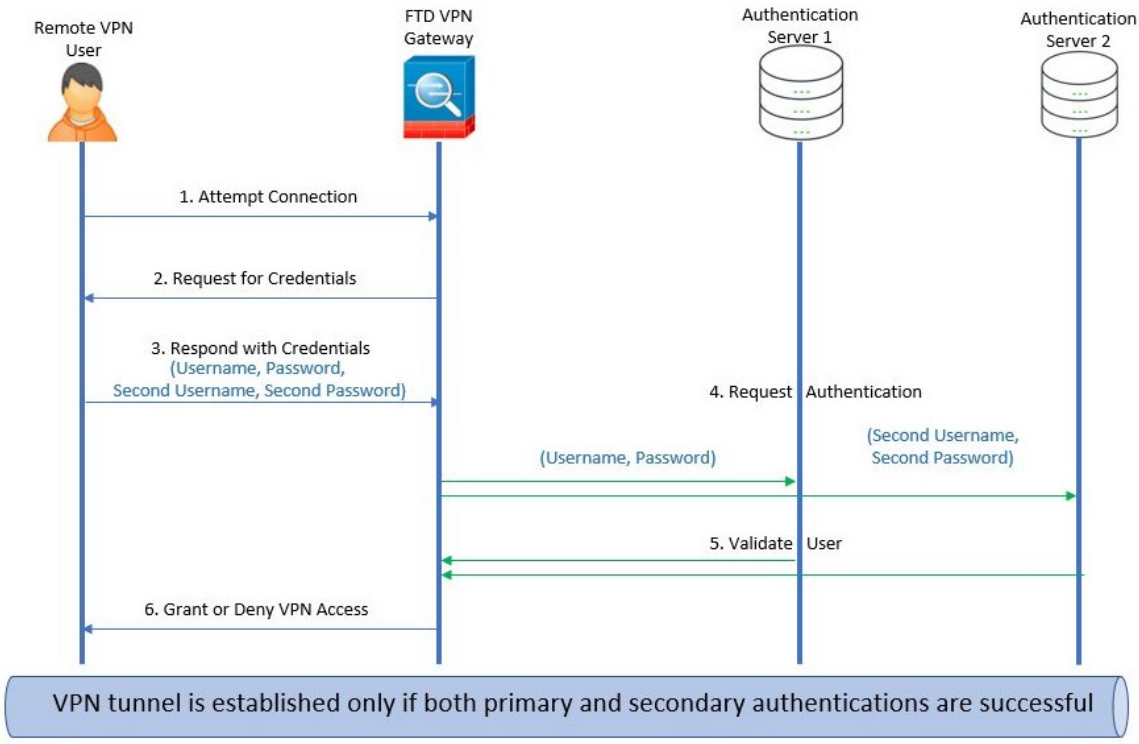
	操作手順	詳細
ステップ 1	Secure Firewall Management Center Web インターフェイスにログインします。	
ステップ 2	RADIUS サーバー グループを作成します。	RADIUS サーバー グループのオプション （1314 ページ）
ステップ 3	RADIUS サーバーをホストとして指定して、新しい RADIUS サーバー グループ内に RADIUS サーバー オブジェクトを作成します。タイムアウトの時間は 60 秒以上に設定します。	RADIUS サーバー オプション （1316 ページ） （注） 二要素認証の場合は、Secure Client プロファイル XML ファイルでもタイムアウトが 60 秒以上に更新されていることを確認してください。
ステップ 4	ウィザードを使用して新しいリモート アクセス VPN ポリシーを設定するか、既存のリモート アクセス VPN ポリシーを編集します。	新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）
ステップ 5	認証サーバーとして RADIUS を選択し、Duo プロキシ サーバーを指定して作成した RADIUS サーバー グループを認証サーバーとして選択します。	リモートアクセス VPN の AAA 設定 （1588 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開 （172 ページ）

セカンダリ認証

Secure Firewall Threat Defense のセカンダリ認証または二重認証は、2 つの異なる認証サーバーを使用して、リモート アクセス VPN 接続にさらにもう 1 つのセキュリティのレイヤを追加します。セカンダリ認証が有効になっている場合、Secure Client VPN のユーザーは VPN ゲートウェイにログインするために 2 組のクレデンシャルを提供する必要があります。

Secure Firewall Threat Defense リモート アクセス VPN は、AAA のみのセカンダリ認証と、クライアント証明書認証方式および AAA 認証方式をサポートします。

図 *312 :* リモート アクセス *VPN* セカンダリ認証または二重認証



関連トピック

リモートアクセス VPN のセカンダリ認証の設定 （1654 ページ）

リモートアクセス VPN のセカンダリ認証の設定

クライアント証明書と認証サーバーの両方を使用するようにリモート アクセス VPN 認証が設定されている場合、VPN クライアント認証はクライアント証明書の検証と AAA サーバーの両方を使用して実行されます。

始める前に

- 2 つの認証（AAA）サーバーの設定：プライマリおよびセカンダリ認証サーバー、必要な ID 証明書。認証サーバーには、RADIUS サーバー、AD または LDAP レルムを使用できます。
- リモート アクセス VPN 設定が機能するように AAA サーバーに Secure Firewall Threat Defense デバイスからアクセスできることを確認します。AAA サーバーへの接続を確実にするために、ルーティングを設定します（[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）]）。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）]をクリックします。または、[追加（Add）] をクリックして、新しいリモートアクセス VPN ポリシーを作成します。

ステップ 3 新しいリモートアクセスVPNポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアントプロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 **[AAA]** > **[認証方式（Authentication Method）]**、[AAA] または [クライアント証明書とAAA（Client Certificate & AAA）] をクリックします。

- [認証方式（Authentication Method）] の選択に応じて、次のようになります。

  [クライアント証明書とAAA（Client Certificate & AAA）] : クライアント証明書と AAA サーバーの両方を使用して認証されます。

  - [AAA] : [認証サーバー（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバーは同じ値になります。ドロップダウン リストから [アカウンティング サーバー（Accounting Server）] を選択します。認証サーバー ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[許可サーバー（Authorization Server）] と [アカウンティング サーバー（Accounting Server）] をそれぞれ手動で選択する必要があります。
  - どの認証方式を選択する場合にも、[ユーザーが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

- [セカンダリ認証を使用（Use secondary authentication）] : VPN セッションのセキュリティを強化するため、プライマリ認証の他にセカンダリ認証を設定します。セカンダリ認証は、[AAA のみ（AAA only）] と [クライアント証明書と AAA（Client Certificate & AAA）] の認証方式にのみ適用されます。

  セカンダリ認証はオプションの機能であり、2 つのセットのユーザー名とパスワードを Secure Client ログイン画面に入力するには VPN ユーザーが必要です。認証サーバーまたはクライアント証明書からセカンダリ ユーザー名を事前入力するように設定することもできます。リモート アクセス VPN 認証は、プライマリとセカンダリの両方の認証が成功した場合にのみ許可されます。いずれの認証サーバーに到達できない場合、1 つの認証が失敗すると、VPN 認証が拒否されます。

  セカンダリ認証の設定前に、2つ目のユーザー名とパスワードのセカンダリ認証のサーバーグループ（AAA サーバー）を設定する必要があります。たとえば、プライマリ認証サーバーを LDAP または Active Directory レルムに、セカンダリ認証を RADIUS サーバーに設定できます。

  （注）

デフォルトでは、セカンダリ認証は必要ありません。

[認証サーバー（Authentication Server）]：VPN ユーザーのセカンダリ ユーザー名とパスワードを提供するセカンダリ認証サーバー。

[セカンダリ認証のユーザー名（Username for secondary authentication）] で次の項目を選択します。

- [プロンプト（Prompt）]：VPN ゲートウェイへのログイン中にユーザー名とパスワードを入力するようユーザーに要求します。
- [プライマリ認証ユーザー名を使用（Use primary authentication username）]：プライマリとセカンダリの両方の認証にプライマリ認証サーバーからユーザー名が取得されます。パスワードは 2 つ入力する必要があります。
- [クライアント証明書からのユーザー名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザー名が事前に入力されます。
  - クライアント証明書のユーザー名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN（識別名）全体をユーザー名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザー ID が自動的に取得されます。

    プライマリとセカンダリのフィールドのマッピングの詳細については、「**認証方式**」の説明を参照してください。
  - [ユーザーログインウィンドウに証明書からユーザー名を事前に入力（Prefill username from certificate on user login window）]：ユーザーが Secure Client クライアント経由で接続したときにクライアント証明書からセカンダリユーザー名を事前に入力します。
    - [ログイン ウィンドウでユーザー名を非表示にする（Hide username in login window）]：セカンダリ ユーザー名はクライアント証明書から事前に入力されますがユーザーには表示されず、ユーザーが事前に入力されたユーザー名を変更しないようにします。
- [VPN セッションのセカンダリ ユーザー名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザー アクティビティのレポートにセカンダリ ユーザー名を使用します。

詳細については、「リモートアクセス VPN の AAA 設定 （1588 ページ）」を参照してください。

関連トピック

接続プロファイルの設定 （1585 ページ）

SAML 2.0 シングルサインオン認証

SAML シングルサインオン認証について

セキュリティ アサーション マークアップ言語（SAML）は、別のコンテキストでのセッションを使用してアプリケーションにユーザーをログインさせるためのオープンスタンダードです。ユーザーが Active Directory（AD）ドメインまたはイントラネットにログインしている場合、組織はすでにユーザーのアイデンティティを認識しています。このアイデンティティ情報を使用し、SAML を使用して Web ベースのアプリケーションなどの他のアプリケーションにユーザーをログインさせます。個々のアプリケーションはログイン情報を保存する必要がなく、ユーザーは個々のアプリケーションの異なるログイン情報セットを覚えて管理する必要はありません。SAML シングルサインオン（SSO）は、ユーザーのアイデンティティをある場所（アイデンティティ プロバイダー）から別の場所（サービスプロバイダー）に転送することによって機能します。

SAML シングルサインオンとの連携：Secure Firewall Threat Defense

Secure Firewall Threat Defense デバイスは、Secure Client を使用したリモートアクセス VPN 接続で SAML 2.0 シングルサインオン（SSO）認証をサポートします。Secure Firewall Threat Defense で SAML 2.0 SSO を構成するには、次のものが必要です。

- **アイデンティティ プロバイダー（IdP）**：Duo Access Gateway がアイデンティティ プロバイダーとして機能し、ユーザー認証を実行してアサーションを発行します。
- **サービスプロバイダー（SP）**：Firewall Threat Defense デバイスがサービスプロバイダーとして機能し、アイデンティティ プロバイダーから認証アサーションを取得します。
- **VPN クライアント**：Secure Client は、組み込みブラウザを介して SAML 2.0 認証を実行します。

SAML 2.0 に関する注意事項と制約事項

- Firewall Threat Defense は、SAML 認証用に次のシグニチャをサポートしています。
  - RSA および HMAC を使用する SHA1
  - RSA および HMAC を使用する SHA2
- Firewall Threat Defense は、すべての SAML IdP でサポートされる SAML 2.0 Redirect-POST バインディングをサポートしています。
- Firewall Threat Defense は SAML SP としてのみ機能します。ゲートウェイ モードやピア モードでアイデンティティ プロバイダーとして動作することはできません。
- SAML ドメインに一致する AD レルムに関連付けられた ID ポリシーがある場合、SAML 認証ユーザーにアクセスポリシーを適用できます。ただし、Azure AD のテナント ID を Threat Defense デバイス上の関連するレルム ID にマッピングする追加設定が必要となるため、Azure AD SAML では機能しません。

- DAP 評価で使用可能な SAML 認証属性は（AAA サーバーから RADIUS 認証応答で送信される RADIUS 属性と同様に）サポートされていません。Firewall Threat Defense は、DAP ポリシーで SAML 対応グループポリシーをサポートします。ただし、ユーザー名属性は SAML ID プロバイダーによってマスクされるため、SAML 認証の使用中はユーザー名属性を確認できません。
- 認証アサーションが適切に処理され、タイムアウトが適切に機能するように、Firewall Threat Defense の管理者は、Firewall Threat Defense と SAML IdP とのクロック同期を確保する必要があります。
- Firewall Threat Defense の管理者は、次の点を考慮して、Firewall Threat Defense と IdP の両方で有効な署名証明書を保持する責任があります。
  - Firewall Threat Defense に IdP を設定する際には、IdP の署名証明書が必須です。
  - Firewall Threat Defense は、IdP から受け取った署名証明書に対して失効チェックを行いません。
- SAML アサーションには、NotBefore と NotOnOrAfter 条件があります。Firewall Threat Defense SAML に設定されているタイムアウトと、これらの条件との相関関係は次のとおりです。
  - NotBefore とタイムアウトの合計が NotOnOrAfter よりも早い場合は、タイムアウトが NotOnOrAfter に優先します。
  - NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。
  - NotBefore 属性が存在しない場合、Firewall Threat Defense はログイン要求を拒否します。NotOnOrAfter 属性が存在せず、SAML タイムアウトが設定されていない場合、Firewall Threat Defense はログイン要求を拒否します。
- 二要素認証（プッシュ、コード、パスワード）のチャレンジ/応答中に FQDN が変更されるため、Firewall Threat Defense がクライアントとのプロキシを強制的に認証する、内部 SAML を使用した展開では Firewall Threat Defense は Duo と連携しません。
- Secure Client で SAML を使用する場合は、次の注意事項に従ってください。
  - 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。
  - 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
  - Web ブラウザに確立された SAML 認証は Secure Client と共有されず、その逆も同じです。
  - 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、Secure Client では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに Secure Client がど

のプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。

- SAML機能を使用するためには、Firewall Threat Defense の Network Time Protocol（NTP）サーバーを IdP NTP サーバーと同期する必要があります。
- 内部 IdP を使用してログインした後に SSO で内部サーバーにアクセスすることはできません。
- SAML IdP NameID 属性は、ユーザーのユーザー名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。

- SAML は Start Before Logon（SBL）をサポートしていません。
- SAML アサーションで受信した複数の属性はサポートされていません。
- ファイアウォールは、 Firewall Management Center で作成したシングル サインオン サーバー オブジェクトの SAML オブジェクト名としてアイデンティティ プロバイダー エンティティIDを使用します（**[オブジェクト（Object）] > [オブジェクト管理（Object Management）] > [AAA サーバー（AAA Server）] > [シングル サインオン サーバー（Single Sign-on Server）]**）。したがって、1 つのファイアウォールで同じアイデンティティ プロバイダーのエンティティ ID を持つ複数の SAML オブジェクトを使用することはできません。

SAML シングルサインオン認証の設定

始める前に

Firewall Threat Defense リモートアクセス VPN で SAML シングルサインオンを設定する前に、次の作業が完了していることを確認してください。

- Duo でアカウントを作成する。
- Duo Access Gateway をダウンロードしてインストールする。
- SAML アイデンティティ プロバイダー（Duo）から次を取得する。
  - アイデンティティ プロバイダー エンティティ ID URL
  - サインイン URL
  - サインアウト URL
  - アイデンティティ プロバイダー証明書
- SAML シングル サインオン サーバー オブジェクトを作成する。詳細については、シングルサインオンサーバーの追加 （1317 ページ）を参照してください。

（注） リモートアクセス VPN ポリシーウィザードを使用して新しいポリシーを作成する際に、[接続プロファイル（Connection Profile）] 設定でシングル サインオン サーバー オブジェクトを作成できます。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** を選択します。

ステップ 2 SAML 認証を設定するリモートアクセス VPN ポリシーの横にある [編集（Edit）] をクリックします。新しいポリシーを作成する場合は、[追加（Add）] をクリックします。

ステップ 3 変更する接続プロファイルで [編集（Edit）] をクリックします。

ステップ 4 [AAA] 設定を選択し、[認証方法（Authentication Method）] ドロップダウンから [SAML] を選択します。

ステップ 5 [認証サーバー（Authentication Server）] として、必要な SAML シングルサインオンサーバーを選択します。

ステップ 6 リモートアクセス VPN に必要な設定を指定します。

ステップ 7 Firewall Threat Defense デバイスでリモートアクセス VPN ポリシーを保存および展開します。

関連トピック

リモートアクセス VPN の AAA 設定 （1588 ページ）

SAML 認証の設定

SAML 認証について

SAML 認証は、AAA およびダイナミック アクセス ポリシー（DAP）フレームワーク内の SAML アサーションで配信されるユーザー属性をサポートしています。SAML アサーション属性は、アイデンティティプロバイダーで名前と値のペアとして設定でき、文字列として解析されます。受信された属性は、DAP レコード内で選択基準を定義するときに使用できるように、DAP で使用できるようになります。SAML アサーション cisco_group_policy は、VPN セッションに適用されるグループポリシーを決定するために使用されます。

ダイナミック アクセス ポリシーの属性表現

DAP テーブルでは、DAP 属性は次の形式で表されます。

```
aaa.saml.name = "value”
```

例：aaa.saml.department = ”finance"

この属性は、次のように DAP 選択で使用できます。

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

複数値属性

複数値属性も DAP でサポートされていて、DAP テーブルにインデックスが付けられます。

```
aaa.saml.name.1 = "value"
aaa.saml.name.2 = "value"
```

Active Directory の memberOf 属性

Active Directory（AD）の memberOf 属性には、LDAP クエリによる処理方法と一致する、特別な処理が行われます。

グループ名は、DN の CN 属性によって表されます。

承認サーバーから受信された属性の例：

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us"
```

ダイナミック アクセス ポリシーの属性：

```
aaa.saml.memberOf.1 = "FTD-VPN-Group"
aaa.saml.memberOf.2 = "Domain Admins"
```

cisco_group_policy 属性の解釈

group-policy は、SAML アサーション属性によって指定できます。Firewall Threat Defense が "cisco_group_policy" 属性を受信すると、対応する値を使用して接続 group-policy が選択されます

SAML 認証の設定

始める前に

DUO などのシングルサインオンサーバーを設定し、必要なアイデンティティ プロバイダー（IdP）およびサービスプロバイダー（SP）の設定を完了していることを確認します。

詳細については、SAML 2.0 シングルサインオン認証 （1657 ページ）を参照してください。

手順

ステップ 1 シングル サインオン サーバー オブジェクトを構成します（まだ構成していない場合）。

a) **[オブジェクト（Object）] > [オブジェクト管理（Object Management）] > [AAAサーバー（AAA Server）] > [シングルサインオンサーバー（Single Sign-on Server）]** を選択します。

b) [シングルサインオンサーバーの追加（Add Single Sign-on Server）] をクリックします。

c) シングルサインオンサーバーの詳細を入力して [保存（Save）] をクリックします。

詳細については、シングルサインオンサーバーの追加 （1317 ページ）を参照してください。

ステップ 2 リモートアクセス VPN 接続プロファイルで SAML 認証を設定します。

a) **[デバイス（Devices）] > [リモートアクセス（Remote Access）]**を選択します。
b) SAML 認証を設定するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックするか、新しいポリシーを作成します。
c) 必要な接続プロファイルを編集し、[AAA] を選択します。
d) [認証サーバー（Authentication Server）] ドロップダウンからシングルサインオン サーバー オブジェクトを選択します。
e) リモートアクセス VPN の設定を保存します。

ステップ 3 DAP ポリシーで SAML 基準を照合します。

a) **[デバイス（Devices）] > [ダイナミックアクセスポリシー（Dynamic Access Policy）]**を選択します。
b) 新しい DAP を作成するか、既存の DAP を編集します。
c) DAP レコードを作成するか、既存のレコードを編集します。
d) **[AAA基準（AAA Criteria）] > [SAML基準（SAML Criteria）] > [SAML基準の追加（Add SAML Criteria）]** をクリックします。
e) SSO サーバーから返された SAML アサーションに基づいて SAML 基準を作成します。

ステップ 4 リモートアクセス VPN の設定を展開します。

関連トピック

接続プロファイルの設定 （1585 ページ）
Firewall Threat Defense グループ ポリシー オブジェクト （1430 ページ）

拡張 セキュアクライアント 設定

Firewall Threat Defense での セキュアクライアント モジュールの設定

セキュアクライアント は、さまざまな Cisco エンドポイント セキュリティ ソリューションと統合することが可能で、複数の セキュアクライアント モジュールを使ってセキュリティを強化できます。

管理対象ヘッドエンド Firewall Threat Defense を使用して、エンドポイントに セキュアクライアント モジュールを配布して管理できます。ユーザーが Firewall Threat Defense に接続すると、セキュアクライアント と必要なモジュールがエンドポイントにダウンロードされ、インストールされます。

バージョン 6.7 以降では、Firewall Management Center によって管理されるヘッドエンド Firewall Threat Defense を使用して、セキュアクライアント モジュールをエンドポイントに配布して管理できます。その後これらのモジュールは、対応するシスコのエンドポイント セキュリティ ソリューションと統合されます。

バージョン 6.4 ～ 6.6 では、FlexConfig を使用して Firewall Threat Defense でこれらのモジュールとプロファイルを有効にできます。詳細については、「Configure AnyConnect Modules and Profiles Using FlexConfig」を参照してください。

利点

Firewall Threat Defense を使用して セキュアクライアント モジュールをエンドポイントに配布して管理すると、以下のタスクを簡単に実行できます。

- 各エンドポイントでの セキュアクライアント モジュールとプロファイルの配布および管理。
- 各エンドポイントでの セキュアクライアント のアップグレード。

セキュアクライアント モジュールのタイプ

AMP イネーブラ

このモジュールを使用して、エンドポイントに Secure Endpointを展開します。このモジュールは、企業内でローカルにホストされているサーバーからエンドポイントに Secure Endpoint をプッシュします。このモジュールが提供する追加のセキュリティエージェントは、ネットワーク内の潜在的なマルウェア脅威を検出し、検出した脅威を削除して企業を保護します。

Cisco Secure Client 5.0 では、AMP イネーブラは macOS 専用です。Windows 版 Cisco Secure Client は、Cisco Secure Endpoint との完全な統合を提供します。

ISE ポスチャ

このモジュールを使用して、Cisco Identity Services Engine（ISE）を使用してウイルス対策、スパイウェア対策、オペレーティングシステムなどのエンドポイント ポスチャ チェックを実行し、エンドポイントのコンプライアンスを評価します。ISE は、次世代のアイデンティティおよびアクセス コントロールポリシーを提供します。ISE ポスチャは、クライアント側評価を実行します。クライアントは、ヘッドエンドからポスチャ要件ポリシーを受信し、ポスチャ データ収集を実行し、結果をポリシーと比較し、評価結果をヘッドエンドに返します。

ネットワークの可視性

このモジュールを使用して、ネットワーク可視性モジュールを使用してエンドポイントアプリケーションの使用状況をモニタリングします。潜在的な動作の異常を発見し、情報に基づいたネットワーク設計の意思決定を行うことができます。キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。使用状況データを Cisco Stealthwatch などの NetFlow 分析ツールと共有できます。

Umbrella ローミングセキュリティ

Cisco Umbrella ローミング セキュリティ サービスを使用した DNS レイヤセキュリティのために、このモジュールを使用できます。Cisco Umbrella はコンテンツフィルタリング、複数ポリシー、強力なレポート、Active Directory の統合などの機能を提供します。

Web セキュリティ

このモジュールを使用して、Cisco Talos を搭載した Cisco Secure Web Appliance（SWA）を有効にします。モジュールは、危険なサイトをブロックし、不明なサイトへのユーザーのアクセスを許可する前にサイトをテストして、エンドポイントを保護します。オンプレミスの WSA またはクラウドベースの Cisco Cloud Web Security のいずれかを介して、Web セキュリティを展開できます。このモジュールは、リリース 4.5 および Secure Client 5.0 の AnyConnect パッケージには含まれていません。

Network Access Manager

このモジュールはセキュアなレイヤ 2 ネットワークを提供し、有線およびワイヤレスネットワークにアクセスするためのデバイス認証を実行します。Network Access Managerは、セキュアなアクセスに必要なユーザおよびデバイス アイデンティティならびにネットワーク アクセス プロトコルを管理します。

Network Access Manager は macOS または Linux には対応していません。

Start Before Login

Start Before Login（SBL）により、ユーザーは Windows へのログイン前に、企業インフラへの VPN 接続を確立できます。SBL モジュールのインストール後、セキュアクライアント VPN プロファイルで SBL を有効にし、リモートアクセス VPN グループポリシーに追加する必要があります。

DART

診断およびレポートツール（DART）はシステムログと他の診断情報を照合して、AnyConnect のインストールと接続の問題をトラブルシュートします。このデータは、トラブルシューティングのために Cisco TAC に送信できます。

6.7 以降のバージョンのデフォルトでは、DART は新しい RA VPN グループポリシーで有効になっていません。6.6 以前のバージョンでは、DART はデフォルトで有効になっています。

フィードバック

カスタマー エクスペリエンス フィードバック（CEF）モジュールにより、使用している、また有効にしたモジュールおよび機能の情報を取得できます。この情報によりユーザーエクスペリエンスを把握できるため、シスコは セキュアクライアント の品質、信頼性、パフォーマンス、ユーザーエクスペリエンスを継続して改善できます。セキュアクライアントは、フィードバックモジュールをエンドポイントにダウンロードしません。フィードバックデータが Cisco フィードバックサーバーに送信されます。

セキュアクライアント モジュールの設定の前提条件

- 使用するモジュールに応じて、関連する製品を設定します。
- Cisco Software Download Center からローカルホストに、以下の セキュアクライアント 関連パッケージをダウンロードします。

- 必要なプラットフォーム用の Cisco セキュアクライアント ヘッドエンド展開パッケージ。

  このパッケージはヘッドエンド用で、すべての セキュアクライアント モジュールが含まれています。Windows の場合、ファイル名は cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg です。

- Profile Editor：プロファイルを必要とするモジュールのプロファイルを作成します。

  セキュアクライアント には、一部のモジュールに対して セキュアクライアント プロファイルが必要です。プロファイルには、モジュールを有効にし、対応するセキュリティサービスに接続するための設定が含まれています。Profile Editor は Windows のみをサポートします。

  次の表に、クライアントプロファイルを必要とするモジュールを示します。

Secure Client モジュール	クライアントプロファイルが必要
AMP イネーブラ	対応
ISE ポスチャ	対応
Network Access Manager	対応
ネットワーク可視性モジュール	対応
Umbrella ローミング セキュア モジュール	対応
Feedback	対応
Web セキュリティ	対応
DART	非対応
Start Before Login	いいえ

- ライセンシング
  - 次のいずれかの Secure Client ライセンスが必要です：Secure Client Premier、Secure Client Advantage、または Secure Client VPN のみ
  - Firewall Management Center Essentials ライセンスにより、輸出規制機能が許可される必要があります。

    Management Center でこの機能を確認するには、[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] の順に選択します。

セキュアクライアント モジュールの設定に関するガイドライン

- すべての セキュアクライアント モジュールは、AnyConnect 4.8 以降および Secure Client 5.0 でサポートされています。

- 異なるモジュールは、異なるファイル拡張子を持つプロファイルをサポートします。以下の表に、モジュールと、プロファイルのサポートされているファイル拡張子を示します。

表 *80*：サポートされるプロファイルのファイル拡張子

モジュール	ファイル拡張子
AMP イネーブラ	*.xml、*.asp
Feedback	*.xml
ISE ポスチャ	*.xml、*.isp
Network Access Manager	*.xml、*.nsp
ネットワークの可視性	*.xml、*.nvmsp
Umbrella ローミングセキュリティ	*.xml、*.json
Web セキュリティ	*.xml、*.wsp、*.wso

- クライアントモジュールごとに1つのエントリのみを追加できます。モジュールのエントリは編集または削除できます。
- ISE ポスチャと Network Access Manager モジュールを使用する場合は、ISE ポスチャモジュールを使用する前に、Network Access Manager をインストールする必要があります。
- Cisco Umbrella ローミング セキュリティ モジュールを有効にする場合は、VPN グループポリシーのスプリットトンネリングで [常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）] オプションを無効にしてください。
- SBL を使用する場合は、セキュアクライアント VPN プロファイルで SBL を有効にする必要があります。

Firewall Threat Defense を使用した セキュアクライアント モジュールの取り付け

始める前に

セキュアクライアント モジュールの設定の前提条件（1664 ページ）およびセキュアクライアント モジュールの設定に関するガイドライン（1665 ページ）トピックを確認してください。

手順

ステップ 1 管理者は、必要に応じて セキュアクライアント モジュールのプロファイルを作成します。

ステップ 2 管理者は、Firewall Management Center を使用して以下を実行します。

a) モジュールを設定し、リモートアクセス VPN グループポリシーにプロファイルを追加します。

b) Firewall Threat Defense に設定を展開します。

ステップ 3 ユーザーは、セキュアクライアント を使用して Firewall Threat Defense への VPN 接続を開始します。

ステップ 4 Firewall Threat Defense はユーザーを認証します。

ステップ 5 セキュアクライアント は更新を確認します。

ステップ 6 Firewall Threat Defense がエンドポイントで セキュアクライアント モジュールとプロファイルを配布します。

次のタスク

セキュアクライアントモジュールのリモートアクセス VPN グループポリシーの設定（1667 ページ）。

セキュアクライアント モジュールのリモートアクセス VPN グループポリシーの設定

Firewall Management Center によって管理される Firewall Threat Defense を使用して、エンドポイントに セキュアクライアント モジュールをインストールして更新するには、セキュアクライアントモジュール設定でリモートアクセス VPN グループポリシーを更新する必要があります。

始める前に

Firewall Management Center でリモートアクセス VPN ポリシーが設定されていることを確認します。

手順

ステップ 1 [デバイス（Devices）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 2 リモートアクセス VPN ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3 接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [グループポリシーの編集（Edit Group Policy）] をクリックします。

ステップ 5 [Secure Client] > [AnyConnect] タブをクリックします。

ステップ 6 [クライアントモジュール（Client Modules）] をクリックします。

ステップ 7 [+] をクリックします。

ステップ 8 [Clientモジュール（Client Module）] ドロップダウンリストからモジュールを選択します。

ステップ 9 [ダウンロードするプロファイル（Profile to download）] ドロップダウンリストからモジュールのプロファイルを選択するか、[+] をクリックしてプロファイルを追加します。

ステップ 10 [モジュールのダウンロードの有効化（Enable module download）] チェックボックスをオンにして、エンドポイントにモジュールをダウンロードします。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 さらにモジュールを追加する場合は、ステップ 7 ～ 11 を繰り返します。

ステップ 13 [保存（Save）] をクリックします。

次のタスク

1. 設定を Threat Defense に展開します。
2. セキュアクライアント を起動し、VPN プロファイルを選択して VPN に接続します。セキュアクライアント は、設定されたモジュールを VPN にインストールします。
3. 設定を確認します。詳細については、「セキュアクライアントモジュール設定の確認（1668 ページ）」を参照してください。

セキュアクライアント モジュール設定の確認

（Firewall Threat Defense）

プロファイルとセキュアクライアントモジュールの設定を表示するには、Firewall Threat Defense で以下のコマンドを使用します。

- **show disk0:**：プロファイルとその設定を表示します。
- **show run webvpn**：Secure Client 設定の詳細を表示します。
- **show run group-policy <ravpn_group_policy_name>**：Secure Client の RA VPN グループポリシーの詳細を表示します。
- **show vpn-sessiondb anyconnect**：アクティブな Secure Client VPN セッションの詳細を表示します。

エンドポイントで

1. セキュアクライアント を使用して、Firewall Threat Defense への VPN 接続を確立します。
2. 設定されたモジュールがダウンロードされ、セキュアクライアント の一部としてインストールされているかどうかを確認します。
3. 設定されたプロファイル（存在する場合）が『すべてのオペレーティングシステムに対するプロファイルの場所』で指定されている場所で使用可能かどうかを確認します。

（Firewall Management Center）

リモートアクセス VPN ダッシュボードを使用して、Firewall Management Center でアクティブなリモートアクセス VPN セッションをモニターできます（[概要（Overview）] > [リモートアクセスVPN（Remote Access VPN）]。ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。

モバイルデバイスでのアプリケーションベース（アプリケーションごとの VPN）のリモートアクセス VPN の設定

セキュアクライアント を使用してモバイルデバイスから VPN 接続を確立すると、個人アプリケーションからのトラフィックを含むすべてのトラフィックが VPN 経由でルーティングされます。

Android または iOS で実行されるモバイルデバイスの場合、VPN トンネルを使用するアプリケーションを制限できます。このアプリケーションベースのリモートアクセス VPN は、Per App VPN と呼ばれます。アプリケーションごとの VPN を使用するには、サードパーティの Mobile Device Manager（MDM）アプリケーションをインストールする必要があります。MDM で VPN トンネル経由で使用できる承認済みアプリケーションのリストを定義する必要があります。Firewall Threat Defense ヘッドエンドでアプリケーションごとの VPN を有効にして、MDM がモバイルデバイスにポリシーを適用できるようにできます。

利点

リモートアクセス VPN を承認済みアプリケーションに制限する利点は以下のとおりです。

- パフォーマンス：企業のネットワーク上の VPN トラフィックを制限し、VPN ヘッドエンドのリソースを解放することができます。
- 保護：モバイルデバイス上の未承認の悪意のあるアプリケーションから、企業の VPN トンネルを保護することができます。

Per App VPN トンネルの設定の前提条件とライセンス

前提条件

- サードパーティの Mobile Device Manager（MDM）をインストールして設定します。

  Firewall Threat Defense ヘッドエンドデバイスではなく、MDM 自体の VPN で許可されるアプリケーションを設定する必要があります。

- Cisco Software Download Center から Cisco AnyConnect 企業アプリケーションセレクタをダウンロードします。

  このツールは、Per App VPN ポリシーを定義するために必要です。

ライセンシング

- Secure Client Premier、または Secure Client Advantage。
- Essentials ライセンスにより輸出規制機能が許可される必要があります。

  Firewall Management Center でこの機能を確認するには、[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] の順に選択します。

モバイルアプリケーションのアプリケーション ID の決定

モバイルデバイスからアプリケーションベースの VPN を許可するように Firewall Threat Defense ヘッドエンドを設定する前に、トンネルで許可するアプリケーションを決定する必要があります。

ユーザーのモバイルデバイスで、MDM にアプリケーションごとのポリシーを設定することを強く推奨します。これにより、ヘッドエンドの設定が簡素化されます。ヘッドエンドで許可されているアプリケーションのリストを設定することにした場合は、エンドポイントのタイプごとに各アプリケーションのアプリケーション ID を決定する必要があります。

iOS でバンドル ID と呼ばれるアプリケーション ID は、逆引き DNS 名です。ワイルドカードとしてアスタリスクを使用できます。たとえば、*. * はすべてのアプリケーションを示し、com.cisco. * はすべてのシスコアプリケーションを示します。

アプリケーション ID を決定するには、次の手順を実行します。

- **Android**：Web ブラウザで Google Play に移動し、アプリカテゴリを選択します。許可するアプリケーションをクリック（またはマウスオーバー）して、URL を確認します。アプリケーション ID は、URL 内の **id=**パラメータに示されます。たとえば、次は Facebook Messenger の URL であるため、アプリケーション ID は com.facebook.orca です。

  https://play.google.com/store/apps/details?id=com.facebook.orca

  独自のアプリケーションなどの Google Play を通じて入手できないアプリケーションの場合は、パッケージ名ビューアアプリケーションをダウンロードして、アプリケーション ID を抽出します。これらの多くの使用可能アプリケーションがあり、そのいずれかが必要なものを提供しますが、シスコはどれも推奨しません。

- **iOS**：バンドル ID を取得する簡単な方法はありません。次の方法で検索できます。

  1. Chrome などのデスクトップの Web ブラウザを使用して、アプリケーション名を検索します。
  2. 検索結果で、Apple App Store からアプリケーションをダウンロードするためのリンクを探します。たとえば、Facebook Messenger は次のようになります。

     https://apps.apple.com/us/app/messenger/id454638411
  3. **id** 文字列の後に数値をコピーします。この例では、**454638411** です。
  4. 新しいブラウザウィンドウを開き、次の URL の末尾に数値を追加します。

     https://itunes.apple.com/lookup?id=

     この例では、次のとおりです。https://itunes.apple.com/lookup?id=454638411
  5. 通常は 1.txt という名前のテキストファイルをダウンロードするように求められます。ファイルをダウンロードします。
  6. ワードパッドなどのテキストエディタでファイルを開き、bundleId を検索します。次に例を示します。

     "bundleId":"com.facebook.Messenger"

この例では、バンドル ID は「com.facebook.Messenger」です。これをアプリケーション ID として使用します。

アプリケーション ID のリストを取得したら、 で説明されているように、ポリシーを設定できます。

アプリケーションベースの VPN トンネルの設定

MDM ソフトウェアをインストールして設定したら、Firewall Threat Defense ヘッドエンドデバイスでアプリケーションベースの VPN を有効にできます。ヘッドエンドで有効にすると、MDM ソフトウェアは、VPN を介して企業のネットワークにトンネリングされるアプリケーションを制御します。

始める前に

- Firewall Management Center にリモートアクセス VPN ポリシーがあることを確認します。
- MDM を使用してアプリケーションごとの VPN を設定し、各デバイスを MDM サーバーに登録します。
- Cisco AnyConnect 企業アプリケーション セレクタ ツールをダウンロードします。

手順

ステップ 1 Cisco AnyConnect 企業アプリケーションセレクタを使用して、Per App VPN ポリシーを定義します。

単純な**すべて許可**のポリシーを作成し、MDM で許可するアプリケーションを定義することを推奨します。ただし、アプリケーションのリストを指定して、ヘッドエンドからリストを許可および制御できます。特定のアプリケーションを含める場合は、一意の名前とアプリケーションのアプリケーション ID を使用して、アプリケーションごとに個別のルールを作成します。アプリケーション ID 取得の詳細については、「モバイルアプリケーションのアプリケーション ID の決定」を参照してください。

AnyConnect 企業アプリケーションセレクタを使用して Android と iOS の両方のプラットフォームをサポートする**すべて許可**のポリシーを作成するには、次の手順を実行します。

a) プラットフォームタイプとして、ドロップダウンリストから [Android] を選択し、以下のオプションを設定します。

- [フレンドリ名（Friendly Name）]：ポリシーの名前を入力します。たとえば、Allow_All とします。
- [アプリケーションID（App ID）]：*.* と入力して、使用可能なすべてのアプリケーションと一致させます。
- 他のオプションはそのままにします。

b) プラットフォームタイプとして、ドロップダウンリストから [iOS] を選択し、以下のオプションを設定します。

- [フレンドリ名（Friendly Name）]：ポリシーの名前を入力します。たとえば、Allow_All とします。
- [アプリケーションID（App ID）]：*.* と入力して、使用可能なすべてのアプリケーションと一致させます。
- 他のオプションはそのままにします。

c) [ポリシー（Policy）]>[ポリシーの表示（View Policy）] を選択して、ポリシーの base64 でエンコードされた文字列を取得します。

この文字列には、Firewall Threat Defense がポリシーを確認できるようにする、暗号化された XML ファイルが含まれています。この値をコピーします。この文字列は、Firewall Threat Defense でアプリケーションごとの VPN を設定するときに必要になります。

ステップ 2 Firewall Management Center を使用して、Firewall Threat Defense ヘッドエンドデバイスでアプリケーションごとの VPN を有効にします。

a) [デバイス（Devices）]>[リモートアクセス（Remote Access）] を選択します。
b) リモートアクセス VPN ポリシーを選択し、[編集（Edit）] をクリックします。
c) 接続プロファイルを選択し、[編集（Edit）] をクリックします。
d) [グループポリシーの編集（Edit Group Policy）] をクリックします。
e) [Secure Client]>[AnyConnect] タブをクリックします。
f) [カスタム属性（Custom Attributes）] をクリックし、[+] をクリックします。
g) [Secure Client属性（Secure Client Attribute）]>[AnyConnect]>[属性（Attribute）] ドロップダウンリストから [Per App VPN] を選択します。
h) [カスタム属性オブジェクト（Custom Attribute Object）] ドロップダウンリストからオブジェクトを選択するか、[+] をクリックしてオブジェクトを追加します。

アプリケーションごとの VPN に新しいカスタム属性オブジェクトを追加する場合は、Cisco AnyConnect Enterprise Application Selector から名前、説明、および base64 でエンコードされたポリシー文字列を入力します。

i) **[Save（保存）]** をクリックします。
j) [追加（Add）] をクリックし、[保存（Save）] をクリックします。

ステップ 3 Firewall Management Center に変更を展開します。

次のタスク

1. セキュアクライアント を起動し、VPN プロファイルを選択して、VPN に接続します。
2. 設定を確認します。詳細については、「アプリケーションごとの設定の確認 （1673 ページ）」を参照してください。

アプリケーションごとの設定の確認

（Firewall Threat Defense）

アプリケーションごとの設定を確認するには、Firewall Threat Defense で以下のコマンドを使用します。

- **show run webvpn**
- **show run group-policy <ravpn_group_policy_name>**
- **show run anyconnect-custom-data**

エンドポイントで

エンドポイントが Firewall Threat Defense との VPN 接続を確立したら、以下の手順を実行します。

1. セキュアクライアント の [統計（Statistics）] アイコンをクリックします。
2. [トンネルモード（Tunnel Mode）] は、[すべてのトラフィックをトンネリング（Tunnel All Traffic）] ではなく [アプリケーショントンネル（Application Tunnel）] になります。
3. [トンネリングされたアプリケーション（Tunneled Apps）] には、MDM でトンネリングを有効にしたアプリケーションがリストされます。

リモート アクセス VPN の例

ユーザーあたりの Secure Client 帯域幅を制限する方法

ここでは、ユーザーが セキュアクライアント を使用して Secure Firewall Threat Defense リモートアクセス VPN ゲートウェイに接続する場合に VPN ユーザーに消費される最大帯域幅を制限する手順について説明します。Firewall Threat Defense で Quality of Service（QoS）ポリシーを使用して最大帯域幅を制限し、単一のユーザーやグループまたは複数のユーザーがリソース全体を引き継ぐことがないようにすることができます。この設定では、重要なトラフィックに優先順位を付け、帯域幅の占有を防止し、ネットワークを管理できます。トラフィックが最大レートを超えると、Firewall Threat Defenseは超過した分のトラフィックをドロップします。

手順	操作手順	詳細
1	レルムを作成および設定します。	LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）

手順	操作手順	詳細
2	新しく作成したレルムで利用可能なユーザーまたはグループの QoS ポリシーおよび QoS ルールを作成します。	• QoS ポリシーの作成については、QoS ポリシーの作成（812 ページ）を参照してください。 • QoS ルールの作成については、QoS ルールの設定（813 ページ）を参照してください。
3	リモートアクセス VPN ポリシーを設定し、ユーザー認証用に新しく作成したレルムを選択します。	新しいリモート アクセス VPN ポリシーの作成（1572 ページ）
4	リモートアクセス VPN ポリシーを展開します。	設定変更の展開（172 ページ）

ユーザーIDベースのアクセスコントロールルールにVPNアイデンティティを使用する方法

手順	操作手順	詳細
1	レルムを作成および設定します。	LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452 ページ）。
2	アイデンティティ ポリシーを作成し、アイデンティティ ルールを追加します。	• アイデンティティポリシーの作成については、アイデンティティ ポリシーの作成（2555 ページ）を参照してください。 • アイデンティティルールの作成については、アイデンティティ ルールの作成（2565 ページ）を参照してください。
3	アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます。	アクセス制御への他のポリシーの関連付け（1765 ページ）
4	リモートアクセス VPN ポリシーを設定し、ユーザー認証用に新しく作成したレルムを選択します。	新しいリモート アクセス VPN ポリシーの作成（1572 ページ）
5	リモートアクセス VPN ポリシーを展開します。	設定変更の展開（172 ページ）

Firewall Threat Defense 複数証明書認証の設定

複数証明書ベースの認証

複数証明書ベースの認証により、Firewall Threat Defense はマシンまたはデバイスの証明書を検証できます。リモートアクセス VPN 接続プロファイルでは、証明書ベースの認証に対して複数の証明書を有効にでき、AAA 認証と組み合わせることができます。リモートアクセス VPN 接続プロファイルで複数証明書オプションを使用すると、証明書を介したマシンとユーザーの両方の証明書認証が可能になり、デバイスが企業支給のデバイスであることを確認し、ユーザーのアイデンティティ証明書を認証して RA VPN アクセスを許可できます。管理者は、セッションのユーザー名の取得元（マシン証明書またはユーザー証明書）を選択できます。

複数証明書ベースの認証が設定されている場合、VPN クライアントから 2 つの証明書が取得されます。

- [最初の証明書（First Certificate）]：エンドポイントを認証するためのマシン証明書。
- [2番目の証明書（Second Certificate）]：VPN ユーザーを認証するためのユーザー証明書。

Firewall Threat Defense 証明書の詳細については、Firewall Threat Defense 証明書の管理 （1456 ページ）を参照してください。

制限事項

- 複数証明書認証では、現在、証明書の数が 2 に制限されています。
- Secure Client では、RSA ベースの証明書のみがサポートされています。
- Secure Client 集約認証の間は、SHA256、SHA384、および SHA512 ベースの証明書のみがサポートされています。
- 証明書認証を SAML 認証と組み合わせることはできません。

証明書からのユーザー名事前入力

ユーザー名事前入力オプションを使用すると、証明書のフィールドを解析して、後続の AAA 認証（プライマリまたはセカンダリ）に使用できます。認証に 2 つの証明書を使用する場合、管理者は、事前入力機能のためにユーザー名を取得する必要がある証明書を選択できます。デフォルトでは、事前入力のユーザー名は、ユーザー証明書（Secure Client から受信する 2 番目の証明書）から取得されます。証明書のみの認証方式が有効になっている場合、事前入力されたユーザー名が VPN セッションのユーザー名として使用されます。AAA と証明書の認証が有効になっている場合は、VPN セッションのユーザー名は事前入力オプションに基づいています。

リモートアクセス VPN の複数証明書認証の設定

1. Secure Firewall Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

2. 既存のリモートアクセスポリシーを編集するか、新しいポリシーを作成してから編集します。

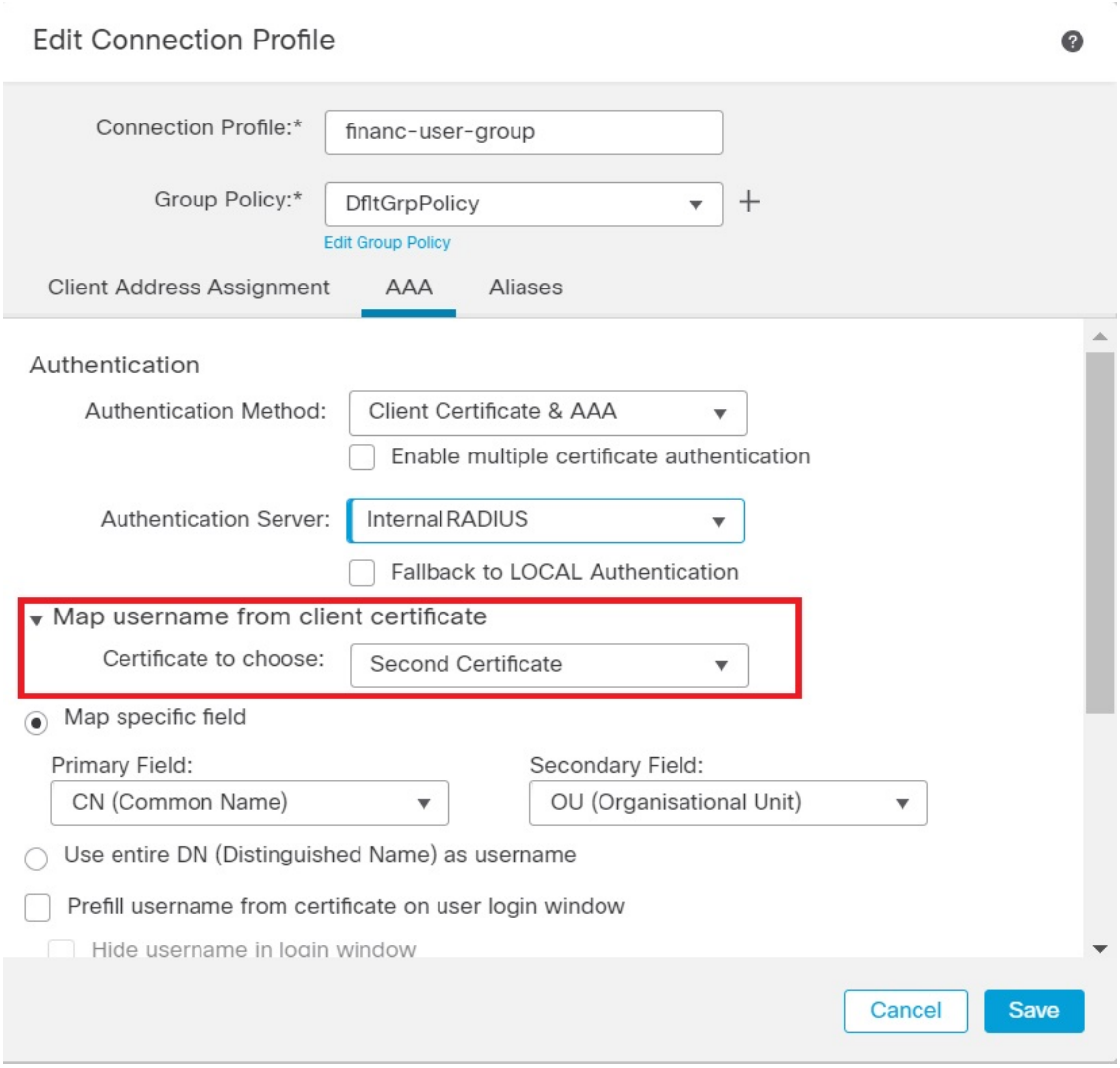
   新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）を参照してください。

3. 複数証明書認証を設定するには、接続プロファイルを選択して [編集（Edit）] をクリックします。

   接続プロファイルの設定 （1585 ページ）を参照してください。

4. [AAA] を選択してから、[認証方式（Authentication Method）] を選択します。

   図 *313*:



- [クライアント証明書のみ（Client Certificate Only）]：ユーザーはクライアント証明書を使用して認証されます。クライアント証明書は、VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザー名はクライアント証明書フィールドの CN および OU からそれぞれ取得されます。クライアント証明書の他の

フィールドにユーザー名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマッピングします。

- [クライアント証明書とAAA（Client Certificate & AAA）]：ユーザーは、AAA とクライアント証明書の両方の認証タイプを使用して認証されます。

5. [複数の証明書認証を有効にする（Enable multiple certificate authentication）] を選択します。
6. [クライアント証明書からのユーザー名のマッピング（Map username from client certificate）] を選択し、[選択する証明書（Certificate to choose）] ドロップダウンから証明書を選択して、VPNセッションのユーザー名をマシン証明書またはユーザー証明書から選択します。
   - [最初の証明書（First Certificate）]：マシン証明書からのユーザー名をマッピングします。
   - [2番目の証明書（Second Certificate）]：VPN ユーザーを認証するためにユーザー証明書からのユーザー名をマッピングします。
7. 必要な接続プロファイル設定およびリモートアクセス VPN 設定を設定します。
8. 接続プロファイルおよびリモートアクセス VPN ポリシーを保存します。リモートアクセス VPN ポリシーを Firewall Threat Defense に展開します。

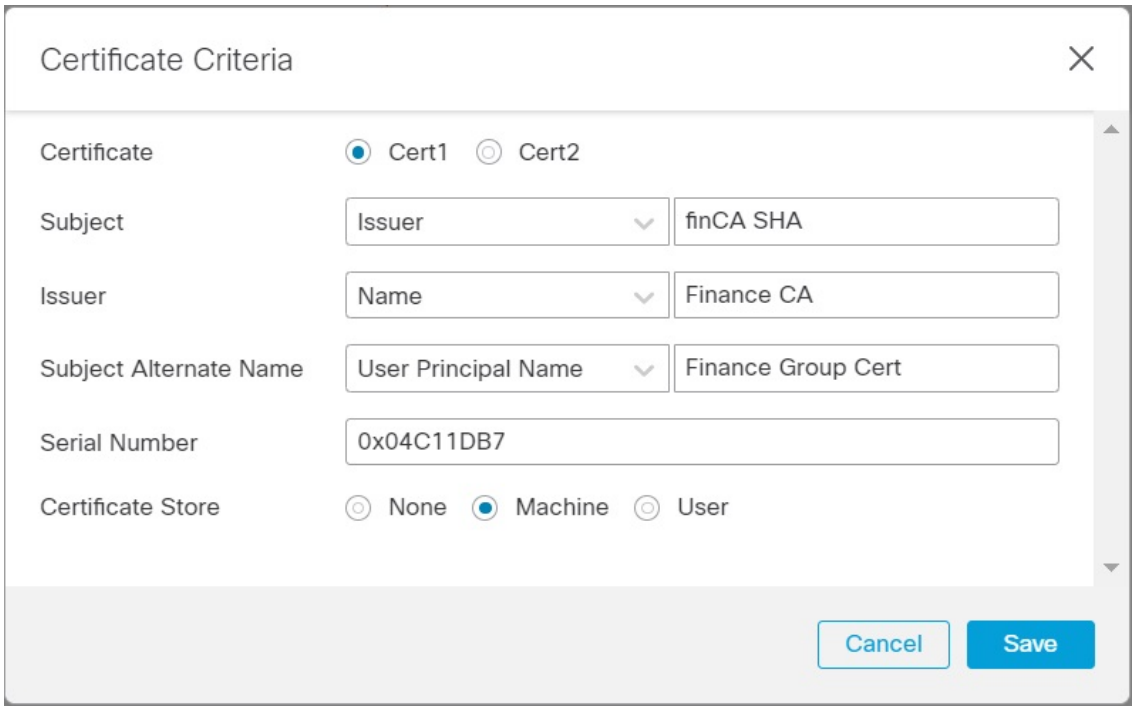
リモートアクセスVPNAAA設定の詳細については、リモートアクセスVPNのAAA設定（1588ページ）を参照してください。

DAP での証明書の設定

DAP レコードで証明書基準属性を設定することもできます。複数証明書認証中に VPN クライアントから受信したユーザーおよびマシンの証明書はダイナミック アクセス ポリシー（DAP）にロードされるため、証明書のフィールドに基づいてポリシーを設定できます。接続試行を認証するために使用された証明書のフィールドに基づいてポリシーを決定できます。

1. [デバイス（Devices）] > [ダイナミック アクセス ポリシー（Dynamic Access Policy）] を選択します。 >
2. 既存の DAP ポリシーを編集するか、新しい DAP ポリシーを作成してからポリシーを編集します。
3. 既存の DAP レコードを選択するか、新しい DAP レコードを作成してからレコードを編集します。
4. **[エンドポイント基準（Endpoint Criteria）]** > **[証明書（Certificate）]**を選択します。
5. 一致基準 [すべて（All）] または [任意（Any）] を選択します。
6. [追加（Add）] をクリックして、証明書属性を追加します。

図 *314 :*



7. 証明書、[Cert1] または [Cert2] を選択します。
8. [サブジェクト（Subject）] を選択し、証明書のサブジェクト値を指定します。
9. [発行者（Issuer）] を選択し、証明書の発行者名を指定します。
10. [サブジェクト代替名（Subject Alternate Name）] を選択し、サブジェクトの代替名を指定します。
11. [シリアル番号（Serial Number）] を指定します。
12. [証明書ストア（Certificate Store）] を選択します（[なし（None）]、[マシン（Machine）]、または [ユーザー（User）]）。

    このオプションでは、エンドポイントで証明書が選択されたストアを確認する条件を追加します。
13. [保存（Save）] をクリックして、証明書条件の設定を完了します。

    必要な DAP レコード設定を設定し、DAP をリモートアクセス VPN に関連付けます。

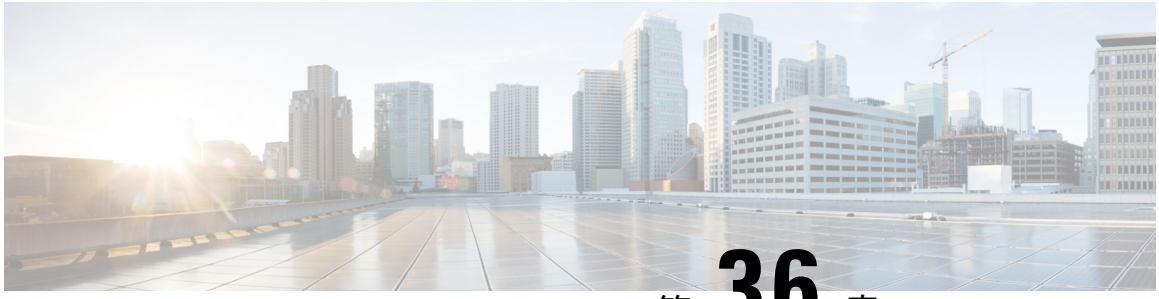
DAP の詳細については、ダイナミック アクセス ポリシー （1683 ページ）を参照してください。

リモートアクセス VPN の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
SAML と証明書のサポート	7.2	任意（Any）	証明書と SAML によるユーザー認証をサポートするように、リモートアクセス VPN 構成ウィザードを更新しました。SAML 認証が開始される前に、マシンまたはユーザー証明書を認証するようにリモートアクセス VPN を設定できます。
IPsec フローがオフロードされます。	7.2	任意（Any）	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
複数の IDP トラストポイントのサポート	7.1	任意（Any）	Secure Firewall Management Center は、Microsoft Azure を使用した複数の ID プロバイダートラストポイントをサポートします。Microsoft Azure では、同じエンティティ ID に対して複数のアプリケーションを設定できますが、アイデンティティ証明書は一意である必要があります。
AnyConnect VPN SAML 外部ブラウザ	7.1	任意（Any）	AnyConnect VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthn、FIDO、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、追加の認証の選択肢を有効にできるようになりました。リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、AnyConnect クライアントが AnyConnect 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。 リモートアクセス VPN 接続プロファイルウィザードが更新され、**SAML ログインエクスペリエンス**を設定できるようになりました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
複数証明書認証	7.0	任意（Any）	Secure Firewall Management Center は、Firewall Threat Defense に対して複数証明書ベースの認証をサポートするようになり、AnyConnect クライアントを使用して VPN アクセスを許可するためにユーザーのアイデンティティ証明書を認証することに加えて、マシンまたはデバイス証明書を検証して、デバイスが会社支給のデバイスであることを確認できます。
VPN ロードバランシング	7.0	任意（Any）	VPN ロードバランシングでは、2 つ以上のデバイスが論理的にグループ化され、スループットやその他のトラフィックパラメータは考慮されずに、グループ化されたデバイス間でリモートアクセス VPN セッションが均等に分散されます。
AnyConnect カスタム属性	7.0	任意（Any）	Secure Firewall Management Center は、AnyConnect カスタム属性をサポートし、AnyConnect クライアント機能を設定するためのインフラストラクチャを、それらの機能に対するハードコードサポートを Firewall Threat Defense に追加することなく、提供するようになりました。
ローカルユーザー認証	7.0	任意（Any）	Secure Firewall Management Center Web インターフェイスを使用して Firewall Threat Defense でローカルにユーザーを設定および管理し、プライマリおよびセカンダリのリモートアクセス VPN 認証用にローカルユーザーを設定できるようになりました。
選択的ポリシーの展開	7.0	任意（Any）	展開時に、リモートアクセス VPN およびサイト間 VPN 設定への変更を含めるか除外するかを選択できるようになりました。
AnyConnect モジュール設定のサポート	6.7	いずれか	Secure Firewall Management Center は、セキュリティを強化するために AnyConnect モジュールとプロファイルの設定をサポートするようになりました。
LDAP 許可のサポート	6.7	いずれか	Secure Firewall Management Center を使用して、リモートアクセス VPN の LDAP 認証を設定できます。
リモートアクセス VPN の SAML シングルサインオンサポート	6.7	いずれか	SAML 2.0 サーバーをリモートアクセス VPN のシングルサインオン認証サーバーとして設定できます。
AnyConnect 管理 VPN トンネルのサポート	6.7	いずれか	Firewall Threat Defense リモートアクセス VPN は、VPN ユーザーが VPN に接続しなくても、企業のエンドポイントの電源がオンになったときにエンドポイントへの VPN 接続を可能にする AnyConnect 管理 VPN トンネルの設定をサポートします。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Datagram Transport Layer Security（DTLS）1.2 のサポート。	6.6	任意（Any）	DTLS 1.2 は、デフォルトの SSL 暗号グループに含まれるようになり、TLS 1.2 とともに構成できます。



第 36 章

ダイナミック アクセス ポリシー

ダイナミック アクセス ポリシー（DAP）を使用すると、VPN 環境のダイナミクスに対応する許可を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。

- Secure Firewall Threat Defense ダイナミック アクセス ポリシーについて （1683 ページ）
- ダイナミック アクセス ポリシーの前提条件 （1685 ページ）
- ダイナミック アクセス ポリシーに関する注意事項と制限事項 （1685 ページ）
- ダイナミック アクセス ポリシー（DAP）の設定 （1686 ページ）
- ダイナミック アクセス ポリシーとリモートアクセス VPN の関連付け （1696 ページ）
- ダイナミック アクセス ポリシーの履歴 （1697 ページ）

Secure Firewall Threat Defense ダイナミック アクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、複数の変数が影響を与える可能性があります。たとえば、頻繁に変更されるイントラネット設定、組織内の各ユーザーが持つさまざまなロール、および設定とセキュリティレベルが異なるリモートアクセスサイトからのログイン試行などです。VPN環境でのユーザー認可のタスクは、スタティックな設定のネットワークでの認可タスクよりもかなり複雑です。

ダイナミック アクセス ポリシーは、特定のユーザートンネルまたはユーザーセッションに関連付ける一連のアクセスコントロール属性を設定して作成できます。これらの属性により、複数のグループメンバーシップやエンドポイントセキュリティの問題に対処します。Firewall Threat Defense では、定義したポリシーに基づき、特定のセッションへのアクセス権が特定のユーザーに付与されます。Firewall Threat Defense デバイスは、ユーザーの認証中に、DAP レコードからの属性を選択または集約することによって DAP を生成します。次に、リモートデバイスのエンドポイントセキュリティ情報および認証されたユーザーの AAA 認可情報に基づいて DAP レコードを選択します。その後、デバイスは選択した DAP レコードをユーザートンネルまたはセッションに適用します。

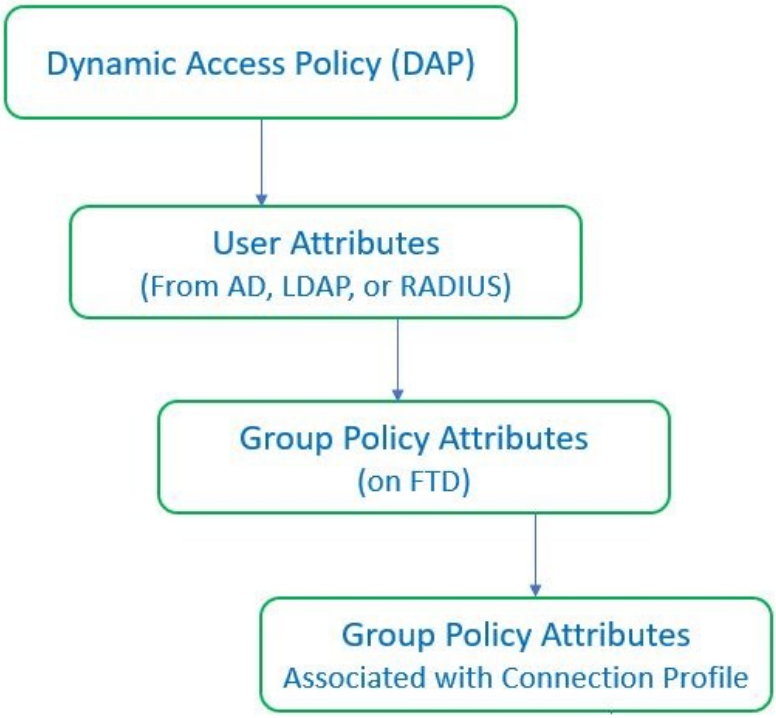
Firewall Threat Defense での権限および属性のポリシー適用階層

Firewall Threat Defense デバイスは、ユーザー認可属性（ユーザー権利またはユーザー権限とも呼ばれる）の VPN 接続への適用をサポートしています。属性は、Firewall Threat Defense の DAP、外部認証サーバー、または認可 AAA サーバー（RADIUS）（あるいはこれらのすべて）、または Firewall Threat Defense デバイスのグループポリシーから適用されます。

Firewall Threat Defense デバイスは、すべてのソースから属性を受信すると、その属性を評価し、集約してユーザーポリシーに適用します。DAP、AAA サーバー、またはグループポリシーから取得した属性の間で衝突がある場合、DAP から取得した属性が常に優先されます。

Firewall Threat Defense デバイスは次の順序で属性を適用します。

図 *315*：ポリシー実施フロー



1. **FTD 上の DAP 属性**：DAP 属性は、他のすべての属性よりも優先されます。
2. **外部 AAA サーバー上のユーザー属性**：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。
3. **FTD で設定されているグループポリシー**：RADIUS サーバーからユーザーの RADIUS Class 属性 IETF-Class-25（OU=group-policy）の値が返された場合、Firewall Threat Defense デバイスはそのユーザーを同じ名前のグループポリシーに入れて、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。

4. **接続プロファイル（トンネルグループと呼ばれる）で割り当てられたグループポリシー**：接続プロファイルには、接続の事前設定と、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。

（注） Firewall Threat Defense デバイスは、デフォルトのグループ ポリシー *DfltGrpPolicy* から継承したシステム デフォルト属性をサポートしていません。ユーザー属性または AAA サーバーのグループポリシーによって上書きされない場合、デバイスは、接続プロファイルに割り当てられたグループポリシーの属性をユーザーセッションに使用します。

ダイナミック アクセス ポリシーの前提条件

ライセンス：

- Firewall Threat Defense には次の セキュアクライアント ライセンスの少なくとも 1 つが必要です。
  - Secure Client Premier
  - Secure Client Advantage
  - Secure Client VPN のみ
- Firewall Threat Defense Essentials ライセンスにより輸出規制機能が許可される必要があります。

ダイナミックアクセスポリシーに関する注意事項と制限事項

- DAP での AAA 属性の照合は、リモートアクセス VPN セッションを認証または認可するときに正しい属性を返すように AAA サーバーが設定されている場合にのみ機能します。
- DAP でサポートされる Secure Client および Secure Firewall ポスチャ パッケージの最小バージョンは 4.6 です。ただし、最新バージョンの Secure Client を使用することを強くお勧めします。
- DAP はクラスタリングまたはマルチインスタンスモードをサポートしていません。
- IPv4 または IPv6 アドレスが割り当てられた DAP 条件は、ローカル認証では機能しません。

ダイナミック アクセス ポリシー（DAP）の設定

ダイナミック アクセス ポリシーの作成

始める前に

ダイナミック アクセス ポリシーを設定する前に、Secure Firewall ポスチャ パッケージがあることを確認してください。Secure Firewall ポスチャ ファイルは、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[VPN]** > **[Secure Client ファイル（Secure Client File）]** で追加できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[ダイナミックアクセスポリシー（Dynamic Access Policy）]** > **[ダイナミックアクセスポリシーの作成（Create Dynamic Access Policy）]**を選択します。

ステップ 2 DAP ポリシーの [名前（Name）] を指定し、必要に応じて [説明（Description）] を指定します。

ステップ 3 ドロップダウンリストから **[HostScanパッケージ（HostScan Package）]** を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

DAP レコードを設定するには、「ダイナミック アクセス ポリシー レコードの作成」を参照してください。

ダイナミック アクセス ポリシー レコードの作成

ダイナミック アクセス ポリシー（DAP）には、ユーザーとエンドポイントの属性を構成する複数の DAP レコードを含めることができます。ユーザーが VPN 接続を試みるときに必要な基準を Firewall Threat Defense が選択および順序付けできるように、DAP 内の DAP レコードに優先順位を付けることができます。

手順

ステップ 1 [デバイス（Devices）] > [ダイナミック アクセス ポリシー（Dynamic Access Policy）] を選択します。 >

ステップ 2 既存のダイナミック アクセス ポリシーを編集するか、[ダイナミック アクセス ポリシーの作成（Create Dynamic Access Policy）] をクリックして新しいポリシーを作成してからポリシーを編集します。

ステップ 3 [DAPレコードの作成（Create DAP Record）] をクリックします。

ステップ 4 [全般（General）] タブをクリックします。

ステップ 5 DAP レコードの [名前（Name）] を指定します。

ステップ 6 DAP レコードの [優先順位（Priority）] を入力します。

値が小さいほど、プライオリティが高くなります。

ステップ 7 DAP レコードが一致した場合に実行するアクションを次から 1 つ選択します。

- **[続行（Continue）]**：セッションにアクセス ポリシー属性を適用します。存在する場合は、次の DAP レコード（優先順位の低い,次のポリシー行）が評価されます。
- [強制終了（Terminate）]：エンドユーザーセッションを強制終了します。
- [検疫（Quarantine）]：接続を隔離します。

ステップ 8 [基準に一致したときユーザーメッセージを表示（Display User Message on Criterion Match）] チェックボックスをオンにして、ユーザーメッセージを追加します。

Firewall Threat Defense で、DAP レコードが一致する場合に、このメッセージがユーザーに表示されます。

ステップ 9 **[トラフィックにネットワーク ACL を適用する（Apply a Network ACL on Traffic）]** チェックボックスをオンにして、ドロップダウンからアクセス制御リストを選択します。

ステップ 10 **[1つまたは複数のセキュア クライアント カスタム属性を適用する（Apply one or more Secure Client Custom Attributes）]** チェックボックスをオンにして、ドロップダウンからカスタム属性オブジェクトを選択します。

ステップ 11 [保存（Save）] をクリックします。

DAP の AAA 基準設定を構成する

DAP は AAA サービスを補完します。用意されている認可属性のセットは限られていますが、それらの属性によって AAA で提供される認可属性を無効にできます。Firewall Threat Defense は、ユーザーの AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。Firewall Threat Defense は、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

手順

ステップ 1 [デバイス（Devices）] > [ダイナミック アクセス ポリシー（Dynamic Access Policy）] を選択します。 >

ステップ 2 既存の DAP ポリシーを編集するか、新しい DAP ポリシーを作成してからポリシーを編集します。

ステップ 3 DAP レコードを選択するか新しいレコードを作成して、DAP レコードを編集します。

ステップ 4 [AAA基準（AAA Criteria）] をクリックします。

ステップ 5 次の [セクション間の一致基準（Match criteria between sections）] のいずれかを選択します。

- [任意（Any）]：いずれかの基準に一致する。
- [すべて（All）]：すべての基準に一致する。
- [なし（None）]：設定された基準のいずれにも一致しない。

ステップ 6 [追加（Add）] をクリックして、必要な **Cisco VPN 基準**を追加します。

Cisco VPN 基準には、グループポリシー、割り当てられた IPv4 アドレス、割り当てられた IPv6 アドレス、接続プロファイル、ユーザー名、ユーザー名 2、必要な SCEP の属性が含まれます。

a) 属性を選択し、**値**を指定します。

b) [別の条件を追加（Add another criteria）] をクリックして、さらに条件を追加します。

c) **[保存（Save）]** をクリックします。

必要な SCEP

ステップ 7 [LDAP基準（LDAP Criteria）]、[RADIUS基準（RADIUS Criteria）]、[SAML基準（SAML Criteria）] を選択し、[属性ID（Attribute ID）] と [値（Value）] を指定します。

ステップ 8 [保存（Save）] をクリックします。

DAP のエンドポイント属性選択基準の設定

エンドポイント属性には、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。Firewall Threat Defense は、エンドポイント属性の集合をセッション確立時に動的に生成し、セッションに関連付けられたデータベースにその属性を保存します。各 DAP レコードには、Firewall Threat Defense がセッションの DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されます。Firewall Threat Defenseは、設定されたすべての条件を満たす DAP レコードだけを選択します。

手順

ステップ 1 **[デバイス（Devices）] > [ダイナミックアクセスポリシー（Dynamic Access Policy）] > [ダイナミックアクセスポリシーの作成（Create Dynamic Access Policy）]**を選択します。

ステップ 2 DAP ポリシーを編集してから、DAP レコードを編集します。

（注）
DAP ポリシーと DAP レコードをまだ作成していない場合は作成します。

ステップ 3 [エンドポイント基準（Endpoint Criteria）] をクリックし、次のエンドポイント基準属性を設定します。

（注）
各タイプのエンドポイント属性のインスタンスを複数作成できます。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

- DAP へのマルウェア対策エンドポイント属性の追加
- DAP へのデバイス エンドポイント属性の追加
- DAP への Secure Client エンドポイント属性の追加 （1691 ページ）
- DAP への NAC エンドポイント属性の追加
- DAP へのアプリケーション属性の追加
- DAP へのパーソナル ファイアウォール エンドポイント属性の追加
- DAP へのオペレーティング システム エンドポイント属性の追加
- DAP へのプロセス エンドポイント属性の追加
- DAP へのレジストリ エンドポイント属性の追加
- DAP へのファイル エンドポイント属性の追加
- DAP への複数証明書認証属性の追加

ステップ 4 [保存（Save）] をクリックします。

DAP へのマルウェア対策エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集し、**[エンドポイント基準（Endpoint Criteria）]** > **[マルウェア対策（Anti-Malware）]**を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックして、属性を追加します。

ステップ 4 [インストール済み（Installed）] をクリックして、選択したエンドポイント属性と付随する修飾子をインストールするか、インストールしないかを指定します。

ステップ 5 [有効（Enabled）] または [無効（Disabled）] を選択して、リアルタイムのマルウェアスキャンをアクティブまたは非アクティブにします。

ステップ 6 [ベンダー（Vendor）] のリストからマルウェア対策ベンダーの名前を選択します。

ステップ 7 マルウェア対策製品の [製品の説明（Product Description）] を選択します。

ステップ 8 マルウェア対策製品の [バージョン（Version）] を選択します。

ステップ 9 [最終更新（Last Update）] からの日数を指定します。

マルウェア対策製品の更新を、指定した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

ステップ 10 [保存（Save）] をクリックします。

DAP へのデバイス エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集し、**[エンドポイント基準（Endpoint Criteria）]**>**[デバイス（Device）]**を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックし、[=] または [≠] 演算子を選択して、次の属性に入力した値と属性が等しいか等しくないかを確認します。

- [ホスト名（Host Name）]：テスト対象のデバイスのホスト名。完全修飾ドメイン名（FQDN）ではなく、コンピュータのホスト名のみを使用します。
- [MACアドレス（MAC Address）]：テスト対象のネットワーク インターフェイス カードの MAC アドレス。アドレスのフォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。
- [BIOSシリアル番号（BIOS Serial Number）]：テスト対象のデバイスの BIOS シリアル番号の値。数値フォーマットは、製造業者固有です。
- [ポート番号（Port Number）]：デバイスのリッスンポート番号。
- [Secure Desktopバージョン（Secure Desktop Version）]：エンドポイントで実行されているホストスキャンイメージのバージョン。
- [OPSWATバージョン（OPSWAT Version）]：OPSWAT クライアントのバージョン。
- [プライバシー保護（Privacy Protection）]：なし、Cache Cleaner、Secure Desktop。
- [TCP/UDPポート番号（TCP/UDP Port Number）]：テスト対象のリスニング状態の TCP または UDP ポート。

ステップ 4 [保存（Save）] をクリックします。

DAP への Secure Client エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集し、**[エンドポイントの基準（Endpoint Criteria）]** > **[Secure Client]** を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックし、[=] または [≠] 演算子を選択して、入力した値と属性が等しいか等しくないかを確認します。

ステップ 4 [クライアントバージョン（Client Version）] と [プラットフォーム（Platform）] を選択します。

ステップ 5 [プラットフォームバージョン（Platform Version）] を選択し、[デバイスタイプ（Device Type）] と [デバイスの固有ID（Device Unique ID）] を指定します。

ステップ 6 [MACアドレス（MAC Addresses）] を MAC アドレスプールに追加します。

（注）
MACアドレスは XX-XX-XX-XX-XX-XX 形式である必要があります。各 X は 16 進数文字です。[別のMACアドレスを追加（Add another MAC Address）] をクリックして、さらにアドレスを追加できます。

ステップ 7 [保存（Save）] をクリックします。

DAP への NAC エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集し、**[エンドポイント基準（Endpoint Criteria）]** > **[NAC]**を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックして、NAC 属性を追加します。

ステップ 4 演算子を、ポスチャトークン文字列に等しい（=）または等しくない（≠）に設定します。ポスチャトークン文字列を [ポスチャステータス（Posture Status）] ボックスに入力します。

ステップ 5 [保存（Save）] をクリックします。

DAP へのアプリケーション属性の追加

手順

ステップ 1 DAP レコードを編集し、**[エンドポイント基準（Endpoint Criteria）]** > **[アプリケーション（Application）]**を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックして、アプリケーション属性を追加します。

ステップ 4 等しい（[=]）または等しくない（[≠]）を選択し、[クライアントタイプ（Client Type）] を指定して、リモートアクセス接続のタイプを示します。

ステップ 5 [保存（Save）] をクリックします。

DAP へのパーソナル ファイアウォール エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集し、**[エンドポイント基準（Endpoint Criteria）]** > **[パーソナルファイアウォール（Personal Firewall）]**を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックして、パーソナルファイアウォール属性を追加します。

ステップ 4 [インストール済み（Installed）] をクリックして、パーソナルファイアウォールのエンドポイント属性と付随する修飾子（[名前（Name）]/[操作（Operation）]/[値（Value）]列の下のフィールド）をインストールするか、インストールしないかを指定します。

ステップ 5 [有効（Enabled）] または [無効（Disabled）] を選択して、ファイアウォール保護をアクティブまたは非アクティブにします。

ステップ 6 リストからファイアウォール [ベンダー（Vendor）] の名前を選択します。

ステップ 7 ファイアウォールの [製品説明（Product Description）] を選択します。

ステップ 8 等しい（[=]）または等しくない（[≠]）演算子を選択し、パーソナルファイアウォール製品の [バージョン（Version）] を選択します。

ステップ 9 [保存（Save）] をクリックします。

DAP へのオペレーティング システム エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集し、**[エンドポイント基準（Endpoint Criteria）]** > **[オペレーティングシステム（Operating System）]**を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックして、エンドポイント属性を追加します。

ステップ 4 等しい（=）または等しくない（≠）演算子を選択し、[オペレーティングシステム（Operating System）] を選択します。

ステップ 5 等しい（=）または等しくない（≠）演算子を選択し、オペレーティングシステムの [バージョン（Version）] を指定します。

ステップ 6 [保存（Save）] をクリックします。

DAP へのプロセス エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集します。

ステップ 2 **[エンドポイント基準（Endpoint Criteria）]** タブをクリックします。

ステップ 3 [プロセス（Process）] をクリックします。

ステップ 4 [一致基準（Match Criteria）] に [すべて（All）] または [任意（Any）] を選択します。

ステップ 5 [+] をクリックして、プロセス属性を追加します。

ステップ 6 [存在する（Exists）] または [存在しない（Does not exist）] を選択します。

ステップ 7 [プロセス名（Process Name）] を指定します。

ステップ 8 [保存（Save）] をクリックします。

DAP へのレジストリ エンドポイント属性の追加

レジストリ エンドポイント属性のスキャンは Windows オペレーティング システムにのみ適用されます。

始める前に

レジストリ エンドポイント属性を設定する前に、どのレジストリ キーをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。

手順

ステップ 1 DAP レコードを編集します。
ステップ 2 **[エンドポイント基準（Endpoint Criteria）]** タブをクリックします。
ステップ 3 [レジストリ（Registry）] をクリックします。
ステップ 4 [一致基準（Match Criteria）] に [すべて（All）] または [任意（Any）] を選択します。
ステップ 5 [+] をクリックして、レジストリ属性を追加します。
ステップ 6 レジストリの [エントリパス（Entry Path）] を選択し、パスを指定します。
ステップ 7 レジストリの有無（**[存在する（Exists）]** または **[存在しない（Does not Exist）]**）を選択します。
ステップ 8 リストからレジストリの [種類（Type）] を選択します。
ステップ 9 等しい（=）または等しくない（≠）演算子を選択し、レジストリキーの **[値（Value）]** を入力します。
ステップ 10 スキャン中にレジストリエントリの大文字と小文字を無視するには、[大文字と小文字を区別しない（Case insensitive）] を選択します。
ステップ 11 [保存（Save）] をクリックします。

DAP へのファイル エンドポイント属性の追加

手順

ステップ 1 DAP レコードを編集します。
ステップ 2 **[エンドポイント基準（Endpoint Criteria）]** タブをクリックします。
ステップ 3 **File** をクリックします。
ステップ 4 一致基準 [すべて（All）] または [任意（Any）] を選択します。
ステップ 5 [+] をクリックして、ファイル属性を追加します。
ステップ 6 [ファイルパス（File Path）] を指定します。
ステップ 7 [存在する（Exists）] または [存在しない（Does not exist）] を選択して、ファイルの存在を示します。
ステップ 8 より小さい（[<]）またはより大きい（[>]）を選択し、ファイルの [最終更新（Last Modified）] 日を指定します。
ステップ 9 等しい（[=]）または等しくない（[≠]）演算子を選択し、[チェックサム（Checksum）] を入力します。
ステップ 10 [保存（Save）] をクリックします。

DAP への証明書認証属性の追加

受信した証明書のいずれかを設定されたルールで参照できるように各証明書をインデックス化できます。これらの証明書フィールドに基づいて、接続試行を許可または拒否する DAP ルールを設定できます。

手順

ステップ 1 DAP レコードを編集し、**[エンドポイント基準（Endpoint Criteria）]** > **[証明書（Certificate）]** を選択します。

ステップ 2 一致基準 [すべて（All）] または [任意（Any）] を選択します。

ステップ 3 [追加（Add）] をクリックして、証明書属性を追加します。

ステップ 4 証明書、[Cert1] または [Cert2] を選択します。

ステップ 5 [サブジェクト（Subject）] を選択し、サブジェクト値を指定します。

ステップ 6 [発行者（Issuer）] を選択し、発行者名を指定します。

ステップ 7 [サブジェクト代替名（Subject Alternate Name）] を選択し、サブジェクト値を指定します。

ステップ 8 [シリアル番号（Serial Number）] を指定します。

ステップ 9 [証明書ストア（Certificate Store）] を選択します（[なし（None）]、[マシン（Machine）]、または [ユーザー（User）]）。

VPN クライアントが証明書ストア情報を送信します。

ステップ 10 [保存（Save）] をクリックします。

DAP の詳細設定の設定

[詳細設定（Advanced）] タブを使用して、AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加できます。たとえば、指定された条件のいずれかを満たす、すべてを満たす、またはいずれも満たさない AAA 属性を使用するように Firewall Threat Defense を設定できます。エンドポイント属性は累積されるため、すべてを満たす必要があります。セキュリティアプライアンスが任意のエンドポイント属性を使用できるようにするには、Lua で適切な論理式を作成し、この手順でその式を入力する必要があります。

手順

ステップ 1 [デバイス（Devices）] > [ダイナミック アクセス ポリシー（Dynamic Access Policy）] を選択します。 >

ステップ 2 DAP ポリシーを編集してから、DAP レコードを編集します。

（注）

DAP ポリシーと DAP レコードをまだ作成していない場合は作成します。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 DAP 設定で使用する一致基準として [AND] または [OR] を選択します。

ステップ 5 [高度な属性照合用のLuaスクリプト（Lua script for advanced attribute matching）] フィールドに Lua スクリプトを追加します。

ステップ 6 [保存（Save）] をクリックします。

ダイナミック アクセス ポリシーとリモートアクセス VPN の関連付け

VPN セッションの認証または認可中にダイナミック アクセス ポリシー（DAP）属性が照合されるように、DAP をリモートアクセス VPN ポリシーに関連付ける必要があります。その後、リモートアクセス VPN をFirewall Threat Defenseに展開できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[リモートアクセス（Remote Access）]** を選択します。

ステップ 2 ダイナミック アクセス ポリシーを関連付けるリモートアクセス VPN ポリシーの横にある [編集（Edit）] をクリックします。

ステップ 3 リモートアクセス VPN のリンクをクリックして、ダイナミック アクセス ポリシーを選択します。

ステップ 4 [ダイナミック アクセス ポリシー（Dynamic Access Policy）] ドロップダウンからポリシーを選択するか、[新しいダイナミック アクセス ポリシーの作成（Create a new Dynamic Access Policy）] をクリックして新しいダイナミック アクセス ポリシーを設定します。

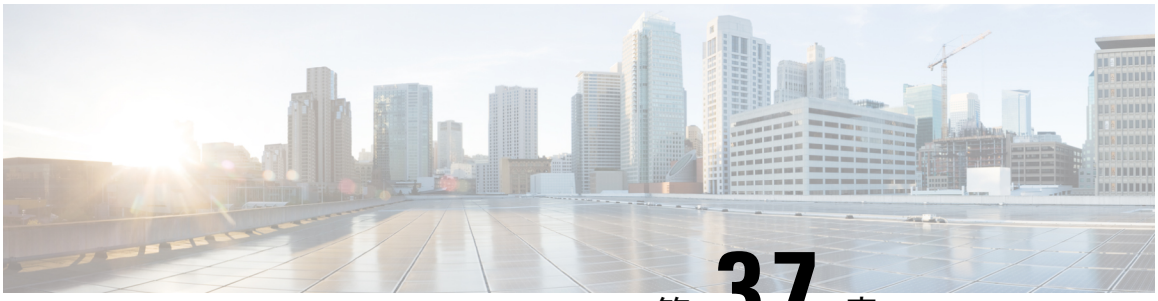
ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、リモートアクセス VPN ポリシーを保存します。

リモートアクセス VPN ユーザーが接続を試みると、VPN は、設定されたダイナミック アクセス ポリシーのレコードおよび属性をチェックします。VPN は、一致するダイナミック アクセス ポリシー レコードに基づいてダイナミック アクセス ポリシーを作成し、VPN セッションで適切なアクションを実行します。

ダイナミック アクセス ポリシーの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ダイナミックアクセスポリシー	7.0	任意（Any）	この機能が導入されました。



第 37 章

VPNのモニタリングとトラブルシューティング

この章では、Firepower Threat Defense VPN のモニタリングツール、パラメータ、統計情報、およびトラブルシューティングについて説明します。

- [サイト間 VPN 概要（Site-to-Site VPN Summary）] ページ （1699 ページ）
- リモートアクセス VPN ダッシュボード （1699 ページ）
- VPN セッションとユーザー情報 （1701 ページ）
- VPN ヘルス イベント （1702 ページ）
- VPN のトラブルシューティング （1703 ページ）

[サイト間 VPN 概要（Site-to-Site VPN Summary）] ページ

[サイト間 VPN 概要（Site-to-Site VPN Summary）] ページを使用して、ユーザーの現在のステータス、デバイス タイプ、クライアント アプリケーション、ユーザーの位置情報、接続時間などの VPN ユーザーに関する統合情報を表示できます。VPN インターフェイス、トンネルステータスなど、設定された VPN トポロジの詳細情報を表示できます。

すべての VPN トポロジについて、編集ボタンと削除ボタンを使用してトポロジを編集または削除できます。SASE トポロジ VPN の場合、トポロジを展開、編集、および削除するオプションがあります。

リモートアクセス VPN ダッシュボード

リモートアクセス仮想プライベートネットワーク（RA VPN）を使用すると、リモートユーザーはネットワークに安全に接続できます。RA VPN ダッシュボードでは、デバイス上のアクティブな RA VPN セッションからのリアルタイムデータを監視でき、ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。

RA VPN ダッシュボード（[概要（Overview）] > [ダッシュボード（Dashboards）] > [リモートアクセス VPN（Remote Access VPN）]）には、Firewall Management Center によって管理される

Threat Defense デバイス上のアクティブな RA VPN セッションのスナップショットが表示されます。

ダッシュボードには以下のウィジェットがあります。

- [アクティブなセッション（Active Sessions）]（表形式ビュー）
- [アクティブなセッション（Active Sessions）]（マップビュー）
- セッション（Sessions）
- [デバイスアイデンティティ証明書（Device Identity Certificates）]

[アクティブなセッション（Active Sessions）]（表形式ビュー）

このウィジェットには、接続されているアクティブな RA VPN ユーザーの表形式のビューが表示されます。ユーザー名、割り当てられた IP、パブリック IP、ログイン時間、VPN ゲートウェイ（Threat Defense デバイス）、クライアント アプリケーション、クライアント オペレーティング システム、接続プロファイル、グループポリシーなど、アクティブな RA VPN セッションの詳細を確認できます。フィルタを使用して、さまざまな基準に基づいて検索を絞り込むことができ、個々のセッションで以下のアクションも実行できます。

- 特定のユーザーのセッションを終了する。
- 特定の VPN ゲートウェイに接続されている特定のユーザーのすべてのセッションを終了する。
- 特定の VPN ゲートウェイに接続されているすべてのセッションを終了する。

クライアントデバイスがデュアルアドレススタックをサポートし、Firewall Threat Defense デバイスの RA VPN 設定で IPv4 および IPv6 アドレスプールが許可されている場合、クライアントはヘッドエンドデバイスとの RA VPN セッションを確立すると、IPv4 および IPv6 アドレスをクライアントのトンネルインターフェイスに割り当てます。RA VPN セッションには、Threat Defense デバイスの IPv4 アドレスと IPv6 アドレスの 2 つの IP アドレスがあります。Firewall Management Center は、同じユーザーの 2 つのセッションを示しています。1 つは IPv4 アドレス、もう 1 つは IPv6 アドレスで、セッション数は 2 つです。

したがって、デバイスで **show vpn-sessiondb l2l filter ipaddress** コマンドが実行されユーザーからの RA VPN セッションが 1 つしかない場合でも、Firewall Management Center は 2 つの異なるセッションを示します。

[アクティブなセッション（Active Sessions）]（マップビュー）

このウィジェットには、デバイスの RA VPN セッションを介して接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。

- ユーザーセッションがある国は、青の色合いで表示されます。
- マップの凡例には、国のセッション数とその国に使用される青の色合いとの相関関係を示すスケールが表示されます。

- マップ上にマウスポインタを合わせると、国名とアクティブなユーザーセッションの総数が表示されます。
- ズームイン、ズームアウト、およびリセットのオプションを使用できます。

セッション（Sessions）

このウィジェットでは、デバイス上のアクティブな RA VPN セッションからのリアルタイムデータを監視でき、次の項目に従って、アクティブな RA VPN セッションの分布をフィルタ処理して表示できます。

- [デバイス（Device）]：デバイスごとのセッション数が表示されます。
- [暗号化タイプ（Encryption Type）]：セキュアクライアント SSL または IPsec セッションの数が表示されます。
- [Secure Clientバージョン（セキュアクライアント Version）]：セキュアクライアント バージョンごとのセッションが表示されます。
- [オペレーティングシステム（Operating System）]：オペレーティングシステムごとのセッションが表示されます。Windows、Linux、Mac、モバイル OS など。
- [接続プロファイル（Connection Profile）]：接続プロファイルごとのセッションが表示されます。

[デバイスアイデンティティ証明書（Device Identity Certificates）]

このウィジェットには、RA VPN ゲートウェイのアイデンティティ証明書の有効期限に関する情報が表示されます。期限切れの証明書と、1 ヵ月以内に期限が切れる証明書を確認できます。[詳細の表示（View Details）] をクリックして、[デバイス（Device）] > [証明書（Certificates）] ページに証明書を表示します。

VPN セッションとユーザー情報

システムは、VPN 関連アクティビティを含む、ネットワーク上のユーザーアクティビティの詳細を伝達するイベントを生成します。システムのモニタリング機能を使用すると、リモートアクセス VPN の問題が存在するかどうか、および存在する場所を迅速に特定できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。オプションで、必要に応じてリモートアクセス VPN ユーザーをログアウトすることができます。

リモート アクセス VPN アクティブ セッションの表示

[分析（Analysis）] > [ユーザー（Users）] > [アクティブなセッション（Active Sessions）]

ユーザー名、ログイン時間、認証タイプ、割り当て済み/パブリック IP アドレス、デバイスの詳細、クライアントのバージョン、エンドポイント情報、スループット、帯域幅消費グループ

ポリシー、トンネルグループなどのサポート情報を使用して、現在ログインしているVPNユーザーを任意の時点で表示できます。また、現在のユーザー情報をフィルタ処理し、ユーザーをログアウトし、要約リストからユーザーを削除することもできます。

（注） 高可用性展開でVPNを構成する場合、アクティブなVPNセッションに対して表示されるデバイス名は、ユーザーセッションを識別したプライマリデバイスまたはセカンダリデバイスである可能性があります。

リモート アクセス VPN ユーザー アクティビティの表示

[分析（Analysis）] > [ユーザ（Users）] > [ユーザ アクティビティ（User Activity）]

ネットワーク上のユーザーアクティビティの詳細を表示できます。システムは履歴イベントを記録し、接続プロファイル情報、IPアドレス、位置情報、接続時間、スループット、デバイス情報などの VPN 関連情報が含まれています。

VPN ヘルス イベント

[ヘルスイベント（Health Events）] ページでは、Firewall Management Center のヘルスモニターで記録された VPN ヘルスイベントを確認できます。デバイス間の 1 つ以上の VPN トンネルがダウンすると、ヘルスモニターは次のイベントを追跡します。

- Secure Firewall Threat Defense のサイト間 VPN
- Secure Firewall Threat Defense のリモート アクセス VPN

VPN ヘルス イベントの表示

Secure Firewall Management Center 上の [ヘルス イベント（Health Events）] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルスイベントが取得されます。表示したいヘルスイベントを生成したモジュールを指定することによって、イベントを絞り込むことができます。

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリストである必要があります。

手順

ステップ 1 **[システム（System）] > [ヘルス（Health）] > [イベント（Events）]** を選択します。

ステップ 2 [モジュール名（Module Name）] 列で [VPN ステータス（VPN Status）] を選択します。

VPN セッションが稼働していても VPN トンネルが非アクティブであるというアラートが発生する場合は、VPN正常性アラートを無効にすることができます。詳細は、次のトピックを参照してください。

- ヘルスモニタリングからのアプライアンスの除外
- 正常性ポリシーモジュールの除外

VPN のトラブルシューティング

このセクションでは、VPN のトラブルシューティング ツールとデバッグ情報について説明します。

システムメッセージ

メッセージ センターは、トラブルシューティングを開始する場所です。この機能を使用すると、システムの使用状況およびステータスについて継続的に生成されるメッセージを確認できます。メッセージセンターを開くには、メインメニューの [展開（Deploy）] ボタンの右隣にある [システムステータス（System Status）] をクリックします。

VPN システム ログ

Firewall Threat Defense デバイスの VPN トラブルシュート syslog のロギングを有効にできます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。VPN ロギングを有効にすると、Firewall Threat Defense デバイスから Firewall Management Center に VPN syslog が送信されます。

すべての VPN syslog には、デフォルトのシビラティ（重大度）レベル [エラー（Errors）] 以上が設定されています（変更されない限り）VPN ロギングは、Firewall Threat Defense プラットフォーム設定を介して管理できます。対象となるデバイスの Firewall Threat Defense プラットフォーム設定ポリシーで [VPNロギング設定（VPN Logging Settings）] を編集して、メッセージのシビラティ（重大度）レベルを調整できます。VPN ロギングの有効化、syslog サーバの設定、およびシステム ログの表示の詳細については、Firewall Threat Defense デバイスの syslog ロギングの設定 （875 ページ） を参照してください。

[トラブルシューティングログ（Troubleshooting Logs）] テーブル（[デバイス（Devices）] > [トラブルシューティングログ（Troubleshooting Logs）]）では、VPN syslog メッセージを表示および分析して、ネットワークとデバイスの設定に関する問題を特定および分離できます。

VPN ログのログレベルをレベル 3（[エラー（Errors）]）に設定することを推奨します。VPN ロギングレベルをレベル 4 以上（[警告（Warnings）]、[通知（Notification）]、[情報（Infromational）]、または [デバッグ（Debugging）]）に設定すると、Firewall Management Center が過負荷になる可能性があります。

（注） サイト間 VPN またはリモートアクセス VPN を設定してデバイスを設定すると、デフォルトで自動的に VPN syslog が Firewall Management Center に送信されます。

debug コマンド

ここでは、debug コマンドを使用して、VPN 関連の問題を診断および解決する方法について説明します。ここで説明するコマンドは、すべてを網羅しているわけではありません。ここには、VPN 関連の問題の診断に役立つコマンドが含まれています。

使用上のガイドライン

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug**コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

デバッグ出力は、CLI セッションでのみ表示できます。出力は、コンソール ポートに接続したときか、または診断 CLI（**system support diagnostic-cli** と入力）で直接入手できます。また、**show console-output** コマンドを使用して、通常の Firepower Threat Defense CLI からの出力を確認することもできます。

特定の機能のデバッグ メッセージを表示するには、**debug** コマンドを使用します。デバッグ メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。すべてのデバッグ コマンドをオフにするには、**no debug all** を使用します。

debug *feature* ［*subfeature*］［*level*］
no debug *feature* ［*subfeature*］

構文の説明

feature	デバッグをイネーブルにする機能を指定します。使用可能な機能を表示するには、**debug ?** コマンドを使用して CLI ヘルプを表示します。
subfeature	（オプション）機能によっては、1つ以上のサブ機能のデバッグ メッセージをイネーブルにできます。使用可能なサブ機能を表示するには ? を使用します。
level	（オプション）デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

例

リモートアクセスVPN上で複数のセッションを実行すると、ログのサイズを考慮するとトラブルシューティングが困難になることがあります。**debug webvpn condition** コマンドを使用して、デバッグ プロセスをより正確に絞り込むためのフィルタを設定できます。

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask*| **prefix** *length*}] | **reset** | **user** *name*}

それぞれの説明は次のとおりです。

- **group** *name* は、グループ ポリシー（トンネル グループまたは接続プロファイルではない）でフィルタ処理を行います。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] は、クライアントのパブリックIPアドレスでフィルタ処理を行います。サブネットマスク（IPv4）またはプレフィックス（IPv6）はオプションです。
- **reset** すべてのフィルタをリセットします。**no debug webvpn condition** コマンドを使用して、特定のフィルタをオフにできます。
- **user** *name* は、ユーザー名でフィルタ処理を行います。

複数の条件を設定すると、条件が結合（ANDで連結）され、すべての条件が満たされた場合にのみデバッグが表示されます。

条件フィルタを設定したら、基本の **debug webvpn** コマンドを使用してデバッグをオンにします。条件を設定するだけではデバッグは有効になりません。デバッグの現在の状態を表示するには、**show debug** および **show webvpn debug-condition** コマンドを使用します。

次に、ユーザー jdoe で条件付きデバッグを有効にする例を示します。

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

関連コマンド

コマンド	説明
show debug	現在アクティブなデバッグ設定を示します。
undebug	ある機能のデバッグを無効にします。このコマンドは **no debug** の同意語です。

debug aaa

デバッグ設定または認証、認可、およびアカウンティング（AAA）設定については、次のコマンドを参照してください。

debug *aaa* ［*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*］

構文の説明

aaa	AAA のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
accounting	（オプション）AAA アカウンティング デバッグを有効にします。
authentication	（オプション）AAA 認証デバッグを有効にします。
authorization	（オプション）AAA 認可デバッグを有効にします。
common	（オプション）AAA 共通デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
internal	（オプション）AAA 内部デバッグを有効にします。
shim	（オプション）AAA shim デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
url-redirect	（オプション）AAA URL リダイレクト デバッグを有効にします。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug aaa	AAA の現在アクティブなデバッグ設定を示します。
undebug aaa	AAA のデバッグを無効にします。このコマンドは **no debug aaa** の同意語です。

debug crypto

暗号に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto* ［*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*］

構文の説明

crypto	*crypto* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
ca	（オプション）PKI デバッグ レベルを指定します。使用可能なサブ機能を表示するには ? を使用します。
condition	（オプション）IPsec/ISAKMP デバッグ フィルタを指定します。使用可能なフィルタを表示するには ? を使用します。
engine	（オプション）暗号エンジン デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ike-common	（オプション）IKE 共通デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ikev1	（オプション）IKE バージョン 1 デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ikev2	（オプション）IKE バージョン 2 デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ipsec	（オプション）IPsec デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
condition	(オプション）暗号化セキュア ソケット API デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
vpnclient	（オプション）EasyVPN クライアント デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto	暗号化の現在アクティブなデバッグ設定を示します。
undebug crypto	暗号化のデバッグを無効にします。このコマンドは **no debug crypto** の同意語です。

debug crypto ca

crypto ca に関連付けられたデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ca* ［*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*］［*1-255*］

構文の説明

crypto ca	*crypto ca* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
cluster	（オプション）PKI クラスタ デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
cmp	（オプション）CMP トランザクション デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
messages	（オプション）PKI の入力/出力メッセージのデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
periodic-authentication	（オプション）PKI 定期認証デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
scep-proxy	（オプション）SCEP プロキシデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
server	（オプション）ローカル CA サーバーのデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
transactions	（オプション）PKI トランザクションデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
trustpool	（オプション）トラストプール デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ca	crypto ca の現在アクティブなデバッグ設定を示します。
undebug	crypto ca のデバッグを無効にします。このコマンドは **no debug crypto ca** の同意語です。

debug crypto ikev1

インターネット キー エクスチェンジ バージョン 1（IKEv1）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ikev1* ［*timers*］［*1-255*］

構文の説明

ikev1	*ikev1* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
timers	（オプション）IKEv1 タイマーのデバッグを有効にします。

1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ikev1	IKEv1 の現在アクティブなデバッグ設定を示します。
undebug crypto ikev1	IKEv1 のデバッグを無効にします。このコマンドは **no debug crypto ikev1** の同意語です。

debug crypto ikev2

インターネット キー エクスチェンジ バージョン 2（IKEv2）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ikev2* ［*ha* | *platform* | *protocol* | *timers*］

構文の説明

ikev2	デバッグ *ikev2* を有効にします。使用可能なサブ機能を表示するには ? を使用します。
ha	（オプション）IKEv2 HA デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
platform	（オプション）IKEv2 プラットフォーム デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
protocol	（オプション）IKEv2 プロトコル デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
timers	（オプション）IKEv2 タイマーのデバッグを有効にします。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ikev2	IKEv2 の現在アクティブなデバッグ設定を示します。
undebugcrypto ikev2	IKEv2 のデバッグを無効にします。このコマンドは **no debug crypto ikev2** の同意語です。

debug crypto ipsec

IPsec に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ipsec* ［*1-255*］

構文の説明

ipsec	*ipsec* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ipsec	IPsec の現在アクティブなデバッグ設定を示します。
undebugcrypto ipsec	IPsec のデバッグを無効にします。このコマンドは **no debug crypto ipsec** の同意語です。

debug ldap

LDAP（Lightweight Directory Access Protocol）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *ldap* ［*1-255*］

構文の説明

ldap	LDAPのデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug ldap	LDAP の現在アクティブなデバッグ設定を示します。
undebugldap	LDAP のデバッグを無効にします。このコマンドは **no debug ldap** の同意語です。

debug ssl

SSLセッションに関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *ssl* ［*cipher* | *device*］［*1-255*］

構文の説明

ssl	SSL のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。

cipher	（オプション）SSL 暗号デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
device	（オプション）SSL デバイス デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug ssl	SSL の現在アクティブなデバッグ設定を示します。
undebug ssl	SSL のデバッグを無効にします。このコマンドは **no debug ssl** の同意語です。

debug webvpn

WebVPN に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

構文の説明

webvpn	WebVPN のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
anyconnect	（任意）WebVPN Secure Client デバッグレベルを指定します。使用可能なレベルを表示するには ? を使用します。
chunk	（オプション）WebVPN チャンク デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
cifs	（オプション）WebVPN CIFS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
citrix	（オプション）WebVPN Citrix デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
compression	（オプション）WebVPN 圧縮デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
condition	（オプション）WebVPN フィルタ条件デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

cstp-auth	（オプション）WebVPN CSTP 認証デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
customization	（オプション）WebVPN カスタマイズデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
failover	（オプション）WebVPN フェールオーバー デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
html	（オプション）WebVPN HTML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
javascript	（オプション）WebVPN Javascript デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
kcd	（オプション）WebVPN KCD デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
listener	（オプション）WebVPN リスナー デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
mus	（オプション）WebVPN MUS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
nfs	（オプション）WebVPN NFS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
request	（オプション）WebVPN 要求デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
response	（オプション）WebVPN 応答デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
saml	（オプション）WebVPN SAML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
session	（オプション）WebVPN セッション デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
task	（オプション）WebVPN タスク デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
transformation	（オプション）WebVPN 変換デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
url	（オプション）WebVPN URL デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
util	（オプション）WebVPN ユーティリティ デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

xml	（オプション）WebVPN XML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

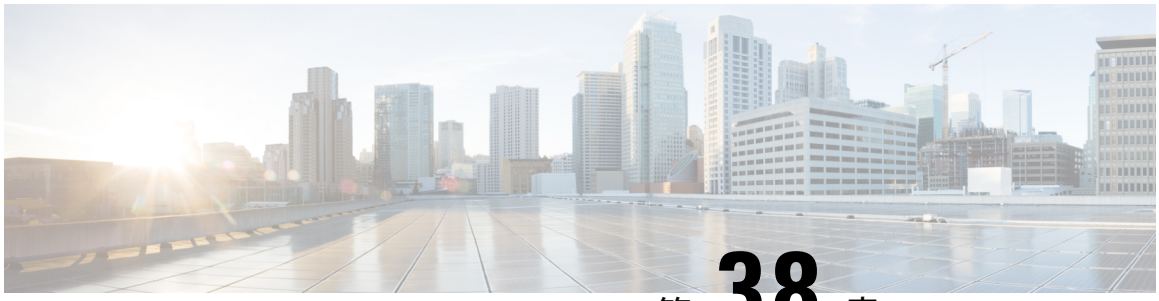
関連コマンド

コマンド	説明
show debug webvpn	WebVPN の現在アクティブなデバッグ設定を示します。
undebug webvpn	WebVPN のデバッグを無効にします。このコマンドは **no debug webvpn** の同意語です。

第 VII 部

アクセス制御

- アクセス制御の概要 （1717 ページ）
- アクセス制御ポリシー （1745 ページ）
- アクセス コントロール ルール （1775 ページ）
- URL フィルタリング, on page 1815
- セキュリティ インテリジェンス （1851 ページ）
- DNS ポリシー （1867 ページ）
- プレフィルタリングおよびプレフィルタ ポリシー （1891 ページ）
- サービスポリシー （1919 ページ）
- 脅威の検出 （1943 ページ）
- エレファントフローの検出 （1953 ページ）
- インテリジェント アプリケーション バイパス （1959 ページ）
- コンテンツ規制 （1969 ページ）



第 38 章

アクセス制御の概要

- アクセス制御の概要 （1717 ページ）
- ルールの概要 （1718 ページ）
- アクセス コントロール ポリシーのデフォルト アクション （1721 ページ）
- ファイルポリシーと侵入ポリシーを使用したディープインスペクション （1723 ページ）
- アクセス コントロール ポリシーの継承 （1728 ページ）
- アプリケーション制御のベストプラクティス （1729 ページ）
- アクセス制御ルールのベストプラクティス （1736 ページ）

アクセス制御の概要

アクセス制御は、（非高速パスを通る）ネットワーク トラフィックの指定、検査、ロギングが可能な階層型ポリシーベースの機能です。

各管理対象デバイスは 1 つのアクセス コントロール ポリシーのターゲットにすることができます。ポリシーのターゲット デバイスがネットワーク トラフィックについて収集したデータは、以下に基づいてそのトラフィックのフィルタや制御に使用できます。

- トランスポート層およびネットワーク層の特定しやすい単純な特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- レルム、ユーザ、ユーザ グループ、または ISE の属性
- カスタム セキュリティ グループ タグ（SGT）
- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入の試みが存在するかどうか
- 時刻と日（サポートされているデバイス上）

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーションベースのブロッキングはシンプルな送信元と宛先のデータを使用しているため、禁止されているトラフィックを初期の段階でブロックできます。これに対し、侵入およびエクスプロイトの検知とブロックは最終防衛ラインです。

ルールの概要

さまざまなポリシータイプ（アクセス制御、SSL、アイデンティティなど）のルールで、ネットワークトラフィックをきめ細かく制御できます。システムは最初の一致のアルゴリズムを使用して、指定した順番でルールに照らし合わせてトラフィックを評価します。

これらのルールにはポリシー全体で一貫していない他の設定が含まれている場合もありますが、次のような基本的な特性や設定メカニズムの多くは共通です。

- 条件：ルールの条件は各ルールが処理するトラフィックを指定します。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。
- アクション：ルールのアクションによって、一致するトラフィックの処理方法が決まります。選択できる [アクション（Action）] リストがルールにない場合でも、ルールには関連付けられたアクションが 1 つある点に注意してください。たとえば、カスタム ネットワーク分析ルールはそのルールの「アクション」としてネットワーク分析ポリシーを使用します。 別の例としては、QoS ルールの場合、どの QoS ルールでもトラフィックのレート制限という同じ動作をするため、明示的なアクションはありません。
- 位置：ルールの位置は評価の順番を決定します。ポリシーを使ってトラフィックを評価すると、システムは指定した順序でトラフィックとルールを照合します。通常は、システムによるトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のルールに従って行われます（追跡とログ記録を行うように設計されたモニタールールは例外です）。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。
- カテゴリ：いくつかのルールタイプを整理するために、各親ポリシーでカスタムのルールカテゴリを作成できます。
- ロギング：多くのルールでは、ルールが処理する接続をシステムがロギングするかどうか、およびロギングの処理方法は、ロギングの設定によって制御されます。一部のルール（ID ルールやネットワーク分析ルールなど）にはロギング設定は含まれません。これは、ルールが接続の最終的な性質を決定するわけではなく、またそのルールが接続をロギングするために特別に設計されているわけではないためです。 別の例としては、QoS ルールにはロギングの設定は含まれていません。これは、レート制限されているというだけの理由で接続をロギングすることはできないためです。
- コメント：一部のルールタイプでは、変更を保存するたびにコメントを追加できます。たとえば、他のユーザーのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ヒント　多くのポリシーエディタでは、右クリック メニューで編集、削除、移動、有効化、無効化など、数多くのルール管理オプションへのショートカットを提供しています。

詳細については、関心のあるルール（アクセス制御ルールなど）について記載されている章を参照してください。

関連トピック

アプリケーション条件とフィルタの設定 （1795 ページ）
アプリケーション制御のベストプラクティス （1729 ページ）

デバイス別のフィルタリング ルール

一部のポリシーエディタでは、該当デバイスによってルールの表示をフィルタ処理することができます。

システムは、ルールがそのデバイスに影響するかどうかを判断するために、ルールのインターフェイス制約を使用します。インターフェイス（セキュリティゾーンまたはインターフェイスグループの条件）でルールを制約すると、インターフェイスが置かれている場所のデバイスがそのルールの影響を受けます。インターフェイス制約のないルールは、すべてのインターフェイスに適用されるので、すべてのデバイスに適用されることになります。

QoS ルールは、常にインターフェイスで制約されます。

手順

ステップ 1　ポリシーエディタで、[ルール（Rules）] をクリックし、[デバイスでフィルタ処理（Filter by Device）] をクリックします。
ターゲット デバイスとデバイス グループのリストが表示されます。

ステップ 2　1 つまたは複数のチェック ボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。または、[すべて（All）] をオンにしてリセットし、すべてのルールを表示します。

ヒント
ポインタをルール基準に合わせると、その値が表示されます。基準がデバイス特有のオーバーライドを持つオブジェクトを表し、そのデバイスだけでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。基準がドメイン特有のオーバーライドを持つオブジェクトを表し、そのドメインのデバイスでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。

ステップ 3　**[OK]** をクリックします。

ルールとその他のポリシーの警告

ポリシーおよびルールエディタでは、トラフィックの分析やフローに悪影響を与える可能性のある設定をアイコンで示します。問題に応じて、システムはユーザがそのようなポリシーを展開しようとするときに警告するか、導入を完全に阻止します。

ヒント　警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。

表 *81* : ポリシーのエラー アイコン

アイコン	説明	例
エラー（）	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまではポリシーを展開できません。	カテゴリおよびレピュテーション ベースのURLフィルタリングを実行するルールは、URLフィルタリング ライセンスのないデバイスをターゲットにする時点まで有効です。その時点で、ルールの横にエラー アイコンが表示され、ポリシーを展開できなくなります。ポリシーを展開するには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、URLフィルタリング ライセンスを有効にする必要があります。
[警告（warning）]（）	ルールに関する警告またはその他の警告が表示されていても、ポリシーを展開することはできます。しかし、警告でマークされている誤った設定は有効になりません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。	プリエンプトされるルール、または誤った設定によりトラフィックを照合できないルールは有効になりません。誤った設定には、空のオブジェクト グループ、一致するアプリケーションがないアプリケーション フィルタ、除外されたLDAPユーザ、無効なポートなどを使用した条件が含まれます。 一方、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題を修正するまでそのポリシーを展開することはできません。
情報（）	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題によってポリシーの展開が阻止されることはありません。	システムは接続でアプリケーショントラフィックまたはWebトラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあります。これにより、アプリケーションとHTTP要求が識別されるように接続が確立されます。

アイコン	説明	例
[ルールの競合（Rule Conflict）]（）	ルール競合分析を有効にすると、競合のあるルールのルールテーブルにこのアイコンが表示されます。	競合には、冗長なルール、冗長なオブジェクト、およびシャドウイングされたルールが含まれます。以前のルールがすでに基準に一致しているため、冗長なルールやシャドウイングされたルールはトラフィックと一致しません。冗長なオブジェクトは、ルールを不必要に複雑にします。

アクセス コントロール ポリシーのデフォルト アクション

新しく作成したアクセス コントロール ポリシーは、デフォルト アクションを使用して、すべてのトラフィックを処理するようにターゲット デバイスに指示します。

単純なアクセス コントロール ポリシーでは、デフォルト アクションは、ターゲット デバイスがすべてのトラフィックをどう処理するかを指定します。より複雑なポリシーでは、デフォルト アクションは次のトラフィックを処理します。

- インテリジェント アプリケーション バイパスで信頼されないトラフィック
- セキュリティ インテリジェンス ブロック リストにないトラフィック
- SSLインスペクションによってブロックされていないトラフィック（暗号化トラフィックのみ）
- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

アクセス コントロール ポリシーのデフォルト アクションにより、追加のインスペクションなしでトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリデータの有無についてトラフィックを検査することもできます。

（注） デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行**できません**。デフォルトアクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。

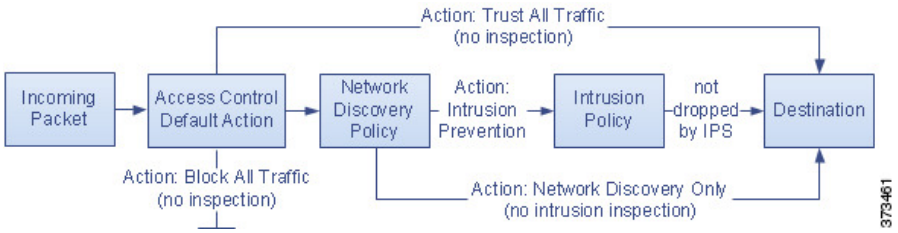
ポリシーを継承している場合、最下位の子孫のデフォルトアクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは基本ポリシーから継承することもできますが、継承したデフォルトアクションを強制的に実施することはできません。

次の表に各デフォルトアクションが処理するトラフィックに対して実施可能なインスペクションの種類を示します。

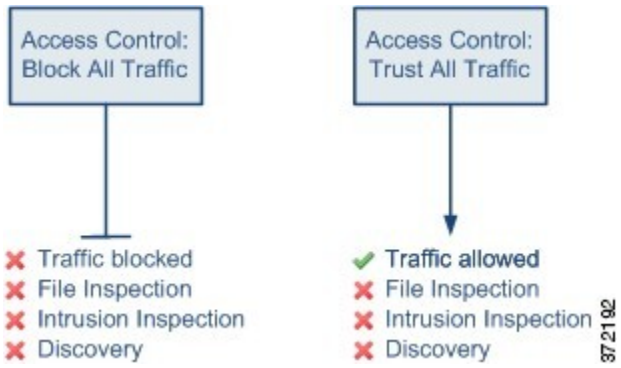
表 *82*: アクセス コントロール ポリシーのデフォルト アクション

デフォルト アクション	トラフィックに対して行う処理	インスペクション タイプとポリシー
アクセス コントロール：すべてのトラフィックをブロック	それ以上のインスペクションは行わずにブロックする	なし
アクセス コントロール：すべてのトラフィックを信頼	信頼（追加のインスペクションなしで最終宛先に許可）	なし
侵入防御（Intrusion Prevention）	ユーザが指定した侵入ポリシーに合格する限り、許可する	侵入、指定した侵入ポリシーおよび関連する変数セットを使用、および 検出（discovery）、ネットワーク検出ポリシーを使用
ネットワーク検出のみ（Network Discovery Only）	許可（allow）	検出のみ（discovery only）、ネットワーク検出ポリシーを使用
基本ポリシーから継承	基本ポリシーで定義	基本ポリシーで定義

次の図は、表を図で表したものです。



次の図は、[すべてのトラフィックをブロック（Block All Traffic）]および[すべてのトラフィックを信頼（Trust All Traffic）] のデフォルト アクションを示しています。



次の図は、[侵入防御（Intrusion Prevention）]および[ネットワーク検出のみ（Network Discovery Only）]のデフォルト アクションを説明しています。

ヒント [ネットワーク検出のみ（Network Discovery Only）]の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入検知および防御のみを目的としている場合は、さまざまな設定でディスカバリを無効にできます。

ファイルポリシーと侵入ポリシーを使用したディープインスペクション

ディープインスペクションは、トラフィックが宛先に対して許可される前の最後のとりでとして、侵入ポリシーとファイルポリシーを使用します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。

  詳細については、侵入検知と防御 （1977 ページ）を参照してください。

- ファイル ポリシーは、システムのファイル制御と マルウェア防御 の機能を管理します。

  詳細については、ネットワークマルウェア防御とファイルポリシー （2243 ページ）を参照してください。

アクセス コントロールはディープ インスペクションの前に発生し、アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

アクセスコントロールポリシーでは、1つの侵入ポリシーを各許可ルール、インタラクティブブロック ルール、およびデフォルト アクションと関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。

アクセス制御ルールに侵入ポリシーとファイルポリシーを関連付けるには、次を参照してください。

- 侵入防御を実行するためのアクセスコントロールルール設定 （2007 ページ）
- マルウェア保護のためのアクセス コントロール ルールの設定 （2253 ページ）

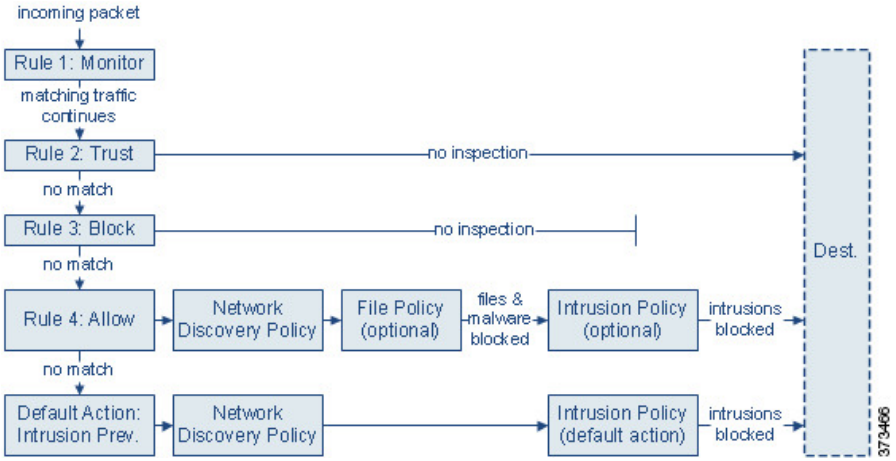
（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

関連トピック

ポリシーがトラフィックで侵入を検査する方法 （1981 ページ）
ファイル ポリシー （2244 ページ）

侵入ポリシーとファイルポリシーを使用したアクセス制御トラフィック処理

次の図は、4 つの異なるタイプのアクセス コントロール ルールとデフォルト アクションを含むアクセス コントロール ポリシーによって制御されている、インラインの侵入防御とマルウェア防御 の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の 3 つのアクセス コントロール ルール（モニター、信頼およびブロック）は一致するトラフィックを検査できません。モニター ルールはネットワーク トラフィックの追跡とロギングを行いますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。（ただし、重要な例外と注意事項をアクセス コントロール ルールのモニター アクション （1781 ページ）で確認してください）。信頼ルールおよびブロック ルールは、どのような種類のインスペクションも追加で

行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセス コントロール ルールに照合されます。

ポリシー内の4番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **ディスカバリ**：**ネットワーク検出ポリシー**：最初に、ネットワーク検出ポリシーがトラフィックのディスカバリデータの有無を検査します。ディスカバリはパッシブ分析で、トラフィックのフローに影響しません。明示的にディスカバリを有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可しても、ディスカバリデータ収集が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニターされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。
- **[マルウェア防御 とファイル制御**：**ファイル ポリシー（AMP for Networks and File Control: File Policy）]**：トラフィックが検出により調査された後、システムが禁止ファイルやマルウェアを調査します。マルウェア防御 は PDF や Microsoft Office ドキュメントなど、多くのタイプのファイルでマルウェアを検出し、必要に応じてブロックします。部門がマルウェア ファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により、特定のファイル タイプの伝送についてネットワーク トラフィックをモニターし、ファイルをブロックまたは許可できます。
- **侵入防御**：**侵入ポリシー**：ファイルインスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映できます。
- **接続先**：前述のすべてのチェックを通過したトラフィックは、その接続先に渡されます。

インタラクティブ ブロック ルール（この図には表示されていません）には、許可ルールと同じインスペクション オプションがあります。これにより、あるユーザーが警告ページをクリック スルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。

モニター以外のアクションに関するポリシー内のアクセスコントロールルールのいずれにも一致しないトラフィックは、デフォルトアクションによって処理されます。このシナリオでは、デフォルトアクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終接続先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルトアクションが割り当てられている場合もあります。システムはデフォルトアクションによって許可されたトラフィックに対しディスカバリ データおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

（注） 場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。ただし、こうしたパケットが検査されていない宛先に到達しないように、こうしたパケットを検査して侵入イベントを生成する侵入ポリシーを（アクセスコントロールポリシーの詳細設定で）指定できます。

ファイル インスペクションおよび侵入インスペクションの順序

アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイル ポリシーに関連付けて、インスペクション プロファイルをさまざまなタイプのトラフィックに照合できます。

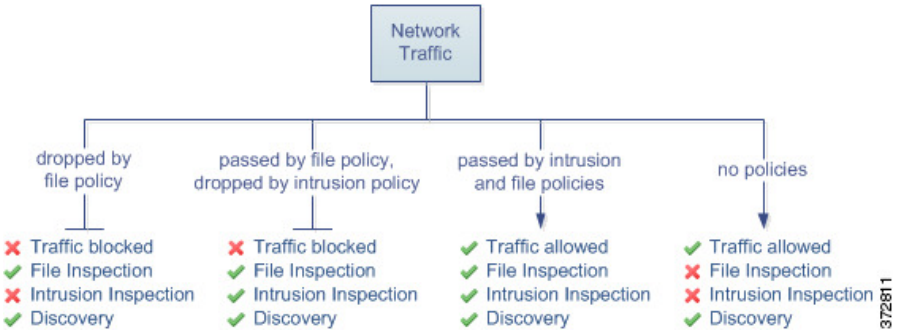
（注） 侵入防御またはネットワーク検出のみのデフォルトアクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイルインスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます。

ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイルポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、「許可」アクセスコントロールルール、またはユーザによりバイパスされた「インタラクティブブロック」アクセスコントロールルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。



アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、侵入のファイル ポリシーによってブロックされたファイルに対してシステムは検査を行いません。ファイルインスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF も検査およびブロックします。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェア インスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェアの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

（注） ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

アクセス コントロール ポリシーの継承

アクセス コントロール ポリシーはネストすることができます。このポリシーでは各ポリシーが先祖（または基本）ポリシーからルールや設定を継承します。この継承を強制することもできますが、下位のポリシーによる先祖ポリシーの上書きを許可することもできます。

アクセス制御は階層型ポリシーベース実装となっています。ドメイン階層を作成するのと同様に、対応するアクセス コントロール ポリシーの階層を作成できます。子孫（あるいは子）アクセス コントロール ポリシーは、直接の親（あるいは基本）ポリシーからルールや設定を継承します。この基本ポリシーにもさらに親ポリシーがあり、その親ポリシーにもさらに、というようにルールや設定が継承されている場合もあります。

アクセス コントロール ポリシーのルールは、親ポリシーの [強制（Mandatory）] ルール セクションと [デフォルト（Default）] のルール セクションの間にネストされています。この実装により、先祖ポリシーの [強制（Mandatory）] ルールは実施される一方、先祖ポリシーの [デフォルト（Default）] ルールは現在のポリシーでプリエンプション処理することが可能です。

次の設定をロックすることで、すべての子孫ポリシーに設定を実行させることができます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

- セキュリティ インテリジェンス：IP アドレス、URL、ドメイン名の最新のレピュテーション インテリジェンスをもとに接続を許可またはブロックされた接続。
- HTTP 応答ページ：ユーザーの Web サイト リクエストをブロックした際、カスタム応答ページあるいはシステム提供の応答ページを表示します。
- 詳細設定：関連するサブポリシー、ネットワーク分析設定、パフォーマンス設定、その他の一般設定オプションを指定します。

ポリシーを継承している場合、最下位の子孫のデフォルトアクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

ポリシーの継承とマルチテナンシー

アクセス制御の階層型ポリシーベース実装はマルチテナンシーを補完します。

通常のマルチドメイン導入環境では、アクセス コントロール ポリシーの階層がドメイン構造に対応しており、管理対象デバイスに最下位レベルのアクセス コントロール ポリシーを適用します。この実装により、ドメインの上層レベルでは選択的にアクセス制御を実施しながらも、ドメインの下層レベルの管理者は展開ごとに設定を調整することが可能です（子孫ドメインの管理者を制限するには、ポリシー継承と適用だけでなく、ロールによる制限を行う必要があります）。

たとえば、所属している部門のグローバル ドメイン管理者は、グローバル レベルのアクセス コントロール ポリシーを作成できます。そして、そのグローバル レベルのポリシーを基本ポリシーとして、機能別にサブドメインに分けられたすべてのデバイスで使用するよう要求することがことが可能です。

サブドメインの管理者が Secure Firewall Management Center にログインしてアクセス制御を設定する際、グローバル レベルのポリシーはそのまま展開できます。あるいは、グローバル レベルのポリシーの範囲内の子孫アクセス コントロール ポリシーを作成、展開することも可能です。

（注） アクセス制御の継承および適用が最も有効に実装されるのは、マルチテナンシーを補完する場合ですが、1 つのドメイン内においてもアクセス制御ポリシーを階層化することが可能です。また、任意のレベルでアクセス コントロール ポリシーを割り当て、展開することもできます。

アプリケーション制御のベストプラクティス

次のトピックでは、アクセス制御ルールを使用してアプリケーションを制御するための推奨されるベストプラクティスについて説明します。

アプリケーション制御に関する推奨事項

アプリケーション制御に関する次の注意事項と制約事項に注意してください。

アダプティブ プロファイルが有効になっていることの確認

アダプティブプロファイルが有効ではない場合（デフォルト状態）、アクセス制御ルールはアプリケーション制御を実行できません。

アプリケーション検出プログラムの自動有効化

検出するアプリケーションに対して有効な検出プログラムがない場合、そのアプリケーションに対してシステムが提供するすべての検出プログラムが自動的に有効になります。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザー定義のディテクタを有効にします。

アプリケーションを識別する前に通過する必要のあるパケットを調べるためのポリシーの設定

システムは、次の両方の条件が満たされるまで、インテリジェント アプリケーション バイパス（IAB）およびレート制限を含むアプリケーション制御を実行できません。

- モニター対象の接続がクライアントとサーバーの間で確立される。
- システムがセッションでアプリケーションを識別する

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバー証明書交換の後に行われる必要があります。

重要 これらの初期パケットをシステムが確実に調べるようにするには、トラフィック識別の前に通過するパケットを処理するためのポリシーの指定 （2747 ページ）を参照してください。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSLハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なアクションを適用します。

（注） システムがアプリケーションを認識できるようにするため、サーバーはアプリケーションのプロトコル要件に準拠する必要があります。たとえば、ACK が期待されるときに ACK ではなくキープアライブパケットを送信するサーバーがある場合、そのアプリケーションは識別されない可能性があり、接続はアプリケーションベースのルールに一致しません。代わりに、接続は別の一致するルールまたはデフォルトアクションによって処理されます。これは、許可したい接続がむしろ拒否される可能性があることを意味します。この問題が発生し、プロトコルの標準規格に準拠するようにサーバーを修正できない場合は、たとえば、IP アドレスとポート番号を照合することで、そのサーバーのトラフィックをカバーする非アプリケーションベースのルールを作成する必要があります。

URL とアプリケーションのフィルタリング用の個別のルールの作成

アプリケーションと URL の基準を組み合わせることで、予期しない結果が生じることがある（特に暗号化されたトラフィックの場合）ため、可能な限り、URL とアプリケーションのフィルタリング用に個別のルールを作成します。

アプリケーションと URL の基準の両方を含むルールは、より一般的なアプリケーションのみまたは URL のみのルールの例外として機能している場合を除き、アプリケーションのみまたは URL のみのルールの後に来る必要があります。

アプリケーションや他のルールより前に配置される URL ルール

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

暗号化および復号トラフィックのアプリケーション制御

システムでは暗号化トラフィックと復号トラフィックを識別してフィルタリングできます。

- 暗号化トラフィック：システムは StartTLS（SMTPS、POPS、FTPS、TelnetS、IMAP など）で暗号化されたアプリケーション トラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバー証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。これらのアプリケーションに `SSL Protocol` タグが付けられます。SSL ルールでは、これらのアプリケーションのみを選択できます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。

- 復号トラフィック：システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに `decrypted traffic` タグを割り当てます。

TLS サーバーアイデンティティ検出とアプリケーション制御

RFC 8446 で定義されている最新バージョンの Transport Layer Security（TLS）プロトコル 1.3 は、セキュアな通信を提供するために多くの Web サーバーで採用されているプロトコルです。TLS 1.3 プロトコルが、セキュリティを強化するためにサーバーの証明書を暗号化する一方で、証明書が、アクセスコントロールルールのアプリケーションおよび URL フィルタリング基準に適合する必要があるため、Firepower システムは、パケット全体を復号せずにサーバー証明書を抽出する方法を提供します。

この機能は、アプリケーションまたは URL の基準に適合させたいトラフィックに関して、特にそのトラフィックの詳細な検査を実行する必要がある場合に、有効にすることを強くお勧めします。サーバー証明書を抽出するプロセスでトラフィックが復号されないため、復号ポリシー は必要ありません。

詳細については、アクセス コントロール ポリシーの詳細設定（1759 ページ）を参照してください。

アプリケーションのアクティブ認証の免除

アイデンティティ ポリシーでは、特定のアプリケーションをアクティブ認証から除外して、トラフィックが引き続きアクセス制御できるようにすることができます。これらのアプリケーションには `User-Agent Exclusion` というタグが付けられます。アイデンティティ ルールでは、これらのアプリケーションだけを選択できます。

ペイロードのないアプリケーション トラフィック パケットの処理

アクセス制御の実行時、システムは、アプリケーションが識別された接続内のペイロードを持たないパケットに対して、デフォルト ポリシー アクションを適用します。

参照先アプリケーション トラフィックの処理

アドバタイズメント トラフィックなどの Web サーバーによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype、Zoho）

一部のアプリケーションは、複数のプロトコルを使用します。このようなアプリケーションのトラフィックを制御するには、関連するすべてのオプションがアクセス コントロール ポリシーの対象となっていることを確認します。次に例を示します。

- Skype：Skype のトラフィックを制御するには、個々のアプリケーションを選択するのではなく、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。

- Zoho：Zohoメールを制御するには、[使用可能なアプリケーション（Available Application）] リストから [Zoho] と [Zohoメール（Zoho mail）] の両方を選択します。

コンテンツ制限機能用にサポートされる検索エンジン

セーフ サーチ フィルタリングは特定の検索エンジンでのみサポートされています。システムは、これらの検索エンジンからのアプリケーション トラフィックに `safesearch supported` タグを割り当てます。

回避的アプリケーション トラフィックの制御

「用途別の注意事項と制限事項 （1735 ページ）」を参照してください。

アプリケーション制御の設定のベストプラクティス

アプリケーションによるネットワークへのアクセスを次のように制御することをお勧めします。

- 安全性の低いネットワークからより安全なネットワークへのアプリケーションアクセスを許可またはブロックするには、アクセス コントロール ルールで**ポート**(選択された宛先ポート) 条件を使用します。

  たとえば、インターネット（安全性が低い）から内部ネットワーク（安全性が高い）へのICMP トラフィックを許可します。

- ユーザーグループによってアクセスされるアプリケーションを許可またはブロックするには、アクセス コントロール ルールで**アプリケーション**条件を使用します。

  たとえば、契約業者グループのメンバーによるFacebookへのアクセスをブロックします。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックする必要があるトラフィックを含め、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえばIPアドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件 (ネットワークやIPアドレスなど) を使用するアクセス コントロール ルールは、一般的な条件 (アプリケーションなど) を使用するルールの前にオーダーする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3 (物理、データリンク、およびネットワーク) の条件を持つルールは、アクセス コントロール ルールで最初に注文する必要があります。レイヤ5、6、および7 (セッション、プレゼンテーション、およびアプリケーション) の条件は、アクセス コントロール ルールの後で順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

次の表に、アクセス コントロール ルールを設定する方法の例を示します。

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	ユーザー	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポート（SSH など）を使用する場合の、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意	設定しない	使用可能なポート：**SSH** [選択した宛先ポート（Selected Destination Port）] に追加	任意	ISE/ISE-PIC でのみ使用。	任意
アプリケーションがポートを使用していない場合の（ICMP など）、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意	設定しない	選択された宛先ポートプロトコル：**ICMP** **タイプ**：**Any**	設定しない	ISE/ISE-PIC でのみ使用。	任意

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	ユーザー	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
ユーザー グループによるアプリケーション アクセス	お客様の選択（この例では [ブロック（Block）]）	お客様の選択	ユーザー グループ（この例では契約業者 グループ）を選択。	アプリケーションの名前（この例では [Facebook]）を選択。	設定しない	設定しない	ISE/ISE-PIC でのみ使用。	お客様の選択

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *83*：アプリケーションの特性

特性	説明	例
タイプ	アプリケーションプロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。

特性	説明	例
リスク（Risk）	アプリケーションが組織のセキュリティポリシーに違反することがある目的で使用される可能性。	ピアツーピアアプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲームアプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。	Facebook はソーシャル ネットワーキングのカテゴリに含まれます。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオ ストリーミング Web アプリケーションには、ほとんどの場合、`high bandwidth` と `displays ads` というタグが付けられます。

用途別の注意事項と制限事項

- Office 365 管理者用ポータル：

  制限：アクセスポリシーのロギングが最初と最後で有効になっている場合、最初のパケットは Office 365 として検出され、接続の終了は Office 365 管理者用ポータルとして検出されます。これがブロッキングに影響を与えないようにする必要があります。

- Skype:

  アプリケーション制御に関する推奨事項 （1729 ページ）を参照してください

- GoToMeeting

  GoToMeeting を完全に検出するには、ルールに次のすべてのアプリケーションが含まれている必要があります。

  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting プラットフォーム
  - LogMeIn
  - STUN

- Zoho:

アプリケーション制御に関する推奨事項 （1729 ページ）を参照してください

- Bittorrent、Tor、Psiphon、および Ultrasurf などの回避的なアプリケーションの場合：

  回避的なアプリケーションの場合、デフォルトでは、信頼性の高いシナリオのみが検出されます。このトラフィックに対するアクション（ブロックや QoS の実装など）を実行する必要がある場合、より効果の高い、さらに積極的な検出の設定が必要なことがあります。これを実行する場合、設定の変更によって誤検出が発生する可能性がありますので、TAC に問い合わせて設定を確認してください。

- WeChat：

  WeChat を許可する場合、WeChat のメディアを選択的にブロックすることはできません。

- RDP（Remote Desktop Protocol）：

  RDP アプリケーションを許可してもファイル転送が許可されない場合は、RDP のルールに TCP と UDP の両方のポート 3389 が含まれていることを確認してください。RDP ファイル転送では UDP が使用されます。

アクセス制御ルールのベストプラクティス

ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。次のトピックでは、ルールのパフォーマンスに関するガイドラインを要約します。

（注） 設定の変更を展開すると、システムはすべてのルールをまとめて評価し、ターゲットデバイスでネットワークトラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲットデバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに展開することはできません。

アクセス制御の一般的なベストプラクティス

次の要件と一般的なベストプラクティスを確認してください。

- プレフィルタポリシーを使用して、不要なトラフィックを早期にブロックし、アクセス制御インスペクションの恩恵を受けないトラフィックを高速パスします。詳細については、「Fastpath プレフィルタリングのベストプラクティス （1897 ページ）」を参照してください。
- 展開のライセンスを取得せずにシステムを設定することはできますが、多くの機能では、展開する前に適切なライセンスを有効にする必要があります。
- アクセス制御ルールは、デバイスのアクセス制御リストとして展開されます。アクセス制御ルールごとに作成されるアクセス制御エントリの数を最小限に抑え、全体的なパフォーマンスを向上させるには、各デバイスのオブジェクトグループ検索を有効にします。オブジェクトグループ検索はデバイス設定であり、アクセス制御ポリシー設定ではないため、

各デバイスを編集して機能を有効にする必要があります。詳細については、「オブジェクトグループ検索の構成 （116 ページ）」を参照してください。

- アクセス コントロール ポリシーを展開しても、そのルールは既存の接続に適用されません。既存の接続のトラフィックは、展開された新しいポリシーによってバインドされません。また、ポリシーヒットカウントは、ポリシーに一致する接続の最初のパケットに対してのみ増加します。したがって、ポリシーに一致する可能性がある既存の接続のトラフィックは、ヒットカウントから除外されます。ポリシールールを効果的に適用するには、既存の接続セッションをクリアしてからポリシーを展開します。
- 可能な限り、複数のネットワークオブジェクトを 1 つのオブジェクトグループに結合します。複数のオブジェクトを（送信元または宛先を個別に）選択すると、システムは（展開時に）オブジェクトグループを自動的に作成します。既存のグループを選択すると、オブジェクトグループの重複を回避し、多数の重複オブジェクトがある場合の CPU 使用率への潜在的な影響を軽減できます。
- システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。

  場合によっては、タップ モードのインライン デバイスを含むパッシブに展開されたデバイスにインライン設定を展開することがシステムによって阻害されます。

  それ以外の場合、ポリシーは正常に展開されますが、パッシブに展開されたデバイスを使用してトラフィックのブロックや変更を試みると、予期しない結果になる可能性があります。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。
- URL フィルタリング、アプリケーション検出、レート制限、インテリジェントアプリケーションバイパスなどの特定の機能では、システムがトラフィックを識別するために、一部のパケットの通過を許可する必要があります。

  これらのパケットが検査されずに接続先に到達しないようにするには、トラフィック識別の前に通過するパケットを処理するためのベストプラクティス （2746 ページ）およびトラフィック識別の前に通過するパケットを処理するためのポリシーの指定 （2747 ページ）を参照してください。
- アクセス コントロール ポリシーのデフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。
- 一部の機能は、特定のデバイスモデルでのみ使用できます。サポートされていない機能は、警告アイコンおよび確認ダイアログ ボックスに示されます。
- syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。
- デフォルトアクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。

- アクセスコントロールルールを作成、順序付け、および実装するためのベストプラクティスについては、アクセス制御ルールのベストプラクティス （1736 ページ） およびサブトピックを参照してください。

順序付けルールのベストプラクティス

一般的なガイドライン：

- 通常、すべてのトラフィックに適用する必要がある最優先順位のルールはポリシーの先頭近くに配置します。
- 固有のルールは一般的なルールよりも優先する必要があります（特に、特定のルールが一般的なルールの例外である場合）。

  そうしないと、トラフィックが先に一般ルールに一致し、適用対象である特定のルールにヒットしません。
- レイヤ 3/4 基準（IP アドレス、セキュリティゾーン、ポート番号など）のみに基づいてトラフィックをドロップするルールはできるだけ上に配置する必要があります。これらの基準に基づくルールでは、一致する接続を識別するための検査は必要ありません。
- 可能な限り、固有のドロップルールはポリシーの最上位近くに配置します。これにより、望ましくないトラフィックへの可能な限り早期の決定が保証されます。
- URL フィルタリング、アプリケーションベース、地理位置情報ベースのルール、および検査が必要なその他のルールは、レイヤ 3/4 基準（IP アドレス、セキュリティゾーン、ポート番号など）のみに基づいてトラフィックをドロップするルールの後（ただしファイルポリシーと侵入ポリシーを指定するルールの前）に配置する必要があります。
- URL フィルタリングルールをアプリケーションルールの上に配置し、アプリケーションルールの後にマイクロ アプリケーション ルールと Common Industrial Protocol（CIP）の下位分類アプリケーション フィルタリング ルールを続けます。
- ファイルポリシーと侵入ポリシーを指定するルールは、ルールの順序の最後に配置する必要があります。これらのルールに関しては、リソースを大量に消費する詳細な検査が必要です。パフォーマンス上の理由から、詳細な検査が必要とされる潜在的な脅威の数を最小限に抑えるために、最初はそれほどリソースを消費しない方法で可能な限り多くの脅威を排除する必要があります。
- 常に、ルールを組織のニーズに適した順序に配置する必要があります。

上記のガイドラインの例外と補足事項は、以下のセクションに記載されています。

ルールのプリエンプション

ルールのプリエンプションが発生するのは、評価する順番が前のルールがトラフィックと一致するために、その後のルールが全くトラフィックと一致しない場合です。ルールの条件により、そのルールが他のルールをプリエンプション処理するかどうかが決まります。次の例で

は、最初のルールが管理トラフィックを許可するため、2 番目のルールがそのトラフィックをブロックできません。

アクセス コントロール ルール 1：管理ユーザを許可
アクセス コントロール ルール 2：管理ユーザをブロック

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初の SSL ルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールをプリエンプション処理します。

SSL ルール 1：VLAN 22 ～ 33 を復号しない
SSL ルール 2：VLAN 27 をブロック

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 がルール 2 をプリエンプション処理し、ルール 2 での VLAN 2 の照合は行われません。

アクセス コントロール ルール 1：送信元ネットワーク 10.4.0.0/16 を許可
アクセス コントロール ルール 2：送信元ネットワーク 10.4.0.0/16、VLAN 2 を許可

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールがプリエンプション処理されます。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 1 URL www.netflix.com をレート制限

条件が 1 つでも異なる場合は、後続のルールがプリエンプション処理されることはありません。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 2 URL www.netflix.com をレート制限

例：プリエンプションを避けるための SSL ルールの順序付け

ここで 1 つのシナリオとして、信頼できる CA（Good CA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックは SSL ポリシーを使用してブロックしたいものの、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。CA 証明書とすべての中間 CA 証明書をアップロードした後、ルールを以下の順序で設定した SSL ポリシーを構成します。

SSL ルール 1：発行元 CN=www.badca.com をブロック
SSL ルール 2：発行元 CN=www.goodca.com を復号しない

上記のルールを逆の順序にすると、不正な CA で信頼されたトラフィックを含め、正当な CA で信頼されたすべてのトラフィックが最初に一致することになります。どのトラフィックも後続の不正な CA ルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

ルールのアクションとルールの順序

ルールのアクションによって、一致したトラフィックの処理方法が決まります。パフォーマンスを向上させるには、リソースを集約的に使用するルールを実行する前に、トラフィックの追加処理を実行または保証しないルールを配置してください。これにより、システムはさらに検査する必要のあるトラフィックだけを転送できます。

以下の例は、一連のルールがすべて同等に重要であり、プリエンプションが問題にならない場合に、さまざまなポリシーでルールを順序付ける方法を示しています。

ルールにアプリケーション条件が含まれている場合は、アプリケーション制御の設定のベストプラクティス （1732 ページ）も参照してください。

最適な順序：復号 ルール

復号にはリソースが必要になるだけでなく、復号後のトラフィックの分析も必要になります。トラフィックを復号するルールは最後に配置します。

（注） 特定の管理対象デバイスはハードウェアの TLS/SSL トラフィックの暗号化と復号をサポートしているため、パフォーマンスが大幅に向上します。詳細については、TLS 暗号化アクセラレーション （2316 ページ）を参照してください。

1. [モニター（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。
2. [ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックをブロックするルール。
3. [復号しない（Do not decrypt）]：暗号化トラフィックを復号しないまま、暗号化セッションをアクセス コントロール ルールに渡すルール。これらのセッションのペイロードにディープ インスペクションは適用されません。
4. [復号 - 既知のキー（Decrypt - Known Key）]：既知の秘密キーを使用して着信トラフィックを復号するルール。
5. [復号 - 再署名（Decrypt - Resign）]：サーバ証明書に再署名することによって発信トラフィックを復号するルール。

最適な順序：アクセス コントロール ルール

複数のカスタム侵入ポリシーと変数セットを使用している場合は特に、侵入、ファイル、マルウェアのインスペクションにリソースが必要です。したがって、ディープインスペクションを呼び出すアクセス コントロール ルールを最後に配置します。

1. [モニター（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。ただし、重要な例外と注意事項をアクセス コントロール ルールのモニター アクション （1781 ページ）で確認してください。

2. [信頼（Trust）]、[ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックを処理するルール。信頼できるトラフィックは、アイデンティティ ポリシーが課す認証要件、およびレート制限の対象となることに注意してください。
3. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションなし）（Interactive Block (no deep inspection)）]：それ以上のインスペクションを行わずにトラフィックのディスカバリを許可するルール。許可されるトラフィックは、アイデンティティ ポリシーが課す認証要件、およびレート制限の対象となることに注意してください。
4. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションあり）（Interactive Block (deep inspection)）]：禁止されているファイル、マルウェア、エクスプロイトのディープ インスペクションを実行するファイル ポリシーまたは侵入ポリシーに関連付けられているルール。

アプリケーション ルールの順序

アプリケーション条件を使用するルールは、ルールのリストでより低い順序に移動すると、トラフィックに一致する可能性が高くなります。

特定の条件 (ネットワークや IP アドレスなど) を使用するアクセス コントロール ルールは、一般的な条件 (アプリケーションなど) を使用するルールの前にオーダーする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および 3 (物理、データリンク、およびネットワーク) の条件を持つルールは、アクセス コントロール ルールで最初に注文する必要があります。レイヤ5、6、および 7 (セッション、プレゼンテーション、およびアプリケーション) の条件は、アクセス コントロール ルールの後で順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

詳細と例については、アプリケーション制御の設定のベストプラクティス（1732 ページ）およびアプリケーション制御に関する推奨事項（1729 ページ）を参照してください。

URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

ルールに例外を設定する場合は、例外を他のルールの上に配置してください。

ルールの簡素化および絞り込みのベストプラクティス

簡素化：設定しすぎない

個々のルール条件を最小化します。できる限り少ない個々の要素をルールの条件に使用します。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。

処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を使用しないでください。冗長な条件を使用すると、展開される設定が大幅に拡張される可能性があります。それにより、デバイスのパフォーマンスに関する問題が発生したり、クラスタおよび高可用性ユニットの再参加において予期しないデバイス動作が発生する場合があります。次に例を示します。

- 複数のインターフェイスを表すセキュリティゾーンは、慎重に使用してください。送信元ネットワークと宛先ネットワークを条件として指定し、これらが、ターゲットのトラフィックに十分に一致する場合は、セキュリティゾーンを指定する必要はありません。
- たとえば、一連の内部インターフェイスをインターネット上の「任意」の宛先と照合する場合は、単に、それらの内部インターフェイスを含む送信元セキュリティゾーンを使用します。ネットワークまたは宛先インターフェイスの基準は必要ありません。

要素をオブジェクトに組み合わせても、パフォーマンスは向上**しません**。たとえば、50 個の IP アドレスを 1 つのネットワーク オブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

アプリケーション検出の推奨事項については、アプリケーション制御の設定のベストプラクティス （1732 ページ）を参照してください。

絞り込み：特にインターフェイスによってリソース消費ルールを絞り込んで制約する

できる限り、ルールの条件を使用してリソース消費ルールが処理するトラフィックを絞り込んで定義します。絞り込まれたルールは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理できるという理由からも重要です。以下は、リソース消費ルールの例です。

- トラフィックを復号する TLS/SSL ルール：復号だけでなく、復号されたトラフィックの更なる分析にもリソースが必要です。絞り込みを細かくし、また可能な場合は、暗号化トラフィックをブロックするか、復号しないようにします。

  Firewall Threat Defense モデルではハードウェアで TLS/SSL 暗号化および復号が実行されます。これによりパフォーマンスが大きく向上します。詳細については、TLS 暗号化アクセラレーション （2316 ページ）を参照してください。

- ディープ インスペクションを呼び出すアクセス コントロール ルール：特に複数のカスタム侵入ポリシーと変数セットを使用している場合、侵入ファイルやマルウェアのインスペクションにはリソースが必要です。ディープインスペクションは必要な場所でのみ呼び出されることを確認してください。

最大のパフォーマンスによるメリットを得るため、インターフェイスによってルールを制約します。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

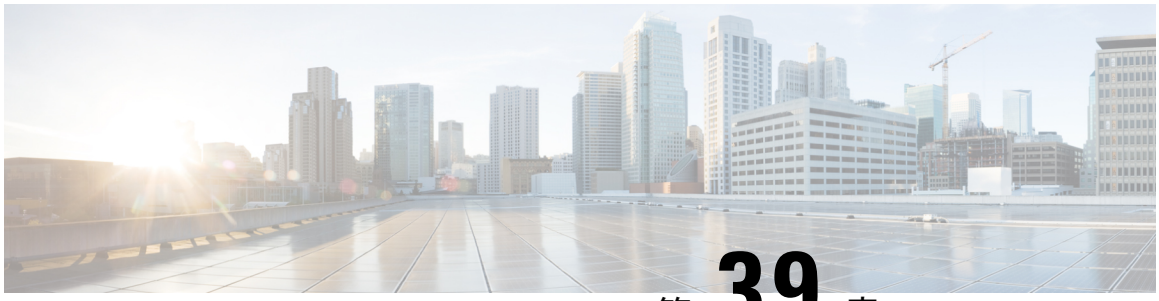
アクセス制御ルールと侵入ポリシーの最大数

ターゲットデバイスでサポートされるアクセス制御ルールまたは侵入ポリシーの最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、多くの要因によって異なります。

デバイスでサポートされる最大を超えるとアクセス コントロール ポリシーは展開できず、再評価する必要があります。

侵入ポリシーのガイドライン：

- アクセス コントロール ポリシーでは、1 つの侵入ポリシーを各許可ルール、インタラクティブ ブロック ルール、およびデフォルト アクションと関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。
- いくつかの侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに1つの侵入ポリシーと変数セットのペアを関連付けることができます。一部のデバイスでは、すべての侵入ポリシーに関して1つの変数セットだけを使用できる場合や、デバイス全体でただ 1 つの侵入ポリシー/変数セット ペアだけを使用できる場合があります。



第 39 章

アクセス制御ポリシー

ここでは、アクセス コントロール ポリシーを使用して作業する方法について説明します。

- アクセス コントロール ポリシーのコンポーネント （1745 ページ）
- システム作成のアクセス コントロール ポリシー （1746 ページ）
- アクセス コントロール ポリシーの要件と前提条件 （1747 ページ）
- アクセス コントロール ポリシーの管理 （1747 ページ）
- アクセス コントロール ポリシーの履歴 （1772 ページ）

アクセス コントロール ポリシーのコンポーネント

アクセス コントロール ポリシーの主な要素は次のとおりです。

名前（Name）と説明（Description）

各アクセス コントロール ポリシーには一意の名前が必要です。説明は任意です。

継承設定（Inheritance Settings）

ポリシー継承により、アクセス コントロール ポリシーの階層を作成することができます。親（または基本）ポリシーは子孫のデフォルト設定を定義、実行します。

ポリシーの継承設定で基本ポリシーを選択できます。また、現在のポリシーで設定をロックすることで、子孫にも同じ設定を継承させることできます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

ポリシー割り当て

各アクセス コントロール ポリシーがそのポリシーを使用するデバイスを識別します。それぞれのデバイスは、1 つのアクセス コントロール ポリシーのみのターゲットに設定できます。

ルール（Rule）

アクセス コントロール ルールは、ネットワーク トラフィックをきめ細かく処理する方法を提供します。先祖ポリシーから継承したルールを含むアクセス コントロール ポリシーのルールには、1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、アクセス コントロール ルールをトラフィックと照合します。

通常、システムは、ルールのすべての条件がトラフィックに一致する最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。条件は単純または複雑にできます。条件の使用は特定のライセンスによって異なります。

デフォルト アクション（Default Action）

デフォルトアクションは、他のアクセス制御設定で処理されないトラフィックをどのように処理し、ロギングするかを定義します。デフォルトアクションにより、追加のインスペクションなしですべてのトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリデータの有無についてトラフィックを検査することもできます。

アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

セキュリティ インテリジェンス（Security Intelligence）

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防衛ラインです。この機能により、最新の IP アドレス、URL、ドメイン名レピュテーションインテリジェンスをもとに接続をブロックすることができます。重要なリソースへの継続的なアクセスを確保するために、ブロックリストのエントリはカスタムブロックしないリストのエントリで上書きできます。

HTTP 応答（HTTP Responses）

システムによりユーザの Web サイト リクエストがブロックされた場合、システム提供の汎用的な応答ページを表示するか、カスタム ページを表示させることができます。ユーザーに警告するページを表示するものの、ユーザーが最初に要求したサイトに進めるようにすることもできます。

ログ

アクセス コントロール ポリシー ロギングの設定を使用して、現在のアクセス コントロール ポリシーのデフォルトの syslog の宛先を設定できます。この設定は、syslog の宛先設定で組み込まれているルールおよびポリシーのカスタム設定で明示的にオーバーライドされない限り、アクセス コントロール ポリシーと、組み込まれているすべての SSL、プレフィルタ、および侵入のポリシーに適用されます。

アクセス コントロールの詳細オプション（Advanced Access Control Options）

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。多くの場合、デフォルト設定が適切です。詳細設定では、トラフィックの前処理、SSL インスペクション、ID、種々のパフォーマンス オプションなどを変更できます。

システム作成のアクセス コントロール ポリシー

デバイスの初期設定に応じて、システム付属のポリシーには次のものが含まれます。

- デフォルトアクセス制御：詳細な検査なしで、すべてのトラフィックをブロックします。

- デフォルト侵入防御：すべてのトラフィックを許可しますが、Balanced Security and Connectivity 侵入ポリシーおよびデフォルトの侵入変数セットを使用して検査も実行します。
- デフォルトネットワーク検出：すべてのトラフィックを許可すると同時に検出データについて検査しますが、侵入やエクスプロイトについては検査しません。

アクセス コントロール ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

アクセス コントロール ポリシーの管理

システム付属のアクセス コントロール ポリシーの編集と、カスタム アクセス コントロール ポリシーの作成が可能です。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]**を選択します。

ページの上部には、オブジェクト管理、侵入ポリシー、ネットワーク分析ポリシー、DNS ポリシー、ポリシーのインポート/エクスポートなどの関連機能への便利なリンクがあります。

ステップ 2 アクセス コントロール ポリシーを管理します。

- 作成：[新規ポリシー（New Policy）] をクリックします。基本的なアクセス コントロール ポリシーの作成 （1748 ページ）を参照してください。
- 継承：子孫を持つポリシーの横にある**プラス**をクリックすると、ポリシーの階層ビューが展開されます。

- 編集：[編集（Edit）]（）をクリックします。アクセス コントロール ポリシーの編集（1749 ページ）を参照してください
- 削除：[削除（Delete）]（） をクリックします。ポリシーを削除する前に、デバイスの割り当てを削除する必要があります。
- [コピー（Copy）]：[その他（More）] メニューから [複製（Clone）] を選択します。[コピー（Copy）]（） をクリックします。デバイスの割り当てはコピーに保持されません。
- [レポート（Report）]：[その他（More）] メニューから [レポートの生成（Generate Report）] を選択します。**[レポート（Report）]**（） をクリックします。
- ポリシーのロックまたはロック解除：アクセス コントロール ポリシーのロック （1752 ページ）を参照してください。

基本的なアクセス コントロール ポリシーの作成

新しいアクセス コントロール ポリシーを作成すると、そのポリシーにデフォルトのアクションと設定が含まれます。ポリシーを作成すると、要件に合わせてポリシーを調整できるよう、すぐに編集セッションに移行します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 オプションで、[基本ポリシーの選択（Select Base Policy）] ドロップダウンリストから基本ポリシーを選択します。

ドメインにアクセス コントロール ポリシーが適用されている場合は、この手順はオプションではありません。適用されているポリシーまたはその子孫のいずれかを基本ポリシーとして選択する必要があります。

基本ポリシーを選択すると、基本ポリシーによってデフォルトアクションが定義されるため、このダイアログボックスで新しいアクションを選択することはできません。デフォルトアクションによって処理される接続のロギングは、基本ポリシーによって異なります。

ステップ 5 基本ポリシーを選択しない場合は、初期の**デフォルトアクション**を指定します。

- [すべてのトラフィックをブロック（Block All Traffic）] を選択すると、[アクセス コントロール：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をデフォルト アクションとするポリシーが作成されます。
- [侵入防御（Intrusion Prevention）] を選択すると、[侵入防御：セキュリティと接続性のバランス（Intrusion Prevention: Balanced Security and Connectivity）] をデフォルト アクションとし、デフォルトの侵入変数セットが関連付けられたポリシーが作成されます。
- [ネットワーク検出（Network Discovery）] を選択すると、[ネットワーク検出のみ（Network Discovery Only）] をデフォルト アクションとするポリシーが作成されます。

デフォルトアクションを選択した場合、デフォルトアクションで処理される接続のロギングは、最初は無効になっています。この設定は、後でポリシーを編集するときに有効にできます。

ヒント
デフォルトですべてのトラフィックを信頼するか、基本ポリシーを選択しデフォルトアクションは継承しないようにする場合は、後でデフォルト アクションを変更できます。

ステップ 6 必要に応じて、ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリック（またはドラッグ アンド ドロップ）して、選択したデバイスを追加します。表示されるデバイスを絞り込むには、[検索（Search）] フィールドに検索文字列を入力します。

このポリシーをすぐに展開するには、この手順を実行する必要があります。

ステップ 7 [保存（Save）] をクリックします。

新しいポリシーが開いて編集できる状態になります。必要に応じてルールを追加したり、その他の変更を加えたりすることが可能です。アクセス コントロール ポリシーの編集 （1749 ページ）を参照してください。

アクセス コントロール ポリシーの編集

アクセス コントロール ポリシーを編集するときは、そのポリシーをロックして、同時に編集する可能性がある別のユーザーによって変更が上書きされないようにする必要があります。

現在のドメインで作成されたアクセス コントロール ポリシーのみ編集できます。また、先祖アクセス コントロール ポリシーによってロックされている設定は編集できません。

（注） ポリシーをロックしない場合は、次の点を考慮してください。ポリシーの編集は、1 つのブラウザウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]**を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 アクセス コントロール ポリシーを編集します。

ヒント
左列でチェックボックスを選択し、検索ボックスの横にある [アクションの選択（Select Action）] ドロップダウンリストから実行するアクションを選択すると、一度に複数のルールを操作できます。ルールの有効化と無効化、コピー、クローン作成、移動、削除、編集、またはヒットカウントや関連イベントの表示には、一括編集を使用できます。

次のような設定の変更やアクションの実行が可能です。

- 名前と説明：名前の横の [編集（Edit）]（✎） をクリックして変更を加え、[保存（Save）] をクリックします。
- デフォルト アクション：[デフォルト アクション（Default Action）] ドロップダウン リストから値を選択します。
- デフォルトアクションの設定：[歯車（Cog）]（⚙） をクリックして変更を加え、[OK] をクリックします。ロギング、外部 syslog サーバーまたは SNMP トラップサーバーの場所、および侵入防御のデフォルトアクションに関連付けられた変数セットの設定を行えます。
- 関連付けられたポリシー：パケットフローのポリシーを編集または変更するには、ポリシー名の下のパケットフロー表示でポリシータイプをクリックします。[プレフィルタルール（Prefilter Rules）]、**[復号（Decryption）]**、[セキュリティインテリジェンス（Security Intelligence）]、および [ID（Identity）] ポリシーを選択できます。必要に応じて、[アクセス制御（Access Control）] をクリックしてアクセスコントロールルールに戻ります。

- ポリシー割り当て：このポリシーの対象となる管理対象デバイスを特定するか、このポリシーをサブドメインに適用するには、[ターゲット：xデバイス（Targeted: x devices）] リンクをクリックします。
- ルール：アクセスコントロールルールを管理し、侵入ポリシーとファイルポリシーを使用して悪意のあるトラフィックを検査およびブロックするには、[ルールの追加（Add Rule）] をクリックするか、既存のルールを右クリックして [編集（Edit）] またはその他の該当するアクションを選択します。アクションは、各ルールの [その他（More）] (⋮) ボタンからも選択できます。アクセスコントロールルールの作成および編集（1788ページ）を参照してください。
- レイアウト：ルールのリストの上にある [グリッド/テーブルビュー（Grid/Table View）] アイコンを使用して、レイアウトを変更します。グリッドビューでは、色分けされたオブジェクトが見やすいレイアウトで表示されます。テーブルビューでは、一度に複数のルールを確認できるように概要リストが表示されます。ビューは、ルールに影響を与えることなく自由に切り替えることができます。
- 列（テーブルビューのみ）：ルールのリストの上にある [列の表示/非表示（Show/Hide Columns）] アイコンをクリックして、テーブルに表示する情報を選択します。情報がない（どのルールでもそれらの条件を使用していない）すべての列をすばやく削除するには、[空の列を非表示（Hide Empty Columns）] をクリックします。すべてのカスタマイズを元に戻すには、[デフォルトに戻す（Revert to Default）] をクリックします。
- ルールのロジックを分析します。[分析（Analyze）] メニューから次のオプションを選択して、ルールのロジックを調べることができます。
  - [ヒットカウント（Hit Count）]：各ルールに一致した接続の数に関する統計を表示します。
  - [ルールの競合を有効/無効にする（Enable/Disable Rule Conflicts）]：ルールが互いに干渉するかどうかに関する情報の表示/非表示を切り替えます。
  - [ルール競合の表示（Show Rule Conflicts）]：冗長ルールまたはシャドウイングされたルールがあるかどうかを表示します。この競合により、特定のルールが接続に一致しなくなる可能性があります。そのため、一致基準の修正、ルールの移動、またはルールの削除が必要になります。
  - [警告を表示（Show Warnings）]：対処する必要がある構成の問題を含むルールがあるかどうかを表示します。
- 追加設定：ポリシーの追加設定を変更するには、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から次のオプションのいずれかを選択します。
  - 詳細設定：前処理、SSLインスペクション、アイデンティティ、パフォーマンス、およびその他の詳細オプションを設定します。アクセス コントロール ポリシーの詳細設定（1759 ページ）を参照してください。
  - HTTP レスポンス：システムが Web サイトの要求をブロックするときにブラウザに表示される情報を指定します。HTTP応答ページの選択（1838ページ）を参照してください。

- 継承設定：このポリシーの基本アクセス コントロール ポリシーを変更し、このポリシーの設定をその子孫ポリシーに適用します。基本アクセス コントロール ポリシーの選択 （1754 ページ）および子孫アクセス コントロール ポリシーでの設定のロック（1755 ページ）を参照してください。
- ロギング：ポリシーのデフォルトのロギングオプションを設定します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセス コントロール ポリシーのロック

アクセス コントロール ポリシーをロックして、他の管理者が編集できないようにすることができます。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。ロックしない場合、複数の管理者がポリシーを同時に編集すると、最初に変更を保存したユーザーによって、他のすべてのユーザーが行った変更が消去されます。

ロックはアクセス コントロール ポリシー自体を目的としています。ポリシーで使用されるオブジェクトにはロックは適用されません。たとえば、ロックされたアクセス コントロール ポリシーで使用されるネットワークオブジェクトを別のユーザーが編集できます。ロックはポリシーを明示的にロック解除するまでそのままなので、ログアウトして後で編集に戻ることができます。

ロックすると、他の管理者にはポリシーへの読み取り専用アクセス権が付与されます。ただし、他の管理者は、ロックされたポリシーを管理対象デバイスに割り当てることができます。

始める前に

アクセス コントロール ポリシーを変更する権限を持つすべてのユーザーロールには、ポリシーをロックしたり、別のユーザーによってロックされたポリシーをロック解除したりする権限があります。

ただし、別の管理者によってロックされているポリシーのロックを解除する権限は、次の権限によって制御される必要があります。**[ポリシー（Policies）]>[アクセス制御（Access Control）]>[アクセス コントロール ポリシー（Access Control Policy）]>[アクセス コントロール ポリシーの変更（Modify Access Control Policy）]>[アクセスコ ントロール ポリシー ロックのオーバーライド（Override Access Control Policy Lock）]**。

カスタムロールを使用している場合、組織がこの権限を割り当てないことで、ロック解除権限が制限されている可能性があります。この権限がないと、ポリシーをロックした管理者のみがロックを解除できます。

手順

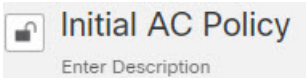
ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]**を選択します。

ステップ 2 ロックまたはロック解除するアクセス コントロール ポリシーの横にある [編集（Edit）]（）をクリックします。

[ロックステータス（Lock Status）]列には、ポリシーがすでにロックされているかどうか、ロックされている場合は誰がロックしたかが表示されます。空のセルは、ポリシーがロックされていないことを示します。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。 または、別のユーザーによってロックされています。

ステップ 3 ポリシー名の横にあるロックアイコンをクリックして、ポリシーをロックまたはロック解除します。



ポリシーが親ポリシーから設定を継承する場合、ロックアイコンをクリックしたときに次のオプションのいずれかを選択する必要があります。

- [このポリシーのロック/ロック解除（Lock/Unlock This Policy）]：ロックまたはロック解除は、このポリシーのみが対象となります。
- [階層内のこのポリシーと親のロック/ロック解除（Lock/Unlock This Policy and Parents in the Hierarchy）]：このポリシーとすべての親ポリシーがロックまたはロック解除されます。親ポリシーが別の管理者によって既にロックされている場合、メッセージが表示され、その親ポリシーをロックすることはできません。ポリシーのロックを解除するときに、アクセス コントロール ポリシー ロックのオーバーライド権限を持っている場合、他のユーザーによってロックされていても、すべての親ポリシーがロック解除されます。

アクセス コントロール ポリシーの継承の管理

継承は、アクセス コントロール ポリシーの基本ポリシーとして別のポリシーを使用することに関連します。これにより、1 つのポリシーを使用して、複数のポリシーに適用できるいくつかのベースライン特性を定義できます。継承がどのように機能するのかについては、アクセス コントロール ポリシーの継承 （1728 ページ） を参照してください。

手順

ステップ 1 変更する継承設定を持つアクセス コントロール ポリシーを編集します。アクセス コントロール ポリシーの編集 （1749 ページ）を参照してください。

ステップ 2 ポリシーの継承を管理します。

- 基本ポリシーの変更：このポリシーの基本アクセス コントロール ポリシーを変更するには、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [継承設定（Inheritance Settings）] を選択し、基本アクセス コントロール ポリシーの選択 （1754 ページ） で説明する手順を実行します。
- 子孫の設定のロック：このポリシーの設定を子孫ポリシーで強制適用するには、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [継承設定（Inheritance Settings）] を選択し、子孫アクセス コントロール ポリシーでの設定のロック （1755 ページ） で説明する手順を実行します。
- ドメインで必須：このポリシーをサブドメインで強制適用するには、[対象：x個のデバイス（Targeted: x devices）] リンクをクリックし、ドメインでのアクセス コントロール ポリシーの強制 （1756 ページ） で説明する手順を実行します
- 基本ポリシーからの設定の継承：基本アクセス コントロール ポリシーから設定を継承するには、[セキュリティ インテリジェンス（Security Intelligence）] をクリックするか、パケットフロー行の最後にあるドロップダウン矢印から [HTTP応答（HTTP Responses）] または [詳細設定（Advanced Settings）] を選択し、基本ポリシーからアクセス コントロール ポリシー設定を継承する （1755 ページ） で説明する手順を実行します。

基本アクセス コントロール ポリシーの選択

1 つのアクセス コントロール ポリシーを別の基本（親）として使用できます。デフォルトでは、子のポリシーが基本ポリシーから設定を継承します。ロック解除された設定を変更することも可能です。

既存のアクセス コントロール ポリシーの基本ポリシーを変更すると、システムで現在のポリシー設定が新しい基本ポリシーの任意のロックされた設定に更新されます。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [継承設定（Inheritance Settings）] を選択します。

ステップ 2 [基本ポリシーの選択（Select Base Policy）] ドロップダウンリストからポリシーを選択します。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

基本ポリシーからアクセス コントロール ポリシー設定を継承する

新しい子ポリシーは、基本ポリシーから多数の設定を継承します。これらの設定は、基本ポリシーでロックされていない場合はオーバーライドできます。

基本ポリシーから後で設定を再継承すると、システムによって基本ポリシーの設定が表示され、コントロールが淡色表示されます。ただし、オーバーライドした内容はシステムによって保存され、その内容は継承を再度無効にすると復元されます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] をクリックするか、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [HTTP応答（HTTP Responses）] または [詳細設定（Advanced Settings）] を選択します。

ステップ 2 継承する設定ごとに、[基本ポリシーから継承（Inherit from base policy）] チェックボックスをオンにします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

子孫アクセス コントロール ポリシーでの設定のロック

アクセス コントロール ポリシーの設定をロックして、すべての子孫ポリシーで設定を適用します。子孫ポリシーでは、ロックされていない設定をオーバーライドできます。

設定をロックするときに、すでに子孫ポリシーで実行されていたオーバーライドを保存して、設定のロックを再度解除したときにオーバーライドを復元できるようにします。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [継承設定（Inheritance Settings）] を選択します。

ステップ 2 [子ポリシーの継承設定（Child Policy Inheritance Settings）] 領域で、ロックする設定をオンにします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 [OK] をクリックして継承設定を保存します。

ステップ 4 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ドメインでのアクセス コントロール ポリシーの強制

ドメイン内の各デバイスが同一の基本アクセス コントロール ポリシーまたは、そのポリシーの子孫ポリシーの 1 つを使用するように強制できます。この手順は、マルチドメイン展開のみに関連するものです。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、[ターゲット：x デバイス（Targeted: x devices）] リンクをクリックします。

ステップ 2 [ドメインに強制（Required on Domains）] をクリックします。

ステップ 3 ドメイン リストを作成します。

- 追加：現在のアクセス コントロール ポリシーを強制適用するドメインを選択して [追加（Add）] をクリックするか、選択したドメインのリストにドラッグ アンド ドロップします。
- 削除：リーフドメインの横にある [削除（Delete）]（🗑）をクリックするか、先祖ドメインを右クリックして [選択項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。検索をクリアするには、[クリア（Clear）]（✕）をクリックします。

ステップ 4 [OK] をクリックしてドメインに強制適用する設定を保存します。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセス コントロール ポリシーのターゲット デバイスの設定

アクセス コントロール ポリシーは、それを使用するデバイスを指定します。それぞれのデバイスは、1 つのアクセス コントロール ポリシーのみのターゲットに設定できます。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、[ターゲット：xデバイス（Targeted: x devices）] リンクをクリックします。

ステップ 2 [ターゲットデバイス（Targeted Devices）] で、ターゲットリストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。
- 削除：1 つのデバイスの横にある [削除（Delete）]（ ） をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。検索をクリアするには、[クリア（Clear）]（ ） をクリックします。

[影響を受けるデバイス（Impacted Devices）] の下に、割り当てられたアクセス コントロール ポリシーが現在のポリシーの子であるデバイスが一覧表示されます。現在のポリシーを変更すると、これらのデバイスに影響します。

ステップ 3 [OK] をクリックしてターゲット デバイス設定を保存します。

ステップ 4 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセス コントロール ポリシーのロギング設定

アクセス コントロール ポリシーのロギング設定を構成するには、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [ロギング（Logging）] を選択します。

アクセス コントロール ポリシーのデフォルトの syslog 宛先と syslog アラートを設定できます。この設定は、syslog の宛先設定が組み込まれているルールとポリシーのカスタム設定で明示的にオーバーライドされない限り、アクセス コントロール ポリシーと組み込まれているすべての SSL/TLS 復号、プレフィルタ、および侵入ポリシーに適用されます。

デフォルトアクションで処理される接続のロギングは、初期設定では無効です。

IPS とファイルおよびマルウェアの設定は通常、syslog メッセージの送信についてページ上部のオプションを選択した後に有効になります。

デフォルト Syslog 設定

- [特定のsyslogアラートを使用して送信する（Send using specific syslog alert）]：このオプションを選択すると、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「*Creating a Syslog Alert Response*」「」の手順で設定したとおりに、選択した syslog アラートに基づいてイベントが送信されます。リストから syslog アラートを選択するか、名前、ロギング ホスト、ポート、機能および重大度を指定することにより syslog アラートを追加できます。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Facilities and Severities for Intrusion Syslog Alerts*」を参照してください。このオプションはすべてのデバイスに適用されます。

  このオプションを使用すると、システムは管理インターフェイスを使用して syslog メッセージをサーバーに送信します。管理インターフェイスから syslog サーバーへのルートがあることを確認します。ルートがあると、メッセージがサーバーに届きません。

- [デバイスに展開したFTDプラットフォーム設定のポリシーで指定されているsyslog設定を使用（Use the syslog settings configured in the FTD Platform Settings policy deployed on the device）]：このオプションを選択してシビラティ（重大度）を選択すると、接続または侵入イベントが選択したシビラティ（重大度）とともに [プラットフォーム設定（Platform Settings）] で設定した syslog コレクタに送信されます。このオプションを使用し、[プラットフォーム設定（Platform Settings）] で行った syslog 設定を統合して、アクセス コントロール ポリシーでその設定を再利用できます。このセクションで選択した重大度はすべての接続イベントと侵入イベントに適用されます。デフォルトの重大度は ALERT です。

  このオプションは、Secure Firewall Threat Defense デバイス 6.3 以降のみに適用されます。

IPS 設定

- [IPSイベントのsyslogメッセージを送信（Send Syslog messages for IPS events）]：IPS イベントを syslog メッセージとして送信します。上記で設定したデフォルトは、オーバーライドしない限り使用されます。

- [オーバーライドの表示/非表示（Show/Hide Overrides）]：デフォルトの syslog 宛先と重大度を使用する場合は、これらのオプションを空のままにします。それ以外の場合は、IPS イベントに別の syslog サーバーの宛先を設定し、イベントの重大度を変更できます。

ファイルおよびマルウェアの設定

- [ファイルおよびマルウェアイベントのsyslogメッセージを送信（Send Syslog messages for File and Malware events）]：ファイルおよびマルウェアイベントを syslog メッセージとして送信します。上記で設定したデフォルトは、オーバーライドしない限り使用されます。

- [オーバーライドの表示/非表示（Show/Hide Overrides）]：デフォルトの syslog 宛先と重大度を使用する場合は、これらのオプションを空のままにします。それ以外の場合は、ファ

イルおよびマルウェアイベントに別のsyslogサーバーの宛先を設定し、イベントの重大度を変更できます。

アクセス コントロール ポリシーの詳細設定

アクセス コントロール ポリシーの詳細設定を構成するには、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Update Intrusion Rules*」で説明しているように、アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細オプションの多くは、ルールの更新によって変更される可能性があることに注意してください。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。

⚠

注意 Snort プロセスを再起動し、トラフィック インスペクションを一時的に中断する詳細設定変更のリストについては、展開またはアクティブ化された際に Snort プロセスを再起動する設定（167 ページ）を参照してください。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。

親ポリシーからの設定の継承

アクセス コントロール ポリシーにベースポリシーがある場合は、ベースポリシーから設定を継承することができます。親ポリシーの設定を使用する設定グループごとに、[ベースポリシーから継承（Inherit from base policy）] を選択します。これらの設定がロックされるように継承が設定されている場合、これらの設定は読み取り専用になり、ポリシーに固有の設定を行うことはできません。

ポリシーに固有の設定を行うことが許可されている場合、編集するには [ベースポリシーから継承（Inherit from base policy）] を選択解除する必要があります。

全般設定

オプション	説明
接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）	ユーザーが要求した各URLに対して保存する文字数をカスタマイズするには詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Limiting Logging of Long URLs」を参照してください。 ユーザーが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔をカスタマイズするには、ブロックされた Web サイトのユーザー バイパス タイムアウトの設定 （1840 ページ）を参照してください。
インタラクティブブロックを一時的に許可する時間(秒)（Allow an Interactive Block to bypass blocking for (seconds)）	ブロックされた Web サイトのユーザー バイパス タイムアウトの設定 （1840 ページ） を参照してください。
URL キャッシュのミス検索の再試行（Retry URL cache miss lookup）	システムは、ローカルに保存されたカテゴリとレピュテーションを持たない URL を初めて検出すると、今後その URL をすばやく処理できるように、そのURLをクラウドで検索して結果をローカルデータストアに追加します。 この設定により、クラウドで URL のカテゴリとレピュテーションを検索する必要がある場合の処理が決まります。 デフォルトでは、この設定は有効になっています。システムは、クラウドのURLのレピュテーションとカテゴリをチェックしている間、トラフィックを一時的に遅延させ、クラウドの判定を使用してトラフィックを処理します。 この設定を無効にした場合、ローカルキャッシュに存在しないURLがシステムで検出されると、トラフィックはただちに渡され、未分類およびレピュテーションのないトラフィック用に設定されたルールに従って処理されます。 パッシブ展開では、システムはルックアップを再試行しません。これは、システムがパケットを保持できないからです。
Threat Intelligence Director を有効にする（Enable Threat Intelligence Director）	このオプションを無効にすると、設定したデバイスへの TID データの公開が停止されます。
DNS トラフィックへのレピュテーション適用を有効にする（Enable reputation enforcement on DNS traffic）	このオプションは、URL フィルタリングのパフォーマンスと有効性を向上させるために、デフォルトで有効になっています。詳細および追加手順については、DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別（ベータ版） （1832ページ）およびサブトピックを参照してください。

オプション	説明
ポリシー適用中のトラフィックの検査	特定の設定でSnortプロセスを再起動する必要がない限り設定の変更を展開する場合にトラフィックを検査するには、必ず、[ポリシーの適用時にトラフィックを検査する（Inspect traffic during policy apply）] がデフォルト値（有効）に設定してください。 このオプションを有効にすると、リソースの需要が高まった場合にいくつかのパケットが検査なしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細については、Snort再起動のシナリオ （162 ページ）を参照してください。

関連するポリシー

詳細設定を使用して、サブポリシー（復号、アイデンティティ、プレフィルタ）をアクセス制御に関連付けます。「アクセス制御への他のポリシーの関連付け （1765 ページ）」を参照してください。

TLS サーバーアイデンティティ検出

RFC 8446 で定義されている最新バージョンの Transport Layer Security（TLS）プロトコル 1.3 は、セキュアな通信を提供するために多くのWebサーバーで採用されているプロトコルです。TLS 1.3プロトコルが、セキュリティを強化するためにサーバーの証明書を暗号化する一方で、証明書が、アクセスコントロールルールのアプリケーションおよびURL フィルタリング基準に適合する必要があるため、Firepower システムは、パケット全体を復号せずにサーバー証明書を抽出する方法を提供します。

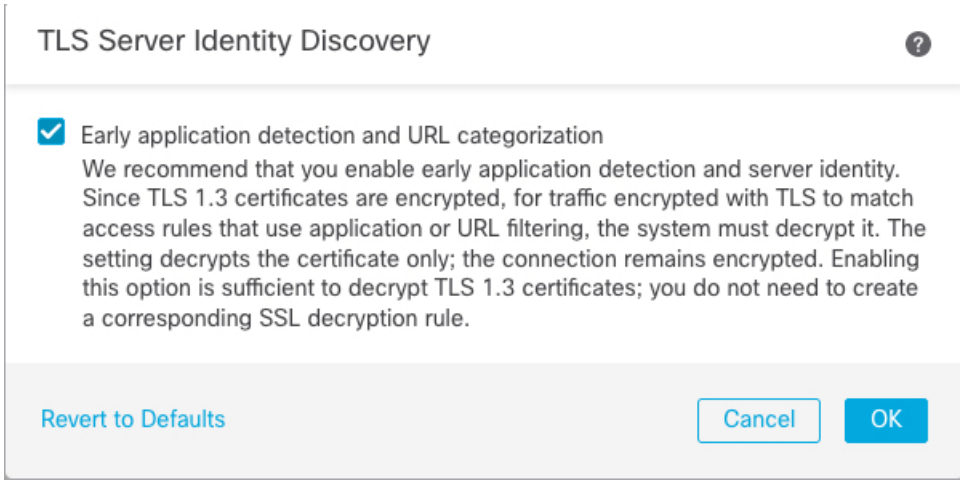
アクセス コントロール ポリシーの詳細設定を指定する場合に、この「TLS サーバーアイデンティティ検出」と呼ばれる機能を有効にできます。

このオプションを有効にする場合は、復号ポリシーの高度な TLS 適応型サーバーのアイデンティティ プローブ オプションも有効にすることをお勧めします。これらのオプションを組み合わせることで、TLS 1.3 トラフィックのより効率的な復号が可能になります。詳細については、TLS 1.3 復号のベストプラクティス （2347 ページ）を参照してください。

TLSサーバーアイデンティティ検出の影響を受ける新しい接続が開始されると、Firewall Threat Defense は元の ClientHello パケットを保持して、接続先のサーバーのアイデンティティを判別してから続行します。Firewall Threat Defense デバイスは、Firewall Threat Defense からサーバーに特殊な接続を送信します。サーバーの応答にはサーバー証明書が含まれ、特殊な接続が終了し、アクセス コントロール ポリシーの要求に応じて元の接続が評価されます。

TLS サーバー ID 検出では、 サーバー名表示（SNI）よりも証明書の共通名（CN）が優先されます。

TLS サーバーアイデンティティ検出を有効にするには、[詳細（Advanced）] タブをクリックし、設定の[編集（Edit）]（✎）をクリックして[早期アプリケーション検出とURL分類（Early application detection and URL categorization）] を選択します。



この機能は、アプリケーションまたは URL の基準に適合させたいトラフィックに関して、特にそのトラフィックの詳細な検査を実行する必要がある場合に、有効にすることを強くお勧めします。サーバー証明書を抽出するプロセスでトラフィックが復号されないため、復号ポリシー は必要ありません。

（注）

- 証明書は復号されているため、ハードウェアプラットフォームによっては、TLSサーバーアイデンティティ検出によってパフォーマンスが低下する場合があります。
- TLSサーバーアイデンティティ検出は、インラインタップモードまたはパッシブモードの展開ではサポートされません。
- TLS サーバーアイデンティティ検出の有効化は、AWS に展開された Secure Firewall Threat Defense Virtual ではサポートされていません。Secure Firewall Management Center で管理されているそのような管理対象デバイスがある場合、接続イベント **PROBE_FLOW_DROP_BYPASS_PROXY** は、デバイスがサーバー証明書の抽出を試みるたびに増加します。
- TLS サーバーアイデンティティ検出は、TLS 1.2 セッションでも動作します。

ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーおよび侵入ポリシーの詳細設定によって、以下が可能になります。

- パケットを検査するために使用され、システムがトラフィックの検査方法を正確に決定する前に合格する必要がある、侵入ポリシーおよび関連付けられる変数セットの指定。

- 多くの前処理オプションを制御する、アクセス コントロール ポリシーのデフォルト ネットワーク分析ポリシーの変更。
- カスタム ネットワーク分析ルールおよびネットワーク分析ポリシーを使用した、特定のセキュリティ ゾーン、ネットワーク、および VLAN に対する前処理オプションの調整。

詳細については、ネットワーク分析ポリシーと侵入ポリシーに対するアクセス コントロールの詳細設定 （2745 ページ）を参照してください。

Threat Defense サービス ポリシー

Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。このポリシーは Firewall Threat Defense デバイスのみに適用され、その他のデバイス タイプの場合には無視されます。このサービス ポリシー ルールは、アクセス制御ルールの後に適用されます。詳細については、サービス ポリシー （1919 ページ）を参照してください。

ファイルおよびマルウェアの設定

ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整 （2289 ページ） に、ファイル制御と マルウェア防御 のパフォーマンス オプションに関する情報が記載されています。

ポートスキャン脅威検出

ポートスキャン ディテクタは、あらゆるタイプのトラフィックでポートスキャン アクティビティを検出および防止し、最終的な攻撃からネットワークを保護するために設計された脅威検出メカニズムです。ポートスキャン トラフィックは、許可されたトラフィックと拒否されたトラフィックの両方で効率的に検出できます。詳細については、を参照してください。脅威の検出 （1943 ページ）

エレファントフローの設定

エレファントフローは、Snort コアの拘束の原因となる可能性がある、大きくて長期間にわたる高速のフローです。システム ストレス、CPU ホグ、パケット ドロップなどを軽減するためにエレファントフローに適用できるアクションは 2 つあります。それらのアクションは次のとおりです。

- 一部またはすべてのアプリケーションをバイパスする：このアクションでは、Snort インスペクションからのフローをバイパスします。
- スロットル：このアクションでは、エレファントフローに動的レート制限ポリシー（10% 削減）を適用します。

インテリジェント アプリケーション バイパスの設定

インテリジェント アプリケーション バイパス（IAB）は、トラフィックがインスペクション パフォーマンスとフローしきい値の組み合わせを超過したときにバイパスするアプリケーションを指定する、または、バイパスに関するテストを行うための、エキスパート レベルの設定です。詳細については、インテリジェントアプリケーションバイパス（1959ページ）を参照してください。

トランスポート層とネットワーク層のプリプロセッサの設定

トランスポート層とネットワーク層のプリプロセッサの詳細設定は、アクセス コントロール ポリシーが展開されるすべてのネットワーク、ゾーン、VLANにグローバルに適用されます。

- **[接続を追跡する際にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）]**：同じ接続で異なる方向に流れるトラフィックの VLAN タグが異なると、トラフィックのリアセンブルやルールの処理に影響を与える場合があります。たとえば、同じ接続のトラフィックを VLAN A で送信し、VLAN B で受信することができます。このオプションを選択すると、VLANヘッダーを無視するようにシステムが構成されます。これにより、デプロイメントでパケットを正しく処理できます。
- **[アクティブ応答の最大数（Maximum Active Responses）]**：アクティブ応答を提供するように設定されたプリプロセッサ/侵入ルールをトリガーする TCP 接続の場合の、TCP 接続ごとのアクティブ応答の最大数。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから[最小応答秒数（Minimum Response Seconds）]を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0 に設定すると、追加のアクティブ応答をトリガーするアクティブ応答ルールが無効になります。
- **[応答最小秒（Minimum Response Seconds）]**：**[最大アクティブ応答数（Maximum Active Responses）]**に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を指定します
- **[セッション終了のロギングしきい値（Session Termination Logging Threshold）]**：シスコ テクニカルサポートからの指示がない限りこのオプションを変更しないでください。このオプションは、ログに記録されるメッセージのバイト数を指定します。セッションが終了し、メッセージが指定のバイト数を超えた場合は、ログに記録されます。オプションを変更するとシステムパフォーマンスに影響する場合があります。

検出拡張の設定

検出拡張設定は、アダプティブプロファイルをアプリケーション検出とアクセス コントロール ポリシーの侵入ルールに使用するかどうかを決定します。通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。アダプティブプロファイルを更新すると、システムは、ネットワーク検出により検出されたホスト情報またはサードパーティからインポートしたホスト情報を使用して処理動作を調整します。

Snort 3 でアダプティブプロファイルを有効にするには、**[有効化（Enable）]** オプションと **[プロファイルの更新を有効化（Enable Profile Updates）]** オプションの両方を選択する必要があります。

- **[有効化（Enable）]**：アクセス制御ルールに対してアダプティブプロファイル（デフォルト状態）を有効にし、マルウェア防御（AMP）を含むアプリケーション/ファイル制御を実行し、侵入ルールでサービスメタデータを使用します。
- **[プロファイルの更新を有効化（Enable Profile Updates）]**：ネットワーク分析ポリシーで手動で設定可能なターゲットベース プロファイルと同様に、プロファイル更新は、ターゲット ホストのオペレーティング システムと同じ方法で、IP パケットの最適化およびストリームのリアセンブルを行うのに役立ちます。その後、侵入ルールエンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。プロファイル更新は、侵入ルールのメタデータをホスト情報と比較して、特定のルールにルールを適用するかどうかを判断します。
- **[アダプティブプロファイル – 属性更新間隔（Adaptive Profiles – Attribute Update Interval）]**：プロファイル更新が有効な場合、ネットワークマップデータを管理センターからその管理対象デバイスに同期する間隔を分単位で制御できます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。このオプションの値を大きくすると、大規模なネットワークでパフォーマンスを向上させることができます。
- **[アダプティブプロファイル – ネットワーク（Adaptive Profiles – Networks）]**：プロファイル更新が有効な場合、オプションで、IP アドレス、アドレスブロック、およびネットワーク変数のカンマ区切りリストにプロファイル更新を制限することで、パフォーマンスを向上できます。ネットワーク変数を使用すると、アクセス コントロール ポリシーのデフォルトの侵入ポリシーにリンクされている変数セットの変数の値が使用されるようになります。たとえば、192.168.1.101、192.168.4.0/24、$HOME_NET というように入力することができます。IPv4 と IPv6 がサポートされます。

  デフォルト値（0.0.0.0/0）は、すべてのネットワークにアダプティブプロファイルの更新を適用します。

パフォーマンス設定および遅延ベースのパフォーマンス設定

侵入防御のパフォーマンス チューニングについて（2225ページ）では、侵入行為についてトラフィックを分析する際のシステムのパフォーマンスを向上させるための情報を提供しています。

遅延ベースのパフォーマンス設定固有の情報については、パケットおよび侵入ルールの遅延しきい値構成（2231 ページ）を参照してください。

暗号化された可視性エンジン

この機能の詳細については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「Encrypted Visibility Engine」の章を参照してください。

アクセス制御への他のポリシーの関連付け

主要ポリシーをアクセス コントロール ポリシーに関連付ける最も簡単な方法は、アクセス コントロール ポリシーのトピックに示されているパケットフローでポリシーのリンクをクリック

することです。関連付けるポリシーをすばやく選択できます。または、このトピックで説明されているように、ポリシーの詳細設定を使用してポリシーを関連付けることもできます。これらのポリシーには以下が含まれます。

- プレフィルタ ポリシー：（レイヤ4の）アウターヘッダによりネットワーク限定を使用した早期のトラフィック処理を実行します。
- 復号ポリシー：セキュアソケットレイヤ（SSL）または Transport Layer Security（TLS）で暗号化されたアプリケーション層プロトコルトラフィックをモニタ、復号、ブロック、または許可します。

⚠

注意 *Snort 2* のみ。SSL ポリシーを追加または削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnortの再起動によるトラフィックの動作 （165 ページ）を参照してください。

- アイデンティティポリシー：トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザー識別を実行します。

始める前に

SSL ポリシーをアクセス コントロール ポリシーに関連付ける前に、アクセス コントロール ポリシーの詳細設定 （1759 ページ）で TLS サーバーアイデンティティ検出に関する情報を確認してください。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 適切な [ポリシー設定（Policy Settings）] 領域の [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 ドロップダウン リストからポリシーを選択します。

ユーザーが作成したポリシーを選択する場合は、表示される編集アイコンをクリックしてポリシーを編集できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ルールヒットカウントの表示

ヒットカウントは、ポリシールールまたはデフォルトアクションが接続に一致した回数を示します。ヒットカウントは、ルールに一致する接続の最初のパケットに対してのみ増加します。この情報を使用してルールの有効性を特定することができます。ヒットカウント情報は、Firewall Threat Defense デバイスに適用されるアクセス制御とプレフィルタルールに対してのみ使用できます。

（注）

- このカウントは、再起動やアップグレードの後も維持されます。
- カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。
- デバイスで展開またはタスクが進行中の場合、デバイスからヒットカウント情報を取得することはできません。
- また、デバイス CLI で **show rule hits** コマンドを使用してルールヒットカウント情報を表示することもできます。
- [アクセスコントロールポリシー（Access Control Policy）] ページから [ヒットカウント（Hit Count）] ページにアクセスした場合、プレフィルタ ルールを表示または編集することはできません。また、その逆も同様です。
- ヒットカウントは、モニターアクションを使用するルールでは使用できません。

始める前に

カスタムユーザーロールを使用する場合は、ロールに次の権限が含まれていることを確認してください。

- デバイスの閲覧：ヒットカウントを確認します。
- デバイスの変更：ヒットカウントを更新します。

手順

ステップ 1 アクセスコントロールポリシーまたはプレフィルタ ポリシー エディタで、ページの右上にある [ヒットカウントの分析（Analyze Hit Counts）] をクリックします。

ステップ 2 [ヒット カウント（Hit Count）] ページで、[デバイスの選択（Select a device）] ドロップダウンリストからデバイスを選択します。

このデバイスのヒットカウントを生成するのが初めてではない場合は、ドロップダウンボックスの横に最後に取得したヒットカウント情報が表示されます。また、[最終展開（Last Deployed）] の時刻を確認して、最新のポリシー変更を確認します。

ステップ 3 必要に応じて、[更新（Refresh）]（） をクリックして、選択したデバイスから現在のヒットカウントデータを取得します。

プレフィルタポリシーでは、[現在のヒットカウントの取得（Fetch Current Hit Count）] をクリックして、最初のヒットカウントデータを取得する必要がある場合があります。

デバイスへの展開が進行している間は、ヒットカウントを更新できません。

ステップ 4 データを表示して分析します。

次を実行できます。

- [プレフィルタ（Prefilter）] または **[アクセス制御（Access Control）]** をクリックして、これらのポリシーのヒットカウントを切り替えます。
- [フィルタ（Filter）] ボックスに検索文字列を入力して、特定のルールを検索します。
- [フィルタ基準（Filter by）] フィールドで [ヒットルール（Hit Rules）] や [ルールにヒットしない（Never Hit Rules）] オプションを選択して、リストを大まかに制限します。ヒットルールを閲覧するときに、[最後（In Last）] フィールドで時間範囲を選択することで（たとえば、過去 1 日）、リストをさらに制限できます。
- （アクセスコントロールポリシーから見た場合）個々のルールで次の操作を実行できます。
  - [編集（Edit）]（） をクリックしてルールを編集します。
  - [削除（Delete）]（） をクリックして、ポリシーからルールを削除します。
  - [スライダ（Slider）]（） をクリックして、ルールを有効または無効にします。
  - ルールの [X] をクリックして、ルールのヒットカウントをクリア（ゼロにリセット）します。この操作は取り消すことができません。
- （プレフィルタポリシーから見た場合）[歯車（Cog）]（） をクリックして表示する列を選択することで、表示される列を変更します。
- （プレフィルタポリシーから見た場合）ルール名をクリックして編集するか、最後の列の [表示（View）]（） をクリックしてルールの詳細を表示します。ルール名をクリックすると、ポリシー ページ内でその名前がハイライトされ、編集できるようになります。
- （プレフィルタポリシーから見た場合）ルールを右クリックし、[ヒットカウントのクリア（Clear Hit Count）] を選択してルールのヒットカウント情報をクリア（ゼロにリセッ

ト）します。Ctrl を押しながらクリックすることで、複数のルールを選択できます。この操作は取り消すことができません。

- ページの左下にある [CSVの生成（Generate CSV）] をクリックして、詳細情報のカンマ区切り値のレポートをページ上で生成します。

ステップ 5 [閉じる（Close）] をクリックしてポリシー ページに戻ります。

ルールの競合および警告の分析

ルール競合に関する警告および情報を表示して、アクセス コントロール ポリシーのロジックを調べ、変更が必要なルールを特定することができます。ルールが重複していると、不要なルールがポリシーに含まれることになる場合があり、それらのルールがトラフィックに一致することはありません。分析は、不要なルールを削除したり、目的のポリシーを適用するために移動または変更する必要があるルールを特定するために役立ちます。

ポリシーの警告とエラーは、ルールが目的のサービスを確実に提供するために理解し、多くの場合に対処する必要がある事柄を示します。

ルール競合分析では、次のタイプの問題が特定されます。

- オブジェクトの重複：ルールのフィールドに含まれる 1 つの要素が、ルールの同じフィールドに含まれる 1 つ以上の要素のサブセットになっています。たとえば、送信元フィールドには、10.1.1.0/24 のネットワークオブジェクトと、ホスト 10.1.1.1 の別のオブジェクトが含まれる場合があります。10.1.1.1 は 10.1.1.0/24 によってカバーされるネットワーク内にあるため、10.1.1.1 のオブジェクトは冗長であり、削除することができます。それにより、ルールが簡素化され、デバイスのメモリも節約できます。
- 冗長なルール：基本ルールでも 2 つのルールによって同じタイプのトラフィックに同じ処理が適用される場合、基本ルールを削除しても最終的な結果は変わりません。たとえば、特定のネットワークの FTP トラフィックを許可するルールに、同じネットワークの IP トラフィックを許可するルールが続き、その間にアクセスを拒否するルールがない場合、最初のルールは冗長であり、削除できます。
- シャドウイング状態のルール：これは、冗長なルールの逆です。この場合は、あるルールが別のルールと同じトラフィックに一致し、2 番目のルールはアクセス リスト内であとに配置されているためにいずれのトラフィックにも適用されません。両方のルールのアクションが同じである場合は、シャドウイング状態のルールを削除できます。2 つのルールがトラフィックに対して異なるアクションを指定している場合、必要なポリシーを導入するには、シャドウイング状態のルールを移動するか、いずれかのルールの編集が必要になる場合があります。たとえば、1 つの送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイング状態のルールでFTP トラフィックを許可する場合などです。

始める前に

分析を実行する場合：

- ルールごとに最初の競合のみが識別されます。問題を修正すると、そのルールがテーブル内の別のルールと競合していると識別される場合があります。ただし、1 つのルールに複数の警告またはエラーがある場合があります。
- ルール競合分析では、送信元/宛先のセキュリティゾーン、ネットワーク、VLAN、およびサービス/ポートの一致条件とアクションのみが考慮されます。他の一致基準は考慮されないため、一見冗長なルールが完全に冗長ではない可能性があります。
- FQDN の IP アドレスは DNS ルックアップの前に知ることができないため、FQDN ネットワークオブジェクトの競合は分析できません。
- 無効になっているルールは無視されます。
- 時間範囲属性は無視されます。異なる期間のルールは、実際にはその時間範囲で冗長ではない場合でも、冗長としてマークされる可能性があります。
- 警告およびエラーとルール競合（機能を有効にする場合）のアイコンがルールテーブルに表示されます。アイコンのリファレンスについては、ルールとその他のポリシーの警告（1720 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policy）]** > **[アクセス制御（Access Control）]** を選択し、アクセス コントロール ポリシーを編集します。

ステップ 2 次のいずれかを実行して、ルールの競合および警告のダイアログボックスを開きます。

- ルール競合を表示するには、[分析（Analyze）] ドロップダウンをクリックし、[ルールの競合を有効にする（Enable Rule Conflicts）] をクリックします。次に、同じメニューから [ルールの競合の表示（Show Rule Conflicts）] をクリックして、特定の結果を表示します。
- ルールの警告およびエラーを表示するには、**[分析（Analyze）]** > **[ルールの警告の表示（Show Rule Warnings）]** をクリックします。
- ルール競合の確認が完了したら、**[分析（Analyze）]** > **[ルールの競合を無効にする（Disable Rule Conflicts）]** をクリックします。

ステップ 3 ルールの競合および警告のダイアログボックスには、次のような機能があります。

- 警告とエラーは、[ルールの競合（Rule Conflicts）] とは別のタブに表示されます。
- 各タブにはサブタブがあり、問題の個別のタイプ（冗長かシャドウイングか、警告かエラーか、など）を調べることができます。アイテムを検索することもできます。
- 各ルール名の横にある [その他（More）] (⋮) は、ルールの編集、無効化、または削除へのショートカットを提供します。

ステップ 4 終了したら、[閉じる（Close）] をクリックします。

ルールの検索

検索を使用してルールを見つけることができ、ルールの数が多い場合は特に役立ちます。

送信元または宛先ネットワークで IP アドレスを（簡易テキスト検索ではなく）検索すると、アドレスに一致するルールが返されます。対象には、完全一致だけでなく、サブネット一致も含まれます。たとえば、10.1.1.1 を検索すると、10.1.1.0/24 のルールも結果に含まれます。

手順

ステップ 1 アクセスコントロールポリシーを編集するときは、[検索（Search）] ボックスをクリックして検索文字列を作成します。

- 単純なテキスト文字列検索の場合は、文字列を入力します。検索では、検索文字列がいずれかの列にあるルールが返されます。
- 特定の列を検索するには、完全な名前（送信元ネットワークなど）の入力を求められるまで列名を入力するか、検索可能なフィールドのリストから名前を選択します。検索タグを選択すると、そのタグの検索文字列を入力できます。例：**送信元ネットワーク 10.1.1.1**。
- 最初の検索後、検索ボックスをクリックすると、最近の検索とタグが表示されます。検索を選択してすばやく繰り返したり、以前の検索やタグを選択してそれらに基づいて同様の検索を作成したりできます。
- 複数のタグで検索文字列を作成する場合は、タグの間にスペースを含めないでください。
- タグを選択すると、対象の列に表示される値を求めるプロンプトが表示されます。検索する値を選択します。
- 検索ボックスの左側にある [フィルタ（FIlter）] アイコンをクリックし、[許可（Allow）]、[ブロック（Block）]、[モニター（Monitor）]、[侵入ポリシー（Intrusion Policy）]、[時間範囲（Time Range）].

ステップ 2 検索ボックスの検索文字列の末尾にカーソルを置き、Enter を押します。

検索文字列に一致するルールは強調表示され、一致しないルールは非表示になります。[一致するルールのみを表示（Show Only Matching Rules）] の選択を解除すると、テーブル全体が表示され、テーブル内のルールが強調表示され、周囲のルールを確認できます。

[一致するルールのみを表示（Show Only Matching Rules）] チェックボックスの横には、ポリシー内のルールの総数と検索文字列に一致する数の比較に関する概要が表示されます。

ステップ 3 検索を閉じて、フィルタ処理も強調表示もされていないテーブルに戻るには、検索ボックスの右側にある [X] をクリックします。検索文字列の末尾にカーソルを置き、Esc キーを押すこともできます。

アクセス コントロール ポリシーの履歴

表 *84 :*

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しいアクセスコントロールポリシーのユーザーインターフェイスとルールの競合分析。	7.3.0	いずれか	7.2 で導入されたアクセス コントロール ポリシーのユーザーインターフェイスは、デフォルトのインターフェイスになりました。また、ルールの競合分析を有効にすると、ポリシーでの以前ルールが原因で一致しない冗長ルールやオブジェクト、およびシャドウルールを特定できます。
アクセスコントロールポリシーのロック。	7.2.0	いずれか	アクセス コントロール ポリシーをロックして、他の管理者が編集できないようにすることができます。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。アクセス コントロール ポリシーを変更する権限を持つすべてのユーザーには、それをロックする権限があります。 ポリシーの編集時にポリシーをロックまたはロック解除するアイコンがポリシー名の横に追加されました。さらに、他の管理者によってロックされたポリシーのロックを解除できるようにする新しい権限（アクセス コントロール ポリシー ロックのオーバーライド）が追加されました。この権限は、デフォルトで管理者、アクセス管理者、およびネットワーク管理者のロールで有効になっています。
ルールのヒットカウントは再起動後も存続します。	7.2.0	いずれか	管理対象デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。**show rule hits** コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。 次のデバイス CLI コマンドを変更しました：**show rule hits**。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
アクセス コントロール ポリシーのユーザビリティの改善。	7.2.0	いずれか	アクセス コントロール ポリシーで使用できる新しいユーザーインターフェイスが追加されました。従来のユーザーインターフェイスを引き続き使用することも、新しいユーザーインターフェイスを試すこともできます。新しいインターフェイスは、ルールリストのテーブルビューとグリッドビュー、列を表示または非表示にする機能、高度な検索機能、無限スクロール機能を備え、アクセス コントロール ポリシーが割り当てられたポリシーに関するパケットフローのビューがより明確になりました。また、ルール作成用の追加/編集ダイアログボックスがシンプルになりました。アクセス コントロール ポリシーの編集中に、従来のユーザーインターフェイスと新しいユーザーインターフェイスを自由に切り替えることができます。
DNS フィルタリング	7.0.0 6.7.0（試験的）	任意（Any）	URL フィルタリングが有効になっていて設定されている場合、カテゴリとレピュテーションのフィルタリングの有効性を強化する新しいオプションが、新しい各アクセス コントロール ポリシーでデフォルトで有効になっています。 詳細については、DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別（ベータ版）（1832 ページ）とサブトピックを参照してください。 [全般設定（General Settings）] の下のアクセス コントロール ポリシーの [詳細（Advanced）] タブに、[DNS トラフィックへのレピュテーション適用を有効にする（Enable reputation enforcement on DNS traffic）] という新しいオプションが追加されました。
TLS サーバーアイデンティティ検出	6.7.0	いずれか	クライアントが TLS 1.3 対応サーバーに接続するときに、アクセス コントロール ポリシーを有効にして URL とアプリケーションの条件を評価します。TLS サーバーアイデンティティ検出により、トラフィックを復号せずにこれらの条件を評価できます。 この機能を有効にすると、モデルによっては、デバイスのパフォーマンスに影響する可能性があります。 アクセス コントロール ポリシーの [詳細設定（Advanced）] タブページに、新しいオプションが追加されました。 • [詳細設定（Advanced）] タブに警告が表示されます。スライダを右に動かすと、TLS サーバーアイデンティティ検出が有効になります。 • [詳細設定（Advanced）] タブページに、[TLS サーバーアイデンティティ検出（TLS Server Identity Discovery）] という新しいオプションが追加されました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しいセキュリティインテリジェンスカテゴリ	—	任意	次のカテゴリは6.6リリースの頃に導入されましたが、6.6に限定されてはいません。 • banking_fraud • high_risk • ioc • link_sharing • malicious • newly_seen • spyware

第 40 章

アクセス コントロール ルール

次の各トピックでは、アクセス コントロール ルールの設定方法について説明します。

- アクセス コントロール ルールの概要 （1775 ページ）
- アクセスコントロールルールの要件と前提条件 （1785 ページ）
- アクセス制御ルールのガイドラインと制限事項 （1786 ページ）
- アクセスコントロールルールの管理 （1787 ページ）
- アクセスコントロールルールの例 （1806 ページ）
- アクセス制御ルールの履歴 （1812 ページ）

アクセス コントロール ルールの概要

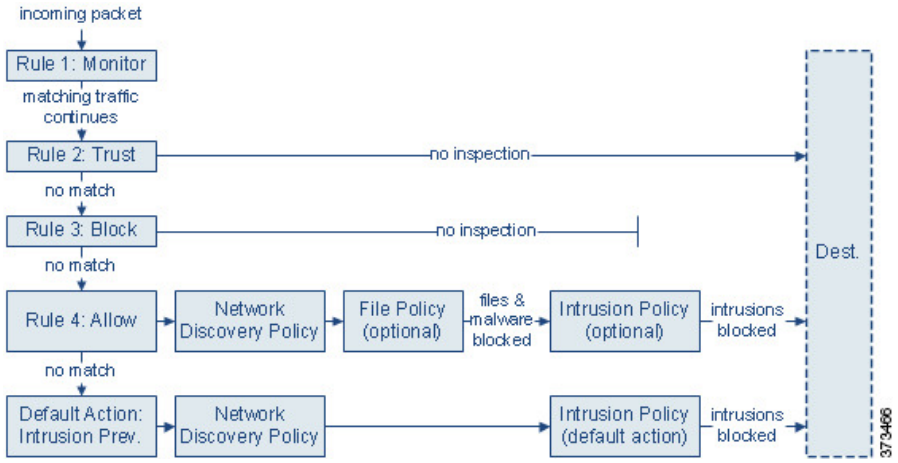
アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理するきめ細かい制御方法が提供されます。

（注） アクセス制御ルールがネットワークトラフィックを評価する前に、セキュリティインテリジェンスのフィルタ処理、暗号解読、ユーザーの識別、および一部の復号と前処理が行われます。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。

また、各ルールにはアクションがあり、これによって一致するトラフィックをモニター、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

次のシナリオでは、インラインの侵入防御展開環境で、アクセス コントロール ルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1**：**モニタ**はトラフィックを最初に評価します。モニタールールはネットワークトラフィックを追跡してログに記録します。システムはトラフィックと追加ルールの照合を継続して、許可するか拒否するかを決定します（ただし、重要な例外と注意事項をアクセス コントロール ルールのモニター アクション （1781 ページ）で確認してください）。
- **ルール 2**：**信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは追加のインスペクションなしで宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。一致しないトラフィックは、引き続き次のルールと照合されます。
- **ルール 3**：**ブロック**はトラフィックを 3 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4**：**許可**は最後のルールです。このルールの場合、一致したトラフィックは許可されますが、トラフィック内の禁止ファイル、マルウェア、侵入、エクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない許可ルールを設定できます。
- **デフォルト アクション**は、いずれのルールにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルトアクションを割り当てることもあります。（デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。）

アクセス コントロール ルールまたはデフォルト アクションによって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザ データについてネットワーク検出ポリシーによるインスペクションの対象になります。検出は明示的には有効にしませんが、拡張したり無効にしたりすることができます。ただし、トラフィックを許可することで、検出データの収

集が自動的に保証されるものではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

暗号化されたトラフィックの通過が暗号解読設定で許可される場合、または暗号解読が設定されていない場合は、そのトラフィックがアクセスコントロールルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、暗号化ペイロードの侵入およびファイル検査を、システムは無効化します。これにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

アクセス コントロール ルールの管理

アクセス コントロール ポリシー エディタの [ルール（Rules）] タブでは、現在のポリシー内のアクセスコントロールルールの追加、編集、分類、検索、フィルタ処理、移動、有効化、無効化、削除、その他の管理が行えます。

アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには不可欠です。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。

検索バーを使用して、アクセス コントロール ポリシー ルールのリストをフィルタ処理します。[一致するルールのみを表示（Show Only Matching Rules）] オプションの選択を解除して、すべてのルールを表示できます。一致したルールが強調表示されます。

ポリシー エディタでは、各アクセス コントロール ルールに対してルールの名前、条件の概要、ルール アクションが表示され、さらにルールのインスペクション オプションや状態を示すアイコンが表示されます。各アイコンの意味は次のとおりです。

- [時間範囲（time range）] オプション（）
- **侵入ポリシー**（）
- **ファイルポリシー**（）
- **ロギング**（）
- [警告（warning）]（）
- **エラー**（）
- [ルールの競合（Rule Conflict）]（）

無効なルールはグレー表示され、ルール名の後に [無効（disabled）] というマークが付きます。

ルールを作成または編集するには、アクセス コントロール ルール エディタを使用します。

：次の操作を実行できます。

- ルール名を設定し、エディタの上部でその配置を選択します。
- エディターの上または下の行を選択して、別のルールの編集に切り替えます。
- 左側のリストを使用してルールアクションを選択し、侵入ポリシーと変数セット、ファイルポリシー、および時間範囲を適用し、ログオプションを設定します。
- ルール名の隣にあるオプションを使用してルールアクションを選択し、侵入ポリシーと変数セット、ファイルポリシー、および時間範囲を適用し、ログオプションを設定します。
- [ソース（Sources）] と [宛先とアプリケーション（Destinations and Applications）] 列を使用して、一致基準を追加します。[すべて（All）] リストからオプションを追加するか、別のタブに移動して、セキュリティゾーンやネットワークなど、必要なタイプのオプションをより簡単に見つけることができます。
- エディタの下部でルールにコメントを追加します。

関連トピック

アクセス コントロール ルールのコンポーネント （1778 ページ）
アクセス制御ルールのベストプラクティス （1736 ページ）

アクセス コントロール ルールのコンポーネント

一意の名前に加え、各アクセスコントロールルールには次の基本コンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

アクセスコントロールポリシー内の各ルールには、1から始まる番号が付きます。ポリシー継承を使用する場合、ルール1は再外部ポリシーの1番目のルールです。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

また、ルールはセクションおよびカテゴリに属していることがあります。これは、単に整理のためであり、ルールの位置に影響しません。ルールの位置は、すべてのセクションとカテゴリにまたがって設定されます。

セクションおよびカテゴリ

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。アクセス コントロール ルールをさらに細かく整理するため、

「必須（Mandatory）」セクション内と「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」セクションと「デフォルト（Default）」セクションの間にネストされます。

条件

条件は、ルールが処理する特定のトラフィックを指定します。条件には単純なものと複雑なものがあり、ライセンスによって用途が異なります。

トラフィックは、ルールで指定されたすべての条件を満たす必要があります。たとえば、アプリケーション条件で HTTP が指定されていて、HTTPS は指定されていない場合、URL カテゴリとレピュテーションの条件は、HTTPS トラフィックには適用されません。

適用時間

ルールを適用する日時を指定できます。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。一致したトラフィックをモニター、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。信頼できるトラフィック、ブロックされたトラフィック、または暗号化されたトラフィックに対しては、詳細な検査は実行されません。

インスペクション（Inspection）

詳細検査オプションは、悪意のあるトラフィックをどのように検査してブロックし、それ以外のものは許可するかを決定します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出たりする前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1 つのルールに一致するトラフィックのレコードを 1 つ保持できます。一般的に、接続の開始時または終了時（あるいは、その両方）にセッションをログに記録できます。接続のログは、データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

説明

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。

関連トピック

アクセス制御ルールのベストプラクティス （1736 ページ）
アクセス コントロール ルールの管理 （1777 ページ）

アクセスコントロールルールの作成および編集 （1788 ページ）
アクセス コントロール ルールのアクション （1781 ページ）
アクセスコントロールルール条件 （1790 ページ）
ファイルポリシーと侵入ポリシーを使用したディープインスペクション （1723 ページ）
アクセス コントロール ルールのコメント

アクセス コントロール ルールの順序

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセスコントロールルールに従ってネットワーク トラフィックを処理します。モニタールールを除いて、トラフィックがルールに一致した後、システムは優先度の低い追加のルールに対してトラフィックの評価は続行しません。

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。さらに細かく整理するため、「必須（Mandatory）」セクション内や「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。カテゴリは、作成した後に移動することはできません。ただし、カテゴリを削除または名前変更したり、ルールをカテゴリ内またはカテゴリ間で移動したりすることはできます。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」ルール セクションと「デフォルト（Default）」ルール セクションの間にネストされます。ルール 1 は、現在のポリシーではなく、最外部ポリシーの 1 番目のルールです。ルールの番号は、すべてのポリシー、セクション、カテゴリにまたがって割り当てられます。

アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールによって、ルールのカテゴリ内またはカテゴリ間でアクセス コントロール ルールを移動および変更することもできます。しかし、ユーザがルールを移動および変更することを制限するには、カスタム ロールを作成できます。アクセスコントロールポリシーの変更権限が割り当てられているユーザは、制限なく、カスタム カテゴリにルールを追加することや、カテゴリ内のルールを変更することができます。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックする必要があるトラフィックを含め、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえばIPアドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件(ネットワークやIPアドレスなど)を使用するアクセス コントロール ルールは、一般的な条件(アプリケーションなど)を使用するルールの前にオーダーする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3(物理、データリンク、およびネットワーク)の条件を持つルールは、アクセス コントロール ルールで最初に注文する必要があります。レイヤ5、6、および7(セッション、プレゼンテーション、およびアプリケーション)の条件は、アクセス コントロール ルールの後で順序付けする必要があります。OSIモデルの詳細については、こちらのWikipediaの記事を参照してください。

ヒント アクセス コントロール ルールの順序を適切に設定することで、ネットワーク トラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

関連トピック

順序付けルールのベストプラクティス （1738 ページ）

アクセス コントロール ルールのアクション

アクセス コントロール ルールには、システムが一致するトラフィックをどのように処理し、ロギングするのかを指定するアクションがあります。モニター、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

アクセス コントロール ポリシーのデフォルトアクションは、モニター以外のアクションをもつどのアクセスコントロールルールの条件にも一致しないトラフィックを処理します。

アクセス コントロール ルールのモニター アクション

[Monitor]アクションは、トラフィックを許可または拒否するように設計されていません。むしろ、その主な目的は、一致するトラフィックが最終的にどのように処理されるかに関係なく、接続ロギングを強制することです。

接続がモニタールールに一致する場合、接続が一致する次の非モニタールールがトラフィック処理とそれ以降のインスペクションを決定する必要があります。さらに一致するルールがない場合、システムはデフォルトアクションを使用する必要があります。

ただし、例外があります。モニタールールにレイヤ7の条件（アプリケーション条件など）が含まれている場合、そのシステムでは早期パケットを通過させ、接続を確立（またはSSLハン

ドシェイクの完了）することができます。これは、接続が後続のルールによってブロックされる必要がある場合でも発生します。これらの早期パケットが後続のルールに対して評価されないためです。こうしたパケットが完全に検査されていない宛先に到達しないように、アクセスコントロールポリシーの詳細設定で、このための侵入ポリシーを指定できます。トラフィック識別の前に通過するパケットのインスペクション（2746ページ）を参照してください。システムはレイヤ7の識別を完了した後、残りのセッショントラフィックに適切なアクションを適用します。

注意 ベストプラクティスとして、広範に定義されたモニタールールのレイヤ7の条件をルールの優先順位内で高く設定しないようにすることで、不注意でトラフィックがネットワークに流入することを防ぎます。さらに、ローカルでバインドされているトラフィックがレイヤ3展開のモニタールールに一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で [Inspect Local Router Traffic] を有効にします。

アクセス コントロール ルールの信頼アクション

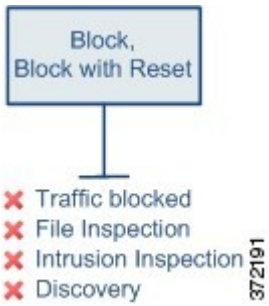
[信頼（Trust）] アクションは、ディープ インスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼処理されたトラフィックも、ID 条件およびレート制限の対象です。

（注）

- FTP や SIP などの一部のプロトコルは、検査プロセスを通じてシステムが開くセカンダリチャネルを使用します。場合によっては、信頼できるトラフィックがすべての検査をバイパスでき、これらのセカンダリチャネルを適切に開くことができません。この問題が発生した場合は、信頼ルールを [許可（Allow）] に変更します。
- ロギング オプションが無効になっている信頼ルールの場合、フロー終了イベントは引き続きシステムで生成されます。ただし、イベントはイベントページには表示されません。
- アクセス コントロール ルールは復号などの他のポリシーの後に評価されるため、接続が信頼されていてもインスペクションなしで高速パスされるとは限りません。たとえば、接続が、復号を必要とする復号ルールと信頼できるアクセス制御ルールの両方に一致する場合、その接続は、信頼ルールによって許可される前に、必要に応じて復号化および検査されます。信頼とは、侵入インスペクションなどの追加のインスペクションが適用されないことを意味します。インスペクションのない接続を許可する場合は、プレフィルタ ポリシーを使用して接続を高速パス処理するか、他のポリシーが接続にインスペクション サービスを適用しないようにします。

アクセス コントロール ルールのブロック アクション

ブロック アクションおよび**リセットしてブロック** アクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。



[HTTP 応答（HTTP response）] ページに一致する Web 要求を除き、リセット ルールを持つブロックが接続をリセットします。これは、システムが Web 要求をブロックするときに表示されるように設定した応答ページは、接続がすぐにリセットされた場合は表示できないためです。

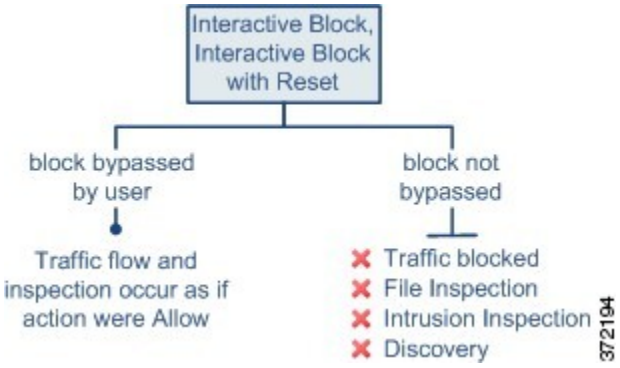
詳細については、「HTTP 応答ページの設定 （1836 ページ）」を参照してください。

関連トピック

HTTP 応答ページの設定 （1836 ページ）

アクセス コントロール ルール インタラクティブ ブロック アクション

[インタラクティブブロック（Interactive Block）] と [リセット付きインタラクティブブロック（Interactive Block with reset）] アクションにより、Web ユーザーは目的の宛先に進む選択肢が与えられます。



ユーザーがブロックをバイパスしている場合、ルールは許可ルールを模倣します。したがって、インタラクティブ ブロック ルールをファイル ポリシーと侵入ポリシーに関連付けることができるため、一致するトラフィックもネットワーク検出の対象となります。

ユーザーがブロックをバイパスしない（できない）場合は、ルールはブロック ルールを模倣します。一致するトラフィックは、追加のインスペクションなしで拒否されます。

インタラクティブブロックを有効にした場合は、ブロックされているすべての接続をリセットできません。これは、接続がすぐにリセットされた場合は応答ページを表示できないためです。[リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを（非インタラクティブに）Web 以外のすべてのトラフィックをリセットしてブロックしても、Web 要求についてはインタラクティブ ブロックは有効になっています。

詳細については、「HTTP 応答ページの設定 （1836 ページ）」を参照してください。

関連トピック

復号ルールのブロックアクション （2388 ページ）

アクセス コントロール ルールの許可アクション

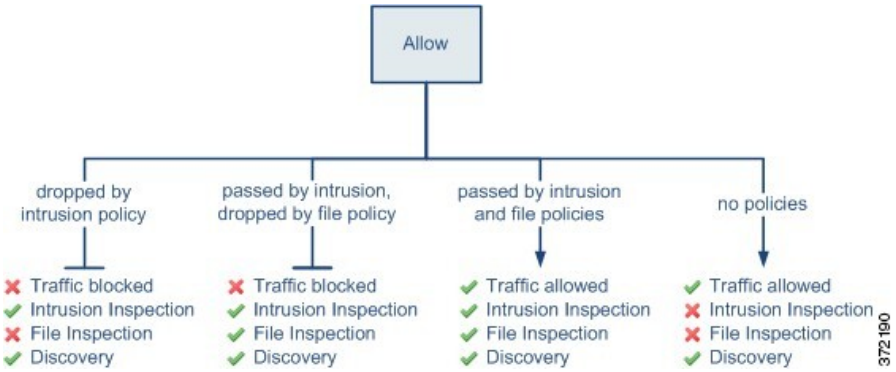
[許可（Allow）] アクションは、一致するトラフィックを通過させます。ただし、引き続き ID 条件およびレート制限の対象となります。

任意で、ディープインスペクションを行い、トラフィックが接続先に到達する前に暗号化されていないトラフィックや復号されたトラフィックを検査、ブロックすることも可能です。

- 侵入ポリシーでは、侵入検知と防御設定に応じてネットワーク トラフィックを分析し、設定内容に応じて違反パケットをドロップすることが可能です。
- ファイル ポリシーでは、ファイルの制御ができます。ファイル制御により、ユーザーが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。

- ネットワークベースの高度なマルウェア保護（AMP）もファイル ポリシーを使用して実行できます。マルウェア防御はファイルのマルウェアを調べ、検出したマルウェアを設定に応じてブロックします。

下の図は、許可ルールの条件（またはユーザーによりバイパスされるインタラクティブブロック ルール）を満たすトラフィックに対して実行されるインスペクションの種類を示しています。侵入インスペクションの前にファイルインスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連のエクスプロイトについては検査されません。



シンプルにするために、この図では、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを示しています。ただし、どちらか1つだけを設定することも可能です。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーが決定します。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーが決定します。

トラフィックが侵入ポリシーとファイルポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可しても、ディスカバリ検査が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニターされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

アクセスコントロールルールの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

アクセス制御ルールのガイドラインと制限事項

- 現在のページに一度に表示できるルールは1000個までに制限されています。したがって、1つのカテゴリ内に3000のルールがあるなど、非常に多くのルールがある場合、カテゴリ内のすべてのルールを選択して削除するなどのアクションを実行しても、すべてのルールは削除されません。対象のすべてのルールを削除するには、ルールを再度選択/削除することが必要な場合があります。
- 実際に使用されているアクセスコントロールルールを編集する場合、その変更は、展開時に確立されている接続には適用されません。更新されたルールは、将来の接続に対する照合に使用されます。ただし、システムが実際に接続を検査している場合（たとえば、侵入ポリシーを使用して）、変更された一致基準またはアクション基準が既存の接続に適用されます。

  Firewall Threat Defense の場合は、Firewall Threat Defense **clear conn** CLI コマンドを使用して確立されている接続を終了させることにより、現在のすべての接続に確実に変更を適用できます。後で接続の送信元が接続の再確立を試み、そのために新しいルールに対して適切に照合されることを前提として、これらの接続を終了しても問題がない場合にのみ、このような処理を行う必要があることに注意してください。
- アクセスルールのVLANタグは、インラインセットにのみに適用されます。このタグは、ファイアウォール インターフェイスに適用されるアクセスルールでは使用できません。
- 完全修飾ドメイン名（FQDN）ネットワークオブジェクトを送信元または宛先の基準として使用するには、プラットフォーム設定ポリシーでデータインターフェイスの DNS も設定する必要があります。システムは、アクセス制御ルールで使用されている FQDN オブジェクトのルックアップを実行するために管理 DNS サーバ設定を使用しません。

  FQDNによるアクセスの制御はベストエフォート型のメカニズムであることに注意してください。次の点を考慮してください。

  - 可能な限り、FQDNルールの代わりにセキュリティインテリジェンスまたはURLフィルタリングを使用します。
  - DNS応答はスプーフィングされる可能性があるため、完全に信頼できる内部DNSサーバーのみを使用します。
  - 一部のFQDNは、特に非常に人気の高いサーバーの場合、数千とはいかなくても、数百の IP アドレスを持つことがあり、それらが頻繁に変更されることがあります。システムはキャッシュされている DNS ルックアップの結果を使用するため、ユーザーはキャッシュに存在しないアドレスを取得する可能性があり、その接続はFQDNルー

ルに合致しません。FQDN ネットワークオブジェクトを使用するルールは、100 未満のアドレスに解決される名前に対してのみ効果的に機能します。

100 を超えるアドレスに解決される FQDN のネットワーク オブジェクト ルールを作成しないことを推奨します。接続のアドレスが解決され、デバイスの DNS キャッシュで使用可能である可能性は低いからです。このような場合は、FQDN ネットワーク オブジェクト ルールの代わりに URL ベースのルールを使用します。

- 人気のある FQDN では、異なる DNS サーバが異なるセットの IP アドレスを返す場合があります。したがって、ユーザが設定したものとは異なる DNS サーバを使用している場合、FQDN ベースのアクセス制御ルールがクライアントで使用されているサイトのすべての IP アドレスに適用されないことがあり、ルールで意図した結果が得られません。
- 一部の FQDN DNS エントリには、非常に短い存続可能時間（TTL）値が設定されています。この結果、ルックアップテーブルで頻繁に再コンパイルが発生し、全体的なシステムパフォーマンスに影響を与える場合があります。
- 8 を超える FQDN が同じ IP アドレスに解決される場合、システムはそれらの FQDN のルールにトラフィックを確実に一致させることができません。IP アドレスごとに最大 8 の FQDN を処理できます。

- アクセス制御ルールごとの一致基準の最大オブジェクト数は 200 です。たとえば、1 つのアクセス制御ルールに最大 200 のネットワークオブジェクトを含めることができます。

アクセスコントロールルールの管理

ここでは、アクセスコントロールルールの管理方法について説明します。

アクセス制御ルール カテゴリの追加

アクセス コントロール ポリシーの必須ルールセクションとデフォルトルールセクションをカスタム カテゴリに分割できます。カテゴリは、作成した後に移動することはできません。ただし、カテゴリを削除または名前変更したり、ルールをカテゴリ内またはカテゴリ間で移動したりすることはできます。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント

ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[Insert new category] を選択することもできます。

ステップ 2 名前を入力します。

ステップ 3 [挿入（Insert）] ドロップダウン リストから、カテゴリを追加する先を選択します。

- カテゴリをセクションのすべての既存カテゴリの下に挿入するには、[必須ルール内（Into Mandatory）] または [デフォルトルール内（into Default）] を選択します。
- 既存のカテゴリの上に挿入するには、[カテゴリの上（above category）] を選択した後、カテゴリを選択します。
- アクセス制御ルールの上または下に挿入するには、[ルールの上（above rule）] または [ルールの下（below rule）] を選択した後、既存のルール番号を入力します。

ステップ 4 **[適用（Apply）]** をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

アクセスコントロールルールの作成および編集

アクセスコントロールルールを使用して、特定のトラフィッククラスにアクションを適用します。ルールを使用すると、望ましいトラフィックを選択的に許可し、望ましくないトラフィックをドロップできます。

手順

ステップ 1 アクセス コントロール ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、[編集（Edit）]（） をクリックします。
- 複数のルールを編集するには、チェックボックスを使用して複数のルールを選択してから、検索ボックスの横にある [アクションの選択（Select Action）] リストで [編集（Edit）] または別のアクションを選択します。
- インライン編集を行うには、つまりルール条件のオブジェクトの構成を変更するには、値を右クリックして [編集（Edit）] を選択します。右クリックメニューを使用して、項目を削除したり、フィルタに追加したり、テキストや値をコピーしたりすることもできます。

代わりに [表示（View）]（） がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 これが新しいルールである場合は、[名前（Name）] を入力します。

ステップ 3 （）ルールコンポーネントを設定します。

複数のルールを一括編集する場合は、オプションのサブセットのみを使用できます。

- [位置（Position）]：ルールの位置を指定します。アクセス コントロール ルールの順序（1780 ページ）を参照してください。
- [アクション（Action）]：ルールの [アクション（Action）] を選択します。アクセス コントロール ルールのアクション （1781 ページ）を参照してください。
- [ディープインスペクション（Deep Inspection）]：（オプション）許可ルールおよびインタラクティブ ブロック ルールの場合は、[侵入ポリシー（Intrusion Policy）]、[変数セット（Variable Set）]、および [ファイルポリシー（File Policy）] のオプションを選択します。侵入ポリシーとファイルポリシーを個別に適用できます。両方を設定する必要はありません。
- [時間範囲（Time Range）]：（オプション）Firewall Threat Defense デバイスの場合、ルールが適用される曜日と時間を選択します。オプションを選択しない場合、ルールは常にアクティブになります。詳細は、時間範囲オブジェクトの作成（1401 ページ）を参照してください。
- [ロギング（Logging）]：[ロギング（Logging）] をクリックし、接続ロギングと SNMP トラップのオプションを指定します。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Best Practices for Connection Logging」を参照してください。
- [条件（Conditions）]：追加するオブジェクト、または送信元か接続先を選択し、[送信元に追加（Add to Sources）] または [宛先とアプリケーションに追加（Add to Destinations and Applications）] をクリックして、接続の一致条件を追加します。タブをクリックして、使用可能なオブジェクトのリストをネットワーク、セキュリティゾーン、アプリケーションなどに限定できます。ただし、送信元と接続先の列には、現在表示しているタブに関係なく、選択したすべてのオブジェクトが常に表示されます。詳細については、アクセスコントロールルール条件 （1790 ページ）を参照してください。
- [コメント（Comments）]：ダイアログボックスの下部にあるコメントリストを開いてコメントを入力し、[投稿（Post）] をクリックしてコメントを追加します。

ステップ 4 [追加（Add）] または [適用（Apply）] をクリックして、ルールを保存します。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

時間ベースのルールを展開する場合は、ポリシーが割り当てられるデバイスのタイムゾーンを指定します。「タイムゾーン （892 ページ）」を参照してください。

設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

アクセス制御ルールのベストプラクティス （1736 ページ）

アクセスコントロールルール条件

ルール条件は、各ルールで対象とする接続の特性を定義します。条件を正確に使用してルールを微調整し、該当するルールで処理する必要があるトラフィックのすべてに、またそのトラフィックのみに適用されるようにします。次のトピックでは、使用できる一致条件について説明します。

セキュリティ/トンネルゾーンのルール条件

セキュリティゾーンとトンネルゾーンを使用して、ルールのトラフィックを選択できます。

セキュリティ ゾーンを利用すると、ネットワークをセグメント化し、複数のデバイスでインターフェイスをグループ化して、トラフィック フローを管理および分類する上で助けになります。トンネルゾーンでは、トンネル内のカプセル化された接続にアクセスコントロールルールを適用するのではなく、トンネルとして処理する必要があるトンネルトラフィック（GRE など）を識別することができます。

セキュリティゾーンを使用して、送信元および宛先インターフェイスごとにトラフィックを制御できます。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加する場合、トラフィックがルールに一致するには、一致するトラフィックが送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過する必要があります。セキュリティゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要がるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

トンネルゾーンを使用する場合は、プレフィルタポリシーに一致するルールがあることを確認して、トンネル化トラフィックをゾーンに関連付けます。次に、ルールの送信元ゾーンとしてトンネルゾーンを選択できます。トンネルゾーンを宛先にすることはできません。トンネルをトンネルゾーンに再ゾーン化するためのプレフィルタルールがない場合、トンネルのアクセスコントロールルールはどの接続にも適用されません。宛先セキュリティゾーンを、特定のインターフェイスを介してデバイスを離れるターゲットトンネルに指定することができます。

セキュリティゾーンに関する注意事項

セキュリティゾーンの基準を決定するときは、次の点を考慮してください。

- 可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。
- アクセスコントロールルールは、デバイス設定で ACL エントリ（ACE）を生成して、可能な限り早期の処理およびドロップを提供します。ルールでセキュリティゾーンを指定すると、ゾーン内のインターフェイスごとに ACE が作成されるため、ACL のサイズが非常に大きくなる可能性があります。アクセスコントロールルールから生成された ACL が大きすぎると、システムパフォーマンスに影響を与える可能性があります。

ネットワークルール条件

ネットワークルール条件とは、トラフィックのネットワークアドレスまたは場所を定義するネットワークオブジェクトまたは地理的位置です。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元（Source）] リストに条件を追加します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先（Destinations）] リストに条件を追加します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加するには、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。

  可能な限り、複数のネットワークオブジェクトを 1 つのオブジェクトグループに結合します。複数のオブジェクトを（送信元または宛先を個別に）選択すると、システムは（展開時に）オブジェクトグループを自動的に作成します。既存のグループを選択すると、オブジェクトグループの重複を回避し、多数の重複オブジェクトがある場合の CPU 使用率への潜在的な影響を軽減できます。

  完全修飾ドメイン名（FQDN）を使用してアドレスを定義するオブジェクトを使用できます。このアドレスは DNS ルックアップによって判別されます。ただし、アクセス コントロール ポリシー内の次のセクションでは、FQDN オブジェクトはサポートされていません：元のクライアントネットワーク、SGT/ISE 属性、ネットワーク分析および侵入ポリシー、セキュリティインテリジェンス、Threat Detection、エレファントフロー設定。

- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、その大陸内のすべての国が選択されます。地理的位置を直接ルールで選択するほかに、作成した位置情報オブジェクトを選択して場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

（注） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

ネットワーク条件での元のクライアント（プロキシ トラフィックのフィルタリング）

一部のルールでは、発信元クライアントに基づいてプロキシトラフィックを処理できます。送信元ネットワーク条件を使用してプロキシサーバーを指定し、次に元のクライアント制約を追加して元のクライアント IP アドレスを指定します。システムはパケットの X-Forwarded-For

（XFF）、True-Client-IP、またはカスタム定義 HTTP ヘッダー フィールドを使用して、元のクライアント IP を判別します。

プロキシの IP アドレスがルールの送信元ネットワークの制約と一致する場合、トラフィックはルールに一致し、さらに元のクライアントの IP アドレスは、ルールの元のクライアント制約に一致します。たとえば、特定の元のクライアントアドレスからのトラフィックを許可するものの、それが特定のプロキシを使用している場合のみに限定するには、以下の 3 つのアクセス コントロール ルールを作成します。

アクセスコントロールルール 1：特定の IP アドレス（209.165.201.1）からのプロキシトラフィックをブロックします。

送信元ネットワーク：209.165.201.1
元のネットワーク クライアント：none または any
アクション：ブロック

アクセス コントロール ルール 2：同じ IP アドレスからのプロキシ トラフィックを許可します。ただし、そのトラフィックのプロキシサーバーが、選択したもの（209.165.200.225 または 209.165.200.238）である場合に限ります。

送信元ネットワーク：209.165.200.225 および 209.165.200.238
元のクライアント ネットワーク：209.165.201.1
アクション：許可

アクセス コントロール ルール 3：同じ IP アドレスからのプロキシ トラフィックを、それが他のプロキシ サーバーを使用する場合はブロックします。

[Source Networks]：any
元のクライアント ネットワーク：209.165.201.1
アクション：ブロック

VLAN タグルール条件

（注） アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense

- インラインセットおよびパッシブインターフェイス：Q-in-Qをサポートします（最大2つのVLANタグをサポート）。
- ファイアウォール インターフェイス：Q-in-Qをサポートしません（1つのVLANタグのみをサポート）。

事前定義のオブジェクトを使用してVLAN条件を作成でき、また1～4094のVLANタグを手動で入力することもできます。VLANタグの範囲を指定するには、ハイフンを使用します。

クラスタでVLANマッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである[トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）]を編集し、[接続の追跡時にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）]オプションを選択します。

ユーザールール条件

接続を開始したユーザー、またはユーザーが属するグループに基づいてトラフィックが照合されます。たとえば、財務グループの全員がネットワークリソースにアクセスすることを禁止するブロックルールを設定できます。

Microsoft Active Directoryレルムのユーザーに対してのみユーザー ルール条件を設定できます。

設定されたレルムのユーザーとグループの設定に加えて、次の特殊なアイデンティティユーザーのポリシーを設定できます。

- [失敗した認証（Failed Authentication）]：キャプティブポータルでの認証に失敗したユーザー。
- [ゲスト（Guest）]：キャプティブポータルでゲストユーザーとして設定されたユーザー。
- [認証不要（No Authentication Required）]：アイデンティティの[認証不要（No Authentication Required）]ルールアクションに一致するユーザー。
- [不明（Unknown）]：識別できないユーザー。たとえば、設定されたレルムによってダウンロードされていないユーザー。

アクセス制御ルールのみの場合、IDポリシーをアクセス コントロール ポリシーに最初に関連付ける必要があります（アクセス制御への他のポリシーの関連付け（1765ページ）を参照）。

アプリケーションルール条件

システムはIPトラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザー定義の再利用可能フィルタを作成できます。

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザー定義ディテクタが有効になります。アプリケーション ディテクタの詳細については、アプリケーション ディテクタの基本 （2633 ページ）を参照してください。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

アプリケーション フィルタの利点

アプリケーション フィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザーがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーション フィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーション トラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーション トラフィックは常に最新のディテクタによってモニターされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *85*：アプリケーションの特性

特性	説明	例
タイプ	アプリケーション プロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲーム アプリケーションはビジネスとの関連性が極めて低いと見なされます。

特性	説明	例
カテゴリ	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも1つのカテゴリに属します。	Facebookはソーシャル ネットワーキングのカテゴリに含まれます。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオ ストリーミング Web アプリケーションには、ほとんどの場合、`high bandwidth` と `displays ads` というタグが付けられます。

関連トピック

アプリケーション制御の設定のベストプラクティス （1732 ページ）

アプリケーション条件とフィルタの設定

アプリケーションの条件またはフィルタを作成するには、使用可能なアプリケーションのリストから、トラフィックを制御するアプリケーションを選択します。オプションとして（推奨）、フィルタを使用して使用可能なアプリケーションを抑制します。フィルタと個別に指定されたアプリケーションを同じ条件で使用できます。

始める前に

- アクセス コントロール ルールでアプリケーション制御を実行するためには、適応型プロファイルの設定 （2937ページ） で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする必要があります。

手順

ステップ 1 ルール エディタまたは設定エディタを起動します。

- アクセスコントロール、暗号解読、QoS ルール条件：ルールエディタで [アプリケーション（Applications）] をクリックします。
- アイデンティティルール条件：ルールエディタで [レルムおよび設定（Realms & Settings）] をクリックし、アクティブ認証を有効にします。アイデンティティ ルールの作成 （2565ページ） を参照してください。
- アプリケーション フィルタ：オブジェクト マネージャの [アプリケーション フィルタ（Application Filters）] ページで、アプリケーション フィルタを追加または編集します。フィルタの一意の**名前**を指定します。
- インテリジェント アプリケーション バイパス（IAB）：アクセス コントロール ポリシー エディタで [詳細（Advanced）] をクリックし、IAB の設定を編集して、[バイパス可能なアプリケーションおよびフィルタ（Bypassable Applications and Filters）] をクリックします。

ステップ 2 [使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

[使用可能なアプリケーション（Available Applications）] に表示されるアプリケーションを抑制するには、1つ以上の**アプリケーション フィルタ**を選択するか、個別のアプリケーションを検索します。

ヒント
サマリー情報とインターネットの検索リンクを表示するには、アプリケーションの横の **情報**（ ） をクリックします。**ロック解除** は、システムが復号されたトラフィックでのみ識別できるアプリケーションを示します。

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、ユーザー定義フィルタはできません。

- 同じ特性（リスク、ビジネス関連性など）の複数のフィルタ：アプリケーショントラフィックは1つのフィルタのみに一致する必要があります。たとえば、中リスク フィルタと高リスク フィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストにすべての中リスク アプリケーションと高リスク アプリケーションが表示されます。
- 異なるアプリケーション特性のフィルタ：アプリケーショントラフィックは、両方のフィルタ タイプに一致する必要があります。たとえば、高リスク フィルタとビジネスとの関連性が低いフィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストに両方の条件を満たすアプリケーションのみが表示されます。

ステップ 3 [アプリケーションの追加（Add Application）] または [ルールに追加（Add to Rule）] をクリックするか、ドラッグアンドドロップします。

ヒント
フィルタとアプリケーションをさらに追加する前に、[フィルタのクリア（Clear Filters）] をクリックして現在の選択をクリアします。

ステップ 4 ルールまたは設定を保存するか、編集を続けます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ポート、プロトコル、および ICMP コードルールの条件

ポート条件により、送信元ポートと宛先ポートに基づいてトラフィックが照合されます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP と UDP のトラフィックは、ポートに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- プロトコル：ポートを使用しないその他のプロトコルを使用してトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーションフィルタリング基準を使用してトラフィックをターゲット指定します。なお、プレフィルタルールではアプリケーション フィルタリングを使用できません。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTP など）にも推奨されます。ポートベースのアクセス コントロールルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP と DNS over UDP の両方を 1 つのアクセスコントロールルールの宛先ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

ポートベースではないプロトコルを照合できます。デフォルトでは、ポート条件を指定しない場合は IP トラフィックを照合します。非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：クラシック デバイスの場合、GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して

すべてのトラフィックを照合します。Firewall Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。

- 復号ルール：これらのルールは TCP ポート条件のみをサポートします。
- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

URL ルール条件

URL 条件を使用してネットワークのユーザーがアクセスできる Web サイトを制御します。

詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについて（1816 ページ）を参照してください。

ダイナミック属性のルール条件

ダイナミック属性には次のものがあります。

- ダイナミックオブジェクト（Cisco Secure 動的属性コネクタ からのものなど）

  動的属性コネクタ では、クラウドプロバイダーからデータ（ネットワークや IP アドレスなど）を収集し、それを Firepower Management Center に送信して、アクセスコントロールルールで使用できるようにします。。

- SGT オブジェクト
- ロケーション IP オブジェクト
- デバイスタイプオブジェクト
- エンドポイント プロファイル オブジェクト

ダイナミック属性は、アクセスコントロールルールの送信元基準および接続先基準として使用できます。次の注意事項に従ってください。

- 異なるタイプのオブジェクトは AND 結合される
- 同様のタイプのオブジェクトは OR 結合される

たとえば、送信元と宛先の基準 SGT 1、SGT 2、およびデバイスタイプ 1 を選択した場合、デバイスタイプ 1 が SGT 1 または SGT 2 で検出された場合、ルールが一致します。

API で作成したダイナミックオブジェクトについて

ダイナミックオブジェクトは、REST API コールを使用するか、クラウドソースから IP アドレスを更新できる Cisco Secure 動的属性コネクタ を使用して取得した 1 つまたは複数の IP アドレスを指定するオブジェクトです。これらのダイナミック オブジェクトは、オブジェクトへの動的な変更を展開しなくても、アクセス制御ルールで使用できます。

動的属性コネクタ の詳細については、『*Cisco Secure Dynamic Attributes Configuration Guide*』（ガイドへのリンク）を参照してください。https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/200/cisco-secure-dynamic-attributes-connector-v200.html

ダイナミックオブジェクトとネットワークオブジェクトの違いは次のとおりです。

- 動的属性コネクタを使用して作成したダイナミックオブジェクトは、作成されるとすぐに Firewall Management Center にプッシュされ、定期的に更新されます。
- API によって作成されたダイナミックオブジェクト：
  - Classless Inter-Domain Routing（CIDR）の有無にかかわらず、ネットワークオブジェクト同様にアクセスコントロールルールで使用できる IP アドレス。
  - 完全修飾ドメイン名またはアドレス範囲をサポートしていません。
  - API を使用して更新する必要があります。

関連トピック

API で作成したダイナミックオブジェクトの追加または編集 （1336 ページ）

ダイナミック属性の条件の設定

アクセス制御ルールにダイナミック属性を設定すると、同じタイプのオブジェクトは OR 結合され、異なるタイプのオブジェクトは AND 結合されます。このトピックの最後に例を示します。

始める前に

複数の動的オブジェクトを作成し、アクセス コントロール ポリシーでの動的オブジェクトの使用方法を理解します。

動的オブジェクトの詳細については、API で作成したダイナミックオブジェクトについて （1336 ページ）を参照してください。

アクセスコントロールポリシーでのダイナミックオブジェクトの詳しい使用方法については、ダイナミック属性のルール条件 （1798 ページ）を参照してください。

手順

ステップ 1 ルールエディタで [Dynamic Attributes] をクリックします。

ステップ 2 [Available Attributes] セクションで、次のいずれかを実行します。

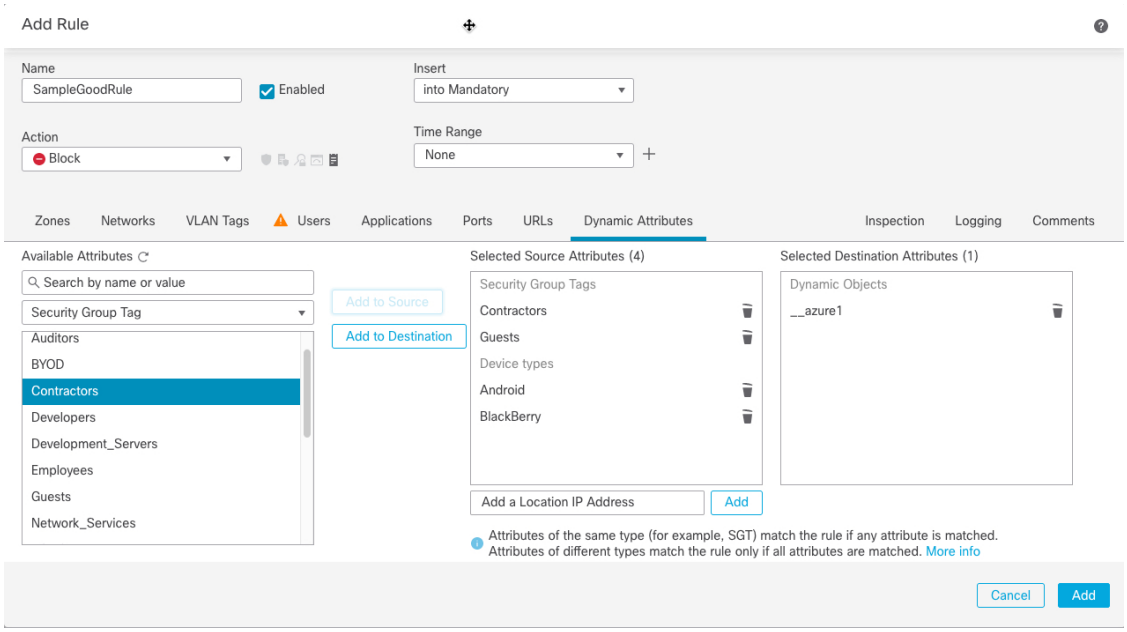
- フィールドに属性の名前の一部またはすべてを入力します。
- [Security Group Tag] または [Dynamic Objects] をクリックして、そのタイプのオブジェクトのみを表示します。

ステップ 3 選択したオブジェクトを適用するには、必要に応じて、[送信元（Sources）]フィールドまたは[宛先とアプリケーション（Destinations and Applications）]フィールドのいずれかで[追加（Add）]（＋）をクリックします。

ステップ 4 ルールの設定を終了したら、[Save] をクリックします。

例：ブロックルールでの複数の送信元条件の使用

次の例では、セキュリティグループタグの契約業者またはゲストからのトラフィックがブロックされ、デバイスタイプ Android または Blackberry が動的オブジェクト **__azure1** にアクセスできなくなります。



次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

時間と日のルール条件

連続する時間範囲または定期的な期間を指定できます。

たとえば、平日の勤務時間、週末、または休日のシャットダウン期間中にのみルールを適用できます。

時間ベースのルールは、トラフィックを処理するデバイスの現地時間に基づいて適用されます。

時間ベースのルールは、FTDデバイスでのみサポートされます。時間ベースのルールを含むポリシーを別のタイプのデバイスに割り当てると、ルールに関連付けられた時間制限はそのデバイスでは無視されます。この場合、警告が表示されます。

アクセス コントロール ルールの有効化と無効化

アクセスコントロールルールを作成すると、そのルールはデフォルトで有効になります。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。アクセス コントロール ポリシーのルール リストを表示したときに、無効なルールはグレー表示されますが、変更は可能です。

また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、ルールを右クリックし、ルールの状態を選択します。

代わりに [表示（View）]（） がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセス コントロール ポリシー間でのアクセス コントロール ルールのコピー

あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。ルールは、アクセスコントロールポリシーの [デフォルト（Default）] セクションまたは [必須（Mandatory）] セクションにコピーできます。

コメントを除く、コピーしたルールのすべての設定は、貼り付けたバージョンに保持されます。

手順

ステップ 1 次のいずれかを実行します。

- 単一のルールをコピーするには、ルールを右クリックし、[別のポリシーにコピー（Copy to Different Policy）] を選択します。
- 複数のルールをコピーするには、それらのチェックボックスをオンにして、[一括アクションの選択（Select Bulk Action）] メニューから [別のポリシーにコピー（Copy to Different Policy）] を選択します。

ステップ 2 [アクセスポリシー（Access Policy）] ドロップダウンリストから宛先アクセス コントロール ポリシーを選択します。

ステップ 3 [ルールの配置（Place Rules）] ドロップダウンリストから、コピーしたルールを配置する場所を選択します。それらは、[必須（Mandatory）] セクションまたは [デフォルト（Default）] セクションのいずれかの下部に配置できます。

ステップ 4 **[コピー（Copy）]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセスコントロールルールのプレフィルタポリシーへの移動

アクセス コントロール ポリシーから関連するデフォルト以外のプレフィルタポリシーにアクセス制御ルールを移動できます。

まず、ユーザー定義のプレフィルタポリシーをアクセス コントロール ポリシーに適用する必要があります。デフォルトのプレフィルタポリシーにはルールを設定できないため、デフォルトのプレフィルタポリシーにはアクセス制御ルールを移動できません。

始める前に

続行する前に、次の条件に注意してください。

- アクセスコントロールルールをプレフィルタポリシーに移動する場合、アクセスコントロールルールのレイヤ7（L7）パラメータは移動できません。L7パラメータは、操作中に削除されます。
- ルールを移動すると、アクセス コントロール ルール構成のコメントが失われます。ただし、ソースアクセスコントロールポリシーに言及する新しいコメントがコピーされたルールに追加されます。
- [アクション（Action）]パラメータとして[モニター（Monitor）]セットを使用してアクセスコントロールルールを移動することはできません。
- アクセスコントロールルールの [アクション（Action）]パラメータは、移動時にプレフィルタルールの適切なアクションに変更されます。アクセスコントロールルールの各アクションが何にマップされるかを知るには、次の表を参照してください。

アクセスコントロールルールのアクション	プレフィルタルールのアクション
許可（Allow）	分析（Analyze）
Block	Block
Block with reset	ブロック（Block）
インタラクティブブロック（Interactive Block）	ブロック（Block）
リセット付きインタラクティブ ブロック（Interactive Block with reset）	ブロック（Block）
信頼（Trust）	高速パス（Fastpath）

- 同様に、次の表に示すように、アクセスコントロールルールで構成されたアクションに基づいて、ルールの移動後にロギング構成が適切な設定になります。

アクセスコントロールルールのアクション	プレフィルタルールの有効なロギング構成
許可（Allow）	どのチェックボックスもチェックされていません。
ブロック（Block）	• 接続開始時にロギング（Log at Beginning of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ
リセットしてブロック（Block with reset）	• 接続開始時にロギング（Log at Beginning of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ
インタラクティブ ブロック	• 接続開始時にロギング（Log at Beginning of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ

アクセスコントロールルールのアクション	プレフィルタルールの有効なロギング構成
リセット付きインタラクティブ ブロック	• 接続開始時にロギング（Log at Beginning of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ
[信頼（Trust）]	• 接続開始時にロギング（Log at Beginning of Connection） • 接続終了時にロギング（Log at End of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ

- ソースポリシーからルールを移動しているときに、別のユーザーがそれらのルールを変更すると、メッセージが表示されます。ページを更新した後、プロセスを続行できます。

手順

ステップ 1 次のいずれかを実行します。

- 単一のルールを移動するには、ルールを右クリックし、[プレフィルタポリシーに移動（Move to Prefilter Policy）] を選択します。
- 複数のルールを移動するには、各ルールのチェックボックスをオンにし、[一括アクションの選択（Select Bulk Action）] メニューから [プレフィルタポリシーに移動（Move to Prefilter Policy）] を選択します。

ステップ 2 [ルールの配置（Place Rules）] ドロップダウンリストから、移動したルールを配置する場所を選択します。

- ルールの最後のセットとして配置するには、[最下部に配置（At the bottom）] を選択します。
- ルールの最初のセットとして配置するには、[最上部に配置（At the top）] を選択します。

ステップ 3 [移動（Move）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセス コントロール ルールの配置

既存のルールをアクセス コントロール ポリシー内で移動したり、新しいルールを目的の場所に挿入することができます。カテゴリにルールを追加または移動すると、そのルールはシステムによってカテゴリの最後に配置されます。

始める前に

アクセス制御ルールのベストプラクティス （1736 ページ） でルールの順序のガイドラインを確認してください。

手順

ステップ 1 次のいずれかを実行します。

- 新しいルール：既存のルール間の線にマウスのカーソルを合わせ、[ルールの追加（Add Rule）]をクリックして、新しいルールを挿入します。場所は、[ルールの追加（Add Rule）] ダイアログボックスの [挿入（Insert）] ボックスで選択されています。別のルールを選択して位置を調整することができます。右クリックメニューから [上にルールを追加（Add Rule Above）] または [下にルールを追加（Add Rule Below）] を選択することもできます。
- ルールテーブルを表示する場合の既存のルール：ルールをクリックして、新しい位置にドラッグします。
- ルールテーブルを表示している場合の既存のルール：1 つのルールを右クリックし、[ルールの再配置（Reposition Rule）] を選択します。複数のルールを 1 つのグループとして移動するには、各ルールのチェックボックスをオンにし、[一括アクションの選択（Select Bulk Action）] メニューから [ルールの再配置（Reposition Rules）] を選択します。
- ルールを編集している場合の既存のルール：ルール名の横にある [ルールの再配置（Reposition Rule）] アイコンをクリックします。

ステップ 2 ルールを移動またはルールを挿入する場所を選択します。

- [必須に挿入（into Mandatory）] または [デフォルトに挿入（into Default）] を選択します。
- [カテゴリに挿入（into Category）] を選択して、カテゴリを選択します。
- [ルールの上（above rule）] または [ルールの下（below rule）] を選択し、ルールを選択します。

ステップ 3 ルールを編集している場合は、[移動（Move）] または [確認（Confirm）] をクリックし、ルールを保存します。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセス制御ルールへのコメントの追加

アクセス コントロール ルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

アクセス コントロール ルールのコメントを検索するには、ルール一覧表示ページの [ルールの検索（Search Rules）] バーを使用します。

手順

ステップ 1 アクセス コントロール ルール エディタで、[コメント（Comments）] をクリックします。

ステップ 2 コメントを入力し、[コメントの追加（Add Comment）] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 3 ルールを保存します。

アクセスコントロールルールの例

次のトピックで、アクセスコントロールルールの例を示します。

セキュリティゾーンを使用したアクセスの制御方法

たとえば、ホストがインターネットに無制限でアクセスできるような導入にする一方、着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したいとします。

それにはまず、内部ゾーンと外部ゾーンという 2 つのセキュリティ ゾーンを作成します。次に、これらのゾーンに 1 つ以上のデバイス上のインターフェイス ペアを割り当て、各ペアの一方のインターフェイスを内部ゾーンに割り当て、もう一方のインターフェイスを外部ゾーンに割り当てます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

（注） 内部（または外部）のすべてのインターフェイスを1つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。

次に、宛先ゾーン条件を内部に設定したアクセス コントロール ルールを構成します。この単純なルールでは、内部ゾーンのいずれかのインターフェイスでデバイスから出力されるトラフィックが照合されます。一致するトラフィックを侵入やマルウェアについて検査するには、ルール アクションとして [許可（Allow）] を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。

アプリケーションの使用を制御する方法

ブラウザ ベースのアプリケーション プラットフォームか、企業ネットワークの内部および外部で転送として Web プロトコルを使用するリッチ メディア アプリケーションかにかかわらず、Web は企業内でアプリケーションを配信するユビキタス プラットフォームになっています。

Firewall Threat Defense は接続を検査し、使用されているアプリケーションを判別します。これにより、特定の TCP/UDP ポートを対象とするだけではなく、アプリケーションを対象としたアクセス制御ルールを記述することが可能になります。したがって、複数の Web ベース アプリケーションが同じポートを使用する場合でも、それらを選択的にブロックまたは許可できます。

特定のアプリケーションを選択して許可またはブロックできることに加えて、種類、カテゴリ、タグ、リスク、ビジネスとの関連性などに基づきルールを記述することもできます。たとえば、リスクが高くビジネス関連性が低いすべてのアプリケーションを識別してブロックするアクセス制御ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

シスコは、システムや脆弱性データベース（VDB）の更新プログラムにより、追加のアプリケーション検出機能を頻繁に更新および追加しています。これにより、リスクの高いアプリケーションをブロックするルールが新しいアプリケーションに自動的に適用され、手動でルールを更新する必要がなくなります。

この使用例では、[アノニマイザー/プロキシ（anonymizer/proxy）] カテゴリに属するアプリケーションをブロックします。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択し、アクセス コントロール ポリシーを編集します。

ステップ 2 [ルールの追加（Add Rule）] をクリックし、アプリケーション制御のルールを設定します。

a) ルールに意味のある名前を付けます（Block_Anonymizers など）。

b) [アクション（Action）] で [ブロック（Block）] を選択します。

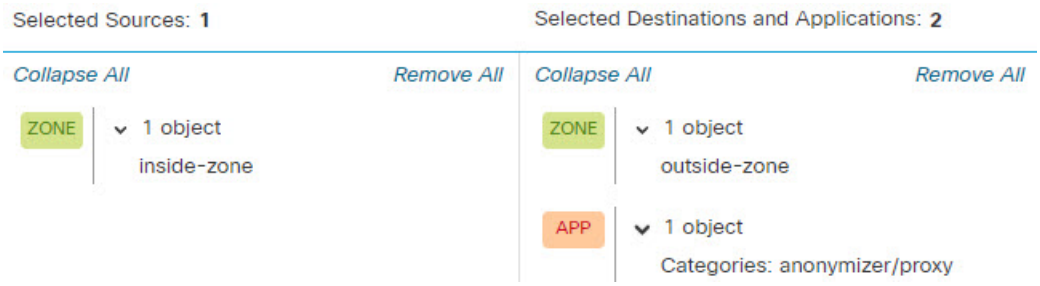
c) ゾーンが設定されており、このルールを内部から外部へのトラフィックに適用する場合は、[ゾーン（Zones）] タブを選択して、内部ゾーンを送信元ゾーンとして選択し、外部ゾーンを宛先ゾーンとして選択します。

d) [アプリケーション（Applications）] タブをクリックし、照合するアプリケーションを選択して、[アプリケーションの追加（Add Application）] をクリックします。

カテゴリやリスクレベルなどの基準を選択すると、基準の右側にあるリストが更新され、基準に一致するアプリケーションが正確に表示されます。記述したルールは、これらのアプリケーションに適用されます。

このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、TFPT は非常に高リスクに分類されています。ほとんどの組織は、このアプリケーションをブロックすることを希望しません。さまざまなフィルタ条件を試して、選択に一致するアプリケーションを確認するには時間がかかります。これらのリストは VDB の更新で変更できることを覚えておいてください。

この例では、[カテゴリ（Categories）] リストからアノニマイザー/プロキシを選択し、[宛先とアプリケーション（Destinations and Applications）] に追加します。一致基準は次の図のようなものになります。



e) ルールアクションの横にある [ロギング（Logging）] をクリックし、接続開始時のロギングを有効にします。syslog サーバーを使用している場合は、そのサーバーを選択できます。

このルールによってブロックされる接続の情報を取得するには、ロギングを有効化する必要があります。

（注）
パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

ステップ 3 このルールを、プロトコルとポートの基準のみを使用するルール（ただし、アプリケーションルールによってブロックされる必要があるトラフィックを許可しないルール）の後に移動します。

アプリケーションの照合にはSnort検査が必要です。プロトコルとポートのみを使用するルールではSnort検査が必要ないため、これらの単純なルールをアクセス コントロール ポリシーの最上位にグループ化することで、システムパフォーマンスを向上させることができます。

ステップ4 変更を展開します。

アプリケーションルールのヒット数および分析ダッシュボードを使用して、このルールのパフォーマンスと、ユーザーがこれらのアプリケーションを試用する頻度を確認できます。

脅威のブロック方法

侵入ポリシーをアクセス コントロール ルールに追加することによって、次世代侵入防御システム（IPS）のフィルタリングを実装できます。侵入ポリシーはネットワーク トラフィックを分析し、トラフィック コンテンツを既知の脅威と比較します。いずれかの接続が監視対象の脅威と一致する場合、システムはその接続をドロップし、こうして攻撃を防止できます。

ネットワーク トラフィックに対して侵入検査を行う前に、他のすべてのトラフィック処理が行われます。侵入ポリシーをアクセス制御ルールに関連付けると、アクセス制御ルールの条件に一致するトラフィックをシステムが通過させる前に、侵入ポリシーを使ってまずトラフィックを検査するようシステムに指示できます。

単にトラフィックを許可するルール上で侵入ポリシーを設定できます。インスペクションは、トラフィックを [信頼（trust）] または [ブロック（block）] するよう設定されたルールでは実行されません。さらに、単純なブロックを使用しない場合は、デフォルトアクションとして侵入ポリシーを設定できます。

潜在的な侵入を許可するトラフィックの検査に加え、セキュリティ インテリジェンス ポリシーを使用することで、既知の不正IPアドレスとのすべてのトラフィック、または既知の不正URLへのすべてのトラフィックを先制的にブロックできます。

この例では、内部の 192.168.1.0/24 ネットワークの外部への侵入を許可する侵入ポリシーを追加し、プリエンプティブブロックを実行するセキュリティ インテリジェンス ポリシーを追加しながら、不要な接続を選択的に排除するブロックルールがすでにあることを前提としています。

始める前に

このルールを使用するすべての管理対象デバイスに IPS ライセンスを適用する必要があります。

この例では、内部および外部インターフェイスのセキュリティゾーン、および内部ネットワークのネットワークオブジェクトがすでに作成されていることを前提としています。

手順

ステップ1 侵入ポリシーを適用するアクセス制御ルールを作成します。

a) アクセス コントロール ポリシーの編集時に、[ルールの追加（Add Rule）] をクリックします。

b) ルールに Inside_Outside などのわかりやすい名前を付け、ルールアクションが [許可（Allow）] であることを確認します。

c) [侵入ポリシー（Intrusion policy）] で、[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] を選択します。デフォルトの変数セットを受け入れるか、独自の変数セットを選択してカスタマイズできます。

ほとんどのネットワークでは、[バランスのとれたセキュリティと接続（Balanced Security and Connectivity）] ポリシーが適しています。このポリシーは適度な侵入保護を提供し、過剰にアグレッシブ（ドロップすべきでないトラフィックがドロップされる可能性がある）でもありません。ドロップされるトラフィックが多すぎる場合は、[セキュリティを上回る接続性（Connectivity over Security）] ポリシーを選択することにより、侵入検査を緩和できます。

アグレッシブなセキュリティが必要な場合は、[接続性を上回るセキュリティ（Security over Connectivity）] ポリシーを試してください。[最大検出（Maximum Detection）] ポリシーでは、ネットワーク インフラストラクチャのセキュリティがよりいっそう重視され、動作にさらに大きな影響を及ぼす可能性があります。

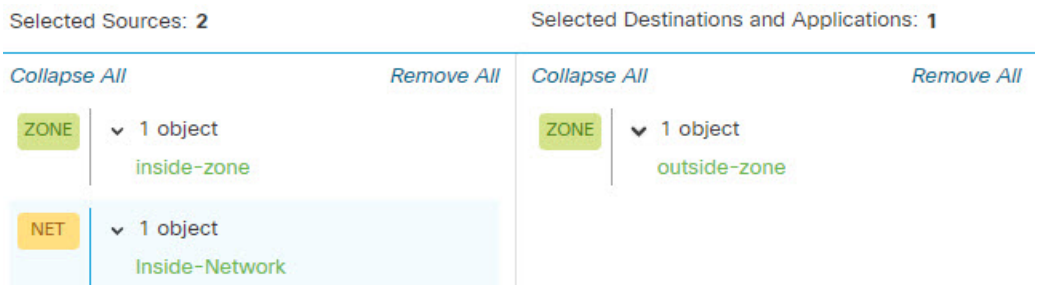
独自のカスタムポリシーを作成する場合は、代わりにそのカスタムポリシーを選択できます。

変数セットの説明は、この例の範囲外です。変数セットとカスタムポリシーの詳細については、侵入ポリシーに関する章をお読みください。

d) [ゾーン（Zones）] タブを選択し、内部セキュリティゾーンを送信元基準に追加し、外部ゾーンを宛先基準に追加します。

e) [ネットワーク（Networks）] タブを選択し、内部ネットワークを定義するネットワークオブジェクトを送信元基準に追加します。

一致基準は次のようになります。



f) [ロギング（Logging）] をクリックし、必要に応じて、接続の開始時または終了時、またはその両方でロギングを有効にします。

g) [適用（Apply）] をクリックしてルールを保存し、[保存（Save）] をクリックして更新されたポリシーを保存します。
h) ルールをアクセス コントロール ポリシーの適切な場所に移動します。

ステップ 2 既知の不正ホストやサイトとの接続を先制的にドロップするためのセキュリティ インテリジェンス ポリシーを設定します。

セキュリティ インテリジェンスを使用して、脅威だとわかっているホストやサイトとの接続をブロックすることで、接続ごとに脅威を特定するためのディープ パケット インスペクションに必要な時間を節約できます。セキュリティ インテリジェンスにより、不必要なトラフィックを早期にブロックして、実際に関心があるトラフィックの処理により多くのシステム時間を残すことができます。

a) アクセス コントロール ポリシーの編集時に、パケットパスで [セキュリティ インテリジェンス（Security Intelligence）] リンクをクリックします。

リンクには、上部の DNS ポリシーと下部のセキュリティ インテリジェンス（ネットワークと URL）の 2 つのポリシーが含まれています。この例では、ネットワークリストと URL リストを設定しています。デフォルトでは、これらのリストにはすでにグローバルブロックリストとブロックしないリストが含まれています。各リストは、項目を追加するまでデフォルトでは空です。

b) [ネットワーク（Networks）] を選択し、セキュリティゾーンの [任意（Any）] を選択した状態で、グローバルリストと最初のセキュリティ インテリジェンス カテゴリ（おそらく [攻撃者（Attackers）]）が表示されるまで、リストを下にスクロールします。[攻撃者（Attackers）] をクリックし、カテゴリ（おそらく Tor_exit_node）の最後までスクロールし、Shift キーを押した状態でクリックしてすべてのカテゴリを選択します。[ブロックリストに追加（Add to Block List）] をクリックします。
c) [URL] タブとセキュリティゾーンの [任意（Any）] を選択し、Shift キーを押した状態でクリックして同じカテゴリの URL バージョンを選択します。[ブロックリストに追加（Add to Block List）] をクリックします。
d) [保存（Save）] をクリックしてポリシーを保存します。
e) 必要に応じて、ネットワークおよび URL オブジェクトをブロックリストまたはブロックしないリストに追加できます。

[ブロックしない（Do Not Block）] リストは、ホワイトリストではなく、例外リストです。例外リストにあるアドレスや URL がブロックリストにも表示されている場合、そのアドレスや URL の接続はアクセス制御ポリシーの通過を許可されます。フィードはこのようにしてブロックできますが、後で必要なアドレスやサイトがブロックされていることに気付いた場合は、例外リストを使用して、フィードを完全に削除することなく、そのブロックをオーバーライドできます。その後、それらの接続はアクセス制御、および侵入ポリシー（設定されている場合）によって評価される点に注意してください。したがって、接続に脅威が含まれている場合は、侵入検査中に特定されてブロックされます。

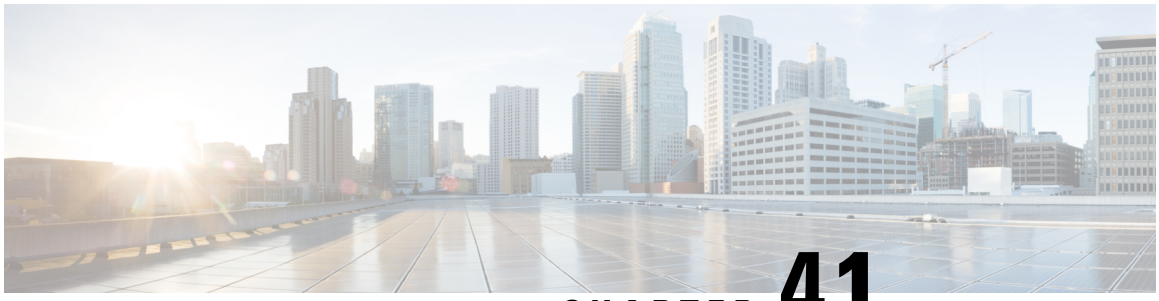
イベントおよびダッシュボードを使用して、ポリシーによって実際にドロップされているトラフィックを特定し、[ブロックしない（Do Not Block）] リストにアドレスや URL を追加する必要があるかどうかを決めます。

ステップ 3 変更を展開します。

アクセス制御ルールの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
アクセス制御ルールごとの一致基準の最大オブジェクト数は 200 です。	7.3	任意（Any）	以前は、1 つのアクセス制御ルールの一致基準ごとに最大 50 個のオブジェクトを含めることができました。たとえば、1 つのアクセス制御ルールに最大 50 のネットワークオブジェクトを含めることができます。制限数は、1 つのルールの一致基準ごとに 200 オブジェクトになりました。 増加したオブジェクト制限を許可するようにアクセス コントロール ポリシーを更新しました。
アクセス制御ルールのコメントの検索	6.7	いずれか	[検索ルール（Search Rules）] バーに、コメントを検索するオプションが追加されました。 新規/変更されたページ：アクセス制御ルールのページ、[検索ルール（Search Rules）] テキスト入力フィールド。 サポートされているプラットフォーム： Firewall Management Center
アクセス コントロール ポリシーとプレフィルタ ポリシー間のルールのコピーまたは移動	6.7	いずれか	あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。また、アクセス制御ルールをアクセス コントロール ポリシーから関連するプレフィルタ ポリシーに移動できます。 新規/変更されたページ：アクセス コントロール ポリシーのページ。選択したルールの右クリック メニューに、コピーおよび移動するための追加オプションがあります。 サポートされているプラットフォーム： Firewall Management Center
アクセス制御ルールの特定の設定の一括編集	6.6	任意（Any）	ポリシー内のルールのリストで、Shift キーまたは Ctrl キーを押したままクリックして複数のルールを選択し、右クリックしてオプションを選択します。一括操作の例：ルールを有効または無効にしたり、ルールアクションを選択したり、ほとんどの検査とロギングの設定を編集したりできます。 新規/変更されたページ：アクセス制御ルールのページ。 サポートされているプラットフォーム： Firewall Management Center

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
設定されたルールの強化された検索	6.6	任意（Any）	設定されたルールの強化された検索。 新規/変更されたページ：アクセス制御ルールのページ。 サポートされているプラットフォーム： Firewall Management Center
ルール適用の時間範囲	6.6	任意（Any）	適用するルールの絶対時間または反復時間、あるいは時間範囲を指定する機能。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。 新規/変更されたページ： • アクセス制御の [ルールの追加（Add Rule）] ページの新しいオプション。 • [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense] ページにある管理対象デバイスのタイムゾーンの指定に関連する新しいオプション。 サポートされているプラットフォーム：Firewall Threat Defense デバイスのみ
アクセス制御ルールページからのオブジェクトの詳細の表示	6.6 以前	任意（Any）	ルールのリストまたはルール設定ダイアログからオブジェクトに関する情報を表示するには、オブジェクトを右クリックします。 新規/変更されたページ：[ポリシー（Policies）]>[アクセス制御（Access Control）] > [アクセス制御（Access Control）]、および [ルールの追加（Add Rule）] ページ。 サポートされているプラットフォーム： Firewall Management Center



CHAPTER 41

URL フィルタリング

アクセスコントロールルールを使用して URL フィルタリングを実行できます。

- URL フィルタリングの概要 （1815 ページ）
- URL フィルタリングのベスト プラクティス （1818 ページ）
- URL フィルタリングのライセンス要件 （1824 ページ）
- URL フィルタリングの要件と前提条件 （1825 ページ）
- カテゴリとレピュテーションを使用した URL フィルタリングの設定方法 （1825 ページ）
- 手動 URL フィルタリング （1833 ページ）
- HTTP 応答ページの設定 （1836 ページ）
- URL フィルタリングのヘルス モニターの設定 （1841 ページ）
- URL カテゴリとレピュテーションの異議申し立て （1841 ページ）
- URL カテゴリセットが変更された場合、アクションを実行 （1842 ページ）
- URL フィルタリングのトラブルシューティング （1844 ページ）
- URL フィルタリングの履歴 （1848 ページ）

URL フィルタリングの概要

URL フィルタリング機能を使用してネットワークのユーザーがアクセスできる Web サイトを制御します。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリング ライセンスでは、URL の一般的な分類（カテゴリ）とリスク レベル（レピュテーション）に基づいて Web サイトへのアクセスを制御することができます。これは推奨オプションです。
- 手動 URL フィルタリング：任意のライセンスで、個々の URL、URL のグループおよび URL リストとフィードを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。詳細については、手動URLフィルタリング （1833ページ）を参照してください。

セキュリティインテリジェンス（1851ページ）も参照してください。悪意のあるURL、ドメイン、およびIP アドレスをブロックするための類似した別の機能です。

URL フィルタリング機能は、Web ブラウザを使用して HTTP/HTTPS プロトコル経由で Web サイトを参照する場合にのみ適用されます。他のアプリケーションでは、URL フィルタリングの代わりに FQDN ベースのアクセスコントロールルールを使用する必要があります。詳細については、「アクセス コントロール ルール」を参照してください。

カテゴリおよびレピュテーションによる URL のフィルタリングについて

URL フィルタリング ライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職カテゴリに属します。

  URL は、複数のカテゴリに属することができます。

- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションの範囲は、[不明なリスク（Unknown Risk）]（レベル 0）または [信頼できない（Untrusted）]（レベル 1）から [信頼できる（Trusted）]（レベル 5）まであります。レピュテーションはホスト名によって決定されます。たとえば、www.cisco.com のすべてのページが同じレピュテーションであると見なされます。

カテゴリおよびレピュテーションベースの URL フィルタリングのメリット

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセス制御を使用すると、ハッキングカテゴリで信頼できない URL をブロックできます。または、QoS を使用すると、ストリーミングビデオ カテゴリのサイトからのトラフィックをレート制限できます。スパイウェアおよびアドウェア カテゴリなど、脅威のタイプのカテゴリもあります。

カテゴリおよびレピュテーションデータを使用すると、ポリシーの作成と管理がより簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。脅威インテリジェンスは、新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは最新の情報を使用して要求された URL をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザーが新しいポリシーを更新したり展開したりするペースを上回って次々と現れては消える可能性があります。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロール ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されてゲームに分類されると、これらのサイトをシステムで自動的にブロックできます。同様に、QoS ルールがすべてのストリーミングビデオサイトをレート制限する場合、システムは自動で新しいストリーミングビデオサイトにトラフィックを制限できます。

- アクセス コントロール ルールですべてのマルウェア サイトをブロックし、あるショッピング ページがマルウェアに感染すると、システムはその URL をショッピング サイトからマルウェア サイトに再分類して、そのサイトをブロックすることができます。
- アクセス制御ルールが信頼できないソーシャル ネットワーキング サイトをブロックし、誰かがプロファイルページに悪意のあるペイロードへのリンクが含まれるリンクを掲載した場合、システムはそのページのレピュテーションを [好ましい（Favorable）] から [信頼できない（Untrusted）] に変更し、それをブロックします。

復号ポリシーの[復号しない（Do Not Decrypt）]ルールのカテゴリベースのフィルタリングの制限

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。

（注） URL フィルタリングとアプリケーション検出を混同しないでください。アプリケーション検出は、Web サイトからのパケットの一部を読み取り、それが何であるか（Facebook メッセージや Salesforce など）をより具体的に判断することに依存します。詳細については、アプリケーション制御の設定のベストプラクティス （1732 ページ）を参照してください。

詳細については、「URL フィルタリングでのカテゴリの使用 （1823 ページ）」を参照してください。

URL カテゴリとレピュテーションの説明

カテゴリの説明

各 URL カテゴリの説明は https://www.talosintelligence.com/categories から入手できます。

これらのカテゴリを表示するには、[脅威カテゴリ（Threat Categories）] を必ずクリックしてください。

レピュテーション レベルの説明

[Web レピュテーション レベル（Web reputation levels）] に移動します。

Cisco Cloud からの URL フィルタリングのデータ

URL フィルタリングライセンスを追加すると、URLフィルタンリング機能が自動的に有効になり、Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。

デフォルトでは、以前にアクセスした Web サイトのローカルキャッシュにカテゴリとレピュテーションがない URL をユーザーが参照すると、その URL が脅威インテリジェンス評価のためにクラウドに送信され、結果がキャッシュに追加されます。

必要に応じて、カテゴリとレピュテーションのローカル URL データセットを使用して、Web ブラウジングを高速化できます。URL フィルタリングを有効にする（または再度有効にする）と、Firewall Management Center は URL データについてシスコに自動的にクエリを実行し、データセットを管理対象デバイスにプッシュします。次に、ユーザーが URL を参照すると、ローカルデータセットとキャッシュのカテゴリとレピュテーション情報は、システムにチェックされてから、脅威インテリジェンス評価のためにクラウドに送信されます。個々のクラウドルックアップを完全に無効にする方法など、ローカルデータセットを使用するためのオプションの詳細については、URL フィルタリング オプション （1827 ページ）を参照してください。

URL データの自動更新はデフォルトで有効になっています。自動更新を無効にしないことを強く推奨します。

URL カテゴリのセットは定期的に変更されることがあります。変更通知を受け取ったら、URL フィルタリング構成を見直して、トラフィックが期待どおりに処理されることを確認します。詳細については、URL カテゴリセットが変更された場合、アクションを実行 （1842 ページ）を参照してください。

URL フィルタリングのベスト プラクティス

URL フィルタリングに関する次のガイドラインと制限事項に注意してください。

カテゴリとレピュテーションによるフィルタリング

その場合は、カテゴリとレピュテーションを使用した URL フィルタリングの設定方法 （1825 ページ）の手順に従ってください。

URL を識別する前に通過する必要があるパケットを検査するポリシーの設定

システムは以下の動作の前に URL をフィルタリングできません。

- モニター対象の接続がクライアントとサーバーの間で確立される。
- システムによりセッションで DNS、HTTP または HTTPS アプリケーションが識別される。
- 要求されたドメインまたは URL がシステムにより識別される（暗号化されるセッションの場合、暗号化されていないドメイン名、ClientHello メッセージまたはサーバー証明書から）。

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、TLS/SSL ハンドシェイクのサーバー証明書交換の後に行われる必要があります。

重要システムが調べなければ通過するこれらの初期パケットをシステムが確実に調べるようにするには、トラフィック識別の前に通過するパケットのインスペクション （2746 ページ）およびサブトピックを参照してください。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、TLS/SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なルール アクションを適用します。

脅威カテゴリのブロック

ポリシーが既知の悪意のあるサイトを識別する脅威カテゴリに明確に対応していることを確認してください。レピュテーションの低いサイトをブロックすることに加えて、これを行います。

たとえば、悪意のあるサイトからネットワークを保護するには、すべての脅威カテゴリをブロックする必要があります。さらに、Talos は、カテゴリが「悪い」（Poor）のサイトのみをブロックすることを推奨しています。セキュリティ態勢が「アグレッシブ」（Aggressive）の場合は、レピュテーションが「疑わしい」（Questionable）のサイトをブロックできますが、それにより、誤検出が多くなる可能性があります。

詳細については、URL カテゴリとレピュテーションの説明（1817 ページ）の URL にある [脅威カテゴリ（Threat Categories）] を参照してください。

URL 条件とルールの順序

- ヒットする必要のある他のすべてのルールの後に URL ルールを配置します。
- URL は複数のカテゴリに属することができます。Web サイトの 1 つのカテゴリを許可し、別のカテゴリをブロックすることができます（明示的に行うか、デフォルト アクションに依存して）。この場合、許可またはブロックが優先されるかどうかに応じて、適切な効果が得られるように URL ルールを作成して順序付けしてください。

ルールに関するその他のガイドラインについては、アクセス制御ルールのベストプラクティス（1736 ページ） を参照してください。

未分類またはレピュテーションのない URL

URL ルールを作成するときは、まず一致させるカテゴリを選択します。[未分類（Uncategorized）] URL を明示的に選択した場合は、レピュテーションによりさらに制約を追加することはできません。

信頼できないレピュテーションの未分類 URL は、[悪意のあるサイト（Malicious Sites）] カテゴリによって処理されます。他のレピュテーション レベル（疑わしいなど）を使用する未分類サイトをブロックする場合は、すべての未分類サイトをブロックする必要があります。

カテゴリとレピュテーション レベルを選択した後に、必要に応じて [不明なレピュテーションに適用（Apply to unknown reputation）] を選択できます。たとえば、レピュテーションが信頼できない、疑わしい、および不明なサイトに適用されるルールを作成できます。

カテゴリとレピュテーションを URL に手動で割り当てることはできませんが、アクセス コントロール ポリシーと QoS ポリシーでは、特定の URL を手動でブロックできます。手動 URL フィルタリング（1833 ページ）を参照してください。URL カテゴリとレピュテーションの異議申し立て（1841 ページ）も参照してください。

暗号化された Web トラフィックの URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングを実行すると、システムは次のように動作します。

- （DNS フィルタリングが有効になっている場合）システムが送信元ドメインを認識済みかどうか、またはドメインがローカル レピュテーション データベースに存在するかどうかを確認します。この状態を確認できた場合は、ドメインのレピュテーションとカテゴリに基づいてアクションを実行します。確認できない場合、アクセス コントロール ポリシーの詳細設定で [Retry URL cache miss lookup] が有効になっていても、システムは暗号化トラフィック向けの設定に基づいてトラフィックを処理します。
- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件がない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- URL リストを使用しません。代わりに、URL オブジェクトとグループを使用する必要があります。
- トラフィックの暗号化に使用された公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合します。また、トランザクション中のどの時点で提示される他の URL（復号後の HTTP URL など）のレピュテーションも評価します。
- サブジェクト共通名内のサブドメインを無視します。
- アクセス制御ルール（または、その他の設定）によってブロックされている暗号化された接続の場合は HTTP 応答ページを表示しません。HTTP 応答ページの制限 （1836 ページ）を参照してください。

URL フィルタリングと TLS サーバーアイデンティティ検出

RFC 8446 で定義されている最新バージョンの Transport Layer Security（TLS）プロトコル 1.3 は、セキュアな通信を提供するために多くの Web サーバーで採用されているプロトコルです。TLS 1.3 プロトコルが、セキュリティを強化するためにサーバーの証明書を暗号化する一方で、証明書が、アクセスコントロールルールのアプリケーションおよび URL フィルタリング基準に適合する必要があるため、Firepower システムは、パケット全体を復号せずにサーバー証明書を抽出する方法を提供します。

アクセス コントロール ポリシーの詳細設定には、[TLS Server Identity Discovery] に [Early application detection and URL categorization] オプションがあり、アプリケーション検出と URL 分類が早期に実行されます。

この機能は、アプリケーションまたは URL の基準に適合させたいトラフィックに関して、特にそのトラフィックの詳細な検査を実行する必要がある場合に、有効にすることを強くお勧めします。サーバー証明書を抽出するプロセスでトラフィックが復号されないため、復号ポリシー は必要ありません。

（注）

- 証明書は復号されているため、ハードウェア プラットフォームによっては、TLS サーバー アイデンティティ検出によってパフォーマンスが低下する場合があります。
- TLS サーバーアイデンティティ検出は、インラインタップモードまたはパッシブモードの展開ではサポートされません。
- TLS サーバーアイデンティティ検出の有効化は、AWS に展開された Secure Firewall Threat Defense Virtual ではサポートされていません。Secure Firewall Management Center で管理されているそのような管理対象デバイスがある場合、接続イベント **PROBE_FLOW_DROP_BYPASS_PROXY** は、デバイスがサーバー証明書の抽出を試みるたびに増加します。
- TLS サーバーアイデンティティ検出は、TLS 1.2 セッションでも動作します。

詳細については、「アクセス コントロール ポリシーの詳細設定（1759 ページ）」を参照してください。

HTTP/2

システムは、TLS 証明書から HTTP/2 URL を抽出できますが、ペイロードから抽出することはできません。

手動 URL フィルタリング

- カスタム セキュリティ インテリジェンス リストまたはフィードオブジェクトを使用して URL を指定します。URL オブジェクトを使用したり、ルールに URL を直接入力したりしないでください。詳細は、手動URLフィルタリングオプション（1834 ページ）を参照してください。
- URL オブジェクトの使用やルールへの URL の直接入力によって、特定の URL を手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。ネットワークトラフィックがURL条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の任意の部分に一致する場合、URL は一致するとみなされます。
- 手動の URL フィルタリングを使用して他のルールの例外を作成する場合は、例外を含む特定のルールを、それらが適用されない場合に適用される一般的なルールの上に配置します。

URL での検索クエリ パラメータ

システムでは、URL 条件を照合する際、URL 内の検索クエリ パラメータは使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

高可用性展開での URL フィルタリング

高可用性での Firepower Management Center を使用した URL フィルタリングのガイドラインについては、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*URL Filtering and Security Intelligence*」を参照してください。

選択したデバイス モデルのメモリ制限

- メモリが不足しているデバイスモデルでは、ローカルで格納される URL データが減少します。したがって、システムはクラウドをより頻繁にチェックして、ローカルデータベースにないサイトのカテゴリとレピュテーションを判断します。

  低メモリ デバイスには、次のデバイスが含まれます。

  - Firepower 1010
  - 8 GB の RAM を搭載したFirewall Threat Defense Virtual

HTTPS トラフィックのフィルタリング

暗号化されたトラフィックをフィルタリングするには、システムは TLS/SSL ハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。

HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。アクセス コントロールまたは QoS ポリシーで HTTPS URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

ヒント　復号ポリシーでは、特定の URL に対するトラフィックの処理と復号は、識別名の復号ポリシールール条件を定義することで実行できます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。HTTPS トラフィックを復号化すると、アクセス制御ルールで復号化されたセッションを評価することができるため、URL フィルタリングが強化されます。

暗号化プロトコルによるトラフィックの制御

アクセス コントロールまたは QoS ポリシー内で URL フィルタリングを実行する場合、暗号化プロトコル（HTTP または HTTPS）は無視されます。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングでは、次の Web サイトへのトラフィックが同様に処理されます。

- http://example.com/
- https://example.com/

HTTP または HTTPS トラフィックとのみ一致するルールを設定するには、アプリケーション条件をルールに追加します。たとえば、それぞれ、アプリケーション条件と URL 条件を含む 2 つのアクセス制御ルールを作成することにより、サイトへの HTTPS アクセスを許可しながら、HTTP アクセスを禁止することができます。

最初のルールでは、Web サイトへの HTTPS トラフィックが許可されます。

アクション：許可
Application: HTTPS
URL: example.com

2 つ目のルールでは、同じ Web サイトへの HTTP アクセスがブロックされます。

Action: Block
Application: HTTP
URL: example.com

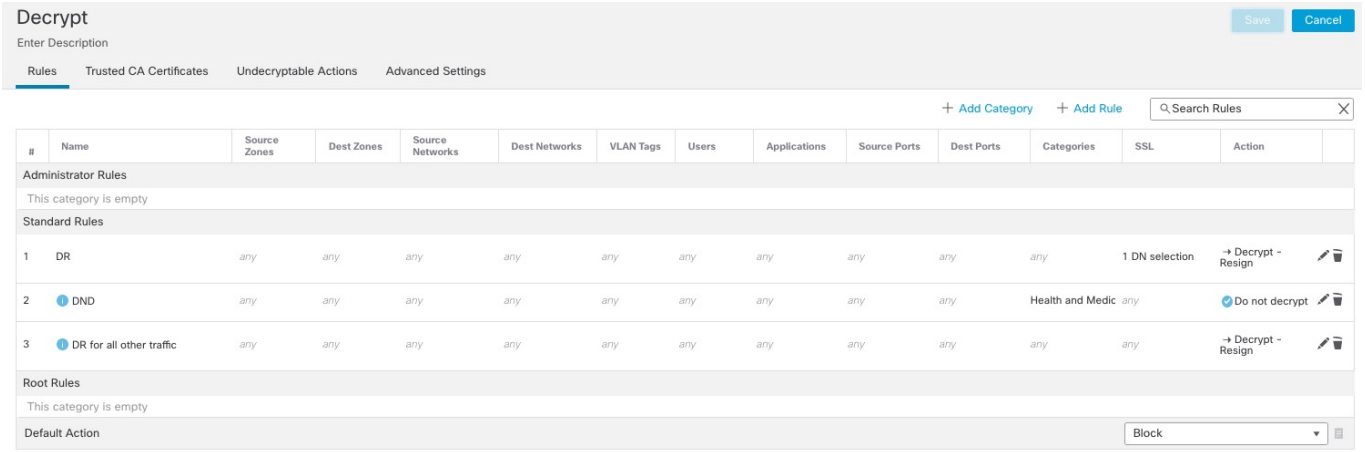
URL フィルタリングでのカテゴリの使用

[復号しない（Do Not Decrypt）] ルールのカテゴリの制限

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。シスコでは、URL フィルタリングカテゴリの継続的な更新と改善に努めていますが、厳密に科学的なものではありません。一部の Web サイトはまったく分類されておらず、一部の Web サイトは不適切に分類されている可能性があります。

理由のないトラフィックの復号を避けるために、[復号しない（Do Not Decrypt）] ルールのカテゴリを過度に使用しないでください。たとえば、[健康と薬（Health and Medicine）] カテゴリには、患者のプライバシーを脅かさない WebMD の Web サイトが含まれています。

以下は、[健康と薬（Health and Medicine）] カテゴリの Web サイトの復号を防ぐ一方で、WebMD およびその他すべての復号を許可することができるサンプル復号ポリシーです。復号ルールに関する一般的な情報については、TLS/SSL 復号の使用上のガイドライン（2351 ページ）を参照してください。



（注） URL フィルタリングとアプリケーション検出を混同しないでください。アプリケーション検出は、Web サイトからのパケットの一部を読み取り、それが何であるか（Facebook メッセージや Salesforce など）をより具体的に判断することに依存します。詳細については、アプリケーション制御の設定のベストプラクティス （1732 ページ）を参照してください。

URL フィルタリングのライセンス要件

Threat Defense ライセンス

- カテゴリとレピュテーション フィルタリング：URL フィルタリング
- 手動フィルタリング：追加のライセンスはありません。

従来のライセンス

- カテゴリとレピュテーション フィルタリング：URL フィルタリング
- 手動フィルタリング：追加のライセンスはありません。

Threat Defense デバイス用の URL フィルタリングライセンス

Cisco Secure Firewall Management Center アドミニストレーション ガイド [英語] の「Licenses」章の「URL Licenses」を参照してください。

URL フィルタリングの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

カテゴリとレピュテーションを使用した URL フィルタリングの設定方法

	操作手順	詳細情報
ステップ 1	正しいライセンスがあることを確認します。	URL フィルタリング ライセンスを URL をフィルタ処理する各管理対象デバイスに割り当てます。
ステップ 2	Firewall Management Center はクラウドと通信して URL フィルタリングデータを取得できることを確認します。	インターネット アクセス要件および通信ポートの要件（Cisco Secure Firewall Management Center アドミニストレーション ガイド）。
ステップ 3	制限事項とガイドラインを理解し、必要なアクションを実行します。	URL フィルタリングのベスト プラクティス （1818 ページ）
ステップ 4	URL フィルタリング機能を有効にします。	カテゴリとレピュテーションを使用した URL フィルタリングの有効化 （1827 ページ）

	操作手順	詳細情報
ステップ 5	カテゴリとレピュテーションによって URL をフィルタ処理するルールを設定します。	URL 条件の設定 （1829 ページ） 悪意のあるサイトに対する最高の保護を実現するには、レピュテーションによってサイトをブロックするとともに、すべての脅威カテゴリに含まれる URL をブロックする必要があります。 （オプション）カテゴリおよびレピュテーションベースの URL フィルタリングの補完または選択的オーバーライド （1835 ページ）
ステップ 6	（オプション）警告ページをクリック スルーすることで Web サイトのブロックをバイパスできるようにします。	HTTP 応答ページの設定 （1836 ページ）
ステップ 7	トラフィックがキー ルールに最初にヒットするようにルールを順序付けます。	URL ルールの順序 （1741 ページ）
ステップ 8	（オプション）URL フィルタリング関連の詳細オプションを変更します。	変更する特別な理由がない限り、通常はデフォルトを使用します。 次のオプションを含む詳細オプションについては、アクセス コントロール ポリシーの詳細設定 （1759 ページ）を参照してください。 • **接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）** • **インタラクティブブロックを一時的に許可する時間(秒)（Allow an Interactive Block to bypass blocking for (seconds)）** • **URL キャッシュのミス検索の再試行（Retry URL cache miss lookup）** • **DNS トラフィックへのレピュテーション適用を有効にする（Enable reputation enforcement on DNS traffic）**
ステップ 9	変更を展開します。	設定変更の展開 （172 ページ）
ステップ 10	システムが将来の URL データの更新を予想どおりに受信することを確認します。	URL フィルタリングのヘルス モニターの設定 （1841 ページ）

	操作手順	詳細情報
ステップ 11	悪意のあるサイトからネットワークを保護する他の機能が有効になっていることを確認します。	「セキュリティインテリジェンス（1851ページ）」を参照してください。

カテゴリとレピュテーションを使用したURLフィルタリングの有効化

このタスクを実行するには、管理者ユーザーである必要があります。

始める前に

カテゴリとレピュテーションを使用したURLフィルタリングの設定方法（1825ページ）に記載されている前提条件を満たす必要があります。

手順

ステップ 1 **[統合（Integration）]** > **[その他の統合（Other Integrations）]**を選択します。
ステップ 2 **クラウド サービス** をクリックします。
ステップ 3 URL フィルタリング オプション （1827 ページ） を設定します。
ステップ 4 [保存（Save）] をクリックします。

URL フィルタリング オプション

URL フィルタリングライセンスを追加すると、URLフィルタンリング機能が自動的に有効になり、Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。

デフォルトでは、システムは脅威インテリジェンス評価のためにすべての URL をクラウドに送信するように設定されていますが、カテゴリおよびレピュテーションデータのローカルデータセットを使用すると、Web ブラウジングを高速化できます。URL フィルタリングを有効にする（または再度有効にする）と、Firewall Management Center は URL データについてシスコに自動的にクエリを実行し、データセットを管理対象デバイスにプッシュします。このプロセスには、時間がかかる場合があります。

暗号化されたトラフィックを SSL ルールを使用して処理する場合は、復号ルール の注意事項と制限事項 （2350 ページ）も参照してください。

自動更新を有効にする（Enable Automatic Updates）

[自動更新を有効にする（Enable Automatic Updates）] をオン（デフォルト）にすると、Firewall Management Center は 30 分ごとにクラウドの更新をチェックします。システムが外部リソースに接触する時間を厳格に制御する必要がある場合は、自動更新を無効にし、代わりにスケジュー

ラを使用して定期的なタスクを作成します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Automated URL Filtering Updates Using a Scheduled Task*」を参照してください。

[今すぐアップデート（Update Now）]

[今すぐアップデート（Update Now）] をクリックして、ワンタイムのオンデマンド URL データ更新を実行します。更新がすでに進行中である場合は、オンデマンド更新を開始できません。通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

URL クエリソース

ユーザーが参照する URL にシステムがカテゴリとレピュテーションを割り当てる方法を選択できます。次のオプションを選択できます。

- [ローカルデータベースのみ（Local Database Only）]：ローカルデータセットのみを使用します。プライバシー上の理由などから、未分類の URL（ローカルデータセットにないカテゴリとレピュテーション）をシスコに送信したくない場合は、このオプションを使用します。ただし、未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致しないことに注意してください。URL に手動でカテゴリやレピュテーションを割り当てることはできません。
- [ローカルデータベースと Cisco Cloud（Local Database and Cisco Cloud）]：可能な場合はローカルデータセットを使用し、Web ブラウジングを高速化します。カテゴリとレピュテーションがローカルデータセットまたは以前にアクセスした Web サイトのキャッシュにない URL をユーザーが参照すると、システムはその URL を脅威インテリジェンス評価のためにクラウドに送信し、結果をキャッシュに追加します。
- [Cisco Cloud のみ（Cisco Cloud Only）]（デフォルト）：ローカルデータセットを使用しません。カテゴリとレピュテーションが以前にアクセスした Web サイトのキャッシュにない URL をユーザーが参照すると、システムはその URL を脅威インテリジェンス評価のためにクラウドに送信し、結果をキャッシュに追加します。このオプションは、最新のカテゴリとレピュテーション情報を保証します。

  このオプションには、Threat Defense バージョン 7.3 が必要です。このオプションを有効にすると、以前のバージョンを実行しているデバイスは、[ローカルデータベースと Cisco Cloud（Local Database and Cisco Cloud）] オプションを使用します。

キャッシュされた URL の期限切れ

URL クエリソースとして [ローカルデータベースのみ（Local Database Only）] を選択した場合、この設定は関係ありません。

カテゴリおよびレピュテーション データのキャッシングにより、Web ブラウジングが高速化されます。デフォルトでは、最速のパフォーマンスを得るため、URL のキャッシュされたデータの有効期限はありません。

古いデータと一致する URL のインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。脅威データの正確性と即時性を向上させるため、短い有効期限を選択します。キャッシュされた URL は、指定された時間が経過した後、ネットワーク上のユーザーが初めてアクセスした後に更新されます。最初のユーザーに更新済みの結果は表示されませんが、この URL に次にアクセスしたユーザーには更新済みの結果が表示されます。

URL 条件の設定

URL のカテゴリとレピュテーションに基づいてサイトへのアクセスを制御することにより、ネットワークを保護します。

始める前に

注目 前提条件として、アクセス コントロール ポリシーの最上位に、カテゴリまたはレピュテーション パラメータを含むモニタリング ルールを少なくとも 1 つ作成してください。これは、特定のアクセス コントロール ポリシーにヒットするいずれかの URL のいずれかのカテゴリまたはレピュテーション データを表示するために不可欠です。

カテゴリまたはレピュテーション パラメータが設定されたルールがアクセス コントロール ポリシーにない場合、Management Center の [接続イベント（Connection Events）] ページには、アクセス コントロール ポリシーにヒットする URL トラフィックの [カテゴリ（Category）] または [レピュテーション（Reputation）] のデータが表示されません。

手順

ステップ 1 ルールエディタで、URL 条件に関して次をクリックします。

- アクセスコントロールまたは QoS：[URL（URLs）] をクリックします。
- SSL：[カテゴリ（Categoy）] をクリックします。

ステップ 2 制御する URL カテゴリを見つけて選択します。

アクセスコントロールまたは QoS ルールでは、[カテゴリ（Categoy）] をクリックしてカテゴリを選択します。

悪意のあるサイトからの効果的な保護を実現するには、すべての脅威カテゴリの URL をブロックする必要があります。さらに、Talos は、カテゴリが「悪い」（Poor）のサイトのみをブロックすることを推奨しています。セキュリティ態勢が「アグレッシブ」（Aggressive）の場合は、レピュテーションが「疑わしい」（Questionable）のサイトをブロックできますが、それにより、誤検出が多くなる可能性があります。脅威カテゴリのリストについては、URL カテゴリとレピュテーションの説明 （1817 ページ）を参照してください。

リストの下部にある矢印をクリックして、使用可能なすべてのカテゴリを表示してください。

ステップ 3 （オプション）レピュテーションを選択して URL カテゴリを制約します。

[未分類（Uncategorized）]URL を明示的にマッチした場合は、レピュテーションによりさらに制約を追加することはできないことに注意してください。レピュテーション レベルを選択すると、ルールアクションに応じて、選択したレベルよりも重大または重大でない他のレピュテーションも含められます。

- [より重大でないレピュテーションを含める（Includes less severe reputations）]：ルールで Web トラフィックを許可または信頼する場合。たとえば、[好ましい（Favorable）]（レベル4）を許可するようアクセスコントロールルールを設定した場合、[信頼できる（Trusted）]（レベル 5）サイトも自動的に許可されます。
- [より重大なレピュテーションを含める（Includes more severe reputations）]：ルールで Web トラフィックをレート制限、復号、ブロック、またはモニターする場合。たとえば、[不審なサイト（Questionable sites）]（レベル 2）をブロックするようアクセスコントロールルールを設定した場合、[信頼できない（Untrusted）]（レベル 1）のサイトも自動的にブロックされます。

ルール アクションを変更すると、URL 条件のレピュテーション レベルが自動的に変更されます。

必要に応じて、[不明なレピュテーションに適用（Apply to unknown reputation）] をオンにします。

ステップ 4 [URLの追加（Add URL）] または [ルールに追加（Add to Rule）] をクリックするか、ドラッグアンドドロップします。

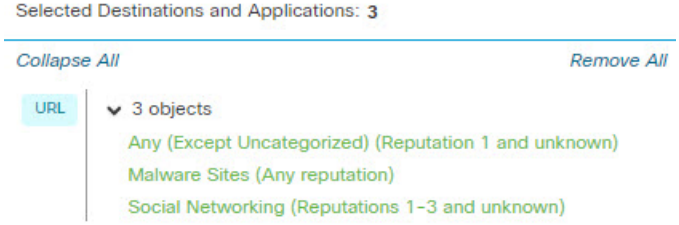
ステップ 5 （オプション）事前定義されたURLオブジェクト、またはアクセスコントロールあるいはQoSルールの URL リストとフィードを選択するには、[URL] をクリックし、オブジェクトを選択して、それらを宛先に追加します。

これらのオブジェクトは、カテゴリベースのフィルタリングではなく、手動の URL フィルタリングを適用します。

ステップ 6 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールの URL 条件

次の図に、すべてのマルウェアサイト、すべての信頼できないサイト、レピュテーションレベルが [普通（Neutral）] 以下のすべてのソーシャル ネットワーキング サイトをブロックするアクセスコントロールルールの URL の条件をします。



次の表では、条件を作成する方法を要約します。

ブロックする URL	カテゴリ	レピュテーション
マルウェア サイト（レピュテーションに関係なく）	Malware Sites	任意
信頼できない URL（レベル 1）	任意（Any）	1 - 信頼できない
ピュテーションレベルが [普通（Neutral）] 以下（レベル1 ー 3）のソーシャルネットワーキングサイト	ソーシャル ネットワーク（Social Network）	3 - 普通

URL 条件を伴うルール

次の表は、URL 条件をサポートするルールと、各ルール タイプがサポートするフィルタリングのタイプを示します。

ルール タイプ	カテゴリとレピュテーションフィルタリングをサポートしますか。	手動フィルタリングのサポート
アクセス コントロール	はい	はい
復号ポリシー	はい	非対応。代わりに識別名条件を使用
QoS	はい	はい

[復号しない（Do Not Decrypt）] ルール条件を持つ 復号ポリシー で URL フィルタリングを使用するには、URL フィルタリングでのカテゴリの使用 （1823 ページ）を参照してください。

URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

ルールに例外を設定する場合は、例外を他のルールの上に配置してください。

DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別（ベータ版）

[Enable reputation enforcement on DNS traffic] オプションは、新しい各アクセス コントロール ポリシーの [Advanced] タブでデフォルトで有効になっています。このオプションは、URL フィルタリングの動作をわずかに変更し、URL フィルタリングが有効で設定されている場合にのみ適用されます。

このオプションが有効になっている場合：

- ブラウザがドメイン名を検索して IP アドレスを取得する際に、システムは URL トランザクションの初期段階でドメインカテゴリとレピュテーションを評価します。
- 暗号化トラフィックのカテゴリとレピュテーションは、多くの場合、復号せずに判断できます。

  DNS フィルタリングで暗号化トラフィックの URL を判断できない場合、そのトラフィックは暗号化トラフィック用の設定を使用して処理されます。

ドメインルックアップ中に URL を識別するための DNS フィルタリングの有効化

新しいアクセス コントロール ポリシーでは、DNS フィルタリングがデフォルトで有効になっています。ただし、この設定を有効にするために、追加の設定が必要になる場合があります。

始める前に

- カテゴリとレピュテーションを使用した URL フィルタリングのライセンスを取得し、有効化して設定する必要があります。

  （DNSフィルタリングでは、[URLs] タブの次の設定を使用しません：[URLグループ（URL groups）]、[URLオブジェクト（URL objects）]、[URLリストとフィード（URL lists and feeds）]、および [URLの入力（Enter URL）] テキストボックスに入力された URL。）

- DNS フィルタリングの制限事項 （1833 ページ）の制限事項を参照してください。

手順

ステップ 1 アクセスコントロール ポリシーの [詳細（Advanced）] タブで、[DNSトラフィックへのレピュテーション適用を有効にする（Enable reputation enforcement on DNS traffic）] を選択します。

ステップ 2 同じポリシーで、URL カテゴリとレピュテーション ブロッキングが設定されている各アクセスコントロールルールについて、次の手順を実行します。

- アプリケーション条件：アプリケーション条件が [any] 以外（または空）の場合は、そのリストに [DNS] を追加します。その他の DNS 関連オプションは、この目的には関係ありません。

- ポート条件：ポート/プロトコル条件が [any] 以外（または空）の場合は、[DNS_over_TCP] および [DNS_over_UDP] を追加します。

ステップ 3 変更を保存します。

次のタスク

変更後は次の操作を実行します：設定変更の展開 （172 ページ）

DNS フィルタリングの制限事項

[Block with reset]、[Interactive Block]、または [Interactive Block with reset] アクションを持つルールに一致するトラフィックは、ルールアクションが [Block] であるかのように処理されます。

エンドユーザーがブロックされた URL にアクセスしようとすると、原因不明の理由によりページに接続できなくなり、接続が乱れて、タイムアウトします。

DNS フィルタリングとイベント

DNS フィルタリングによって生成される接続イベントは、[DNS クエリ（DNS Query）]、[URL カテゴリ（URL Category）]、[URL レピュテーション（URL Reputation）]、[宛先ポート（Destination Port）] の各フィールドを使用してログに記録されます。DNS Query フィールドにはドメイン名が保持されます。 DNS フィルタリング照合の場合 URL フィールドは空白になります。[宛先ポート（Destination Port）] は 53 です。

以下の点にも注意してください。

- アクセス コントロール ルール アクションが [許可（Allow）] または [信頼（Trust）] の場合、同じトラフィックに対して 2 つの接続イベントが生成されます。1 つは DNS フィルタリング用（[DNS クエリ（DNS Query）] フィールドに入力）、もう 1 つは URL フィルタリング用（[URL] フィールドに入力）です。
- システムが特定の URL に初めて遭遇すると、その 1 つのセッションに対して 2 つのイベントが発生します。1 つは、DNS クエリに対して未分類/レピュテーションがないことを示すイベント、もう 1 つは、URL の実際のカテゴリとレピュテーションを示すイベントです。これらのイベントは DNS 中に取得され、標準の URL フィルタリングを使用した処理中にセッションに適用されます。

手動 URL フィルタリング

アクセス コントロール ルールおよび QoS ルールでは、個々の URL、URL のグループ、または URL のリストとフィードを手動でフィルタリングすることで、カテゴリとレピュテーション ベースの URL のフィルタリングを補足したり、選択的にオーバーライドしたりできます。

例：

- アクセス コントロールを使用して組織に適していない Web サイトのカテゴリをブロックできます。ただし、カテゴリに適切な Web サイトが含まれ、アクセスを提供したい場合、そのサイトに対して手動の許可ルールを作成し、カテゴリのブロック ルールの前に配置できます。
- カテゴリベースの URL フィルタリングを使用しない場合は、アクセス コントロール ポリシー内に許可またはブロック ルールを作成して、URL または URL のグループを手動で許可またはブロックできます。特殊なライセンスなしでこのタイプの URL フィルタリングを実行することができます。

手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

注意 手動 URL フィルタリングの実装方法によっては、URL マッチングが意図したものにならない可能性があります。「手動URLフィルタリングオプション（1834ページ）」を参照してください。

手動 URL フィルタリングオプション

手動 URL フィルタリング用の URL を指定する方法は、いくつかあります。

オプション	説明
（ベストプラクティス） カスタムセキュリティインテリジェンスURLリストまたはフィードオブジェクトを使用します。	これは、手動 URL フィルタリングの推奨される手法です。 新しいリストかフィードを作成するか、アクセスコントロールまたは QoS ルールで既存のリストかフィードを選択できます。 詳細については、カスタム セキュリティ インテリジェンスのリストとフィード（1392ページ）とサブトピックを参照してください。

オプション	説明
URL オブジェクトは、個別にまたはグループとして使用しますURL オブジェクトについては、「URL （1404 ページ）」で説明します。 または アクセスコントロールルールに URL を直接入力します（Web インターフェイスのルールページの [URL の入力（Enter URL）] オプション）。	パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。1 つ以上の / を含める場合、文字列の部分一致には URL 文字列全体が使用されます。次に、次のいずれかに該当する場合、URL は一致と見なされます。 • 文字列が URL の先頭にある。 • 文字列がドットの後に続く。 • 文字列の先頭にドットが含まれている。 • 文字列が :// 文字の後に続く。 たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。 （注） サーバーは再構成でき、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部（つまり / 文字を含む URL 文字列）をブロックまたは許可するために手動の URL フィルタリングは使用しないことをお勧めします。 [URL の入力（Enter URL）] オプションはワイルドカードをサポートしていません。

カテゴリおよびレピュテーションベースの URL フィルタリングの補完または選択的オーバーライド

アクセスコントロールルールまたは QoS ルールでは、セキュリティ インテリジェンス URL リストおよびフィードを使用して、カテゴリおよびレピュテーションベースの URL フィルタリングルールを補足したり、それらに例外を指定することができます

重要 この手順で設定しているリストまたはフィードにカテゴリまたはレピュテーションベースのルールの例外が含まれている場合は、ルールの順序で、それらのルールの上にこのルールを配置します。

SSL ルールで、識別名条件を使用して並列動作を設定します。

始める前に

- カテゴリとレピュテーションを使用して URL フィルタリングを設定します。URL 条件の設定 （1829 ページ） を参照してください。
- 手動 URL フィルタリングの重要なベストプラクティスを理解します。URL フィルタリングのベストプラクティス（1818 ページ）および手動 URL フィルタリングオプション（1834 ページ）を参照してください。

- 手動フィルタリングに使用する URL を含む 1 つ以上のセキュリティ インテリジェンス オブジェクト（リストまたはフィード）を設定します。カスタムセキュリティインテリジェンスのリストとフィード （1392 ページ） を参照してください。

手順

ステップ 1 ルールを定義するアクセス コントロール ポリシーまたは QoS ポリシーに移動します。

ステップ 2 新しい条件を追加するルールを作成または編集します。

- カテゴリまたはレピュテーションベースの URL フィルタリングルールを補足する場合は、既存のルールを編集します。
- カテゴリまたはレピュテーションベースの URL フィルタリングルールをオーバーライドしたり、それらの例外を作成する場合は、新しいルールを作成します。

ステップ 3 宛先 URL の基準として作成したリストかフィードを選択します。

ステップ 4 ルールを保存します。

HTTP 応答ページの設定

アクセス制御の一部として、アクセス コントロール ルールあるいはアクセス コントロール ポリシーのデフォルト アクションを使って、システムが Web リクエストをブロックしたときに表示する HTTP 応答ページを設定できます。

表示される応答ページは、セッションのブロック方法によって異なります。

- **ブロック応答ページ**により、接続が拒否されたことを示すデフォルトのブラウザページまたはサーバー ページは上書きされます。
- [インタラクティブ ブロック応答（Interactive Block Response）] ページ：ユーザーに警告しますが、ユーザーはボタンをクリック（あるいはページを更新）して要求したサイトをロードできます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

応答ページを選択していない場合、インタラクションや説明なしでシステムはセッションをブロックします。

HTTP 応答ページの制限

- システムは、アクセス制御ルールまたはアクセス制御ルールのデフォルト アクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）暗号化されていないか、または復号された HTTP/HTTPS 接続の場合にのみ、応答ページを表示しま

す。システムは、他のポリシーまたはメカニズムによってブロックされた接続の応答ページは表示しません。

- システムは、接続がリセットされた場合（RST パケットが送信）された場合は、応答ページを表示できません。応答ページを有効にすると、システムその接続を優先します。[リセットしてブロック（Block with reset）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] をルール アクションとして選択した場合、システムは応答ページを表示し、一致する Web 接続をリセットしません。ブロックされた Web 接続のリセットを確認するには、応答ページを無効にする必要があります。

  ルールに一致する Web 以外のすべてのトラフィックがリセットによりブロックされます。

- アクセス制御ルール（または、その他の設定）によってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。アクセス制御ルールは SSL ポリシーを設定しなかった場合に暗号化された接続を評価し、それ以外の場合は、SSL ポリシーが暗号化されたトラフィックを受け渡します。

  たとえば、システムは HTTP/2 セッションまたは SPDY セッションを復号できません。これらのプロトコルのいずれかを使用して暗号化された Web トラフィックがアクセス制御ルールの評価に達したが、セッションがブロックされている場合、システムは応答ページを表示しません。

  ただし、システムは、SSL ポリシーによって復号された後に、アクセス制御ルールまたはアクセス制御ルールのデフォルトアクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）接続の場合に、応答ページを表示します。このような場合、システムは応答ページを暗号化して、再暗号化された SSL ストリームの最後にそれを送信します。

- Web トラフィックがプロモートされたアクセス コントロール ルール（単純なネットワーク条件のみの早期に適用されたブロッキングルール）のためにブロックされている場合、システムは応答ページを表示しません。

- URL が「http」または「https」を指定せずに入力され、ブラウザがポート 80 で接続を開始し、ユーザーが応答ページをクリックスルーし、その後、接続がポート 443 にリダイレクトされる場合、この URL への応答はすでにキャッシュされているため、ユーザーには 2 番目のインタラクティブな応答ページが表示されません。

- システムは、システムが要求された URL を識別する前にトラフィックがブロックされた場合は、応答ページを表示しません。URL フィルタリングのベスト プラクティス （1818 ページ）を参照してください。

HTTP 応答ページの要件と前提条件

モデルのサポート

いずれか（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

HTTP 応答ページの選択

HTTP応答ページを確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。ページが小さいほど、正常に表示される傾向にあります。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [HTTPレスポンス（HTTP Responses）] を選択します。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [応答ページをブロック（Block Response Page）] および [応答ページのインタラクティブ ブロック（Interactive Block Response Page）] を選択します。

- [System-provided]：一般的な応答が表示されます。[表示（View）]（ ）をクリックすると、このページのコードが表示されます。
- [Custom]：カスタム応答ページが作成されます。ポップアップウィンドウが表示されます。このウィンドウに事前入力されているシステム提供コードを [編集（Edit）]（）をクリックして置換または変更できます。カウンタで使用した文字数が表示されます。
- [None]：応答ページを無効にして、インタラクションや説明なしでセッションをブロックします。アクセス コントロール ポリシー全体でインタラクティブ ブロッキングを無効にするには、このオプションを選択します。

ステップ 3 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

HTTP 応答ページでのインタラクティブ ブロッキングの設定

インタラクティブブロッキングを設定すると、ユーザは警告を読んだ後に当初要求したサイトを読み込むことができます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

ヒント アクセス コントロール ポリシー全体に対してインタラクティブ ブロッキングを素早く無効にするには、システム提供のページもカスタムページも表示しないでください。そうすると、システムにより操作なしですべての接続がブロックされます。

ユーザがインタラクティブ ブロックをバイパスしない場合、一致するトラフィックは拒否され、追加のインスペクションは行われません。ユーザがインタラクティブブロックをバイパスするとアクセス コントロール ルールはトラフィックを許可しますが、引き続きトラフィックはディープ インスペクションやブロッキングの対象となる場合があります。

デフォルトでは、ユーザのバイパスは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間有効です。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブ ブロック ルールに適用されます。ルールごとに制限を設定することはできません。

インタラクティブ ブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけです。システムが最初にユーザに警告すると、ロギングされた接続開始イベントはシステムにより [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションでマークされます。ユーザーがブロックをバイパスすると、セッションが記録される追加の接続イベントに [許可（Allow）] アクションが付きます。

インタラクティブ ブロッキングの設定

次の手順では、ユーザーが URL フィルタリングルールをバイパスできるようにする方法について説明します。

手順

ステップ 1 アクセス コントロールの一部として、Web トラフィックと一致するアクセス コントロール ルールを設定します。アクセスコントロールルールの作成および編集（1788 ページ）を参照してください。

- アクション：ルール アクションを [インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定します。アクセス コントロール ルール インタラクティブ ブロック アクション（1784 ページ）を参照してください。

- 条件：URL 条件を使用して、インタラクティブにブロックする Web トラフィックを指定します。URL 条件（URL フィルタリング）を参照してください。
- ロギング：ユーザーがブロックをバイパスすると想定し、それに応じてロギング オプションを選択します。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「許可された接続のロギング」を参照してください。
- インスペクション：ユーザーがブロックをバイパスすると想定し、それに応じてディープインスペクション オプションを選択します。アクセス制御の概要（1717 ページ）を参照してください。

ステップ 2 （オプション）アクセス コントロール ポリシーの [HTTP応答（HTTP Responses）] で、カスタム インタラクティブ ブロックの HTTP 応答ページを選択します。HTTP 応答ページの選択（1838 ページ）を参照してください。

ステップ 3 （オプション）アクセス コントロール ポリシーの [詳細（Advanced）] 設定で、ユーザーのバイパス タイムアウトを変更します。ブロックされた Web サイトのユーザー バイパス タイムアウトの設定（1840 ページ）を参照してください。

ユーザーはブロックをバイパスした後、そのページを参照でき、タイムアウト期間が経過するまで警告は表示されません。

ステップ 4 アクセス コントロール ポリシーを保存します。

ステップ 5 設定変更を展開します設定変更の展開（172 ページ）を参照してください。

ブロックされた Web サイトのユーザー バイパス タイムアウトの設定

次の手順では、ユーザーが URL フィルタリング ブロックをバイパスした後に閲覧できる時間を設定する方法について説明します。タイムアウトになると、ユーザーはブロックを再度バイパスする必要があります。

手順

ステップ 1 をクリックしてポリシーを編集します。**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]**

ステップ 2 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 3 [全般設定（General Settings）] の横にある [編集（Edit）]（ ） をクリックします。

代わりに [表示（View）]（ ）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 4 [ブロックをバイパスするためのインタラクティブ ブロックを許可する期間（秒）（Allow an Interactive Block to bypass blocking for (seconds)）] フィールドに、ユーザー バイパスの期限が切れるまでの経過時間を秒数で入力します。

この値を0に設定すると、インタラクティブブロック応答が一度表示され、ユーザーバイパスが期限切れになることはありません。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

URL フィルタリングのヘルス モニターの設定

次のヘルス ポリシーは、システムに URL カテゴリとレピュテーション データを取得または更新に問題がある場合は通知します。

- URL フィルタリング モニター
- デバイスでの脅威データの更新

これらが希望どおりに構成されていることを確認するには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「ヘルスモジュール」と「ヘルスモニタリングの構成」を参照してください。

URL カテゴリとレピュテーションの異議申し立て

Talos によって割り当てられたカテゴリまたはレピュテーションに食い違いがある場合は、再評価の要求を提出できます。

始める前に

シスコ アカウントのクレデンシャルが必要になります。

手順

ステップ 1 Firewall Management Center Web インターフェイスで、以下のいずれかを実行します。

異議申し立てオプションの場所	異議申し立てオプションへのパス
[クラウドサービス（Cloud Services）] 設定ページ	a. **[統合（Integration）] > [その他の統合（Other Integration）] > [クラウドサービス（Cloud Services）]** ページに移動します。 b. [URL のカテゴリとレピュテーションの異議申し立て（Dispute URL categories and reputations）] を選択します。
[手動 URL ルックアップ（Manual URL Lookup）] ページ	a. [分析（Analysis）] > [詳細（Advanced）] > [URL] から [手動 URL ルックアップ（Manual URL Lookup）] ページに移動します。 b. 問題の URL を検索します。 c. テーブルの行の末尾にある [異議申し立て（Dispute）] を表示するには、結果のリスト内の関連エントリにマウスのポインタをおき、[異議申し立て（dispute）] をクリックします。
URL 接続イベント	a. [分析（Analysis）] > [接続（Connections）] メニューで、URL が含まれているテーブルがあるページに移動します。 b. [URL カテゴリ（URL Category）] 列または [URL レピュテーション（URL Reputation）] 列（必要な場合は非表示列を表示） の項目を右クリックしてオプションを選択します。

Talos の Web サイトが個別のブラウザ ウィンドウに開きます。

ステップ 2 シスコのクレデンシャルで Talos サイトにサインインします。

ステップ 3 情報を確認し、Talos ページで手順を実行します。

ステップ 4 提出された異議申し立ての処理方法と予想される応答に関する情報を Talos で探します。

異議申し立てプロセスは Firepower 製品に依存しません。

URL カテゴリセットが変更された場合、アクションを実行

URL フィルタリング カテゴリのセットは、新しい Web のトレンドと進化する使用パターンに合わせてときどき変更されます。

これらの変更は、ポリシーとイベントの両方に影響します。

スケジュールされている URL カテゴリ変更の少し前と変更後に、この変更の影響を受けるアクセス コントロール ポリシー、SSL ポリシー、および QoS ポリシーのルールのリスト、および編集するルールの [URL] または [Category] にアラートが表示されます。

これらのアラートが表示された場合は、対処する必要があります。

（注） このトピックの説明どおりに設定された URL カテゴリへの更新は、新しい URL を既存のカテゴリに単純に追加したり、誤って分類された URL を再分類する変更とは異なります。このトピックは個々の URL のカテゴリ変更には適用されません。

手順

ステップ 1 アクセス コントロール ポリシーのルールの横にアラートが表示された場合は、アラートの上にマウスを置いて詳細を確認します。

ステップ 2 アラートが URL カテゴリの変更について言及している場合は、ルールを編集してさらなる詳細を確認します。

ステップ 3 [ルール（Rule）] ダイアログの [URL] または [カテゴリ（Category）] にマウスカーソルを合わせると、変更のタイプに関する一般情報が表示されます。

ステップ 4 カテゴリの横にアラートが表示された場合は、このアラートをクリックして詳細を表示します。

ステップ 5 [More information] リンクが変更の説明に表示されている場合は、そのリンクをクリックするとカテゴリに関する情報が Talos の Web サイトに表示されます。

または、URL カテゴリとレピュテーションの説明（1817ページ） のリンクですべてのカテゴリのリストと説明を確認してください。

ステップ 6 変更のタイプに応じて、適切なアクションを実行します。

カテゴリ変更のタイプ	システムで実行されること	自分で実行すべきこと
既存のカテゴリはまもなく廃止される予定です	まだ廃止されていません。影響を受けるルールを変更するには数週間かかります。 その期間内にアクションを実行しない場合は、システムは最終的にポリシーを再展開することはできません。	このカテゴリを含むすべてのルールからこのカテゴリを削除します。同様の新しいカテゴリがある場合は、代わりにそのカテゴリを使用することを検討してください。
新しいカテゴリが追加されます	デフォルトでは、システムは新たに追加されたカテゴリを使用しません。	新しいカテゴリに新しいルールを作成することを検討します。
既存のカテゴリは削除されます。	該当するカテゴリは取り消し線が引かれた状態で（つまり、カテゴリ名全体に線が引かれた状態で）ルールに表示されます。	ポリシーを展開する前にルールから古いカテゴリを削除する必要があります。

ステップ 7 これらの変更についてSSLルール（[カテゴリ（Category）]）を確認し、必要に応じてアクションを実行します。

ステップ 8 これらの変更について QoS ルール（[URL]）を確認し、必要に応じてアクションを実行します。

次のタスク

設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

URL カテゴリとレピュテーションの変更：イベントへの影響

- URLカテゴリが変更されるとカテゴリ変更の前にシステムによって処理されたイベントは元のカテゴリ名に関連付けられ、「**Legacy**」というラベルがつけられます。カテゴリ変更後にシステムが処理したイベントは新しいカテゴリに関連付けられます。

  より古い、レガシー イベントは時間の経過とともにシステムからエージ アウトします。

- 処理された時点でURLにレピュテーションがない場合は、イベント ビューア内のURL レピュテーションは空になります。

URL フィルタリングのトラブルシューティング

予想される URL カテゴリが [カテゴリ（Categories）] リストにない

URL フィルタリング機能は、セキュリティ インテリジェンス機能とは異なる一連のカテゴリを使用します。表示されると予想されるカテゴリは、セキュリティ インテリジェンス カテゴリである可能性があります。これらのカテゴリを表示するには、アクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブにある [URL（URLs）] タブを調べます。

初期パケットが検査されずに渡される

「トラフィック識別の前に通過するパケットのインスペクション （2746ページ）」およびサブトピックを参照してください。

DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別（ベータ版） （1832 ページ）も参照してください。

ヘルス アラート：「URL フィルタリングの登録に失敗しました（URL Filtering registration failure）」

Firewall Management Center とプロキシが Cisco Cloud に接続できることを確認します。次のトピックの URL フィルタリングおよびURL カテゴリに関する情報が必要な場合があるかもしれません：Cisco Secure Firewall Management Center アドミニストレーション ガイドの「インターネット アクセス要件」および「通信ポートの要件」。

特定の URL のカテゴリとレピュテーションはどのようにしたら確認できますか。

手動ルックアップを実行します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Finding URL Category and Reputation」を参照してください。

手動ルックアップ試行時のエラー：「<URL> のクラウド ルックアップに失敗しました（Cloud Lookup Failure for <URL>）」

機能が適切に有効になっていることを確認します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Finding URL Category and Reputation」の前提条件を参照してください。

URL はその URL カテゴリとレピュテーションに基づいて誤って処理されたように見えます。

問題：システムはURL カテゴリとレピュテーションに基づいてURL を正しく処理しません。

対処方法:

- URL カテゴリと URL に関連付けられているレピュテーションが想定どおりであることを確認します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Finding URL Category and Reputation」を参照してください。
- 次の問題は、カテゴリとレピュテーションを使用したURL フィルタリングの有効化（1827 ページ）を使用してアクセスできる、URL フィルタリング オプション（1827 ページ）で説明した設定で対処できる場合があります。
  - URL キャッシュに古い情報が保存されている可能性があります。URL フィルタリング オプション（1827 ページ）の [キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定に関する情報を参照してください。
  - クラウドからの最新情報でローカルのデータセットが更新されていない可能性があります。URL フィルタリング オプション（1827 ページ）の [自動更新を有効にする（Enable Automatic Updates）] 設定に関する情報を参照してください。
  - 最新のデータに関してクラウドを確認しないようにシステムが設定されている可能性があります。URL フィルタリング オプション（1827 ページ）の [不明URLをCisco Cloud に問い合わせる（Query Cisco cloud for unknown URLs）] 設定に関する情報を参照してください。
- クラウドを確認せずに URL にトラフィックを渡すようにアクセス コントロール ポリシーが設定されている可能性があります。アクセス コントロール ポリシーの詳細設定（1759 ページ） で、[URL キャッシュ ミス ルックアップを再試行する（Retry URL cache miss lookup）] 設定に関する情報を参照してください。
- URL フィルタリングのベスト プラクティス（1818 ページ）も参照してください。
- SSL ルールを使用して URL を処理した場合は、復号ルールの注意事項と制限事項（2350 ページ）およびSSL ルールの順序を参照してください。

- URL を処理している思われるアクセス制御ルールを使用して URL が処理されていることを確認し、アクセス制御ルールが想定どおりに機能していることを確認します。ルールの順序を考慮します。
- Firewall Management Center のローカル URL カテゴリおよびレピュテーション データベースがクラウドから正常に更新されており、管理対象デバイスが Firewall Management Center から正常に更新されていることを確認します。

  これらのプロセスのステータスは、[URL フィルタリング モニタ（URL Filtering Monitor）] モジュールおよび [デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールのヘルス モニタでレポートされます。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Health」 を参照してください。

ローカル URL カテゴリおよびレピュテーション データベースを即座に更新する場合、**[統合（Integration）] > [その他の統合（Other Integrations）]** に移動し、**クラウド サービス** をクリックしてから [今すぐアップデート（Update Now）] をクリックします。詳細については、URL フィルタリング オプション （1827 ページ）を参照してください。

URL カテゴリまたはレピュテーションが正しくありません。

アクセス コントロールまたは QoS ルールの場合：ルールの順序に細心の注意を払って、手動フィルタリングを使用します。手動 URL フィルタリング （1833 ページ）およびURL 条件の設定 （1829 ページ）を参照してください。

SSL ルールの場合：手動フィルタリングはサポートされていません。代わりに識別名条件を使用します。

URL カテゴリとレピュテーションの異議申し立て （1841 ページ）も参照してください。

Web ページのロードに時間がかかる

セキュリティとパフォーマンスのトレードオフがあります。いくつかのオプションを次に示します。

- [キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定の変更を検討します。**[統合（Integration）] > [その他の統合（Other Integrations）]** をクリックし、**クラウド サービス** を選択します。詳細については、URL フィルタリング オプション （1827 ページ）を参照してください。
- アクセス コントロール ポリシーの詳細設定 （1759 ページ）の [URL キャッシュのミス検索の再試行（Retry URL cache miss lookup）] 設定の選択解除を検討します。

イベントに URL カテゴリおよびレピュテーションは含まれていません

- アクセス コントロール ポリシーに適用可能な URL ルールが含まれていること、ルールがアクティブになっていること、およびポリシーが関連するデバイスに展開されていることを確認します。
- URL ルールと一致する前に接続が処理される場合、URL カテゴリとレピュテーションはイベントに表示されません。

- 接続を処理するルールでは、URL カテゴリとレピュテーションを構成する必要があります。
- SSL ルールの [カテゴリ（Categories）] タブで URL カテゴリを設定した場合でも、アクセス コントロール ポリシーのルールで [URL（URLs）] タブを設定する必要があります。

DNS フィルタリングが機能していない

ドメインルックアップ中に URL を識別するための DNS フィルタリングの有効化 （1832 ページ）に説明されているすべての前提条件とステップを満たしていることを確認します。

エンドユーザーがブロックされたURLにアクセスしようとすると、ページがスピンしてタイムアウトする

DNS フィルタリングが有効になっていて、エンドユーザーがブロックされている URL にアクセスすると、ページはスピンしますが読み込まれません。エンドユーザーには、ページがブロックされたことが通知されません。これは現在、DNS フィルタリングが有効になっている場合の制限です。

DNS フィルタリングの制限事項 （1833 ページ）を参照してください。

イベントに[URLカテゴリ（URL Category）]と[レピュテーション（Reputation）]が含まれるが、[URL] フィールドが空白

[DNSクエリ（DNS Query）] フィールドに値が入力されていて、[URL] フィールドが空の場合、これは DNS フィルタリング機能が有効になっているときに予想されるものです。

DNS フィルタリングとイベント （1833 ページ）を参照してください。

1 つのトランザクションに対して複数のイベントが生成される

1 つの Web トランザクションが 2 つの接続イベントを生成することがあります。1 つは DNS フィルタリング用で、もう 1 つは URL フィルタリング用です。これは、DNS フィルタリングが有効になっていて、次の場合に予想されるものです。

- トラフィックのアクセス コントロール ルール アクションが [許可（Allow）] または [信頼（Trust）] である。
- システムが URL を初めて検出した。

「DNS フィルタリングとイベント （1833 ページ）」を参照してください。

URL フィルタリングの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しい URL カテゴリ	リリース 7.0 タイムフレームの新機能、すべてのリリースに適用	任意（Any）	新しい URL カテゴリ：プライベート IP アドレス 詳細については、Talosintelligence.com を参照してください
DNS フィルタリング	7.0 6.7（ベータ版）	任意（Any）	各アクセス コントロール ポリシーの詳細設定の新しいオプションにより、カテゴリとレピュテーションによる、Web トラフィックのより早期のフィルタリングが可能になります。 この機能は新規インストール時にデフォルトで有効になっています。 サポートされるプラットフォーム：サポートされているバージョンの Firewall Management Center および管理対象デバイス。
レピュテーションが不明なサイトの処理を指定する機能	6.7	いずれか	レピュテーションが不明な URL の処理を指定できるようになりました。 変更された画面：アクセス コントロール ポリシーと QoS ポリシーの URL ルール、および SSL ポリシーのカテゴリルールで、レピュテーション選択エリアの下にこのための新しいチェックボックスが含まれています。 サポートされるプラットフォーム：すべて

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新規および変更された URL カテゴリ レピュテーション レベルの新しい名前	6.5	任意（Any）	次の変更は、アクセス コントロール ポリシーおよび QoS ポリシーの URL ルールと SSL ポリシーのカテゴリ ルールに適用されます。 一連の URL カテゴリが変更されました。現在、URL ルールを作成するときに選択するカテゴリの 2 つの「ページ」があります。 各レピュテーション レベルに関連付けられている名前が変更されました。 新しいカテゴリとレピュテーションの名前の説明については、URL カテゴリとレピュテーションの説明（1817ページ）を参照してください。 アップグレード固有の詳細については、バージョン 6.5 のリリース ノートとアップグレード手順も参照してください。 カテゴリ セットの変更が将来ある場合、ルールには警告するためのアイコンが表示されます。 変更された画面：アクセス コントロール ポリシー、SSL ポリシー、および QoS ポリシーの URL ルール、URL カテゴリに関連するイベント データ サポートされるプラットフォーム：リリース 6.5 を実行している Firewall Management Center およびデバイス。
従来のデバイス ライセンスへの細かい変更	6.5	任意（Any）	従来のライセンスを使用するデバイスでは、デバイスが Firewall Management Center に登録され、URL フィルタリング ライセンスがデバイスに割り当てられるまで、URL フィルタリングは有効になりません。 サポートされるプラットフォーム：NGIPSv および ASA with FirePOWER Services デバイス。
Cisco Cloud から URL データを取得するためのアドレスが変更されました。	6.5	任意（Any）	Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Internet Access Requirements」 の URL フィルタリングの行を参照してください。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
割り当てられている URL カテゴリに異議を唱える機会	6.5	任意（Any）	システムによって URL に割り当てられたカテゴリに不満がある場合は、カテゴリを変更する要求を提出できます。 新規/変更された画面： • [分析（Analysis）] メニューの接続イベントのテーブルにある URL カテゴリまたはレピュテーションを右クリックしたときの新しいメニュー オプション。 • [URL ルックアップ（URL Lookups）] ページの新しいボタン（**[分析（Analysis）] > [詳細（Advanced）] > [URL]**）。（URL 上にポインタを合わせるとボタンが表示されます）。 • **[システム（System）] > [統合（Integration）] > [クラウド サービス（Cloud Services）]**ページの新しいオプション サポート対象プラットフォーム：すべて
[Cisco CSI] タブの名前が [クラウド サービス（Cloud Services）] に変更されました。	6.4	任意（Any）	変更された画面と移動：**[システム（System）] > [統合（Integration）] > [Cisco CSI]**は**[システム（System）] > [統合（Integration）] > [クラウド サービス（Cloud Services）]**になりました。 サポートされているプラットフォーム： Firewall Management Center
URL フィルタリング情報をさまざまな場所から新しい URL フィルタリングの章に移動しました。	6.3	任意（Any）	URL フィルタリングのクラウド通信の設定に関する情報を新しい URL フィルタリングの章に移動しました。その他の特定の URL フィルタリングの情報をこの章の他の場所に移動しました。章内の Cisco CSI のトピックの構成に関連する変更を加えました。
新規オプション：キャッシュされた URL の期限切れ	6.3	任意（Any）	この新しいコントロールを使用して、古いデータで一致している URL のインスタンスを最小限に抑えるため、新しい URL カテゴリおよびレピュテーションとパフォーマンスとのバランスを取ります。 変更された画面：**[システム（System）] > [統合（Integration）] > [Cisco CSI]**。 サポート対象プラットフォーム：すべて
変更されたメニューパス	6.3	任意（Any）	[手動 URL ルックアップ（Manual URL Lookup）] ページへのパスが**[分析（Analysis）] > [ルックアップ（Lookup）] > [URL]**か**[分析（Analysis）] > [詳細（Advanced）] > [URL]**に変更されました。

第 42 章

セキュリティ インテリジェンス

以下のトピックでは、セキュリティインテリジェンスの概要（トラフィックのブロックリストと許可リストの使用、基本設定など）を示します。

- セキュリティ インテリジェンスについて （1851 ページ）
- セキュリティ インテリジェンスのベストプラクティス （1852 ページ）
- セキュリティ インテリジェンスのためのライセンス要件 （1853 ページ）
- セキュリティ インテリジェンスの要件と前提条件 （1853 ページ）
- セキュリティ インテリジェンス送信元 （1854 ページ）
- セキュリティ インテリジェンスの設定 （1855 ページ）
- セキュリティ インテリジェンス モニタリング （1863 ページ）
- セキュリティ インテリジェンス ブロッキングのオーバーライド （1864 ページ）
- セキュリティ インテリジェンスのトラブルシューティング （1865 ページ）
- セキュリティ インテリジェンス ブロック リストへの登録の履歴 （1866 ページ）

セキュリティ インテリジェンスについて

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティインテリジェンスは疑わしい IP アドレス、URL、ドメイン名が関連する接続をレピュテーション インテリジェンスを使用して迅速にブロックします。これは、セキュリティ インテリジェンス ブロック リストと呼ばれます。

セキュリティインテリジェンスはアクセス制御の初期のフェーズであり、大量のリソースを消費する評価をシステムが実行する前に行われます。ブロックリストにより、インスペクションの必要がないトラフィックを迅速に除外できるため、パフォーマンスが向上します。

（注） ブロックリストを使用して、高速パストラフィックをブロックすることはできません。プレフィルタ評価の実行は、セキュリティインテリジェンスによるフィルタリングの前に行われます。FastPath が適用されたトラフィックは、セキュリティインテリジェンスを含め、以降のすべての評価をバイパスします。

カスタムのブロックリストを設定できますが、シスコでは定期的に更新されるインテリジェンスフィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。

ブロックしないリストとモニター専用ブロックリストを使用して、セキュリティインテリジェンスブロックリスト機能の精度を上げることができます。これらのメカニズムは、ブロックリストによりトラフィックがブロックされないようにしますが、一致するトラフィックを自動的に信頼したり FastPath を適用したりすることは**しません**。ブロックしないリストに追加されたトラフィックや、セキュリティインテリジェンスの段階でモニターされるトラフィックは、意図的に残りのアクセスコントロールによる分析が適用されます。

（注） 検出シグニチャまたはマルウェア URL を含むセキュリティ インテリジェンス設定により、Firewall Threat Defense トラブルシューティング ファイルがスキャンされたときに、誤った脅威アラートが発生する可能性があります。

関連トピック

セキュリティ インテリジェンス （1384 ページ）

セキュリティ インテリジェンスのベストプラクティス

- システムが提供するセキュリティ インテリジェンス フィードによって検出されたすべての脅威をブロックするようにアクセス コントロール ポリシーを設定します。設定例：セキュリティインテリジェンスブロック （1862 ページ）を参照してください。
- シスコが提供するセキュリティ インテリジェンス フィードをカスタム脅威データで補足する場合、または新しい脅威を手動でブロックする場合は、次のようにします。
  - IP アドレスの場合は、カスタムのセキュリティ インテリジェンスのリストおよびフィードか、ネットワークオブジェクトまたはグループを使用します。これらを作成するには、セキュリティインテリジェンス （1384ページ）およびネットワーク （1349 ページ）とそのサブトピックを参照してください。これらをセキュリティ インテリジェンスに使用するには、セキュリティインテリジェンスの設定 （1855ページ）を参照してください。セキュリティ インテリジェンス ポリシーで使用されるネットワークオブジェクトには、IPS ライセンスが必要です。
  - IP とドメインの場合は、カスタムのセキュリティ インテリジェンスのリストおよびフィードを使用し、オブジェクトまたはグループは使用しません。詳細については、手動 URL フィルタリングオプション （1834 ページ）を参照してください。
  - イベントからブロックリストにエントリを追加することもできます。グローバルおよびドメインのセキュリティインテリジェンスリスト （1387ページ）を参照してください。

- 新しいフィードをテストする場合、またはパッシブ展開の場合は、アクションをブロックからモニターのみに設定します。セキュリティ インテリジェンス モニタリング（1863 ページ）を参照してください。
- 特定のサイトまたはアドレスをセキュリティ インテリジェンスのブロッキングから除外する必要がある場合は、セキュリティ インテリジェンス ブロッキングのオーバーライド（1864 ページ）を参照してください。
- Firepower 展開が Cisco XDR と統合されていて、カスタムのセキュリティ インテリジェンスのリストおよびフィードを使用している場合は、そのリストとフィードで Security Services Exchange を必ず更新します。詳細については、Security Services Exchange のオンラインヘルプでイベントの自動プロモーションを設定するための手順を参照してください。この統合に関する一般的な情報については、Cisco Secure Firewall Management Center アドミニストレーション ガイド の「*SecureX* 統合の有効化」を参照してください。
- システムで提供されるセキュリティ インテリジェンスのカテゴリは、時間の経過とともに通知なしに変更される場合があります。定期的に変更を確認し、それに応じてポリシーを変更することを計画する必要があります。
- また、悪意のあるサイトからの保護を強化するために、URL フィルタリング（個別のライセンス要件がある個別の機能）を設定する必要もあります。「URL フィルタリング（1815 ページ）」を参照してください。

セキュリティ インテリジェンスのためのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

セキュリティ インテリジェンスの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者

- アクセス管理者
- ネットワーク管理者

重要 SIポリシーを正常に適用するには、デバイスにネットワーク検出ポリシーを適用する必要があります。

セキュリティ インテリジェンス送信元

- システムが提供するフィード

  シスコは、ドメイン、URL、およびIPアドレスについて定期的に更新されるインテリジェンスフィードへのアクセスを提供します。詳細については、セキュリティインテリジェンス （1384 ページ）を参照してください。

  名前に「TID」が含まれるフィードがある場合、このフィードはセキュリティ インテリジェンスによって使用されません。代わりに、このフィードは、Secure Firewall Threat Intelligence Director （2941 ページ）で説明されている機能によって使用されます。

- サードパーティフィード

  オプションで、Cisco 提供のフィードをサードパーティのフィードで補完できます。これらのフィードは、Secure Firewall Management Center が定期的にインターネットからダウンロードする動的リストです。カスタムセキュリティインテリジェンスフィード（1394ページ）を参照してください。

- カスタムブロックリストまたはフィード（またはオブジェクトまたはグループ）

  手動で作成したリストまたはフィードを使用して、特定の IP アドレス、URL、またはドメイン名をブロックします（IPアドレスの場合、ネットワークオブジェクトまたはグループを使用することもできます）。

  たとえば、フィードによってまだブロックされていない悪意のあるサイトまたはアドレスに気付いた場合は、これらのサイトをカスタム セキュリティ インテリジェンス リストに追加し、このカスタムリストをアクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブでブロックリストに追加します。カスタムセキュリティインテリジェンス リスト（1396 ページ）およびセキュリティインテリジェンスの設定 （1855 ページ）を参照してください。

  IPアドレスの場合、リストやフィードではなく、オプションでネットワークオブジェクトをこの目的に使用できます。詳細については、ネットワーク （1349ページ）を参照してください（URLの場合、他の方法よりもリストとフィードを使用することを強くお勧めします）。

- カスタムのブロックしないリストまたはフィード

特定のサイトまたはアドレスのセキュリティインテリジェンスブロックを無効にします。セキュリティインテリジェンスブロッキングのオーバーライド（1864ページ）を参照してください。

- グローバルブロックリスト（ネットワーク、URL、DNS ごとに 1 つ）

  イベントの確認中に、セキュリティインテリジェンスがそのソースからの今後のトラフィックを処理する場合は、イベントの IP アドレス、URL、またはドメインを該当するグローバルブロックリストにすぐに追加できます。グローバルおよびドメインのセキュリティインテリジェンスリスト （1387 ページ）を参照してください。

- グローバルブロックしないリスト（ネットワーク、URL、DNS ごとに 1 つ）

  イベントの確認中に、セキュリティインテリジェンスがそのソースからの今後のトラフィックをブロックしたくない場合は、イベントの IP アドレス、URL、またはドメインを該当するグローバルブロックしないリストにすぐに追加できます。「グローバルおよびドメインのセキュリティインテリジェンスリスト （1387 ページ）」を参照してください。

セキュリティ インテリジェンスの設定

各アクセス コントロール ポリシーには、セキュリティ インテリジェンス オプションがあります。ネットワークオブジェクト、URL オブジェクトとリスト、およびセキュリティ インテリジェンスフィードとリストをブロックリストまたはブロックしないリストに追加でき、これらはすべてセキュリティゾーンによって制約できます。アクセス コントロール ポリシーに DNS ポリシーを関連付け、ドメイン名をブロックリストまたはブロックしないリストに追加することもできます。

ブロックしないリストに含まれるオブジェクトの数とブロックリストに含まれるオブジェクトの数の合計が、125 個のネットワークオブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

始める前に

- ヒント：推奨される最小構成については、設定例：セキュリティインテリジェンスブロック （1862 ページ）も参照してください。
- すべてのオプションを選択できるようにするには、少なくとも 1 つの管理対象デバイスを Management Center に追加します。
- パッシブ展開の場合、またはモニター専用にセキュリティ インテリジェンス フィルタリングを設定する場合は、ロギングを有効にします。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Logging Connections with Security Intelligence」を参照してください。
- ドメインのセキュリティ インテリジェンス アクションを実行する DNS ポリシーを設定します。詳細については、「DNS ポリシー （1867 ページ）」を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 次の選択肢があります。

- [ネットワーク（Networks）] をクリックして、ネットワークオブジェクト（IP アドレス）を追加します。

  （注）
  セキュリティ インテリジェンス ポリシーで使用されるネットワークオブジェクトには、IPS ライセンスが必要です。

- [URL（URLs）] をクリックして、URL オブジェクトを追加します。

ステップ 3 ブロックしないリストまたはブロックリストに追加する [Available Objects] を検索します。次の選択肢があります。

- [名前または値で検索（Search by name or value）] フィールドに入力して、利用可能なオブジェクトを検索します。**リロード**（ ） または [クリア（Clear）]（ ） をクリックして、検索文字列をクリアします。

- 既存のリストまたはフィードがニーズを満たしていない場合は、[追加（Add）] ( ) をクリックし、[新規ネットワークリスト（New Network List）] または [新規 URL リスト（New URL List）] を選択し、セキュリティ インテリジェンス フィードの作成（1395 ページ）または新しいセキュリティ インテリジェンス リストの Secure Firewall Management Center へのアップロード（1397 ページ）の説明に従って続行します。

- 既存のオブジェクトがニーズを満たしていない場合は、[追加（Add）]( ) をクリックし、[新規ネットワークオブジェクト（New Network Object）] または [新規 URL オブジェクト（New URL Object）] を選択し、ネットワーク オブジェクトの作成（1351 ページ）の説明に従って続行します。

セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。

ステップ 4 追加する 1 つ以上の**利用可能なオブジェクト**を選択します。

ステップ 5 （オプション）[利用可能なゾーン（Available Zone）] を選択して、選択したオブジェクトをゾーンごとに制約します。

システムが提供するセキュリティ インテリジェンス リストをゾーンで制約することはできません。

（注）
SI リストの [すべて（Any）] ゾーンは、セキュリティゾーンの一部であるインターフェイスにのみ適用されます。ただし、例外として、セキュリティゾーンに関連付けられたインターフェイスがデバイスにない場合、[すべて（Any）] ゾーンはどのインターフェイスにも一致します。

たとえば、デバイスに 5 つのインターフェイスがあり、それらのどれもセキュリティゾーンに関連付けられていない場合、[すべて（Any）] ゾーンに割り当てられた SI リストは、デバイスのすべてのインターフェイスのトラフィックに対して検査されます。そのデバイスのセキュリティゾーンに 1 つのインターフェイスを追加すると、ゾーンが SI リストに対して [すべて（Any）] に設定されている他の 4 つのインターフェイスの SI 検査が効果的に削除されます。他の 4 つのインターフェイスをセキュリティゾーンに追加すると、それらは [すべて（Any）] ゾーンにアタッチされている SI リストによって評価されます。

ステップ 6 [Add to Do Not Block list] または [Add to Block list] をクリックするか、選択したオブジェクトをクリックしていずれかのリストにドラッグします。

ブロックしないリストまたはブロックリストからオブジェクトを削除するには、[削除（Delete）]（ ）をクリックします。複数のオブジェクトを削除するには、オブジェクトを選択し、右クリックして [Delete Selected] を選択します。

ステップ 7 （オプション）ブロックリストのオブジェクトをモニター専用に設定するには、[ブロックリスト（Block List）] にリストされている該当するオブジェクトを右クリックし、[モニター専用（ブロックしない）（Monitor-only (do not block)）] を選択します。

システムが提供するグローバル セキュリティ インテリジェンス リストをモニター専用に設定することはできません。

ステップ 8 [DNS ポリシー（DNS Policy）] ドロップダウン リストから DNS ポリシーを選択します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

セキュリティ インテリジェンス （1384 ページ）
Snort 再起動のシナリオ （162 ページ）

セキュリティ インテリジェンス オプション

アクセス制御ポリシーエディタの [セキュリティ インテリジェンス（Security Intelligence）] タブを使用して、ネットワーク（IP アドレス）と URL セキュリティ インテリジェンスを構成し、ドメインにセキュリティ インテリジェンスを設定した DNS ポリシーにアクセス制御ポリシーを関連付けます。

使用可能なオブジェクト

使用可能なオブジェクトは次のとおりです。

- システム提供のフィードによって入力されたセキュリティインテリジェンスのカテゴリ。

  詳細については、セキュリティインテリジェンス カテゴリ （1859ページ）を参照してください。

- システム提供のグローバルのブロックリストとブロックしないリスト。

  説明については、セキュリティインテリジェンス送信元（1854ページ）を参照してください。

- [オブジェクト（Object）] > [オブジェクト管理（Object Management）] > [セキュリティインテリジェンス（Security Intelligence）] で作成するセキュリティインテリジェンスのリストとフィード。

  説明については、セキュリティインテリジェンス送信元（1854ページ）を参照してください。

- [オブジェクト（Object）] > [オブジェクト管理（Object Management）] の各ページで設定されている、ネットワークと URL のオブジェクトとグループ。これらは、前の箇条書きのセキュリティ インテリジェンス オブジェクトとは異なります。

  ネットワークオブジェクトの詳細については、ネットワーク （1349ページ）を参照してください。（URL には、オブジェクトやグループではなく、セキュリティ インテリジェンスのリストまたはフィードを使用します。）

使用可能なゾーン

システムが提供するグローバルリストを除いて、ゾーンごとにセキュリティインテリジェンスフィルタリングを制約できます。

例：パフォーマンスを向上させるために、ターゲットの適用が必要になる場合があります。より具体的な例として、電子メールトラフィックを処理するセキュリティゾーンでのみ、スパムをブロックできます。

複数のゾーンでオブジェクトのセキュリティ インテリジェンス フィルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをブロックリストまたはブロックしないリストに追加する必要があります。

DNS ポリシー

セキュリティ インテリジェンスを使用して DNS トラフィックを照合するには、セキュリティインテリジェンス設定の DNS ポリシーを選択する必要があります。

ブロックリストまたはブロックしないリストの使用、または DNS リストまたはフィードに基づくトラフィックのモニタリングには、以下の条件もあります。

- DNS セキュリティ インテリジェンスのリストとフィードを設定します。セキュリティ インテリジェンス （1384 ページ）を参照してください。

- DNS ポリシーを作成します。詳細については、基本的な DNS ポリシーの作成（1871 ページ）を参照してください。
- DNS リストまたはフィードを参照する DNS ルールを設定します。詳細については、DNS ルールの作成と編集（1874 ページ）を参照してください。
- DNS ポリシーはアクセス コントロール ポリシーの一部として展開するため、両方のポリシーを関連付ける必要があります。詳細については、DNS ポリシーの導入（1883 ページ）を参照してください。

ブロックしないリスト

セキュリティインテリジェンスブロッキングのオーバーライド（1864ページ）を参照してください。

リスト内のすべてのオブジェクトを選択するには、オブジェクトを右クリックします。

ブロックリスト

設定例：セキュリティインテリジェンスブロック（1862ページ）およびこの章の他のトピックを参照してください。

ブロックリストのビジュアルインジケータの説明については、ブロックリストのアイコン（1861ページ）を参照してください。

リスト内のすべてのオブジェクトを選択するには、オブジェクトを右クリックします。

ログ

デフォルトで有効になっているセキュリティ インテリジェンス ロギングは、アクセス制御ポリシー対象のデバイスが処理するブロックされ、監視対象である接続はすべてロギングされます。ただし、システムはブロックしないリストの一致はロギングしません。ブロックしないリストの接続のロギングは、その接続の最終的な傾向によって異なります。ブロックリストの接続については、ブロックリストのオブジェクトをモニターのみに設定する前にロギングを有効にする必要があります。

ロギング設定を有効化、無効化、または表示するには、ブロックリストでオブジェクトを右クリックします。

関連トピック

グローバルおよびドメインのセキュリティインテリジェンスリスト （1387 ページ）
セキュリティ インテリジェンス リストとマルチテナンシー （1387 ページ）

セキュリティ インテリジェンス カテゴリ

セキュリティインテリジェンスのカテゴリは、セキュリティインテリジェンス（1384ページ）で説明されているシステム提供のフィードによって決定されます。

これらのカテゴリは、次の場所で使用されます。

- アクセス コントロール ポリシーの [Security Intelligence] タブの [Networks] サブタブ
- アクセス コントロール ポリシーの [Security Intelligence] タブの [Networks] タブの横にある [URLs] サブタブ
- [DNS rule configuration] ページの [DNS] タブの DNS ポリシー
- トラフィックが上記の場所のブロック設定またはモニター設定と一致する場合に生成されるイベント

（注） 組織で Secure Firewall Threat Intelligence Directorを使用している場合：イベントを表示すると、アクションが TID によって実行されたことを示すカテゴリ（`TID URL` ブロックなど）が表示されることがあります。

カテゴリはクラウドから Talos によって更新されます。このリストは、Firepower リリースとは無関係に変更される場合があります。

表 *86 : Cisco Talos Intelligence Group*（*Talos*） フィードカテゴリ

セキュリティインテリジェンス カテゴリ	説明
攻撃者	悪意のある発信アクティビティが知られているアクティブスキャナやホスト
Banking_fraud	電子バンキングに関連する詐欺行為を行うサイト
Bogon	Bogon ネットワークおよび割り当てられていない IP アドレス
Bots	バイナリ マルウェア ドロッパをホストするサイト
CnC	botnets 用のホスト C & C サーバを有するサイト
仮想通貨マイニング	プールと財布へのリモートアクセスを提供するホスト (cryptocurrency のマイニングのため)
Dga	C & C サーバのランデブー ポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム
Exploitkit	クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット
High_risk	セキュリティグラフからの OpenDNS 予測セキュリティアルゴリズムと一致するドメインとホスト名
Ioc	侵害の兆候（IOC）に関与していることが観察されているホスト
Link_sharing	権限のないファイルを共有する web サイト

セキュリティインテリジェンス カテゴリ	説明
悪意のある（Malicious）	他のより詳細な脅威カテゴリに必ずしも適合しているわけではない、悪意のある動作を示しているサイト
Malware	マルウェアバイナリまたはエクスプロイト キットを有するサイト
Newly_seen	最近登録されたドメイン、またはテレメトリでまだ認識されていないドメイン **注目** 現在、このカテゴリにはアクティブなフィードがなく、将来の使用のために予約されています。
Open_proxy	匿名 Web ブラウジングを許可するオープン プロキシ
Open_relay	スパム用に使用されることが既知のオープン メール リレー
Phishing	フィッシング ページを有するサイト
応答	悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL
Spam	スパムを送信することが知られているメール ホスト
スパイウェア	スパイウェアおよびアドウェアのアクティビティを含む、提供する、またはサポートすることが知られているサイト
Suspicious	疑いがあり、既知のマルウェアと同様の特性を持つようなファイル
Tor_exit_node	Torアノニマイザーネットワークの出口ノードサービスを提供することが知られているホスト

ブロックリストのアイコン

アクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブの [ブロックリスト（Block list）] に、次のビジュアルインジケータが表示される場合があります。

アイコンまたはビジュアルインジケータ	説明
Block ( )	オブジェクトはブロックするように設定されています。
モニター（）	オブジェクトは監視専用に設定されています。 セキュリティ インテリジェンス モニタリング（1863 ページ）を参照してください

アイコンまたはビジュアルインジケータ	説明
オブジェクトが取り消し線付きのテキストで表示される	同じオブジェクトがブロックをオーバーライドする [ブロックしない（Do Not Block）] リストにもあります。

設定例：セキュリティインテリジェンスブロック

システムにより定期的に更新されるセキュリティ インテリジェンス フィードによって検出可能なすべての脅威をブロックするようにアクセス コントロール ポリシーを設定します。

ブロックしないリストに含まれるオブジェクトの数とブロックリストに含まれるオブジェクトの数の合計が、125 個のネットワークオブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

始める前に

- すべてのオプションを選択できるようにするには、少なくとも 1 つの管理対象デバイスを Management Center に追加します。
- ドメインのセキュリティ インテリジェンスの脅威カテゴリをすべてブロックするように DNS ポリシーを設定します。詳細については、DNS ポリシー（1867 ページ）を参照してください。
- ブロックするエンティティのカスタムリストがある場合、または設定する予定がある場合は、各タイプ（URL、DNS、ネットワーク）のセキュリティ インテリジェンス オブジェクトを作成します。「セキュリティインテリジェンス（1384 ページ）」を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックします。

ステップ 2 新しいアクセス コントロール ポリシーを作成するか、既存のポリシーを編集します。

ステップ 3 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 4 [Networks] をクリックして、IP アドレスのブロック条件を追加します。

a) [Networks] リストを下にスクロールし、[Global] リストの下にリストされているすべての脅威カテゴリを選択します。

b) これらの脅威をブロックするセキュリティゾーンを選択します（該当する場合）。

c) [Add to Block List] をクリックします。
d) ブロックするアドレスを含むカスタムリストまたはフィードを作成している場合は、上記と同じ手順を使用してブロックリストに追加します。

ステップ 5 [URL] をクリックしてURLのブロック条件を追加し、[Networks] で実行した手順を繰り返します。

ステップ 6 [DNS ポリシー（DNS Policy）] ドロップダウン リストから DNS ポリシーを選択します。DNS ポリシーの概要 （1867 ページ） を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- これらの接続のロギングを有効にします。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Logging Connections with Security Intelligence」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。
- 保護を強化するには、悪意のあるURLをブロックするようにURLフィルタリングを設定します。「URL フィルタリング （1815 ページ）」を参照してください。

セキュリティ インテリジェンス モニタリング

モニタリングでは、セキュリティインテリジェンスによってブロックされるはずのトラフィックの接続イベントをログに記録しますが、トラフィックをブロックすることはありません。モニタリングは、特に次の場合に役立ちます。

- 実装する前のフィードテスト。

  たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニター専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

- パフォーマンスを最適化するためのパッシブ展開。

  パッシブに展開された管理対象デバイスはトラフィック フローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

（注） 構成されている場合、Secure Firewall Threat Intelligence Director は実行されるアクション（モニターまたはブロック）に影響を与える可能性があります。詳細については、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）を参照してください。

セキュリティ インテリジェンス モニタリングを設定するには：

設定例：セキュリティインテリジェンスブロック （1862 ページ）の手順に従ってセキュリティ インテリジェンス ブロックを設定したら、ブロックリストで該当する各オブジェクトを右クリックし、[モニターのみ（Monitor-only）] を選択します。システムが提供するセキュリティ インテリジェンス リストをモニター専用に設定することはできません。

セキュリティ インテリジェンス ブロッキングのオーバーライド

必要に応じて、ブロックしないリストを使用して、特定のドメイン、URL、または IP アドレスが、セキュリティ インテリジェンスのリストまたはフィードによってブロックされないようにすることができます。

たとえば、以下を行うことができます。

- 信頼できるセキュリティ インテリジェンス フィードで時折発生する誤検出ブロックをオーバーライドする
- レピュテーションに基づいて早期にブロックするのではなく、特定のトラフィックを詳細に検査する
- セキュリティ インテリジェンス ブロッキングからのゾーンに基づいて、該当しなければ制限されたトランザクションを免除する

  たとえば、不適切に分類された URL をブロックしないリストに追加した後、組織内でそれらの URL にアクセスする必要があるユーザーが使用しているセキュリティゾーンによりブロックしないリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネスニーズを持つユーザーだけが、ブロックしないリスト上の URL にアクセスできます。

（注） Do Not Block リストのエントリは、ブロックリストから除外されるだけです。セキュリティ インテリジェンス ポリシーを通過する接続には、アクセスコントロールルールが適用されます。したがって、Do Not Block リストのエントリは、その後、アクセスコントロールルールまたは侵入ポリシーによってブロックされる可能性があります。Do Not Block エントリは、常にブロックリストから除外する必要があります。

手順

ステップ 1 オプション 1：イベントの IP アドレス、URL、またはドメインを、グローバルのブロックしないリストに追加します。グローバルおよびドメインのセキュリティインテリジェンスリスト（1387 ページ）を参照してください。

ステップ 2 オプション 2：カスタムのセキュリティ インテリジェンスのリストまたはフィードを使用します。

a) カスタムのセキュリティ インテリジェンスのリストまたはフィードを作成します。カスタム セキュリティ インテリジェンス リスト（1396 ページ）またはセキュリティ インテリジェンス フィードの作成（1395 ページ）を参照してください。

b) IP アドレス（ネットワーク）と URL の場合：アクセス コントロール ポリシーを編集し、[セキュリティインテリジェンス（Security Intelligence）] タブをクリックしてから、[ネットワーク（Networks）] または [URL（URLs）] サブタブでカスタムのリストまたはフィードをクリックし、[ブロックしないリストに追加（Add to Do Not Block List）] をクリックします。

c) 変更を保存します。

d) ドメイン（DNS）の場合：セキュリティ インテリジェンス オプション（1857 ページ）トピックの「DNS ポリシー」セクションを参照してください。

e) 変更を展開します。

セキュリティ インテリジェンスのトラブルシューティング

セキュリティ インテリジェンスのトラブルシューティングについては、次の項を参照してください。

セキュリティインテリジェンスのカテゴリが使用可能なオプションのリストに表示されない

症状：アクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブで、[利用可能なオプション（Available Options）] の下にある [ネットワーク（Networks）] タブにセキュリティ インテリジェンス カテゴリ（CnC や Exploitkit など）が表示されない。

原因：

- Management Center に少なくとも 1 つの管理対象デバイスが追加されるまで、これらのカテゴリは表示されません。すべての TALOS フィードを取得するには、デバイスを追加する必要があります。

- URL フィルタリング機能は、セキュリティ インテリジェンス機能とは異なる一連のカテゴリを使用します。表示されると予想されるカテゴリは、URL フィルタリングカテゴリである可能性があります。URL フィルタリングカテゴリを表示するには、アクセスコントロールルールの [URL] タブを調べます。

セキュリティ インテリジェンス ブロック リストへの登録の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しいセキュリティインテリジェンスカテゴリ	すべて	すべて	Talos では、次の新しいセキュリティ インテリジェンス カテゴリを追加しました。 • banking_fraud • ioc • high_risk • link_sharing • malicious • newly_seen • spyware 新しいカテゴリに対応するようにアクセス制御と DNS ポリシーを更新し、定期的に将来の変更を確認する必要があります。 新規/変更されたページ：[セキュリティインテリジェンス（Security Intelligence）] タブの [ネットワーク（Network）] および [URL（URLs）] サブタブ、[DNSポリシー（DNS policies）] の [DNSルール（DNS rules）] サポートされているプラットフォーム： Firewall Management Center

第 43 章

DNS ポリシー

次のトピックでは、DNS ポリシーと DNS ルールについて、および管理対象デバイスに DNS ポリシーを導入する方法について説明します。

- DNS ポリシーの概要 （1867 ページ）
- Cisco Umbrella DNS ポリシー （1868 ページ）
- DNS ポリシーの構成要素 （1869 ページ）
- DNS ポリシーのライセンス要件 （1870 ページ）
- DNS ポリシーの要件と前提条件 （1870 ページ）
- DNS および Cisco Umbrella DNS ポリシーの管理 （1871 ページ）
- DNS ルール （1873 ページ）
- DNS ルールの作成方法 （1879 ページ）
- DNS ポリシーの導入 （1883 ページ）
- Cisco Umbrella DNS ポリシー （1883 ページ）

DNS ポリシーの概要

DNS ベースのセキュリティ インテリジェンスにより、セキュリティ インテリジェンス ブロックリストを使用して、クライアントが要求したドメイン名に基づいてトラフィックをブロックできるようになります。シスコが提供するドメイン名のインテリジェンスを使用して、トラフィックをフィルタリングできます。また、環境に合わせて、ドメイン名のカスタムリストやフィードを設定することも可能です。

DNS ポリシーのブロックリストに登録されたトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません（侵入、エクスプロイト、マルウェアなどについてだけでなくネットワーク検出についても）。セキュリティ インテリジェンス ブロックしないリストを使用してブロックリストより優先させて、アクセスコントロールルールによる評価を強制することができます。また、セキュリティインテリジェンスフィルタリングに「モニター専用」設定を使用でき、パッシブ展開環境ではこの設定が推奨されます。この設定では、ブロックリストによってブロックされたであろう接続をシステムが分析できるだけでなく、ブロックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

（注） 期限切れのため、またはクライアントの DNS キャッシュやローカル DNS サーバーのキャッシュがクリアされているか、期限切れであるために、DNS サーバーでドメイン キャッシュが削除されない場合に、DNS ベースのセキュリティ インテリジェンスが意図したとおりに機能しないことがあります。

DNS ポリシーおよび関連付けられた DNS ルールを使用して DNS ベースのセキュリティ インテリジェンスを設定します。デバイスにこれを展開するには、アクセス コントロール ポリシーに DNS ポリシーを関連付けてから管理対象デバイスに設定を展開する必要があります。

Cisco Umbrella DNS ポリシー

管理センターの Cisco Umbrella DNS 接続は、DNS クエリを Cisco Umbrella にリダイレクトするのに役立ちます。これにより、Cisco Umbrella で要求を検証し、ドメイン名に基づき要求を許可またはブロックし、要求に DNS ベースのセキュリティポリシーを適用できます。Cisco Umbrella を使用する場合、Cisco Umbrella 接続を設定して（[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）] > [Cisco Umbrella 接続（Cisco Umbrella Connection）]）DNS クエリを Cisco Umbrella へリダイレクトできます。

Umbrella Connector は、システムの DNS インスペクションの一部です。既存の DNS インスペクション ポリシーマップにより、DNS インスペクションの設定に基づいて要求をブロックするか、または、要求をドロップすることに決定した場合、その要求は Cisco Umbrella へ転送されません。これにより、次の 2 系統の保護が可能になります。

- ローカル DNS インスペクションポリシー
- Cisco Umbrella のクラウドベースのポリシー

DNS ルックアップ要求を Cisco Umbrella へリダイレクトすると、Umbrella Connector は EDNS（DNS の拡張機能）レコードを追加します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。クラウドベースのポリシーでこれらの条件を使用することで、FQDN のレピュテーションだけでなくアクセスを制御することができます。また、DNSCrypt を使用して DNS 要求を暗号化し、ユーザー名と内部の IP アドレスのプライバシーを確保することもできます。

Management Center から Cisco Umbrella に DNS 要求をリダイレクトするには、次の手順を実行します。

1. Cisco Umbrella の接続設定を設定する
2. Cisco Umbrella DNS ポリシーを作成および設定します。
3. Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付けます。
4. 変更を展開します。

管理センターで Cisco Umbrella DNS Connector を設定する方法の詳細については、「Cisco Secure Firewall Management Center 向け Cisco Umbrella DNS Connector の設定」を参照してください。

DNS ポリシーの構成要素

DNS ポリシーにより、ブロックリストを使用してドメイン名に基づいて接続をブロックしたり、ブロックしないリストを使用してそのような接続をこのタイプのブロックから除外したりできます。次のリストに、DNS ポリシーの作成後に変更可能な設定を示します。

名前（Name）と説明（Description）

各 DNS ポリシーには固有の名前が必要です。説明は任意です。

ルール（Rule）

ルールは、ドメイン名に基づいてネットワーク トラフィックを処理する詳細な方法を提供します。DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、トラフィックを DNS ルールと上から順に照合します。

DNS ポリシーを作成すると、システムはこれを DNS ルールのデフォルトのグローバルブロックしないリストおよび DNS ルールのデフォルトのグローバルブロックリストに入力します。両方のルールは、それぞれのカテゴリで先頭の位置に固定されます。これらのルールは変更できませんが無効にすることはできます。

（注） Firewall Management Center でマルチテナンシーが有効になっている場合、システムは先祖ドメインと子孫ドメインを含むドメインの階層に編成されます。これらのドメインは、DNS 管理で使用されるドメイン名とは別になります。

子孫のリストには、システムのサブドメインユーザーのブロックリストまたはブロックしないリストに載っているドメインが含まれます。先祖ドメインから、子孫のリストの内容を表示することはできません。サブドメインユーザーがドメインをブロックリストまたはブロックしないリストに追加しないようにするには、次の手順を実行します。

- 子孫のリストのルールを無効にします。
- アクセス コントロール ポリシーの継承設定を使用してセキュリティ インテリジェンスを適用します。

ルールはシステムにより次の順序で評価されます。

- DNS ルールのグローバル ブロックしないリスト（有効になっている場合）
- 子孫 DNS ブロックしないリストルール（有効な場合）
- [ブロックしない（Do Not Block）] アクションを使用したルール
- DNS ルールのグローバルブロックリスト（有効になっている場合）
- 子孫 DNS ブロックリストルール（有効な場合）

- [ブロックしない（Do Not Block）] 以外のアクションを使用したルール

通常、システムによるDNベースのネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。トラフィックに一致する DNS ルールがない場合、システムは、関連付けられたアクセス コントロール ポリシー ルールに基づいてトラフィックの評価を続行します。DNS ルール条件は単純または複雑のどちらでも構いません。

DNS ポリシーのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

DNS ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

重要 トラフィックの DNS 検証を成功させるには、デバイスにネットワーク検出ポリシーを適用する必要があります。

DNS および Cisco Umbrella DNS ポリシーの管理

[DNSポリシー（DNS Policy）]ページ（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[DNS]**）を使用して、DNS および Cisco Umbrella DNS のカスタムポリシーを管理します。

ユーザーが作成するカスタムポリシーに加えて、デフォルトの DNS ポリシーとデフォルトの Cisco Umbrella DNS ポリシーが用意されています。デフォルトの DNS ポリシーでは、デフォルトのブロックリストとブロックしないリストが使用されます。このシステム付属のカスタムポリシーは編集して使用できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[DNS]**を選択します。

ステップ 2 DNS ポリシーを以下のように管理します。

- 比較：DNS ポリシーを比較するには、[ポリシーの比較（Compare Policies）]をクリックして、ポリシーの比較 （190 ページ）で説明する手順を実行します。
- コピー：DNS ポリシーをコピーするには、[コピー（Copy）]（）をクリックして、DNS ポリシーの編集 （1872 ページ）で説明する手順を実行します。
- 作成：新しい Cisco Umbrella DNS ポリシーを作成するには、**[新しいポリシー（New Policy）]** > **[Cisco Umbrella DNSポリシー（Umbrella DNS Policy）]**をクリックし、Cisco Umbrella DNS ポリシーを作成する （1887 ページ）の説明に従って続行します。
- 削除：DNS または Cisco Umbrella DNS ポリシーを削除するには、[削除（Delete）]（）をクリックし、ポリシーの削除を確認します。
- 編集：既存の DNS ポリシーを変更するには、[編集（Edit）]（）をクリックし、DNS ポリシーの編集 （1872 ページ）で説明する手順を実行します。既存の Cisco Umbrella DNS ポリシーを変更するには、[編集（Edit）]（）をクリックし、Cisco Umbrella DNS ポリシーとルールの編集 （1887 ページ）の説明に従って続行します。

基本的な DNS ポリシーの作成

新しい DNS ポリシーを作成した場合、デフォルト設定が含まれています。その後、ポリシーを編集して動作をカスタマイズする必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[DNS]**を選択します。

ステップ 2 **[DNSポリシーの追加（Add DNS Policy）]** > **[DNSポリシー（DNS Policy）]**をクリックします。

ステップ 3 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

ポリシーを設定します。「DNS ポリシーの編集 （1872 ページ）」を参照してください。

DNS ポリシーの編集

DNS ポリシーを同時に編集できるのは 1 ユーザのみであり、使用できるのは単一のブラウザ ウィンドウのみです。複数のユーザが同じポリシーを保存しようとすると、最初に保存された変更のセットのみが保持されます。

セッションのプライバシーを保護するために、ポリシー エディタで活動が行われずに 30 分が経過すると、警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[DNS]**を選択します。

ステップ 2 編集する DNS ポリシーの横にある[編集（Edit）]（✎）をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 DNS ポリシーを編集します。

- 名前と説明：名前または説明を変更するには、フィールドをクリックして新しい情報を入力します。
- ルール：DNS ルールを追加、分類、有効化、無効化、または管理する場合は、[ルール（Rules）]をクリックして、DNS ルールの作成と編集 （1874 ページ）の説明に従って続行します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 必要に応じて、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Logging Connections with Security Intelligence*」の説明に従ってい新しいポリシーをさらに設定します。
- 設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

DNS ルール

DNS ルールは、ホストが要求するドメイン名に基づいてトラフィックを処理します。セキュリティ インテリジェンスの一部として、この評価は、トラフィックの復号の後、アクセス コントロール評価の前に適用されます。

システムは指定した順序でトラフィックを DNS ルールと照合します。ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。

各 DNS ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールが処理する特定のトラフィックを指定します。DNS ルールには、DNS フィードまたはリスト条件が含まれている必要があり、セキュリティゾーン、ネットワーク、または VLAN によってトラフィックと照合することができます。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。

- **[ブロックしない（Do Not Block）]** アクションのトラフィックが許可され、さらにアクセス制御インスペクションを受けます。
- モニターされるトラフィックは、残りの DNS ブロックリストのルールによりさらに評価されます。トラフィックが DNS ブロックリストルールに一致しない場合、アクセスコントロールルールによりインスペクションを受けます。そのトラフィックのセキュリティ インテリジェンス イベントは、システムにより記録されます。
- ブロックリストのトラフィックは、それ以上のインスペクションは行われずにドロップされます。[Domain Not Found] 応答を返したり、DNS クエリをシンクホール サーバにリダイレクトしたりすることもできます。

関連トピック

セキュリティ インテリジェンスについて （1851 ページ）

DNS ルールの作成と編集

DNS ポリシーでは、ブロックリストルールおよびブロックしないリストルールに合計 32767 個まで DNS リストを追加できます。つまり、DNS ポリシーのリストの数が 32767 を超えることはできません。

手順

ステップ 1 DNS ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[DNS ルールの追加（Add DNS Rule）] をクリックします。
- 既存のルールを編集するには、[編集（Edit）]（） をクリックします。

ステップ 2 [Name] を入力します。

ステップ 3 ルール コンポーネントを設定するか、またはデフォルトを受け入れます。

- [アクション（Action）]：ルールの [アクション（Action）] を選択します。DNS ルールのアクション （1876 ページ）を参照してください。
- [条件（Conditions）]：ルールの条件を設定します。DNS ルールの条件 （1877 ページ）を参照してください。
- [有効（Enabled）]：ルールを有効にするかどうかを指定します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

DNS ルールの管理

DNS ポリシー エディタの [ルール（Rules）] タブでは、ポリシー内の DNS ルールの追加、編集、移動、有効化、無効化、削除、その他の管理が行えます。

各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。その他のアイコンは、[警告（warning）]（）、**エラー**（）、および**その他の重要情報**（）を表します。無効なルールはグレー表示され、ルール名の下に [無効（disabled）] というマークが付きます。

DNS ルールの有効化と無効化

作成した DNS ルールは、デフォルトで有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。DNS ポリシーのルール リストを表示すると、無効なルールはグレー

表示されますが、変更は可能です。また、DNS ルール エディタを使用して DNS ルールを有効または無効にできることに注意してください。

手順

ステップ 1 DNS ポリシー エディタで、ルールを右クリックしてルール状態を選択します。
ステップ 2 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

DNS ルールの評価順序

DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、トラフィックを DNS ルールと上から順に照合します。ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。

- モニタールールでは、システムはまずトラフィックを記録し、その後、優先順位の低い DNS ブロックリストルールに対してトラフィックの評価を続行します。
- モニタールール以外では、トラフィックがルールに一致した後、システムは優先順位の低い追加の DNS ルールに対してトラフィックの評価は続行**しません**。

ルールの順序については、以下の点い注意してください。

- DNS のグローバルブロックしないリストは常に最初に使用され、他のすべてのルールに優先します。
- [ブロックしないリスト（Do-Not-Block List）] セクションは [ブロックリスト（Block List）] セクションに優先します。ブロックしないリストのルールは常に他のルールに優先します。
- DNS のグローバルブロックリストは [ブロックリスト（Block List）] セクション内で常に最初に使用され、他のすべてのモニターのルールやブロックリストのルールに優先します。
- [ブロックリスト（Block List）] セクションには、モニターのルールとブロックリストのルールが含まれます。
- 初めて DNS ルールを作成したときは、[ブロックしない（Do Not Block）] アクションを割り当てるとそれはシステムにより [ブロックしないリスト（Do-Not-Block List）] セクションの最後に配置され、他のアクションを割り当てると [ブロックリスト（Block List）] セクションの最後に配置されます。

ルールをドラッグ アンド ドロップして、これらの順序を変更できます。

DNS ルールのアクション

すべての DNS ルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- 処理：第一に、ルールアクションは、ブロックリストまたはブロックしないリストに基づいて、システムがルールの条件に一致するトラフィックをブロックするか、ブロックしないか、またはモニターするかを制御します
- ロギング：ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）を参照してください。

[ブロックしない（Do Not Block）] アクション

[ブロックしない（Do Not Block）] アクションでは、トラフィックは検査の次のフェーズであるアクセス制御ルールに渡されます。

システムは [ブロックしない（Do Not Block）] リストの一致をログに記録しません。これらの接続のロギングは、その接続の最終的な傾向によって異なります。

モニタ アクション

[モニター（Monitor）] アクションは接続ロギングを強制するように設計されています。つまり、一致するトラフィックが即時に許可またはブロックされることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタールール以外の一致する最初の DNS ルールが、システムがトラフィックをブロックするかどうかを決定します。一致する追加のルールがなければ、トラフィックはアクセス コントロール評価の対象となります。

DNS ポリシーによってモニターされる接続については、システムは、接続終了セキュリティインテリジェンスと接続イベントを Firewall Management Center データベースにロギングします。

ブロックアクション

これらのアクションは、どんな種類のインスペクションもなく、トラフィックをブロックします。

- [ドロップ（Drop）] アクションはトラフィックをドロップします。
- [検出されないドメイン（Domain Not Found）] アクションは、存在しないインターネットドメインの応答を DNS クエリに返し、これによりクライアントが DNS 要求を解決することを防ぎます。

- [シンクホール（Sinkhole）] アクションは、応答内のシンクホールオブジェクトの IPv4 または IPv6 アドレスを DNS クエリに返します（A および AAAA レコードのみ）。シンクホール サーバーは、IP アドレスへの後続の接続をロギングするか、またはロギングしてブロックすることができます。[シンクホール（Sinkhole）] アクションを設定する場合、シンクホール オブジェクトも設定する必要があります。

[ドロップ（Drop）] または [検出されないドメイン（Domain Not Found）] のアクションに基づいてブロックされた接続の場合は、システムが接続開始のセキュリティ インテリジェンス イベントと接続イベントをログに記録します。ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続終了イベントはありません。

[Sinkhole] のアクションに基づいてブロックされる接続の場合、ロギングはシンクホールオブジェクトの設定に応じて決まります。シンクホール オブジェクトを、シンクホール接続をロギングのみするよう設定している場合、システムは、後続の接続の接続終了イベントをロギングします。シンクホール オブジェクトを、シンクホール接続をロギングしてブロックするよう設定している場合、システムは、後続の接続の接続開始イベントをロギングし、その後、その接続をブロックします。

DNS ルールの条件

DNS ルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は単純または複雑のどちらでも構いません。DNS ルール内の DNS フィードまたはリスト条件を定義する必要があります。また、必要に応じてセキュリティ ゾーン、ネットワーク、または VLAN によってトラフィックを制御できます。

DNS ルールに条件を追加するときは、以下に留意してください。

- ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。
- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、DNS フィードまたはリスト条件およびネットワーク条件を含み、VLAN タグ条件を含まないルールは、セッション中の VLAN タグに関係なく、ドメイン名と送信元または宛先に基づいてトラフィックを評価します。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、最大で 50 DNS のリストとフィードに基づいてトラフィックをブロックする単一のルールを使用できます。

以降のトピックでは DNS ルールの条件についてさらに詳しく説明します。

セキュリティゾーンルール条件

セキュリティゾーンはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することで、トラフィックフローを管理、分類、および復号しやすくします。

セキュリティゾーンは、トラフィックをその送信元と宛先のセキュリティゾーンで制御または復号します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ヒント　ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

ネットワークルール条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注）　アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

VLAN タグルール条件

（注） アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

DNS ポリシー ルールの条件

DNS リスト、フィード、またはカテゴリにクライアントにより要求されたドメイン名が含まれる場合、DNS ルール内の DNS 条件によりトラフィックを制御できます。DNS ルール内で DNS 条件を定義する必要があります。

グローバルまたはカスタムのブロックリストまたはブロックしないリストを DNS 条件に追加するかどうかにかかわらず、システムは設定されたルールアクションをトラフィックに適用します。たとえばルールにグローバルブロックしないリストを追加し、[ドロップ（Drop）]アクションを設定すると、システムは検査の次のフェーズに渡すことが許可されている必要があるすべてのトラフィックをブロックします。

DNS ルールの作成方法

次のトピックでは、DNS ルールの作成方法について説明します。

DNS およびセキュリティ ゾーンに基づくトラフィックの制御

DNS ルール内のゾーン条件によって、その送信元セキュリティゾーン別にトラフィックを制御することができます。セキュリティゾーンは、複数のデバイス間に配置されている場合がある 1 つ以上のインターフェイスのグループです。

手順

ステップ 1 DNS ルールエディタで、[ゾーン（Zones）] をクリックします。

ステップ 2 [Available Zones] から追加するゾーンを見つけて選択します。追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 セキュリティ ゾーンをクリックするか、または右クリックして、[Select All] を選択します。

ステップ 4 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 **[DNS]** タブをクリックし、制御している DNS 名を含むリストまたはフィードを追加します。詳細については、DNS リストまたはフィードに基づくトラフィックの制御 （1882 ページ）を参照してください。

ステップ 6 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

DNS およびネットワークに基づくトラフィックの制御

DNS ルール内のネットワーク条件によって、その送信元 IP アドレス別にトラフィックを制御することができます。制御するトラフィックの送信元 IP アドレスを明示的に指定できます。

手順

ステップ 1 DNS ルールエディタで、[ネットワーク（Networks）] をクリックします。

ステップ 2 [利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけて選択します。

- ネットワークオブジェクト（後で条件に追加可能）をその場で追加するには、[利用可能なネットワーク（Available Networks）] リストの上にある[追加（Add）] (＋)をクリックし、ネットワーク オブジェクトの作成 （1351 ページ）の説明に従って続行します。
- 追加するネットワーク オブジェクトを検索するには、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプ

トをクリックし、オブジェクトのいずれかのコンポーネントのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する送信元 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク（Source Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

ステップ 5 **[DNS]** タブをクリックし、制御している DNS 名を含むリストまたはフィードを追加します。詳細については、DNS リストまたはフィードに基づくトラフィックの制御 （1882 ページ）を参照してください。

ステップ 6 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

DNS および VLAN に基づくトラフィックの制御

DNS ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。

VLAN ベースの DNS ルール条件を作成するときは、VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

手順

ステップ 1 DNS ルールエディタで、[VLANタグ（VLAN Tags）] を選択します。

ステップ 2 [利用可能な VLAN タグ（Available VLAN Tags）] で、追加する VLAN を選択します。

- VLAN タグオブジェクトをここで追加するには（後で条件に追加できます）、[利用可能なVLANタグ（Available VLAN Tags）] リストの上にある[追加（Add）] (＋)をクリックし、VLAN タグ オブジェクトの作成 （1424 ページ）の説明に従って進みます。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する VLAN タグを追加します。[Selected VLAN Tags] リストの下にある [Enter a VLAN Tag] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[Add] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

ステップ 5 **[DNS]** タブをクリックし、制御している DNS 名を含むリストまたはフィードを追加します。詳細については、DNS リストまたはフィードに基づくトラフィックの制御（1882 ページ）を参照してください。

ステップ 6 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

DNS リストまたはフィードに基づくトラフィックの制御

手順

ステップ 1 DNS ルールエディタで、[DNS] をクリックします。

ステップ 2 次のように、[DNS リストおよびフィード（DNS Lists and Feeds）] から追加する DNS リストおよびフィードを検索して選択します。

- DNS リストまたはフィード（後で条件に追加可能）をその場で追加するには、[DNSリストおよびフィード（DNS Lists and Feeds）] リストの上にある [追加（Add）] (＋) をクリックし、セキュリティ インテリジェンス フィードの作成（1395 ページ）の説明に従って続行します。
- 追加する DNS リスト、フィード、またはカテゴリを検索するには、[DNS リストおよびフィード（DNS Lists and Feeds）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。
- システム提供の脅威カテゴリの説明については、セキュリティ インテリジェンス カテゴリ （1859 ページ）を参照してください。

ステップ 3 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

DNS ポリシーの導入

DNS のポリシー設定の更新を終了した後に、アクセス コントロール設定の一部としてこれを展開する必要があります。

- セキュリティインテリジェンスの設定（1855ページ）で説明されているように、DNS ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

Cisco Umbrella DNS ポリシー

管理センターの Cisco Umbrella DNS 接続は、DNS クエリを Cisco Umbrella にリダイレクトするのに役立ちます。これにより、Cisco Umbrella で要求を検証し、ドメイン名に基づき要求を許可またはブロックし、要求に DNS ベースのセキュリティポリシーを適用できます。Cisco Umbrella を使用する場合、Cisco Umbrella 接続を設定して（[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）] > [Cisco Umbrella 接続（Cisco Umbrella Connection）]）DNS クエリを Cisco Umbrella へリダイレクトできます。

Umbrella Connector は、システムの DNS インスペクションの一部です。既存の DNS インスペクション ポリシーマップにより、DNS インスペクションの設定に基づいて要求をブロックするか、または、要求をドロップすることに決定した場合、その要求は Cisco Umbrella へ転送されません。これにより、次の 2 系統の保護が可能になります。

- ローカル DNS インスペクションポリシー
- Cisco Umbrella のクラウドベースのポリシー

DNS ルックアップ要求を Cisco Umbrella へリダイレクトすると、Umbrella Connector は EDNS（DNS の拡張機能）レコードを追加します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。クラウドベースのポリシーでこれらの条件を使用することで、FQDN のレピュテーションだけでなくアクセスを制御することができます。また、DNSCrypt を使用して DNS 要求を暗号化し、ユーザー名と内部の IP アドレスのプライバシーを確保することもできます。

Management Center から Cisco Umbrella に DNS 要求をリダイレクトするには、次の手順を実行します。

1. Cisco Umbrella の接続設定を設定する
2. Cisco Umbrella DNS ポリシーを作成および設定します。
3. Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付けます。
4. 変更を展開します。

管理センターで Cisco Umbrella DNS Connector を設定する方法の詳細については、「Cisco Secure Firewall Management Center 向け Cisco Umbrella DNS Connector の設定」を参照してください。

DNS 要求を Cisco Umbrella にリダイレクトする方法

ここでは、Firewall Management Center を使用してデバイスから Cisco Umbrella に DNS 要求をリダイレクトする手順について説明します。

手順	操作手順	詳細
1	前提条件を満たしていることを確認する	Cisco Umbrella DNS コネクタを設定するための前提条件 （1884 ページ）
2	Cisco Umbrella の接続設定を設定する	Cisco Umbrella の接続設定の設定 （1885 ページ）
3	Cisco Umbrella DNS ポリシーを作成する	Cisco Umbrella DNS ポリシーを作成する （1887 ページ）
4	Cisco Umbrella DNS ポリシーを設定する	Cisco Umbrella DNS ポリシーとルールの編集 （1887 ページ）
5	Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付ける	Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付ける （1888 ページ）

Cisco Umbrella DNS コネクタを設定するための前提条件

表 *87*：サポートされる最小プラットフォーム

製品	バージョン
Secure Firewall Threat Defense	6.6 以降
Secure Firewall Management Center	7.2 以降

- https://umbrella.cisco.com で Cisco Umbrella のアカウントを確立し、http://login.umbrella.com で Umbrella にログインします。
- Cisco Umbrella サーバーから Firewall Management Center に CA 証明書をインポートします。Cisco Umbrella で、[展開（Deployments）] > [構成（Configuration）] > [ルート証明書（Root Certificate）] を選択し、証明書をダウンロードします。

  Cisco Umbrella 登録サーバーとの間で HTTPS 接続を確立するために、ルート証明書をインポートする必要があります。証明書は、SSL サーバー検証のために信頼される必要があります。これは、Firewall Management Center ではデフォルトのオプションではありません。Firewall Management Center でデバイスの以下の証明書をコピーして貼り付けます（[デバイス（Device）] > [証明書（Certificates）]）。

MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
SaZMkE4f97Q=

Management Center に証明書を追加する場合は、[CAのみ（CA Only）] チェックボックスをオンにします。

- デバイスに証明書をインストールします。
- Cisco Umbrella から次のデータを取得します。
  - 組織 ID
  - ネットワークデバイスキー
  - ネットワーク デバイス シークレット
  - レガシー ネットワーク デバイス トークン
- Firewall Management Center がインターネットに接続していることを確認します。
- Firewall Management Center で、輸出規制機能オプションのある基本ライセンスが有効になっていることを確認します。
- api.opendns.com を解決するように DNS サーバーが設定されていることを確認します。
- Firewall Management Center がポリシー構成の management.api.umbrella.com を解決できることを確認します。
- api.opendns.com への Firewall Threat Defense ルートを設定します。

Cisco Umbrella の接続設定の設定

Cisco Umbrella の接続設定では、Cisco Umbrella にデバイスを登録するために必要なトークンを定義します。

始める前に

Cisco Umbrella https://umbrella.cisco.com でアカウントを確立し、https://dashboard.umbrella.com で Cisco Umbrella にログインし、Cisco Umbrella への接続を確立するために必要な情報を取得します。

手順

ステップ 1 **[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）] > [Cisco Umbrella接続（Cisco Umbrella Connection）]**を選択します。

ステップ 2 次の詳細を取得し、[一般（General）] 設定に追加します。

- [組織ID（Organization ID）]：Cisco Umbrella で組織を識別する一意の番号。すべての Umbrella 組織は、Umbrella の個別のインスタンスであり、独自のダッシュボードを持ちます。組織は名前と組織 ID によって識別されます。
- [ネットワークデバイスキー（Network Device Key）]：Cisco Umbrella から Umbrella ポリシーを取得するためのキー。
- [ネットワークデバイスシークレット（Network Device Secret）]：Cisco Umbrella から Umbrella ポリシーを取得するためのシークレット。
- [レガシーネットワークデバイストークン（Legacy Network Device Token）]：Cisco Umbrella レガシー ネットワーク デバイス API トークンは、Cisco Umbrella ダッシュボードを通じて発行されます。Cisco Umbrella では、ネットワークデバイスを登録するために API トークンが必要です。

ステップ 3 [詳細設定（Advanced）] から次のオプションを設定できます。

- [DNSCrypt公開キー（DNSCrypt Public Key）]：DNSCrypt は、エンドポイントと DNS サーバー間の DNS クエリを認証および暗号化します。DNScrypt を有効にするには、証明書の検証に DNScrypt の公開キーを設定できます。このキーは、32 バイトの 16 進数値で、B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79 に事前設定されています。これは、Umbrella エニーキャストサーバーの公開キーです。
- [管理キー（Management Key）]：VPN ポリシーのために Umbrella クラウドからデータセンターの詳細を取得するためのキー。
- [管理シークレット（Management Secret）]：VPN のために Umbrella クラウドからデータセンターを取得するために使用されるシークレット。

ステップ 4 [接続のテスト（Test Connection）] をクリックします。Cisco Umbrella Cloud が Firewall Management Center から到達可能かどうかをテストします。必要な組織 ID とネットワークデバイスの詳細を指定すると、Cisco Umbrella 接続が作成されます。

ステップ 5 [保存（Save）] をクリックします。

Cisco Umbrella DNS ポリシーを作成する

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[DNS]**を選択します。

ステップ 2 **[DNSポリシーの追加（Add DNS Policy）]** > **[Umbrella DNSポリシー（Umbrella DNS Policy）]** をクリックします。

ステップ 3 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

ポリシーを設定します。「Cisco Umbrella DNS ポリシーとルールの編集 （1887 ページ）」を参照してください。

Cisco Umbrella DNS ポリシーとルールの編集

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[DNS]**を選択します。

ステップ 2 [DNSポリシー（DNS Policy）] ページで、編集する Cisco Umbrella DNS ポリシーを選択してクリックします。[編集（Edit）]（✎）

Cisco Umbrella 保護ポリシーの更新

Cisco Umbrella から最新の Cisco Umbrella 保護ポリシーを取得するには、[Cisco Umbrella保護ポリシーの最終更新日（Umbrella Protection Policy Last Updated）] の横にある [更新（Refresh）] アイコンをクリックします。

Management Center の Cisco Umbrella 接続設定を設定または変更するには、**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[クラウドサービス（Cloud Services）]** > **[Cisco Umbrella 接続（Cisco Umbrella Connection）]** に移動します。

ステップ 3 Cisco Umbrella DNS ポリシーエディタで、Cisco Umbrella DNS ルールを選択して [編集（Edit）]（✎） をクリックします。

ステップ 4 以下のルール コンポーネントを設定するか、デフォルトを受け入れます。

- [Cisco Umbrella保護ポリシー（Umbrella Protection Policy）]：デバイスに適用する Cisco Umbrella ポリシーの名前を指定します。

- [バイパスドメイン（Bypass Domain）]：Cisco Umbrella をバイパスして、代わりに設定済みの DNS サーバーに直接移動させるための DNS 要求のローカルドメインの名前を指定します。

  たとえば、すべての内部接続が許可されることを想定して、内部 DNS サーバーで組織のドメイン名のすべての名前を解決できます。

- [Dnscrypt]：DNSCrypt を有効にしてデバイスと Cisco Umbrella 間の接続を暗号化します。

  DNSCrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。DNSCrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラスマップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。

- [アイドルタイムアウト（Idle Timeout）]：アイドルタイムアウトを設定します。その時間が経過するまでサーバーからの応答がない場合、クライアントから Umbrella サーバーへの接続は削除されます。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付けます。詳細については、「Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付ける （1888 ページ）」を参照してください。

Cisco Umbrella DNS ポリシーとアクセス コントロール ポリシーを関連付ける

Cisco Umbrella DNS ポリシーは、デバイスに展開する前に、アクセス コントロール ポリシーに関連付ける必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス制御（Access Control）] に移動し、編集するアクセスポリシーを選択します。

ステップ 2 [セキュリティインテリジェンス（Security Intelligence）] を選択します。

ステップ 3 [Cisco Umbrella DNSポリシー（Umbrella DNS Policy）] ドロップダウンリストから、Cisco Umbrella DNS ポリシーを選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

第 44 章

プレフィルタリングおよびプレフィルタポリシー

- プレフィルタリングについて （1891 ページ）
- Fastpath プレフィルタリングのベストプラクティス （1897 ページ）
- カプセル化されたトラフィックの処理のベストプラクティス （1898 ページ）
- プレフィルタポリシーの要件と前提条件 （1899 ページ）
- プレフィルタリングの設定 （1900 ページ）
- トンネル ゾーンおよびプレフィルタリング （1907 ページ）
- プレフィルタルールのアクセス コントロール ポリシーへの移動 （1912 ページ）
- プレフィルタ ポリシーのヒット カウント （1914 ページ）
- 大規模フローのオフロード （1914 ページ）
- プレフィルタリングの履歴 （1918 ページ）

プレフィルタリングについて

プレフィルタはアクセス制御の最初のフェーズで、システムがより大きいリソース消費の評価を実行する前に行われます。プレフィルタリングはシンプルかつ高速で、初期に実行されます。プレフィルタリングでは、限定された外部ヘッダーを基準にしてトラフィックを迅速に処理します。内部ヘッダーを使用し、より堅牢なインスペクション機能を備えた後続の評価とこのプレフィルタリングを比較します。

次の目的でプレフィルタリングを設定します。

- パフォーマンスの向上：インスペクションを必要としないトラフィックの除外は、早ければ早いほど適切です。特定のタイプのプレーン テキストをファストパスまたはブロックし、カプセル化された接続を検査することなく外側のカプセル化ヘッダーに基づいてトンネルをパススルーします。早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。
- カプセル化トラフィックに合わせたディープインスペクションの調整：同じ検査基準を使用してカプセル化接続を後で処理できるように、特定のタイプのトンネルを再区分できま

す。アクセス制御はプレフィルタ後に内側のヘッダーを使用するため、再区分は必須です。

プレフィルタ ポリシーについて

プレフィルタリングは、ポリシーベースの機能です。デバイスに割り当てるには、そのデバイスに割り当てられているアクセス コントロール ポリシーに割り当てます。

ポリシー コンポーネント：ルールとデフォルト アクション

プレフィルタ ポリシーでは、トンネル ルール、プレフィルタ ルール、デフォルト アクションに基づいてネットワーク トラフィックを処理します。

- トンネル ルールとプレフィルタ ルール：最初にプレフィルタ ポリシーのルールが、指定した順序でトラフィックを処理します。トンネル ルールは指定のトンネルのみを照合するもので、再ゾーニングをサポートします。プレフィルタ ルールはより広範囲の制約を設けるもので、再ゾーニングをサポートしていません。詳細については、トンネルとプレフィルタのルール （1893 ページ）を参照してください。
- デフォルト アクション（トンネルのみ）：トンネルがどのルールとも一致しない場合は、デフォルト アクションによって処理されます。デフォルト アクションは、そのトンネルをブロックするか、あるいは個々のカプセル化された接続のアクセス制御を継続します。デフォルト アクションでトンネルの再ゾーニングを行うことはできません。

  カプセル化されていないトラフィックに対するデフォルト アクションはありません。カプセル化されていない接続がどのプレフィルタ ルールにも一致しない場合、システムはアクセス制御を継続します。

接続ロギング

プレフィルタポリシーで FastPath された接続およびブロックされた接続のログを記録できます。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Other Connections You Can Log*」を参照してください。

接続イベントには、すべてのトンネルを含め、ロギングされる接続がプレフィルタ処理されるのかどうか、また、どのようなプレフィルタ処理を行うのかに関する情報が含まれています。この情報は、イベント表示（ワークフロー）、ダッシュボード、およびレポートで表示することができ、相関基準として使用できます。FastPath された接続やブロックされた接続は、ディープインスペクションの対象外であるため、これらの接続に関連する接続イベントに含まれる情報は限定的となります。

デフォルト プレフィルタ ポリシー

すべてのアクセス コントロール ポリシーにプレフィルタ ポリシーが関連付けられています。

カスタム プレフィルタリングを設定しなければ、システムはデフォルト ポリシーを使用します。このシステム提供のポリシーの初期設定では、すべてのトラフィックをアクセス制御の次

のフェーズに渡します。デフォルト ポリシーのデフォルト アクションを変更し、ロギングのオプションを設定することはできますが、ルールの追加や削除はできません。

プレフィルタ ポリシーの継承とマルチテナンシー

アクセス制御は、マルチテナンシーを補完する階層型実装となっています。プレフィルタ ポリシーの関連付けは、その他の詳細設定と同様にロックすることが可能で、これによりすべての子孫アクセス コントロール ポリシーでこの関連付けが強制的に継承されます。詳細については、「アクセス コントロール ポリシーの継承 （1728 ページ）」を参照してください。

トンネルとプレフィルタのルール

トンネルとプレフィルタのどちらのルールを設定するかは、照合するトラフィックのタイプと、実行するアクションや詳細な分析によって異なります。

特性	トンネル ルール	プレフィルタ ルール
主な機能	プレーンテキストのパススルートンネルをすばやく fastpath、ブロック、または再ゾーニングします。	初期段階の操作の影響を受ける他の接続をすばやく高速パス化またはブロックします。
カプセル化とポート/プロトコル条件	カプセル化の条件は、カプセル化ルールの条件 （1907 ページ）にリストされる選択済みプロトコルについて、プレーンテキスト トンネルのみと照合されます。	ポート条件では、トンネル ルールより広範囲のポートおよびプロトコル制約を使用できます。ポート、プロトコル、および ICMP コードルールの条件 （819 ページ）を参照してください。
ネットワーク条件	トンネル エンドポイント条件は、処理対象にするトンネルのエンドポイントを制約します。ネットワークルール条件 （816 ページ）を参照してください。	ネットワーク条件は、各接続の送信元ホストと宛先ホストを制約します。ネットワークルール条件 （816 ページ）を参照してください。
方向（Direction）	双方向または単方向（構成可）。 トンネル ルールはデフォルトで双方向であるため、トンネル エンドポイント間のすべてのトラフィックを処理できます。	単方向のみ（構成不可）。 プレフィルタ ルールは、送信元から宛先へ送信されるトラフィックのみと照合されます。許可された接続のリターントラフィックも許可されます。
詳細分析のためのセッションの再ゾーニング	トンネル ゾーンを使用する場合にサポートされます。トンネル ゾーンおよびプレフィルタリング （1907 ページ）を参照してください。	未サポート

プレフィルタリングとアクセス コントロール

プレフィルタとアクセス コントロール ポリシーのどちらを使用しても、トラフィックをブロックしたり信頼したりできますが、プレフィルタリングの「信頼」機能の方がより多くのインスペクションをスキップするため、「高速パス」と呼ばれます。次の表ではこれについて説明し、プレフィルタリングとアクセス コントロールのその他の違いを示します。これは、カスタム プレフィルタリングを設定するかどうかの決定に役立ちます。

カスタム プレフィルタリングを設定しない場合は、アクセス コントロール ポリシーに初期に配置されたブロックおよび信頼ルールにより、プレフィルタ機能に近づけることのみ可能です（複製するのではなく）。

特性	プレフィルタリング	アクセス制御	詳細
主な機能	特定のタイプのプレーンテキストのパススルー トンネル（カプセル化ルールの条件（1907ページ）を参照）を迅速に高速パス処理またはブロックしたり、後続のインスペクションをそのカプセル化されたトラフィックに適合させたりします。 早期処理による利点が得られる他の接続を高速パス処理またはブロックします。	コンテキスト情報やディープ インスペクションの結果など、単純または複雑な基準を使用して、すべてのネットワーク トラフィックを検査および制御します。	プレフィルタリングについて（1891 ページ）
実装	プレフィルタ ポリシー プレフィルタ ポリシーは、アクセス コントロール ポリシーによって呼び出されます。	アクセス コントロール ポリシー アクセス コントロール ポリシーがメインの構成です。サブポリシーの呼び出しに加えて、アクセス コントロール ポリシーの独自のルールがあります。	プレフィルタ ポリシーについて（1892 ページ） アクセス制御への他のポリシーの関連付け （1765 ページ）
アクセス コントロール内のシーケンス	最初。 トラフィックは、他のすべてのアクセス コントロール構成の前にプレフィルタ基準と照合されます。 したがって、プレフィルタ ポリシーでの高速パス処理では、他の多くのポリシーとインスペクションがスキップされます。	最後（Last）： セキュリティ インテリジェンスや復号など、接続を検査する可能性のあるその他のポリシーは、アクセス制御ルールが評価される前に適用されます。	—

特性	プレフィルタリング	アクセス制御	詳細
ルール アクション	少ない。 追加のインスペクションを停止したり（高速パス処理とブロック）、他のアクセス コントロールによる追加の分析を許可したり（分析）できます。	多い。 アクセス コントロール ルールには、モニタリング、ディープインスペクション、リセットしてブロック、インタラクティブブロッキングなどのさまざまなアクションがあります。	トンネルとプレフィルタ ルールのコンポーネント （1902 ページ） アクセス コントロール ルールのアクション （1781 ページ）
バイパス機能	高速パス ルール アクション。 プレフィルタ段階のトラフィックの高速パス処理では、その後のすべてのインスペクションと次のような処理をバイパスします。 • セキュリティ インテリジェンス • アイデンティティ ポリシーによって課される認証要件 • SSL 復号 • アクセスコントロールルール • パケットペイロードの詳細な検査 • 検出 • レート制限	信頼ルール アクション。 アクセス コントロール ルールによって信頼されるトラフィックのみが侵入検査とディスカバリを免除されます。インスペクションが必要な別のポリシーが最終的に信頼される接続に適用される場合でも、接続は検査されます。 信頼とは、接続に侵入ポリシーもファイル ポリシーも適用しないことを意味します。	アクセス コントロール ルールの概要 （1775 ページ）
ルール基準	制限。 プレフィルタ ポリシーのルールでは、単純なネットワーク基準、つまりIPアドレス、VLANタグ、ポート、およびプロトコルを使用します。 トンネルについては、トンネル エンドポイント条件によって、トンネルの両側にあるネットワーク デバイスのルーテッド インターフェイスのIPアドレスを指定します。	堅牢。 アクセス コントロール ルールでは、ネットワーク基準を使用しますが、パケット ペイロードで使用できるユーザー、アプリケーション、要求されたURL、およびその他のコンテキスト情報も使用します。 ネットワーク条件によって、送信元と宛先ホストのIP アドレスが指定されます。	トンネルとプレフィルタのルール （1893 ページ） プレフィルタルール条件 （1904 ページ） トンネルルール条件 （1907ページ）

特性	プレフィルタリング	アクセス制御	詳細
IP ヘッダーの使用（トンネル処理）	最も外側。 外部ヘッダーを使用して、プレーンテキストのパススルー トンネル全体を処理できます。 カプセル化されていないトラフィックについては、プレフィルタリングで引き続き「外部」ヘッダーが使用され、この場合は唯一のヘッダーになります。	可能な限り内側。 カプセル化されていないトンネルについては、アクセス コントロールは、トンネル全体ではなく、個々のカプセル化された接続に適用されます。	パススルー トンネルとアクセス制御 （1896 ページ）
さらに分析するためのカプセル化された接続の再ゾーン化	トンネルされたトラフィックを再ゾーン化します。 トンネルゾーンにより、後続のインスペクションをプレフィルタされたカプセル化トラフィックに適合させることができます。	トンネル ゾーンを使用。 アクセス コントロールでは、プレフィルタリング中に割り当てたトンネル ゾーンを使用します。	トンネル ゾーンおよびプレフィルタリング （1907 ページ）
接続のロギング	高速パス処理およびブロックされたトラフィックのみ。許可された接続は、他の構成によってログに記録されることがあります。	任意の接続。	Cisco Secure Firewall Management Center アドミニストレーション ガイドの「ログ可能なその他の接続」
サポートされるデバイス	Secure Firewall Threat Defense のみ。	すべて。	—

パススルー トンネルとアクセス制御

プレーンテキスト（暗号化されていない）トンネルでは、複数の接続をカプセル化できます。これらのトンネルは、多くの場合、連続していないネットワーク間をつなぎます。したがって、IP ネットワークでカスタム プロトコルをルーティングする場合や、IPv4 ネットワークで IPv6 トラフィックをルーティングする場合などには特に役立ちます。

外側のカプセル化ヘッダーには、トンネル エンドポイント（トンネルのいずれかの側にあるネットワーク デバイスのルーテッド インターフェイス）の送信元と宛先の IP アドレスが指定されます。内側のペイロードヘッダーには、カプセル化された接続の実際のエンドポイントの送信元と宛先の IP アドレスが指定されます。

通常、ネットワーク セキュリティ デバイスは、プレーンテキスト トンネルをパススルー トラフィックとして扱います。つまり、ネットワーク セキュリティ デバイスはトンネル エンドポイントのうちの 1 つではないということです。代わりに、ネットワーク セキュリティ デバイ

スはトンネルエンドポイントの間に展開されて、それらのエンドポイント間を流れるトラフィックをモニタします。

一部のネットワーク セキュリティ デバイスは、外部 IP ヘッダーを使用してセキュリティポリシーを適用します。プレーン テキスト トンネルの場合でも、これらのデバイスはカプセル化された個々の接続とそのペイロードを制御したりその内容を把握したりすることはできません。

それとは対照的に、システムは以下のようにアクセス制御を活用します。

- 外側のヘッダーの評価：まず、プレフィルタで外側のヘッダーを使用してトラフィックを処理します。この段階で、プレーン テキストのパススルー トンネル全体をブロックすることも、FastPath を適用することもできます。
- 内側のヘッダーの評価：次に、アクセス制御の残り（および QoS などのその他の機能）では、最も内側にあるヘッダーの検出可能レベルを使用して、可能な限り詳細なレベルでインスペクションと処理が行われるようにします。

  パススルー トンネルが暗号化されていなければ、システムはこの段階で、カプセル化された個々の接続に対処します。カプセル化されたすべての接続に対処するには、トンネルの再ゾーン分割（トンネル ゾーンおよびプレフィルタリング （1907 ページ）を参照）を行う必要があります。

アクセス制御では、暗号化されたパススルー トンネルの内容を把握しません。たとえば、アクセス制御ルールは、パススルー VPN トンネルを 1 つの接続と見なします。システムは外側のカプセル化ヘッダーに含まれる情報だけを使用して、トンネル全体を処理します。

Fastpath プレフィルタリングのベストプラクティス

プレフィルタルールで fastpath アクションを使用すると、一致するトラフィックは検査をバイパスし、単にデバイスを介して送信されます。このアクションは、信頼できるトラフィックと、利用可能などのセキュリティ機能でもメリットを得られないトラフィックに使用してください。

次のタイプのトラフィックは、fastpath アクションに最適です。たとえば、エンドポイントまたはサーバーの IP アドレスに対して送受信されるトラフィックの fastpath のルールを設定できます。使用するポートに基づいてルールをさらに制限できます。

- デバイスを通過する VPN トラフィック。つまり、このデバイスは VPN トポロジのエンドポイントではありません。
- 内部ネットワーク上の信頼されたエンドポイント間の SQL トラフィック。
- スキャナのトラフィック。スキャナプローブにより、侵入ポリシーから多くの誤検知応答が発生する可能性があります。
- 音声/ビデオ。
- バックアップ。

- Firewall Threat Defense デバイスを通過する管理トラフィック（sftunnel）。（アクセス コントロールポリシーを使用して）管理トラフィックでディープインスペクションを実行すると、問題が発生する可能性があります。管理センターと管理対象デバイス間のポート TCP/8305 に基づいてプレフィルタリングできます。

カプセル化されたトラフィックの処理のベストプラクティス

このトピックでは、カプセル化されたトラフィックの次のタイプについてガイドラインを説明します。

- Generic Routing Encapsulation (GRE)
- Point-to-Point Tunneling Protocol（PPTP）
- IPinIP
- IPv6inIP
- Teredo

GRE トンネルの制限事項

GRE トンネル処理は、IPv4 および IPv6 のパッセンジャーフローに限定されます。PPTP や WCCP などの他のプロトコルは、GRE トンネル内ではサポートされません。

管理対象デバイスの Snort バージョンサポートについて

管理対象デバイスで使用されるインスペクションエンジンは、Snort と呼ばれます。Snort 3 は Snort 2 よりも多くの機能をサポートしています。これらがネットワーク上の管理対象デバイスにどのように影響するかを理解するには、次のことを知っておく必要があります。

- デバイスがサポートする Snort のバージョン

  Snort のバージョンサポートは、『*Cisco Firepower Compatibility Guide*』のバンドルされたコンポーネントに関するセクションで確認することができます。

- Firewall Management Center および Firewall Threat Defense ソフトウェアが Snort 2 および Snort 3 をサポートする方法

  Snort 2 および Snort 3 の制約事項については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「Firewall Management Center の Snort 3 機能の制約事項 - Managed Firewall Threat Defense」トピックを参照してください。

GRE v1 および PPTP による外部フロー処理のバイパス

GRE v1（ステートフル GRE とも呼ばれる）および PPTP トラフィックは、外部フロー処理をバイパスします。

パッセンジャフロー処理は IPv6inIP および Teredo でサポートされていますが、次の制限が適用されます。

- セッションは、ロードバランシングされていない単一のトンネルを経由する
- HA またはクラスタリング レプリケーションがない
- プライマリフローとセカンダリフローの関係は維持されない
- プレフィルタポリシーのホワイトリストとブラックリストはサポートされない

GRE v0 シーケンス番号フィールドはオプションである必要がある

ネットワーク上でトラフィックを送信するすべてのエンドポイントは、オプションとしてシーケンス番号フィールドを使用して GREv0 トラフィックを送信する必要があります。それ以外の場合、シーケンス番号フィールドは削除されます。RFC 1701 と RFC 2784 はどちらも、シーケンスフィールドをオプションとして指定しています。

トンネルがインターフェイスで機能する方法

プレフィルタおよびアクセスコントロールポリシールールは、ルーテッドインターフェイス、トランスペアレントインターフェイス、インラインセットインターフェイス、インラインタップインターフェイス、およびパッシブインターフェイスのすべてのトンネルタイプに適用されます。

参考資料

GRE および PPTP プロトコルの詳細については、以下を参照してください。

- RFC 1701、RFC 2784、および RFC 2890（GRE プロトコル v0）
- RFC 2637（PPTP および GRE プロトコル v1）

プレフィルタポリシーの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者

- ネットワーク管理者

プレフィルタリングの設定

カスタムプレフィルタリングを実行するには、プレフィルタポリシーを設定し、そのポリシーをアクセス コントロール ポリシーに割り当てます。管理対象デバイスへのプレフィルタポリシーの割り当ては、アクセス コントロール ポリシーを介して行われます。

ポリシーの編集は、1 つのブラウザウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[プレフィルタ（Prefilter）]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックして、カスタム プレフィルタ ポリシーを作成します。

新しいプレフィルタ ポリシーには、ルールや、すべてのトンネル トラフィックを分析するデフォルト アクションはありません。新しいプレフィルタ ポリシーでは、ロギングやトンネルの再ゾーン分割は実行されません。既存のポリシーを [コピー（Copy）]（ ） または [編集（Edit）]（） することもできます。

ステップ 3 プレフィルタ ポリシーのデフォルト アクションとそのロギング オプションを設定します。

- デフォルトアクション：サポートされるプレーンテキスト、パススルー トンネルのデフォルト アクションを選択します。[すべてのトンネル トラフィックを分析（Analyze all tunnel traffic）]（アクセス コントロールあり）または [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）]。
- デフォルトアクションのロギング：デフォルトアクションの横にある **ロギング**（ ）をクリックします。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Logging Connections with a Policy Default Action」を参照してください。デフォルト アクションのロギングは、ブロックされたトンネルに対してのみ設定できます。

ステップ 4 トンネルおよびプレフィルタ ルールを設定します。

カスタム プレフィルタ ポリシーでは、両方の種類のルールを任意の順序で使用できます。照合する特定のタイプのトラフィックおよび実行するアクションまたは追加の分析に応じてルールを作成します。トンネルとプレフィルタのルール （1893 ページ）を参照してください。

注意

トンネル ルールを使用してトンネル ゾーンを割り当てる場合は、注意してください。再ゾーン分割されたトンネルでの接続は、後の評価でセキュリティ ゾーンの制約に一致しない可能性があります。詳細については、トンネル ゾーンおよびプレフィルタリング （1907ページ）を参照してください。

ルールコンポーネントの設定の詳細については、「トンネルとプレフィルタ ルールのコンポーネント （1902 ページ）」を参照してください。

ステップ 5 ルールの順序を評価します。ルールを移動するには、クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ルールを適切に作成して順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれてしまう可能性があります。詳細については、アクセス制御ルールのベストプラクティス （1736 ページ）を参照してください。

ステップ 6 プレフィルタ ポリシーを保存します。

ステップ 7 トンネル ゾーンの制約をサポートする設定では、再ゾーン分割されたトンネルを適切に処理します。

トンネルゾーンを送信元ゾーンの制約として使用し、再ゾーン分割されたトンネルでの接続を照合します。

ステップ 8 プレフィルタ ポリシーを管理対象デバイスに展開されたアクセス コントロール ポリシーに関連付けます。

「アクセス制御への他のポリシーの関連付け （1765 ページ）」を参照してください。

ステップ 9 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

（注）
プレフィルタポリシーを展開しても、そのルールは既存のトンネルセッションに適用されません。したがって、既存の接続のトラフィックは、展開された新しいポリシーでバインドされません。また、ポリシーヒットカウントは、ポリシーに一致する接続の最初のパケットに対してのみ増加します。したがって、ポリシーに一致する可能性がある既存の接続のトラフィックは、ヒットカウントから除外されます。ポリシールールを効果的に適用するには、既存のトンネルセッションをクリアしてからポリシーを展開します。

次のタスク

時間ベースのルールを展開する場合は、ポリシーが割り当てられるデバイスのタイムゾーンを指定します。「タイムゾーン （892 ページ）」を参照してください。

トンネルとプレフィルタ ルールのコンポーネント

状態（有効/無効）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

ルールの番号は1から始まります。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、ルールタイプ（トンネルまたはプレフィルタ）に関係なく、そのトラフィックを処理するルールです。

操作

ルールのアクションによって、一致したトラフィックの処理とログ記録の方法が決まります。

- [高速パス（Fastpath）]：アクセス制御、ID 要件、レート制限を含む、すべての詳細な検査および制御から一致するトラフィックを免除します。トンネルを高速パス化すると、すべてのカプセル化された接続が高速パス化されます。
- [ブロック（Block）]：どのような種類の検査も行わずにトラフィックを照合します。トンネルをブロックすると、カプセル化されたすべての接続がブロックされます。
- [分析（Analyze）]：残りのアクセス制御で内部ヘッダーを使用して引き続きトラフィックを分析できるようにします。アクセス制御および関連するディープ インスペクションによって渡された場合、このトラフィックはレート制限も行われる場合があります。トンネル ルールの場合は、[トンネル ゾーンの割り当て（Assign Tunnel Zone）] オプションを指定して、再ゾーニングを有効にします。

（注） アクションが **Fastpath** で、ロギングオプションが無効になっているプレフィルタルールの場合、フロー終了イベントがシステムで引き続き生成されます。このイベントは、Management Center のイベントページには表示されません。

方向（トンネル ルールのみ）

トンネル ルールの方向によって、システムの送信元と宛先の条件に従った処理方法が決まります。

- 送信元からのトンネルのみを照合します（単方向）。送信元から宛先へ送信されるトラフィックのみを照合します。一致するトラフィックは、指定された送信元インターフェイスまたはトンネル エンドポイントから発信され、宛先インターフェイスまたはトンネル エンドポイントを通過する必要があります。許可された接続のリターントラフィックも許可されます。

- 送信元と宛先からのトンネルを照合します（双方向）。送信元から宛先へ送信されるトラフィックと宛先から送信元へ送信されるトラフィックの両方を照合します。この効果は、単方向のルールを2つ作成した場合と同じで、一方のルールがもう一方のルールのミラーとなります。

プレフィルタ ルールは常に単方向です。

トンネル ゾーンの割り当て（トンネル ルールのみ）

トンネル ルールで、トンネル ゾーン（既存のゾーンまたはオンザフライで作成したゾーン）を割り当てると、一致するゾーンが再ゾーニングされます。再ゾーニングするには、分析アクションが必要です。

トンネルを再ゾーニングすると、アクセス制御ルールなどの他の構成で、すべてのトンネルのカプセル化された接続の所属先が同じであると認識させることができます。トンネルに割り当てられたトンネルゾーンをインターフェイスの制約として使用すると、カプセル化された接続に合わせた検査を実行することができます。詳細については、トンネルゾーンおよびプレフィルタリング （1907 ページ）を参照してください。

注意 トンネル ゾーンを割り当てるときには注意が必要です。再ゾーニングされたトンネルの接続は、後から実行される評価でセキュリティ ゾーンの制約と一致しないことが検出される可能性があります。トンネル ゾーン実装の簡単なウォークスルーと、再ゾーニングするトラフィックを明示的に処理せずに再ゾーニングする理由については、トンネル ゾーンの使用 （1908 ページ）を参照してください。

条件

条件は、ルールが処理する特定のトラフィックを指定します。トラフィックは、ルールのすべての条件と一致し、ルールと一致する必要があります。各条件の種類には、ルール エディタ内に独自のタブがあります。

トラフィックをプレフィルタリングするには、次の外部ヘッダー制約を使用します。トンネルルールは、カプセル化プロトコルで制約する必要があります。

- インターフェイス：インターフェイスルール条件 （816 ページ）
- ネットワーク（プレフィルタルール）/トンネルエンドポイント（トンネルルール）：ネットワークルール条件 （816 ページ）
- VLAN：VLAN タグルール条件 （1792 ページ）
- ポート（プレフィルタルール）/カプセル化およびポート（トンネルルール）：プレフィルタルールのポートルール条件 （1906ページ）またはカプセル化ルールの条件 （1907ページ）
- 時間範囲—時間と日のルール条件 （1800 ページ）

ログ

システムが記録する処理済みトラフィックのレコードは、ルールのロギング設定によって管理します。

トンネルとプレフィルタのルールでは、高速パスが適用されたトラフィックとブロックされたトラフィック（[高速パス（Fastpach）] と [ブロック（Block）] のアクション）をログに記録することができます。詳細分析（[分析（Analyze）] アクション）の対象となるトラフィックでは、一致する接続が他の構成で記録されている可能性がありますが、プレフィルタポリシーでのログ記録は無効になります。ロギングは、カプセル化フローではなく、内部フローで実行されます。詳細については、『Cisco Secure Firewall Management Center アドミニストレーションガイド』の「Logging Connections with Tunnel and Prefilter Rules」を参照してください。

説明

ルールで変更を保存するたびに、コメントを追加することができます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ルールを保存した後で、これらのコメントを編集または削除することはできません。

関連トピック

アクセス制御ルールのベストプラクティス （1736 ページ）

プレフィルタルール条件

ルール条件を使用すると、プレフィルタポリシーを微調整して、制御するネットワークをターゲットにすることができます。詳細については、次の項を参照してください。

インターフェイスルール条件

インターフェイスルールの条件は送信元インターフェイスと宛先インターフェイスによってトラフィックを制御します。

ルールタイプと導入環境でのデバイスにより、セキュリティゾーンやインターフェイスグループと呼ばれる定義済みのインターフェイスオブジェクトを使用してインターフェイス条件を構築できます。インターフェイスオブジェクトはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することによってトラフィックフローを制御し、分類しやすくします。インターフェイス（Interface） （1346 ページ）を参照してください。QoS ルールは、ルーテッドインターフェイスのみに適用できます。

ヒント インターフェイスによってルールを制約するのは、システムパフォーマンスを改善するための最適な方法の 1 つです。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

ネットワークルール条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注） アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

VLAN タグルール条件

（注） アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

プレフィルタルールのポートルール条件

ポート条件により、送信元ポートと宛先ポートに基づいてトラフィックが照合されます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP と UDP のトラフィックは、ポートに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- プロトコル：ポートを使用しないその他のプロトコルを使用してトラフィックを制御できます。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP と DNS over UDP の両方を 1 つのアクセスコントロールルールの宛先ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

ポートベースではないプロトコルを照合できます。デフォルトでは、ポート条件を指定しない場合は IP トラフィックを照合します。プレフィルタルールで他のプロトコルと一致するようにポート条件を設定できますが、GRE、IP 内の IP、IP 内の IPv6、および Toredo ポート 3544 を一致させる場合は、代わりにトンネルルールを使用する必要があります。

時間と日のルール条件

連続する時間範囲または定期的な期間を指定できます。

たとえば、平日の勤務時間、週末、または休日のシャットダウン期間中にのみルールを適用できます。

時間ベースのルールは、トラフィックを処理するデバイスの現地時間に基づいて適用されます。

時間ベースのルールは、FTDデバイスでのみサポートされます。時間ベースのルールを含むポリシーを別のタイプのデバイスに割り当てると、ルールに関連付けられた時間制限はそのデバイスでは無視されます。この場合、警告が表示されます。

トンネルルール条件

ルール条件を使用すると、トンネルポリシーを微調整して、制御するネットワークをターゲットにすることができます。トンネルルールでは、次の条件を使用できます。

- [インターフェイスオブジェクト（Interface Objects）]：接続が通過するデバイスインターフェイスを定義するセキュリティゾーンまたはインターフェイスグループ。インターフェイスルール条件 （816 ページ） を参照してください。
- [トンネルエンドポイント（Tunnel Endpoints）]：トンネルの送信元 IP アドレスと宛先 IP アドレスを定義するネットワークオブジェクト。
- [VLANタグ（VLAN Tags）]：トンネルの最も外側の VLAN タグ。VLAN タグルール条件 （1792 ページ） を参照してください。
- [カプセル化とポート（Encapsulation and Ports）]：トンネルのカプセル化プロトコル。カプセル化ルールの条件 （1907 ページ） を参照してください。
- [時間範囲（Time Range）]：ルールがアクティブな日時。時間範囲を指定しない場合、ルールは常にアクティブです。「時間と日のルール条件 （1800ページ）」を参照してください。

カプセル化ルールの条件

カプセル化の条件は、トンネル ルールに固有です。

この条件では、カプセル化プロトコルによって特定のタイプのプレーンテキスト、パススルートンネルを制御します。ルールを保存する前に、一致するプロトコルを1つ以上選択する必要があります。次のオプションを選択できます。

- GRE（47）
- IP-in-IP（4）
- IPv6-in-IP（41）
- Teredo（UDP（17）/3455）

トンネル ゾーンおよびプレフィルタリング

トンネルゾーンを使用すれば、プレフィルタリングを使って後続のトラフィック処理をカプセル化された接続に合わせることができます。

システムは通常最も内側の検出可能なレベルのヘッダーを使用してトラフィックを処理するため、特殊なメカニズムが必要になります。これにより、可能な限りきめ細かなインスペクションが保証されます。ただし、これは、パススルートンネルが暗号化されていない場合、システムは個々のカプセル化された接続に対して処理を行うことも意味しています。パススルートンネルとアクセス制御 （1896 ページ）を参照してください。

トンネルゾーンはこの問題を解決します。アクセス制御の最初のフェーズ（プレフィルタリング）で、特定のタイプのプレーンテキスト、パススルートンネルを識別するために外側のヘッ

ダーを使用できます。次に、それらのトンネルは、カスタム トンネル ゾーンを割り当てることで再ゾーン化できます。

トンネルを再ゾーニングすると、アクセス制御ルールなどの他の構成で、すべてのトンネルのカプセル化された接続の所属先が同じであると認識させることができます。トンネルに割り当てられたトンネル ゾーンをインターフェイスの制約として使用すると、カプセル化された接続に合わせた検査を実行することができます。

トンネル ゾーンは、その名称にもかかわらず、セキュリティ ゾーンではありません。トンネル ゾーンは、インターフェイスの一式を表すわけではありません。トンネル ゾーンは、場合によっては、カプセル化された接続に関連付けられているセキュリティ ゾーンに置き換わるタグとして考える方がより正確です。

⚠

注意 トンネル ゾーンの制約をサポートする設定の場合、再ゾーン化されたトンネル内の各接続はセキュリティ ゾーンの制約とは一致**しません**。たとえば、トンネルを再ゾーン化した後、アクセス コントロール ルールでは、そのカプセル化された各接続を、それらの新しく割り当てられたトンネル ゾーンと突き合わせることができますが、元のセキュリティ ゾーンと突き合わせることはできません。

トンネル ゾーン実装の簡単なウォークスルーと、再ゾーニングするトラフィックを明示的に処理せずに再ゾーニングする理由については、トンネル ゾーンの使用 （1908 ページ）を参照してください。

トンネル ゾーンの制約をサポートする設定

トンネル ゾーンの制約をサポートするのは、アクセス コントロール ルールだけです。

他のどの設定もトンネル ゾーンの制約をサポートしません。たとえば、QoS を使用してプレーン テキスト トンネル全体をレート制限することはできず、個々のカプセル化されたセッションをレート制限できるだけです。

トンネル ゾーンの使用

この例の手順は、トンネル ゾーンを使用してさらに分析するために GRE トンネルを再ゾーン化する方法をまとめたものです。この例で説明されている概念は、プレーンテキストのパススルー トンネルにカプセル化された接続に合わせてトラフィック インスペクションを調整する必要があるシナリオにも適応できます。

組織の内部トラフィックが信頼済みセキュリティゾーンを通過する状況について考えてみましょう。信頼済みセキュリティゾーンは、さまざまな場所に展開された複数の管理対象デバイスにわたる一連のインターフェイスを表します。組織のセキュリティ ポリシーでは、エクスプロイトとマルウェアのディープ インスペクション後の内部トラフィックを許可する必要があります。

内部トラフィックには、特定のエンドポイント間のプレーンテキストのパススルー GRE トンネルが含まれている場合があります。このカプセル化されたトラフィックのトラフィック プロファイルは、「通常」の局間アクティビティとは異なるため（おそらく既知かつ無害）、セ

キュリティ ポリシーに従いながら、特定のカプセル化された接続のインスペクションを制限できます。

この例では、構成の変更を展開した後、次のようになります。

- 信頼済みゾーンで検出されたプレーンテキストのパススルーGREカプセル化トンネルは、個別のカプセル化接続が1セットの侵入およびファイル ポリシーによって評価されます。
- 信頼済みゾーンの他のすべてのトラフィックは、侵入およびファイル ポリシーの別のセットで評価されます。

このタスクは、GREトンネルの再ゾーン化によって実行します。再ゾーン化を実行すると、アクセス コントロールによって、GRE カプセル化接続が元の信頼済みセキュリティ ゾーンではなくカスタム トンネル ゾーンに関連付けられます。再ゾーン化は、アクセス制御によるカプセル化されたトラフィックの処理方法に起因して必要になります。「パススルー トンネルとアクセス制御（1896ページ）」と「トンネル ゾーンおよびプレフィルタリング（1907ページ）」を参照してください

手順

ステップ 1 カプセル化されたトラフィック向けのディープインスペクションを実行するカスタムの侵入およびファイル ポリシーを設定し、カプセル化されていないトラフィックには別の侵入およびファイル ポリシーのセットを設定します。

ステップ 2 信頼済みセキュリティ ゾーンを通過するGREトンネルを再ゾーン化するようにカスタム プレフィルタリングを設定します。

カスタム プレフィルタ ポリシーを作成し、アクセス コントロールに関連付けます。そのカスタム プレフィルタ ポリシーで、トンネル ルール（この例では**GRE_tunnel_rezone**）と対応するトンネル ゾーン（**GRE_tunnel**）を作成します。詳細については、プレフィルタリングの設定（1900 ページ）を参照してください。

表 *88 : GRE_tunnel_rezone* トンネル ルール

ルール コンポーネント	説明
インターフェイス オブジェクト条件	信頼済みセキュリティ ゾーンを送信元インターフェイス オブジェクトと宛先インターフェイス オブジェクトの両方の制約として使用して、内部のみのトンネルを照合します。
トンネル エンドポイント条件	組織で使用されている GRE トンネルの送信元と宛先のエンドポイントを指定します。 トンネル ルールは、デフォルトでは双方向です。[トンネルの照合（Match tunnels from）] オプションを変更しない場合は、どのエンドポイントを送信元として指定し、どのエンドポイントを宛先として指定するかは重要ではありません。
カプセル化条件	GRE トラフィックを照合します。

ルールコンポーネント	説明
トンネルゾーンの割り当て	**GRE_tunnel** トンネル ゾーンを作成し、ルールに一致するトンネルに割り当てます。
操作	（残りのアクセス コントロールで）分析します。

ステップ 3 再ゾーン化されたトンネルの接続を処理するようにアクセス コントロールを設定します。

管理対象デバイスに展開されたアクセス コントロール ポリシーでは、再ゾーン化したトラフィックを処理するルール（この例では**GRE_inspection**）を設定します。詳細については、アクセスコントロールルールの作成および編集 （1788 ページ）を参照してください。

表 *89 : GRE_inspection* アクセス コントロール ルール

ルールコンポーネント	説明
セキュリティゾーン条件	GRE_tunnel セキュリティゾーンを送信元ゾーン制約として使用し、再ゾーン化されたトンネルを照合します。
操作	ディープ インスペクションを有効にして許可します。 カプセル化された内部トラフィックのインスペクションを実行するように調整されたファイルおよび侵入ポリシーを選択します。

注意
この手順をスキップすると、再ゾーン化された接続は、セキュリティゾーンによって制約されていない**任意の**アクセス コントロール ルールに一致する場合があります。再ゾーン化された接続がどのアクセス コントロール ルールにも一致しない場合は、アクセス コントロール ポリシーのデフォルトアクションによって処理されます。意図してそのようにしていることを確認してください。

ステップ 4 信頼済みセキュリティゾーンを通過するカプセル化されていない接続を処理するようにアクセス コントロールを設定します。

同じアクセス コントロール ポリシーで、信頼済みセキュリティ ゾーン内の再ゾーン化されていないトラフィックを処理するルール（この例では **internal_default_inspection**）を設定します。

表 *90 : internal_default_inspection* アクセス コントロール ルール

ルールコンポーネント	説明
セキュリティゾーン条件	信頼済みセキュリティ ゾーンを送信元ゾーンと宛先ゾーンの両方の制約として使用して、再ゾーン化されていない内部のみのトラフィックを照合します。

ルールコンポーネント	説明
操作	ディープ インスペクションを有効にして許可します。 カプセル化されていない内部トラフィックのインスペクションを実行するように適合されたファイルおよび侵入ポリシーを選択します。

ステップ 5 既存のルールに対して相対的な新しいアクセス コントロール ルールの位置を評価します。ルールの順序を必要に応じて変更します。

2つの新しいアクセス コントロール ルールを隣同士に配置した場合は、最初にどちらを配置するかは重要ではありません。GRE トンネルを再ゾーン化したため、2つのルールは互いをプリエンプション処理することはできません。

ステップ 6 すべての変更された構成を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

トンネル ゾーンの作成

次の手順では、オブジェクトマネージャでトンネルゾーンを作成する方法について説明します。トンネルルールの編集時にゾーンを作成することもできます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。
ステップ 2 オブジェクト タイプのリストから **[トンネル ゾーン（Tunnel Zone）]** を選択します。
ステップ 3 [トンネル ゾーンの追加（Add Tunnel Zone）] をクリックします。
ステップ 4 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。
ステップ 5 [保存（Save）] をクリックします。

次のタスク

- カスタム事前フィルタリングの一部として、トンネル ゾーンをプレーン テキストのパススルー トンネルに割り当てます。プレフィルタリングの設定 （1900 ページ）を参照してください。

プレフィルタルールのアクセスコントロールポリシーへの移動

プレフィルタルールをプレフィルタポリシーから関連するアクセス コントロール ポリシーに移動できます。

始める前に

続行する前に、次の条件に注意してください。

- アクセス コントロール ポリシーに移動できるのは、プレフィルタルールだけです。トンネルルールは移動できません。
- プレフィルタルールは、関連付けられたアクセス コントロール ポリシーにのみ移動できます。
- インターフェイスグループが設定されているプレフィルタルールは移動できません。
- プレフィルタルールの [アクション（Action）] パラメータは、移動時にアクセスコントロールルールの適切なアクションに変更されます。プレフィルタルールの各アクションが何にマップされるかを知るには、次の表を参照してください。

プレフィルタルールのアクション	アクセスコントロールルールのアクション
分析（Analyze）	許可
Block	Block
高速パス（Fastpath）	[信頼（Trust）]

- 同様に、次の表に示すように、プレフィルタルールで構成されたアクションに基づいて、ルールの移動後にロギング構成が適切な設定になります。

プレフィルタルールのアクション	アクセスコントロールルールの有効なロギング構成
分析（Analyze）	どのログ設定も有効ではありません。
ブロック（Block）	• 接続開始時にロギング（Log at Beginning of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ

プレフィルタルールのアクション	アクセスコントロールルールの有効なロギング構成
高速パス（Fastpath）	• 接続開始時にロギング（Log at Beginning of Connection） • 接続終了時にロギング（Log at End of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ

- ルールを移動すると、プレフィルタルール構成のコメントが失われます。ただし、ソースのプレフィルタポリシーに言及する新しいコメントが、移動後のルールに追加されます。
- ソースポリシーからルールを移動しているときに、別のユーザーがそれらのルールを変更すると、FMC にメッセージが表示されます。ページを更新した後、プロセスを続行できます。

手順

ステップ 1 プレフィルタ ポリシー エディタで、マウスを左クリックして移動するルールを選択します。

ヒント
複数のルールを選択するには、キーボードの Ctrl（Control）キーを使用します。

ステップ 2 選択したルールを右クリックし、[別のポリシーに移動（Move to another policy）] を選択します。

ステップ 3 [アクセスポリシー（Access Policy）] ドロップダウンリストから宛先アクセス コントロール ポリシーを選択します。

ステップ 4 [ルールの配置（Place Rules）] ドロップダウンリストから、移動したルールを配置する場所を選択します。

- [デフォルト（Default）] セクションの最後のルールセットとして配置するには、[一番下（[デフォルト]セクション内）（At the bottom (within the Default section)）] を選択します。
- [必須（Mandatory）] セクションの最初のルールセットとして配置するには、[一番上（[必須]セクション内）（At the top (within the Mandatory section)）] を選択します。

ステップ 5 [移動（Move）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

プレフィルタ ポリシーのヒット カウント

ヒットカウントは、一致する接続に対してポリシールールがトリガーされた回数を示します。

プレフィルタ ポリシー ヒット カウントの表示に関する詳細詳細については、ルールヒットカウントの表示 （1767 ページ）を参照してください。

大規模フローのオフロード

Cisco Secure Firewall 3100、Firepower 4100/9300 シャーシ では、プレフィルタポリシーによってファストパスされるように設定した特定のトラフィックは、Firewall Threat Defense ソフトウェアではなくハードウェア（具体的には NIC 内）で処理されます。これらの接続フローをオフロードすると、特に大規模なファイル転送などのデータ集約型アプリケーションの場合、スループットが向上し、遅延が減少します。この機能は、データセンターで特に役立ちます。これは、静的フロー オフロードと呼ばれます。

さらに、デフォルトでは、Firewall Threat Defense デバイスは信頼を含む他の基準に基づいてフローをオフロードします。これは、動的フロー オフロードと呼ばれます。

オフロードされたフローは、引き続き制限付きステートフルインスペクション（基本的なTCP フラグおよびオプションのチェックなど）を受信します。システムは必要に応じてさらなる処理のためにファイアウォール システムへのパケットを選択的に増やすことができます。

大規模フローをオフロードすることでメリットが得られるアプリケーションの例は次のとおりです。

- ハイパフォーマンス コンピューティング（HPC）調査サイト。ここでは、Firewall Threat Defense デバイスがストレージと高コンピューティング ステーション間で展開されます。1 つの調査サイトが NFS 経由の FTP ファイル転送またはファイル同期を使用してバックアップを行うと、大量のデータ トラフィックがすべての接続に影響を与えます。NFS を介する FTP ファイル転送およびファイル同期のオフロードによって、他のトラフィックへの影響が軽減されます。
- 主にコンプライアンス目的で使用される High Frequency Trading（HFT）。ここでは、Firewall Threat Defense デバイスがワークステーションと Exchange 間で展開されます。セキュリティは通常は問題にはなりませんが、遅延は大きな問題です。

次のフローをオフロードできます。

- （静的フロー オフロードのみ）プレフィルタポリシーにより FastPath される接続。
- 標準または 802.1Q タグ付きイーサネット フレームのみ。
- （動的フローオフロードのみ）：

- インスペクションエンジンが検査の必要がなくなったと判断した検査済みのフロー。これらのフローには次が含まれます。
  - 信頼アクションを適用し、セキュリティゾーン、送信元と宛先のネットワーク、およびポートの一致のみに基づくアクセスコントロールルールによって処理されるフロー。
  - 復号ポリシー を使用した復号に選択されていない TLS/SSL フロー。
  - インテリジェントアプリケーションバイパス（IAB）ポリシーで、明示的か、またはフロー バイパスのしきい値を超えているために信頼されているフロー。
  - ファイルポリシーまたは信頼ポリシーに一致し、そのフローが信頼できると判断されたフロー。
  - 検査する必要がなくなった許可されたフロー。
- 次の IPS プリプロセッサが検査したフロー：
  - SSH および SMTP。
  - FTP プリプロセッサのセカンダリ接続。
  - Session Initiation Protocol（SIP）プリプロセッサのセカンダリ接続。
- キーワードを使用する侵入ルール（オプションとも呼ばれる）。

- 動的フロー オフロードは、Cisco Secure Firewall バージョン 7.6 以前のバージョンを実行している Cisco Secure Firewall 3100 ではサポートされていません 。

重要 上記の詳細、例外、および制限については、フロー オフロードの制限事項 （1916 ページ）を参照してください。

静的フロー オフロードの使い方

ハードウェアに適格なトラフィックをオフロードするには、**FastPath** アクションを適用するプレフィルタポリシールールを作成します。TCP/UDP にはプレフィルタ ルールを使用し、GRE にはトンネル ルールを使用します。

（推奨されていません。）静的フローオフロードを無効にし、副産物として動的フローオフロードを無効にするには、FlexConfig を使用して **no flow-offload enable** コマンドを実行します。このコマンドの詳細については、https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html から入手可能な『*Cisco ASA Series Command Reference*』を参照してください。

動的フロー オフロードの使い方

動的フロー オフロードは、。

動的オフロードを無効にするには：

```
> configure flow-offload dynamic whitelist disable
```

動的オフロードを再度有効にするには：

```
> configure flow-offload dynamic whitelist enable
```

動的オフロードは、事前フィルタリングが構成されているかどうかに関係なく、静的フローオフロードが有効になっている場合にのみ発生することに注意してください。

フロー オフロードの制限事項

すべてのフローをオフロードできるわけではありません。オフロードの後でも、フローを特定の条件下でのオフロードから除外することができます。次に、制限事項の一部を示します。

デバイスによる制限

この機能は、以下のデバイスでサポートされています。

- Cisco Secure Firewall 3100
- Firepower 4100/9300

オフロードできないフロー

次のタイプのフローはオフロードできません。

- IPv6 アドレッシングなど、IPv4 アドレッシングを使用しないフロー。
- TCP、UDP、GRE 以外のプロトコルに対するフロー。

（注） PPTP GRE 接続はオフロードできません。

- パッシブ、インラインまたはインライン タップ モードで設定されたインターフェイス上のフロー。ルーテッドインターフェイスおよびスイッチドインターフェイスがサポートされている唯一のタイプです。
- （Secure Firewall 3100）。トンネリングされたフローの内部ヘッダーに基づくオフロード。
- （Secure Firewall 3100）。マルチインスタンス オフロード。
- Snort またはその他のインスペクション エンジンによるインスペクションが必要なフロー。FTP など場合によっては、コントロール チャネルはオフロードできませんがセカンダリ データ チャネルはオフロードできます。
- デバイスで終端する IPsec および TLS/DTLS VPN 接続。
- 暗号化または復号を必要とするフロー。たとえば、復号ポリシーによって復号される接続です。

- ルーテッド モードのマルチキャスト フロー。ブリッジグループにメンバーインターフェイスが 2 つしかない場合、トランスペアレントモードでサポートされます。
- TCP インターセプト フロー。
- TCP ステートバイパスフロー。同じトラフィックにフローオフロードと TCP ステートバイパスを設定することはできません。
- セキュリティ グループでタグ付けされたフロー。
- クラスタで非対称フローが発生した場合に備えて、別のクラスタノードから転送されるリバースフロー。
- クラスタ内の一元化されたフロー（フローのオーナーが制御ユニットでない場合）。
- IP オプションを含むフローは動的にオフロードできません。

その他の制限事項

- フローオフロードとデッド接続検出（DCD）は互換性がありません。オフロードできる接続に DCD を設定しないでください。
- フローオフロード条件に一致する複数のフローがキューイングされて、ハードウェア上の同じ場所に同時にオフロードされる場合、最初のフローのみがオフロードされます。他のフローは通常どおりに処理されます。これをコリジョン（衝突）といいます。この状況の統計を表示するには、CLI で **show flow-offload flow** コマンドを使用します。
- ダイナミック フローのオフロードによってすべての TCP ノーマライザのチェックが無効になります。
- オフロードされたフローはFXOSインターフェイスを通過しますが、それらのフローの統計は論理デバイスインターフェイスには表示されません。したがって、論理デバイスインターフェイスのカウンタとパケットレートには、オフロードされたフローは反映されません。

特定のデバイスでサポートされていない動的フローオフロード

Secure Firewall 3100では、動的フローオフロードはサポートされていません。

オフロードを無効にする条件

フローがオフロードされた後、フロー内のパケットは次の条件を満たす場合に Firewall Threat Defense に返され、さらに処理されます。

- タイムスタンプ以外の TCP オプションが含まれている。
- フラグメント化されている。
- これらは等コストマルチパス（ECMP）ルーティングの対象であり、入力パケットは 1 つのインターフェイスから別のインターフェイスに移動する。

プレフィルタリングの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
プレフィルタルールのアクセスコントロールポリシーへの移動	6.7	いずれか	プレフィルタルールをプレフィルタポリシーから関連するアクセスコントロール ポリシーに移動できます。 新規/変更されたページ：プレフィルタポリシーページで、選択したルールの右クリックメニューに、新しい [別のポリシーに移動（Move to another policy）] オプションが表示されます。 サポートされているプラットフォーム： Firewall Management Center
時間ベースのルール	6.6	任意（Any）	Firewall Threat Defense デバイスのタイムゾーンによって決定される日時に応じて、プレフィルタおよびトンネルルールを適用する機能。 アクセス制御ルールの履歴（1812ページ）の説明を参照してください。
プレフィルタルールページからのオブジェクトの詳細の表示	6.6	任意（Any）	導入された機能：プレフィルタルールを表示するときに、オブジェクトまたはオブジェクトグループの詳細を表示するオプション。 新しいオプション：プレフィルタルールリストの次のいずれかの列の値を右クリックすると、オブジェクトの詳細を表示するオプションが提供されます：[送信元ネットワーク（Source Networks）]、[接続先ネットワーク（Destination Networks）]、[送信元ポート（Source Port）]、[接続先ポート（Destination Port）]、および[VLANタグ（VLAN Tag）]。 サポートされているプラットフォーム： Secure Firewall Management Center

第 45 章

サービスポリシー

Firepower Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。サービス ポリシーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

- Firepower Threat Defense のサービス ポリシーについて （1919 ページ）
- サービスポリシーの要件と前提条件 （1922 ページ）
- サービス ポリシーのガイドラインと制限事項 （1922 ページ）
- Threat Defense サービスポリシーの設定 （1923 ページ）
- サービス ポリシーのルールの例 （1934 ページ）
- サービス ポリシーのモニタリング （1940 ページ）
- Threat Defense サービスポリシーの履歴 （1941 ページ）

Firepower Threat Defense のサービス ポリシーについて

Firepower Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。サービスポリシーを使用すると、デバイスまたは特定のインターフェイスに着信するすべての接続に同じサービス以外を適用することができます。

トラフィック クラスはインターフェイスと拡張アクセス コントロール リスト（ACL）の組み合わせです。ACL の「許可」ルールによってクラスに含まれる接続が決定されます。ACL の「拒否」トラフィックには、そのトラフィックに適用されているサービスがないというだけで、これらの接続は実際にはドロップされません。IP アドレスと TCP/UCP ポートを使用し、必要な精度で対応する接続を特定できます。

トラフィック クラスには 2 つのタイプがあります。

- インターフェイスベースのルール：サービス ポリシー ルールでセキュリティ ゾーンまたはインターフェイス グループを指定すると、インターフェイス オブジェクトに含まれているすべてのインターフェイスを通過する ACL の「許可」トラフィックにルールが適用されます。

特定の機能では、入力インターフェイスに適用されたインターフェイスベースのルールがグローバル ルールよりも常に優先されます。入力インターフェイスベースのルールを接続に適用すると、対応するグローバル ルールは無視されます。入力インターフェイスまたはグローバル ルールが適用されていない場合は、出力インターフェイスのインターフェイス サービス ルールが適用されます。

- グローバル ルール：すべてのインターフェイスにこれらのルールが適用されます。インターフェイスベースのルールを接続に適用しない場合は、グローバル ルールが確認され、ACL で「許可」されているすべての接続に適用されます。何も適用しない場合は、どのサービスも適用されずに接続が続行されます。

特定の接続が一致するのは、特定の機能のインターフェイス ベースまたはグローバルのいずれか 1 つのトラフィック クラスのみです。特定のインターフェイス オブジェクト/トラフィック フローの組み合わせには設定できるルールは 1 つのみです。

サービス ポリシーのルールは、アクセス制御ルールの後に適用されます。これらのサービスは、許可している接続にのみ設定されます。

FlexConfig とその他の機能にサービス ポリシーを関連付ける方法

バージョン 6.3(0) よりも前では、接続関連のサービス ルールは TCP_Embryonic_Conn_Limit と TCP_Embryonic_Conn_Timeout の事前定義の FlexConfig オブジェクトを使用して設定できました。これらのオブジェクトを削除し、Firepower Threat Defense Service サービス ポリシーを使用してルールを作り直す必要があります。これらの接続関連コマンドの実装にカスタム FlexConfig オブジェクトを作成した場合（**set connection** コマンド）は、それらのオブジェクトも削除し、サービス ポリシー経由で機能を実装する必要があります。

接続関連のサービス ポリシーの機能は、その他のサービスルールで実装された機能とは異なる機能グループとして処理されます。そのため、トラフィック クラスが重複する問題に直面することはありません。ただし、次を設定する際には十分注意してください。

- QoS ポリシー ルールはサービス ポリシー CLI を使用して実装されます。これらのルールは接続ベースのサービス ポリシー ルールよりも前に適用されます。ただし、QoS と接続の両方の設定を同じトラフィック クラスか、または重複するトラフィック クラスに適用できます。

- FlexConfig ポリシーを使用してカスタマイズされたアプリケーションのインスペクションと NetFlow を実装できます。**show running-config** コマンドを使用して、サービス ルールをすでに設定している **policy-map** コマンド、**class-map** コマンド、**service-policy** コマンドなど、CLI を調査できます。NetFlow とアプリケーション インスペクションは QoS および接続の設定との互換性はありますが、FlexConfig を実装する前に既存の設定を把握しておく必要があります。接続の設定は、アプリケーション インスペクションと NetFlow よりも前に適用されます。

（注） Firepower Threat Defense サービス ポリシーから作成されたトラフィック クラスは **class_map_***ACLname* という名前になります。*ACLname* はサービス ポリシー ルールで使用された拡張 ACL オブジェクトの名前。

接続設定に関する情報

接続の設定は、Firewall Threat Defense を経由する TCP フローなどのトラフィック接続の管理に関連するさまざまな機能で構成されます。一部の機能は、特定のサービスを提供するために設定する名前付きコンポーネントです。

接続の設定には、次が含まれています。

- **さまざまなプロトコルのグローバル タイムアウト**：すべてのグローバル タイムアウトにデフォルト値があるため、早期の接続の切断が発生した場合にのみグローバル タイムアウトを変更する必要があります。Firepower Threat Defense のプラットフォーム ポリシーにグローバル タイムアウトを設定します。**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択します。
- **トラフィック クラスごとの接続タイムアウト**：サービス ポリシーを使用して、特定のタイプのトラフィックのグローバル タイムアウトを上書きできます。すべてのトラフィック クラスのタイムアウトにデフォルト値があるため、それらの値を設定する必要はありません。
- **接続制限と TCP 代行受信**：デフォルトでは、Firewall Threat Defense を経由する（または宛先とする）接続の数に制限はありません。サービス ポリシー ルールを使用して特定のトラフィック クラスに制限を設定することで、サービス妨害（DoS）攻撃からサーバーを保護できます。特に、初期接続（TCP ハンドシェイクを完了していない初期接続）に制限を設定できます。これにより、SYN フラッディング攻撃から保護されます。初期接続の制限を超えると、TCP 代行受信コンポーネントは、プロキシ接続に関与してその攻撃が抑制されていることを確認します。
- **Dead Connection Detection（DCD; デッド接続検出）**：アイドル タイムアウトの設定を超えたために接続が閉じられるように、頻繁にアイドル状態になっても有効な接続を維持する場合、Dead Connection Detection をイネーブルにして、アイドル状態でも有効な接続を識別してそれを維持することができます（接続のアイドル タイマーをリセットすることによって）。アイドル時間を超えるたびに、DCD は接続の両側にプローブを送信して、接続が有効であることを両側で合意しているかどうかを確認します。**show service-policy** コマンド出力には、DCD からのアクティビティ量を示すためのカウンタが含まれています。**show conn detail** コマンドを使用すると、発信側と受信側の情報およびプローブの送信頻度を取得できます。
- **TCP シーケンスのランダム化**：それぞれの TCP 接続には 2 つの ISN（初期シーケンス番号）が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバーで生成されます。デフォルトでは、Firewall Threat Defense は、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。ランダム化により、攻撃者が新しい接続

に使用される次のISNを予測して新しいセッションをハイジャックするのを阻止します。ただし、TCP シーケンスのランダム化は、TCP SACK（選択的確認応答）を実質的に破棄します。クライアントが認識するシーケンス番号がサーバーが認識するものと異なるためです。必要に応じて、トラフィック クラスごとにランダム化をディセーブルにすることができます。

- **TCP 正規化**：TCP ノーマライザは、異常なパケットから保護します。一部のタイプのパケット異常をトラフィック クラスで処理する方法を設定できます。FlexConfigポリシーを使用して TCP 正規化を設定できます。
- **TCPステートバイパス**：ネットワークで非対称ルーティングを使用するかどうかをチェックする TCP ステートをバイパスできます。

サービスポリシーの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

サービス ポリシーのガイドラインと制限事項

- サービス ポリシーは、ルーテッド モードまたはトランスペアレント モードのいずれかのルーテッド インターフェイスまたはスイッチ インターフェイスのみに適用されます。インライン セットまたはパッシブ インターフェイスには適用されません。
- 特定のインターフェイスまたはグローバル ポリシーに最大 25 のトラフィック クラスを設定できます。つまり、25 を超えるサービス ポリシー ルールを特定のセキュリティ ゾーンまたはインターフェイス グループのグローバル ポリシーに設定することはできません。ただし、インターフェイスの場合、同じインターフェイスをセキュリティ ゾーンとインターフェイス グループに表示できるため、実際の制限はゾーンやグループではなく、インターフェイスに基づきます。したがって、ゾーン/グループのメンバーシップに基づき、ゾーン/グループごとに 25 のルールを設定できない場合があります。

- 特定のインターフェイス オブジェクト/トラフィック フローの組み合わせに設定できるルールは 1 つのみです。
- コンフィギュレーションに対してサービスポリシーの変更を加えた場合は、すべての新しい接続で新しいサービスポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。すべての接続に新しいポリシーをすぐに使用するには、現在の接続を切断し、新しいポリシーを使用して再度接続できるようにする必要があります。SSH またはコンソール CLI セッションから **clear conn** コマンドまたは **clear local-host** コマンドを入力します。

Threat Defense サービスポリシーの設定

Threat Defense サービスポリシーを使用して、特定のトラフィッククラスにサービスを適用できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。サービス ポリシーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]**を選択し、編集する Threat Defense サービスポリシーのアクセス コントロール ポリシーで [編集（Edit）]（✎） をクリックします。

ステップ 2 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。

ステップ 3 [Threat Defenseサービスポリシー（Threat Defense Service Policy）] グループで [編集（Edit）]（✎） をクリックします。

既存のポリシーが表示されたダイアログボックスが開きます。ポリシーは番号付きのルールのリストから構成されており、グローバル ルール（すべてのインターフェイスに適用）とインターフェイスベースのルールに分かれています。テーブルには、インターフェイス オブジェクトおよび拡張アクセス コントロール リスト名（これらの組み合わせでルールのトラフィッククラスを定義）と適用されたサービスが表示されます。

ステップ 4 次のいずれかを実行します。

- [ルールの追加（Add Rule）] をクリックして、新しいルールを作成します。サービス ポリシー ルールの設定 （1924 ページ）を参照してください。
- [編集（Edit）]（✎） をクリックして、既存のルールを編集します。サービス ポリシー ルールの設定 （1924 ページ）を参照してください。
- [削除（Delete）]（🗑） をクリックしてルールを削除します。

- ルールをクリックし、移動先の新しい場所までドラッグします。インターフェイスとグローバル リスト間ではルールはドラッグできません。その代りに、ルールを編集してインターフェイス/グローバル設定を変更する必要があります。接続と一致するリスト内の最初のルールが接続に適用されます。

ステップ 5 ポリシーの編集が終了したら、[OK] をクリックします。

ステップ 6 [詳細（Advanced）] ウィンドウで [保存（Save）] をクリックします。[保存（Save）] をクリックするまで、変更は保存されません。

サービス ポリシー ルールの設定

特定のトラフィック クラスにサービスを適用するサービス ポリシー ルールを設定します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセス リスト（Access List）] > [拡張（Extended）] に移動し、ルールが適用されるトラフィックを定義する拡張アクセス リストを作成します。ルールは、拡張アクセス リスト内の許可ルールに一致するすべての接続に適用されます。ACL ルールは正確に定義し、サービスが必要なトラフィックにのみサービス ポリシー ルールが適用されるようにします。

インターフェイスベースのルールを作成している場合は、割り当てられたデバイスにインターフェイスを設定し、それらのインターフェイスをセキュリティ ゾーンまたはインターフェイス グループに追加する必要もあります。

手順

ステップ 1 [Threat Defenseサービスポリシー（Threat Defense Service Policy）] ダイアログボックスがまだ表示されていない場合は、**[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択してアクセス コントロール ポリシーを編集し、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択して、[Threat Defenseサービスポリシー（Threat Defense Service Policy）] を編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] をクリックして、新しいルールを作成します。
- [編集（Edit）]（ ） をクリックして、既存のルールを編集します。

サービス ポリシー ルール ウィザードが開き、ルールの設定プロセスの手順が表示されます。

ステップ 3 [インターフェイス オブジェクト（Interface Object）] 手順で、ポリシーを使用するインターフェイスを定義するオプションを選択します。

- [グローバルに適用（Apply Globally）]：すべてのインターフェイスに適用されるグローバル ルールを作成するには、このオプションを選択します。

- [インターフェイス オブジェクトを選択（Select Interface Objects）]：インターフェイスベースのルールを作成するには、このオプションを選択します。次に、目的のインターフェイスを含むセキュリティゾーンまたはインターフェイスオブジェクトを選択し、[>]をクリックして、それらを [次（Next）] 選択済みリストに移動します。サービス ポリシー ルールは、選択したオブジェクトに含まれる各インターフェイスで設定されますが、ゾーンやグループ自体には設定されません。

インターフェイスの基準が完成したらクリックします。

ステップ 4 [トラフィック フロー（Traffic Flow）] 手順で、ルールが適用される接続を定義する拡張 ACL オブジェクトを選択して [次へ（Next）] をクリックします。

ステップ 5 [接続の設定（Connection Setting）] 手順で、このトラフィック クラスに適用するサービスを設定します。

- [TCP 状態バイパスの有効化（Enable TCP State Bypass）]（TCP 接続のみ）：TCP 状態バイパスを実装します。TCP 状態バイパスの対象である接続は、インスペクション エンジンによる検査はされず、すべての TCP 状態のチェックと TCP 正規化をバイパスします。詳細については、非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス）（1928 ページ）を参照してください。

  （注）
  TCP状態バイパスは、トラブルシューティングのために、または非対称ルーティングを解決できない場合に使用します。この機能は複数のセキュリティ機能を無効化するため、定義が狭いトラフィック クラスを指定して適切に実装しないと、多数の接続が発生することがあります。

- [TCP シーケンス番号のランダム化（Randomize TCP Sequence Number）]（TCP 接続のみ）：TCP シーケンス番号のランダム化を有効にするか、無効にするかを示します。デフォルトでは、ランダム化が有効になっています。詳細については、TCP シーケンスのランダム化のディセーブル（1932 ページ）を参照してください。

- [デクリメント TTL の有効化（Enable Decrement TTL）]（TCP 接続のみ）：クラスに一致するパケットの存続可能時間（TTL）をデクリメントします。存続可能時間を減らすと、TTL が 1 のパケットはドロップされますが、接続に TTL がもっと長いパケットが含まれている可能性があるという仮定の下に、セッションに対して接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL が 1 で送信されるため、存続可能時間を減らすと予期しない結果が生じることがある点に注意してください。

  （注）
  Firewall Threat Defense デバイスをトレースルートに表示する場合は、デクリメント TTL オプションを設定し、プラットフォームの設定のポリシーに ICMP 到達不能レート制限も設定する必要があります。Firewall Threat Defense デバイスをトレースルートに表示する（1938 ページ）を参照してください。

- [接続（Connections）]：クラス全体で許可される接続の数を制限します。次のオプションを設定可能です。

- [TCP と UDP の最大数（Maximum TCP and UDP）]（TCP または UDP 接続のみ）：クラス全体で許可される同時接続の最大数（0 ～ 2000000）。TCP の場合、この数は確立された接続にのみ適用されます。デフォルトは 0 で、この場合は接続数が制限されません。制限がクラスに適用されるため、1 つの攻撃ホストがすべての接続を使い果たし、クラスに一致する他のホストが使用できる接続がなくなる可能性があります。この問題を改善するには、クライアントごとの制限を設定します。
- [最大初期接続数（Maximum Embryonic）]（TCP 接続のみ）：許可される TCP の同時初期接続（TCP ハンドシェイクで完了しない接続）の最大数（0~2000000）。デフォルトは 0 で、この場合は接続数が制限されません。0 以外の制限を設定することで、TCP 代行受信をイネーブルにします。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。また、クライアントごとのオプションを設定して、SYN フラッディングから保護します。詳細については、SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信）（1934 ページ）を参照してください。

- [クライアントあたりの接続数（Connections Per Client）]：特定のクライアント（送信元 IP アドレス）で許可される接続数の制限。次のオプションを設定可能です。
  - [TCP と UDP の最大数（Maximum TCP and UDP）]（TCP または UDP 接続のみ）：クライアントごとに許可される同時接続の最大数（0 ～ 2000000）。TCP の場合は、確立済み接続、ハーフオープン（初期）接続、ハーフクローズ接続が含まれます。デフォルトは 0 で、この場合は接続数が制限されません。このオプションでは、クラスに一致する各ホストに許可される同時接続の最大数が制限されます。
  - [最大初期接続数（Maximum Embryonic）]（TCP 接続のみ）：クライアントごとに許可される TCP の同時初期接続の最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。詳細については、SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信）（1934 ページ）を参照してください。

- [接続のSYN Cookie MSS（Connections Syn Cookie MSS）]：初期接続数制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）（48 ～ 65,535）。デフォルトは 1380 です。この設定は、接続またはクライアントごと、あるいは両方に対して [最大初期接続数（Maximum Embryonic）] を設定する場合にのみ意味があります。

- [接続タイムアウト（Connections Timeout）]：トラフィック クラスに適用されるタイムアウトの設定。これらのタイムアウトで、プラットフォーム設定ポリシーに定義されているグローバル タイムアウトがオーバーライドされます。次の設定を行えます。
  - [初期接続（Embryonic）]（TCP 接続のみ）：TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウト期間（0:0:5 ～ 1193:00:00）。デフォルト値は 0:0:30 です。
  - [ハーフクローズ（Half Closed）]（TCP 接続のみ）：ハーフクローズ接続が閉じられるまでのアイドル タイムアウト期間（0:0:30 ～ 1193:0:0）。デフォルト値は 0:10:0 です。ハーフクローズ接続は、Dead Connection Detection（DCD; デッド接続検出）の影響を受けません。また、システムは、ハーフクローズ接続の切断時にリセットを送信しません。

- [アイドル（Idle）]（TCP、UDP、ICMP、IP 接続）：プロトコルの確立された接続が閉じた後のアイドル タイムアウト期間（0:0:1 ～ 1193:0:0）。デフォルトは 1:0:0 です。ただし、デフォルトが 0:2:0 である [TCP 状態バイパス（TCP State Bypass）] オプションを選択している場合を除く。
- [タイムアウト時に接続をリセット（Reset Connection Upon Timeout）]（TCP 接続のみ）：アイドル接続が削除された後に、両方のエンド システムに TCP RST パケットを送信するかどうかを示します。

- [デッド接続の検出（Detect Dead Connections）]（TCP 接続のみ）：Dead Connection Detection（DCD; デッド接続検出）を有効にするかどうかを示します。アイドル接続の期限が切れる前に、システムはエンドホストにプローブを送信して接続が有効であるかどうかを判断します。両方のホストが応答した場合は、接続が維持されます。それ以外の場合は、接続が解放されます。トランスペアレント ファイアウォール モードで動作している場合、エンドポイントにスタティック ルートを設定する必要があります。オフロードもされている接続では DCD を構成できないため、プレフィルタポリシーで高速パス処理している接続では DCD を構成しないでください。発信側と受信側で送信された DCD プローブの数を追跡するには、Firewall Threat Defense CLI で **show conn detail** コマンドを使用します。

  次のオプションを設定します。

  - [検出のタイムアウト（Detection Timeout）]：DCD プローブに応答がない場合に別のプローブを送信するまで待機する時間（hh:mm:ss 形式で、0:0:1 ～ 24:0:0 の範囲で指定）。デフォルト値は 0:0:15 です。

    クラスタまたは高可用性構成で動作しているシステムでは、間隔を 1 分（0:1:0）未満に設定しないことを推奨します。接続をシステム間で移動する必要がある場合、必要な変更には 30 秒以上かかり、変更が行われる前に接続が削除される場合があります。
  - [検出の再試行（Detection Retries）]：接続がデッドであると宣言する前に行われる DCD の再試行の連続失敗回数（1 ~ 255）。デフォルトは 5 です。

ステップ 6 [終了（Finish）] をクリックして変更を保存します。

ルールは適切なリスト（インターフェイスまたはグローバル）の下部に追加されます。グローバル ルールは上から下の順に照合されます。インターフェイス リスト内のルールは、各インターフェイス オブジェクトで上から下の順に照合されます。定義が狭いトラフィック クラスのルールは、定義が広いルールの上に配置し、適切なサービスが適用されるようにします。各リスト内のルールはドラッグ アンド ドロップで移動できます。リスト間でルールを移動することはできません。

非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス）

ネットワークで非対称ルーティング環境を設定し、特定の接続の発信フローと着信フローが 2 つの異なる Firewall Threat Defense デバイスを通過できる場合は、影響を受けるトラフィックに TCP ステートバイパスを実装する必要があります。

ただし、TCPステートバイパスによってネットワークのセキュリティが弱体化するため、非常に詳細に限定されたトラフィック クラスでバイパスを適用する必要があります。

ここでは、問題と解決策についてより詳細に説明します。

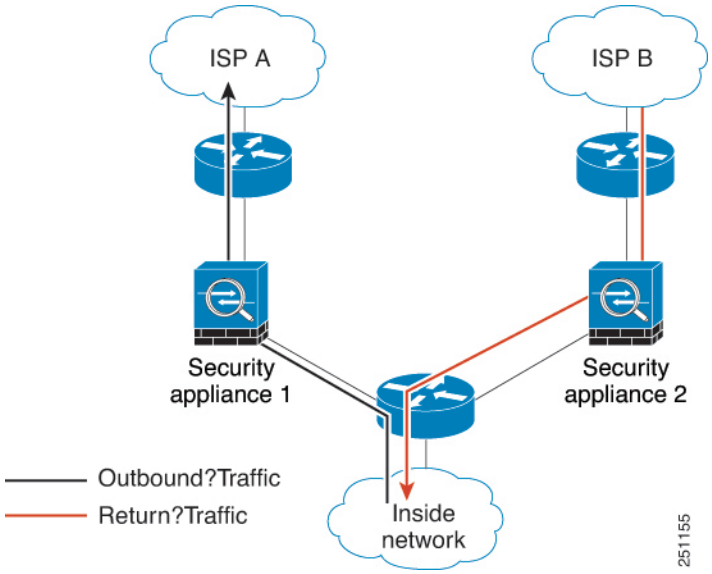
非対称ルーティングの問題

デフォルトで、Firewall Threat Defenseを通過するすべてのトラフィックは、適応型セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて許可またはドロップされます。Firewall Threat Defense では、各パケットの状態（新規接続であるか、または確立済み接続であるか）がチェックされ、そのパケットをセッション管理パス（新規接続の SYN パケット）、高速パス（確立済みの接続）、またはコントロール プレーン パス（高度なインスペクション）に割り当てることによって、ファイアウォールのパフォーマンスが最大化されます。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーのあらゆる面の再検査を受けることなくFirewall Threat Defenseを通過できます。この機能によってパフォーマンスは最大になります。ただし、SYNパケットを使用してファストパスにセッションを確立する方法、およびファストパスで行われるチェック（TCP シーケンス番号など）が、非対称ルーティングソリューションの障害となる場合があります。これは、接続の発信フローと着信フローの両方が同じ Firewall Threat Defense デバイスを通過する必要があるためです。

たとえば、ある新しい接続がセキュリティ アプライアンス 1 に到達するとします。SYNパケットはセッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続パケットがセキュリティ アプライアンス 1 を通過した場合、高速パス内のエントリに一致するのでこのパケットは送信されます。しかし、後続のパケットがセキュリティ アプライアンス 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、パケットはドロップされます。次の図は、非対称ルーティングの例を示したもので、アウトバウンド トラフィックはインバウンド トラフィックとは異なる Firewall Threat Defense を通過しています。

図 *316* : 非対称ルーティング



アップストリーム ルータに非対称ルーティングが設定されており、トラフィックが 2 つの Firewall Threat Defense デバイスを通過することがある場合は、特定のトラフィックに対して TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションを無効化します。この機能では、UDP 接続の処理と同様の方法で TCP トラフィックが処理されます。指定されたネットワークと一致した非 SYN パケットが Firewall Threat Defense デバイスに入った時点で高速パスエントリが存在しない場合、高速パスで接続を確立するために、そのパケットはセッション管理パスを通過します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

TCP ステート バイパスのガイドラインと制限事項

TCP ステート バイパスでサポートされない機能

TCP ステート バイパスを使用するときは、次の機能はサポートされません。

- アプリケーションインスペクション：インスペクションでは、着信トラフィックと発信トラフィックの両方が同じ Firewall Threat Defense を通過する必要があるため、インスペクションは TCP ステート バイパス トラフィックに適用されません。
- Snort インスペクション：インスペクションでは着信トラフィックと発信トラフィックが同じデバイスを通過する必要があります。ただし、Snort インスペクションは、TCP ステート バイパストラフィックでは自動的にバイパスされません。また、TCP ステート バイ パスを設定する同じトラフィック クラスにプレフィルタ fastpath ルールを設定する必要もあります。そうしないと、TCP ノーマライザも関与していないため、パケットが予期せずドロップされる可能性があります。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号ランダム化：Firewall Threat Defense では接続の状態が追跡されないため、これらの機能は適用されません。

- TCP 正規化：TCP ノーマライザはディセーブルです。
- ステートフル フェールオーバー。

TCP ステート バイパスのガイドライン

変換セッションは Firewall Threat Defense ごとに個別に確立されるため、TCP ステート バイパス トラフィック用に両方のデバイスでスタティック NAT を設定する必要があります。ダイナミック NAT を使用すると、デバイス 1 でのセッションに選択されるアドレスは、デバイス 2 でのセッションに選択されるアドレスとは異なります。

TCP ステート バイパスの設定

非対称ルーティング環境で TCP ステートチェックをバイパスするには、影響を受けるホストまたはネットワークのみに適用するトラフィッククラスを注意深く定義してから、サービスポリシーを使用してトラフィッククラスで TCP ステートバイパスを有効にします。また、同じトラフィックに対応するプレフィルタ fastpath ポリシーを設定してトラフィックもインスペクションをバイパスさせる必要もあります。

バイパスによってネットワークのセキュリティが低下するため、そのアプリケーションをできるだけ制限します。

手順

ステップ 1 トラフィック クラスを定義する拡張 ACL を作成します。

たとえば、10.1.1.1 to 10.2.2.2 からの TCP トラフィックのトラフィック クラスを定義するには、次の手順を実行します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。
d) オブジェクトの [名前（Name）]（bypass など）を入力します。
e) [追加（Add）] をクリックしてルールを追加します。
f) アクションは [許可（Allow）] のままにします。
g) [送信元（Source）] リストの下に 10.1.1.1 と入力して [追加（Add）] をクリックし、[宛先（Destination）] リストの下に 10.2.2.2 と入力して [追加（Add）] をクリックします。
h) [ポート（Port）] をクリックし、[選択済みの送信元ポート（Selected Source Ports）] リストの下で [TCP (6)] を選択して [追加（Add）] をクリックします。ポート番号は入力せず、すべてのポートをカバーするプロトコルとして TCP を単純に追加します。
i) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。
j) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 TCP ステート バイパスのサービス ポリシー ルールを設定します。

たとえば、このトラフィック クラスの TCP ステート バイパスをグローバルに設定するには、次の手順を実行します。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックし、[Threat Defenseサービスポリシー（Threat Defense Service Policy）] の [編集（Edit）]（ ） をクリックします。[
c) [ルールの追加（Add Rule）] をクリックします。
d) **[グローバルに適用（Apply Globally）] > [次へ（Next）]** を選択します。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) [TCP ステート バイパスの有効化（Enable TCP State Bypass）] を選択します。
g) （オプション）バイパスされる接続の [アイドル（Idle）] タイムアウトを調整します。デフォルトは 2 分です。
h) [終了（Finish）]をクリックしてルールを追加します。必要に応じて、ルールをサービス ポリシー内の必要な位置にドラッグアンドドロップします。
i) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
j) [詳細（Advanced）] で [保存（Save）]をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

ステップ 3 トラフィック クラスのプレフィルタ fastpath のルールを設定します。

プレフィルタ ルール内に ACL オブジェクトを使用できません。そのため、プレフィルタ ルールに直接か、またはクラスを定義するネットワーク オブジェクトを最初に作成するかのいずれかでトラフィック クラスを再度作成する必要があります。

次の手順では、アクセス コントロール ポリシーに接続されているプレフィルタ ポリシーがすでにあることを前提としています。プレフィルタポリシーをまだ作成していない場合は、**[ポリシー（Policies）] > [プレフィルタ（Prefilter）]**に移動して、まずポリシーを作成します。アクセス コントロール ポリシーに接続し、ルールを作成するには、この手順を使用できます。

この手順は 10.1.1.1 から 10.2.2.2 への TCP トラフィックの fastpath ルールを作成する例に沿っています。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択して、TCP バイパス サービス ポリシー ルールを含むポリシーを編集します。
b) ポリシーの説明のすぐ下の左側にある [プレフィルタ ポリシー（Prefilter Policy）] のリンクをクリックします。
c) [プレフィルタ ポリシー（Prefilter Policy）] ダイアログボックスで、適切なポリシーがまだ選択されていないデバイスに割り当てるポリシーを選択します。この時点ではまだ [OK] をクリックしないでください。

   デフォルトのプレフィルタ ポリシーにはルールを追加できないため、カスタム ポリシーを選択する必要があります。

d) [プレフィルタ ポリシー（Prefilter Policy）] ダイアログボックスで、[編集（Edit）]（✎）をクリックします。このアクションによって、ポリシーの編集が可能な新しいブラウザウィンドウが開きます。

e) [プレフィルタ ルールの追加（Add Prefilter Rule）] をクリックし、次のプロパティを使用してルールを設定します。

- [名前（Name）]：自分にとってわかりやすい名前（TCPBypass など）。
- [アクション（Action）]：[Fastpath] を選択します。
- [インターフェイスオブジェクト（Interface Objects）]：TCP ステートバイパスをグローバルルールとして設定した場合は送信元も宛先もデフォルトの [任意（any）] のままにします。インターフェイスベースのルールを作成した場合は、[送信元インターフェイス オブジェクト（Source Interface Objects）] リストのルールに使用したものと同じインターフェイス オブジェクトを選択し、宛先は [任意（any）] のままにします。
- [ネットワーク（Networks）]：[送信元ネットワーク（Source Networks）] リストに 10.1.1.1 を、[宛先ネットワーク（Destination Networks）] リストに 10.2.2.2 を追加します。ネットワーク オブジェクトを使用するか、またはアドレスを手動で追加することができます。
- [ポート（Ports）]：[選択済み送信元ポート（Selected Source Ports）] で、TCP(6) を選択し、**ポートを入力せずに** [追加（Add）] をクリックします。こうすることで、TCP ポート番号に関係なく、すべての（および唯一の）TCP トラフィックにルールが適用されます。

f) [追加（Add）] をクリックしてプレフィルタ ポリシーにルールを追加します。

g) [保存（Save）] をクリックしてプレフィルタ ポリシーに変更を保存します。

これで、プレフィルタ編集ウィンドウを閉じてアクセス コントロール ポリシーの編集ウィンドウに戻ることができます。

h) アクセス コントロール ポリシーの編集ウィンドウには [プレフィルタ ポリシー（Prefilter Policy）] ダイアログボックスが開かれたままになっています。[OK] をクリックしてプレフィルタ ポリシーの割り当てに変更を保存します。

i) プレフィルタ ポリシーの割り当てを変更した場合は、アクセス コントロール ポリシーで [保存（Save）] をクリックしてその変更を保存します。

これで、影響を受けるデバイスに変更を展開できます。

TCP シーケンスのランダム化のディセーブル

各 TCP 接続には 2 つの初期シーケンス番号（ISN）が割り当てられており、1 つはクライアントで生成され、もう 1 つはサーバで生成されます。Firewall Threat Defense デバイスは、着信と発信の両方向で通過する TCP SYN の ISN をランダム化します。

保護対象のホストのISNをランダム化することにより、攻撃者が新しい接続に使用される次のISNを予測して新しいセッションをハイジャックするのを阻止します。ただし、TCP シーケンスのランダム化は、TCP SACK（選択的確認応答）を実質的に破棄します。クライアントが認識するシーケンス番号がサーバーが認識するものと異なるためです。

たとえば、データがスクランブルされるため、必要に応じて TCP 初期シーケンス番号ランダム化を無効化することができます。次に、ランダム化を無効にする状況をいくつか示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- デバイスで eBGP マルチホップを使用していて、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- Firewall Threat Defense デバイスによる接続のシーケンス番号のランダム化が不要な WAAS デバイスを使用する場合。
- ISA 3000 のハードウェア バイパスを有効にしている場合、ISA 3000 がデータ パスの一部でなくなると、TCP 接続はドロップされます。

手順

ステップ 1 トラフィック クラスを定義する拡張 ACL を作成します。

たとえば、任意のホストから 10.2.2.2 に送信される TCP トラフィックのトラフィック クラスを定義するには、次の手順を実行します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。
d) オブジェクトの [名前（Name）]（preserve-sq-no など）を入力します。
e) [追加（Add）] をクリックしてルールを追加します。
f) アクションは [許可（Allow）] のままにします。
g) [送信元（Source）] リストを空白のままにして、[宛先（Destination）] リストの下に 10.2.2.2 と入力して、[追加（Add）] をクリックします。
h) [ポート（Port）] をクリックし、[選択済みの送信元ポート（Selected Source Ports）] リストの下で [TCP (6)] を選択して [追加（Add）] をクリックします。ポート番号は入力せず、すべてのポートをカバーするプロトコルとして TCP を単純に追加します。
i) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。
j) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 TCP シーケンス番号のランダム化を無効にするサービス ポリシー ルールを設定します。

たとえば、このトラフィック クラスのランダム化をグローバルに無効にするには、次の手順を実行します。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックし、[Threat Defenseサービスポリシー（Threat Defense Service Policy）] の [編集（Edit）]（） をクリックします。[
c) [ルールの追加（Add Rule）] をクリックします。
d) **[グローバルに適用（Apply Globally）] > [次へ（Next）]** を選択します。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) [TCP シーケンス番号のランダム化（Randomize TCP Sequence Number）] の選択を解除します。
g) （オプション）その他の接続オプションを必要に応じて調節します。
h) [終了（Finish）]をクリックしてルールを追加します。必要に応じて、ルールをサービス ポリシー内の必要な位置にドラッグアンドドロップします。
i) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
j) [詳細（Advanced）] で[保存（Save）]をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

これで、影響を受けるデバイスに変更を展開できます。

サービス ポリシーのルールの例

次のトピックにサービス ポリシー ルールの例を示します。

SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信）

攻撃者が一連の SYN パケットをホストに送信すると、SYN フラッディング サービス妨害（DoS）攻撃が発生します。これらのパケットは通常、スプーフィングされた IP アドレスから発信されます。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、正規ユーザーからの接続要求に対してサービスを提供できなくなります。

SYN フラッディング攻撃を防ぐために初期接続数を制限できます。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

接続の初期接続しきい値を超えると、Firewall Threat Defense はサーバーのプロキシとして動作し、その接続がターゲットホストの SYN キューに追加されないように、SYN Cookie 方式を使用してクライアント SYN 要求に対する SYN-ACK 応答を生成します。SYN クッキーは、基本的に秘密を作成するために、MSS、タイムスタンプ、およびその他の項目の数学的ハッシュから構築される SYN-ACK で返される最初のシーケンス番号です。Firewall Threat Defense は、正しいシーケンス番号で有効な時間ウィンドウ内にクライアントから返された ACK を受信する

と、クライアントが本物であることを認証し、サーバーへの接続を許可できます。プロキシを実行するコンポーネントは、TCP 代行受信と呼ばれます。

接続制限を設定すると、サーバを SYN フラッド攻撃から保護できます。必要に応じて、TCP 代行受信の統計情報を有効にして、ポリシーの結果をモニタできます。次の手順では、エンドツーエンドのプロセスについて説明します。

始める前に

- 保護するサーバーの TCP SYN バックログ キューより低い初期接続制限を設定していることを確認します。これより高い初期接続制限を設定すると、有効なクライアントが、SYN 攻撃中にサーバーにアクセスできなくなります。初期接続制限に適切な値を決定するには、サーバーの容量、ネットワーク、サーバーの使用状況を入念に分析してください。
- Secure Firewall Threat Defense デバイス上の CPU コア数によっては、各コアによる接続の管理方法が原因で、同時接続および初期接続の最大数が設定されている数を超える場合があります。最悪の場合、デバイスは最大 n-1 の追加接続および初期接続を許可します。ここで、n はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。モデルのコア数を確認するには、デバイスの CLI で **show cpu core** コマンドを入力します。

手順

ステップ 1 保護するサーバのリストであるトラフィック クラスを定義する拡張 ACL を作成します。

たとえば、IP アドレスが 10.1.1.5 と 10.1.1.6 の Web サーバーを保護するためのトラフィック クラスを定義します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。
d) オブジェクトの [名前（Name）]（protected-servers など）を入力します。
e) [追加（Add）] をクリックしてルールを追加します。
f) アクションは [許可（Allow）] のままにします。
g) [送信元（Source）] リストを空白のままにして、[宛先（Destination）] リストの下に 10.1.1.5 と入力して、[追加（Add）] をクリックします。
h) また、[宛先（Destination）] リストの下に 10.1.1.6 と入力して、[追加（Add）] をクリックします。
i) [ポート（Port）] をクリックし、利用可能なポートのリストで [HTTP] を選択して、[宛先に追加（Add to Destination）] をクリックします。サーバーで HTTPS 接続もサポートされている場合は、HTTPS ポートも追加します。
j) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。
k) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 初期接続制限を設定するサービス ポリシールールを設定します。

たとえば、同時初期接続の合計を 1000 接続に設定し、クライアントごとの制限を 50 接続に設定する場合は、次の手順を実行します。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックし、[Threat Defenseサービスポリシー（Threat Defense Service Policy）] の [編集（Edit）]（） をクリックします。[
c) [ルールの追加（Add Rule）] をクリックします。
d) **[グローバルに適用（Apply Globally）]** > **[次へ（Next）]** を選択します。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) **[接続（Connections）]** > **[最大初期接続数（Maximum Embryonic）]** に 1000 を入力します。
g) **[クライアントあたりの接続数（Connections Per Client）]** > **[最大初期接続数（Maximum Embryonic）]** に 50 を入力します。
h) （オプション）その他の接続オプションを必要に応じて調節します。
i) [終了（Finish）]をクリックしてルールを追加します。必要に応じて、ルールをサービスポリシー内の必要な位置にドラッグアンドドロップします。
j) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
k) [詳細（Advanced）]で[保存（Save）]をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

ステップ 3 （オプション）TCP 代行受信の統計情報のレートを設定します。

TCP代行受信では次のオプションを使用して、統計情報の収集レートが決定されます。すべてのオプションにはデフォルト値があります。それらのレートがニーズに合っている場合は、この手順を省略できます。

- [レート間隔（Rate Interval）]：履歴監視ウィンドウのサイズ（1 ～ 1440 分）。デフォルトは 30 分です。この間隔の間に、システムは攻撃の数を 30 回サンプリングします。
- [バースト レート（Burst Rate）]：Syslog メッセージ生成のしきい値（25 ～ 2147483647）。デフォルトは 1 秒間に 400 です。バースト レートを超えると、デバイスは Syslog メッセージ 733104 を生成します。
- [平均レート（Average Rate）]：Syslog メッセージ生成の平均レートのしきい値（25 ～ 2147483647）。デフォルトは 1 秒間に 200 回です。平均レートを超えると、デバイスは Syslog メッセージ 733105 を生成します。

これらのオプションを調整する場合は、次の手順を実行します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) **[FlexConfig]** > **[テキスト オブジェクト（Text Object）]** を選択します。
c) システム定義オブジェクト threat_defense_statistics の [編集（Edit）]（） をクリックします。

d) 値は直接変更できますが、[オーバーライド（Override）]セクションを開き、[追加（Add）]をクリックして、デバイス オーバーライドを作成することを推奨します。
e) （アクセス コントロール ポリシーの割り当てを介して）サービス ポリシーを割り当てるデバイスを選択し、[追加（Add）] をクリックして、選択済みリストにデバイスを移動します。
f) [オーバーライド（Override）] をクリックします。
g) オブジェクトには 3 つのエントリが必要なため、3 になるまで必要に応じて [カウント（Count）] をクリックします。
h) レート間隔、バースト レート、および平均レートとして 1 ～ 3 の順序で必要な値を入力します。オブジェクトの説明を参照し、正しい順序で値を入力していることを確認してください。
i) [オブジェクトのオーバーライド（Object Override）] ダイアログボックスで [追加（Add）] をクリックします。
j) [テキスト オブジェクトの編集（Edit Text Object）] ダイアログボックスで [保存（Save）] をクリックします。

ステップ 4 TCP 代行受信の統計情報を有効にします。

TCP 代行受信の統計情報を有効にするには FlexConfig ポリシーを設定する必要があります。

a) **[デバイス（Devices）] > [FlexConfig]** を選択します。
b) ポリシーをすでにデバイスに割り当てている場合は、そのポリシーを編集します。割り当てていない場合は、新しいポリシーを作成して、影響を受けるデバイスに割り当てます。
c) [利用可能な FlexConfig（Available FlexConfig）] リストで [Threat_Detection_Configure] を選択して [>>] をクリックします。オブジェクトが [選択済み追加 FlexConfig（Selected Append FlexConfigs）] リストに追加されます。
d) [保存（Save）] をクリックします。
e) （オプション）[プレビュー設定（Preview Config）] をクリックし、いずれかのデバイスを選択することで、設定が正しいことを確認できます。

次の展開時にデバイスに書き込まれる CLI コマンドが生成されます。それらのコマンドには、サービス ポリシーおよび脅威検出の統計情報に必要なコマンドが含まれます。プレビューの下にスクロールして、追加された CLI を確認します。デフォルト値を使用している場合、TCP 代行受信の統計情報のコマンドは、次のようになります（わかりやすくするために改行されています）。

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

ステップ 5 これで、影響を受けるデバイスに変更を展開できます。

ステップ 6 次のコマンドを使用して、デバイスの CLI から TCP 代行受信の統計情報をモニターします。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]：攻撃を受けて保護された上位 10 のサーバーを表示します。**all** キーワードは、トレースされているすべてのサーバーの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。

システムはレート間隔の間に攻撃の数を 30 回サンプリングするため、デフォルトの 30 分間隔の場合、60 秒ごとに統計情報が収集されます。

（注）
shun コマンドを使用して、ホスト IP アドレスへの攻撃をブロックできます。ブロックを削除するには、**no shun** コマンドを使用します。

- **clear threat-detection statistics tcp-intercept**TCP 代行受信の統計情報を削除します。

例：

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
 Time)>
------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

Firewall Threat Defense デバイスをトレースルートに表示する

デフォルトでは、Firewall Threat Defense デバイスは、トレースルートにホップとして表示されません。表示されるようにするには、デバイスを通過するパケットの存続可能時間を減らし、ICMP 到達不能メッセージのレート制限を増やす必要があります。これを行うには、サービスポリシールールを設定し、ICMP プラットフォーム設定ポリシーを調整する必要があります。

（注） 存続可能時間を減らすと、TTL が 1 のパケットはドロップされますが、接続に TTL がもっと長いパケットが含まれている可能性があるという仮定の下に、セッションに対して接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL が 1 で送信されるため、存続可能時間を減らすと予期しない結果が生じることがある点に注意してください。トラフィック クラスを定義する際には、これらの考慮事項に注意してください。

手順

ステップ 1 Traceroute レポートを有効にするトラフィック クラスを定義する拡張 ACL を作成します。

たとえば、OSPF トラフィックを除く、すべてのアドレスのトラフィック クラスを定義するには、次の手順を実行します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。

d) オブジェクトの [名前（Name）]（traceroute-enabled など）を入力します。
e) [追加（Add）] をクリックして、OSPF を除外するルールを追加します。
f) アクションを [ブロック（Block）] に変更し、[ポート（Port）] をクリックします。[宛先ポート（Destination Ports）] リストの下でプロトコルとして [OSPFIGP (89)] を選択し、[追加（Add）] をクリックして、プロトコルを選択済みリストに追加します。
g) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、OSPF ルールを ACL に追加します。
h) [追加（Add）] をクリックして、その他すべての接続を含めるルールを追加します。
i) アクションは [許可（Allow）] のままにして、[送信元（Source）] と [宛先（Destination）] リストの両方を空にします。
j) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。

   OSPF 拒否ルールが [すべて許可（Allow Any）] ルールの上にあることを確認します。必要に応じて、ルールをドラッグアンドドロップして移動します。

k) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 存続可能時間の値をデクリメントするサービス ポリシールールを設定します。

たとえば、存続可能時間をグローバルにデクリメントするには、次の手順を実行します。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックし、[Threat Defenseサービスポリシー（Threat Defense Service Policy）] の [編集（Edit）]（✎） をクリックします。[
c) [ルールの追加（Add Rule）] をクリックします。
d) [グローバルに適用（Apply Globally）] を選択して、[次へ（Next）] をクリックします。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) [デクリメント TTL の有効化（Enable Decrement TTL）] を選択します。
g) （オプション）その他の接続オプションを必要に応じて調節します。
h) [終了（Finish）] をクリックしてルールを追加します。必要に応じて、ルールをサービスポリシー内の必要な位置にドラッグアンドドロップします。
i) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
j) [詳細（Advanced）] で [保存（Save）] をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

   これで、影響を受けるデバイスに変更を展開できます。

ステップ 3 ICMP 到達不能メッセージのレート制限を増やします。

a) **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択します。

b) ポリシーをすでにデバイスに割り当てている場合は、そのポリシーを編集します。割り当てていない場合は、新しい Threat Defense プラットフォーム設定ポリシーを作成して、影響を受けるデバイスに割り当てます。
c) 目次から [ICMP] を選択します。
d) [レート制限（Rate Limit）] を（50 などに）増やします。レート制限内で十分な数の応答が生成されるように、[バーストサイズ（Burst Size）] を 10 などに増やすこともできます。

ICMP ルールテーブルは、このタスクには無関係なので、空のままにすることができます。

e) [保存（Save）] をクリックします。

ステップ 4 これで、影響を受けるデバイスに変更を展開できます。

サービス ポリシーのモニタリング

デバイスの CLI を使用してサービスポリシー関連の情報をモニターできます。次に、便利なコマンドをいくつか示します。

- **show conn** [**detail**]

  接続情報を表示します。詳細情報は、フラグを使用して特別な接続の特性を示します。たとえば、「b」フラグは、TCP ステート バイパスの対象であるトラフィックを示します。

  detail キーワードを使用すると、デッド接続検出（DCD）プローブの情報が表示されます。この情報は、発信側と応答側で接続がプローブされた頻度を示します。たとえば、DCD 対応接続の接続詳細は次のようになります。

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show service-policy**

  Dead Connection Detection（DCD; デッド接続検出）の統計情報を含むサービス ポリシーの統計情報を表示します。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  攻撃を受けて保護された上位 10 サーバーを表示します。**all** キーワードは、トレースされているすべてのサーバーの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。システムはレート間隔の間に攻撃の数を 30 回サンプリングするため、デフォルトの 30 分間隔の場合、60 秒ごとに統計情報が収集されます。

Threat Defense サービスポリシーの履歴

特長	最小 Firewall Management Center	最小 Firewall Threat Defense	説明
Threat Defense サービスポリシー	6.3	任意（Any）	Threat Defense サービスポリシーをアクセス コントロール ポリシーの高度なオプションの一部として設定できるようになりました。Threat Defense サービスポリシーを使用して、特定のトラフィッククラスにサービスを適用できます。サポートされている機能には、TCP ステートバイパス、TCP シーケンス番号のランダム化、パケットでの存続可能時間（TTL）の値の減分、デッド接続検出、トラフィック クラスごとおよびクライアントごとの接続および初期接続の最大数の制限の設定、初期接続、ハーフクローズ接続、およびアイドル接続のタイムアウトなどがあります。 新規画面：**[ポリシー（Policies）]**>**[アクセス制御（Access Control）]**>**[アクセス制御（Access Control）]**、[詳細（Advanced）] タブ、[Threat Defenseサービスポリシー（Threat Defense Service Policy）]。 サポートされているプラットフォーム： Secure Firewall Threat Defense
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	6.5	任意（Any）	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新しい/変更されたコマンド：**show conn**（出力のみ） サポートされているプラットフォーム： Secure Firewall Threat Defense
初期接続の最大セグメントサイズ（MSS）を設定します。	7.1	任意（Any）	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 追加または変更された画面：[Add/Edit Service Policy] ウィザードの [Connection Settings]

第 46 章

脅威の検出

脅威検出のポートスキャンディテクタは、あらゆるタイプのトラフィックでポートスキャンアクティビティを検出および防止し、最終的な攻撃からネットワークを保護するために設計されたメカニズムです。ポートスキャントラフィックは、許可されたトラフィックと拒否されたトラフィックの両方で効率的に検出できます。

ポートスキャンとは、攻撃者が攻撃の準備段階として使用することが多いネットワーク偵察の形式です。ポートスキャンでは、攻撃者はホストがサポートするネットワークプロトコルまたはサービスのタイプを特定し、細工されたパケットを標的のホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

- ポートスキャンの検出と防止 （1943 ページ）
- ポートスキャン防止のベストプラクティス （1945 ページ）
- 脅威検出の要件と前提条件 （1946 ページ）
- 脅威検出のガイドラインと制限事項 （1946 ページ）
- ポートスキャンの検出と防止の設定 （1947 ページ）
- 脅威検出のモニタリング （1950 ページ）
- 脅威検出の履歴 （1952 ページ）

ポートスキャンの検出と防止

脅威検出を使用して、ポートスキャンアクティビティを特定します。システムを使用してポートスキャンを検出し、検出時にイベントを発行できます。必要に応じて、スキャナを自動的にブロックしてポートスキャンを防止するようにシステムを設定することもできます。ポートスキャンを防止する場合、システムはイベントを送信し、設定された期間攻撃者をブロックします。

ポートスキャン検出の事前定義された感度レベル

検出設定を構成するときは、以下の事前定義された感度レベルから選択します。[カスタム（Custom）] を除き、各レベルには、設定された時間間隔内にスキャンする必要があるポート

（TCP/UDP）、プロトコル（IP）、またはホスト（TCP/UDP/IP/ICMP）の数に対する各プロトコルの値が事前に設定されています（秒単位）。また、すべてのタイプのスキャン/スイープが有効になります。

（注） ポート/プロトコルをカウントするときに、現在のパケットのポート/プロトコルが前のパケットと異なる場合、脅威検出によって番号が増加します。たとえば、10 個のポート セットでランダムに接続を開くアプリケーションがある場合、スキャンされるポートの合計数が増えすぎて、インターバル内にポート番号を超えてしまう可能性があります。システムは一意のポートだけをカウントするわけではありません。

間隔内でこの数を超えると、スキャン攻撃を示している可能性があります。ポートスキャンイベントは、移動時間間隔枠で、ポート/プロトコル/ホストの数が超過した場合にのみ生成されます。

- [低（Low）]：このレベルでは、ポートスキャン検出に最短の時間枠を使用し、ポート/プロトコル/ホスト数を高くします。したがって、最もアグレッシブなスキャナのポートスキャンイベントのみが表示されます。誤検出を抑えるためには、この感度レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタ処理されたスキャン）が見逃される可能性があることに注意してください。
  - **間隔**（TCP/UDP/IP/ICMP）：60 秒。
  - **TCP/UDP ポートスキャンのポート数**：120。
  - **TCP/UDP ポートスイープのホスト数**：180。
  - **IP プロトコルスキャンのプロトコル数**：30。
  - **IP プロトコルスイープのホスト数**：25。
  - **ICMP ホスト スイープのホスト数**：50。
- [中（Medium）]：このレベルでは、間隔とポート/プロトコル/ホスト数の両方に中程度の値が使用されます。ただし、ネットワークアドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。このようなホストはスキャナ無視リストに追加します。これはデフォルトの感度レベルであり、初期使用に適しています。
  - **間隔**（TCP/UDP/IP/ICMP）：90 秒。
  - **TCP/UDP ポートスキャンのポート数**：90。
  - **TCP/UDP ポートスイープのホスト数**：150。
  - **IP プロトコルスキャンのプロトコル数**：15。
  - **IP プロトコルスイープのホスト数**：20。
  - **ICMP ホストスイープのホスト数**：30。

- [高（High）]：このレベルでは、ポートスキャン検出にはるかに長い時間枠を使用し、ポート/プロトコル/ホストの数を低くします。このレベルでは、最もアグレッシブでないポートスキャン/スイープのイベントも表示される可能性が高いため、すべての攻撃者を認識できる確率が高まります。一方、このレベルでは発行されるポートスキャンイベントの数が最も多くなり、誤検出の数が最大になる可能性があります。
  - **間隔**（TCP/UDP/IP/ICMP）：600 秒（10 分）。
  - **TCP/UDP ポートスキャンのポート数**：60。
  - **TCP/UDP ポートスイープのホスト数**：100。
  - **IP プロトコルスキャンのプロトコル数**：10。
  - **IP プロトコルスイープのホスト数**：10。
  - **ICMP ホストスイープのホスト数**：20。
- [カスタム（Custom）]：事前定義された感度レベルとは異なる設定を行う場合、または特定のタイプのスキャン/スイープを無効にする場合、レベルは自動的にカスタムに切り替わります。オプションを調整する場合は、まず目的に最も近いレベルを選択し、必要に応じて値を編集します。

ポートスキャン防止のベストプラクティス

ポートスキャン防止モードでは、意図しないトラフィックの停止が発生する場合があります。防止モードでは、ホストは設定された期間中、すべてのプロトコルでネットワークをさらに詳しくスキャンすることができません。正当なトラフィックがブロックされないように、検出と防止のパラメータを注意して確認してください。

防止モードでポートスキャンを設定する前に、以下の手順を実行することを強く推奨します。

1. 検出モードでポートスキャンの使用を開始します。
2. 生成されたポートスキャンイベントを確認します。
3. 感度レベル、モニタリング対象ネットワーク、スキャナの無視リスト、およびターゲットの無視リストを調整します。事前定義された感度レベルが状況に適していない場合は、必要に応じてカスタム設定を構成します。
4. 誤検出がなくなり、イベントレートがネットワーク内のポートスキャンの正確な状況を反映するまで、このプロセスを繰り返します。識別された残りのスキャナをブロックしても問題がないことを確認します。

脅威検出の要件と前提条件

モデルのサポート

バージョン 7.2 以降および Snort 3 を実行している Threat Defense 。

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

脅威検出のガイドラインと制限事項

- 脅威検出には Snort 3 が必要です。管理対象デバイスは、バージョン 7.2 以降である必要があります。Snort 2、または 7.2 より前のバージョンのデバイスでは、NAP ポリシーを使用してポートスキャンを設定できます。脅威検出機能は、NAP ポリシーのポートスキャン機能と同じではないことに注意してください。アクセス コントロール ポリシーに割り当てられている Snort 3 を使用していない、または バージョン 7.2 より前のデバイスがある場合、それらのサポートされていないデバイスに脅威検出設定は展開されません。
- 7.1 以前を実行しているデバイスの NAP ポリシーでポートスキャンを設定した場合、その設定は、7.2 へのアップグレード時に脅威検出機能に変換されません。脅威検出を手動で設定する必要があります。NAP と脅威検出のポートスキャンオプションは似ていますが、全く同じではありません。
- 脅威検出を設定すると、NAP ポリシーのポートスキャン設定はすべて無視され、脅威検出をサポートするデバイスでは設定されません。
- Snort 3 の NAP ポートスキャン機能は、バージョン 7.2 以降のデバイスでは常に無視されます。ポートスキャンを設定するには、Threat Defense 設定を使用する必要があります。
- 脅威検出は、デバイスを通過するトラフィックに対してのみ機能します。デバイス宛てのトラフィックに対しては機能しません。
- 高可用性設定では、ポートスキャン統計はスタンバイ装置に同期されません。ただし、ブロックされたホストは同期され、フェールオーバー時に期間が終了するまでブロックされ続けます。
- （Threat Defense バージョン 7.2 ～ 7.7 を実行しているデバイス）。クラスタ内のノードの場合、個々のクラスタ ノードで検出と防御が行われます。つまり、ノード B がホストか

らのトラフィックを検出してブロックした場合、ポートスキャン統計はクラスタノード間で同期されないため、ノード A はそのアクションを認識しません。

- インラインセットの場合、または等コストマルチパス（ECMP）トラフィックゾーンの一部として設定されているインターフェイスの場合、検出と防御はゾーンレベルで行われます。ホストのポートスキャン統計は、ゾーンのすべてのインターフェイスにわたって蓄積されます。同様に、ホストが設定されたしきい値を超えると、対応するゾーンのすべてのインターフェイスでブロックされます。
- 脅威検出機能によって生成されるポートスキャン イベントは、Snort がポートスキャンで発行するものと同じですが、イベントを取得するためにポートスキャンの侵入ルールを有効にする必要はありません。脅威検出は、侵入ポリシーの実装に関係なく機能します。

ポートスキャンの検出と防止の設定

ポートスキャンとは、攻撃者が攻撃の準備段階として使用することが多いネットワーク偵察の形式です。ポートスキャンでは、攻撃者はホストがサポートするネットワークプロトコルまたはサービスのタイプを特定し、細工されたパケットを標的のホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

脅威検出を有効にして、ポート スキャン アクティビティを監視できます。また、必要に応じて一定期間スキャナを自動的にブロックすることができます。

始める前に

FQDN、ワイルドカードマスク、any、any-ipv4、および any-ipv6 ネットワークオブジェクトは、ポートスキャン設定ではサポートされていません。これらのオブジェクトは、[監視（Monitor）]、[スキャナを無視（Ignore Scanner）]、[ターゲットを無視（Ignore Target）]、および [除外（Exclude）] フィールドには表示されません。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。次に、[Threat Detection] の横にある [編集（Edit）]（✎） をクリックします。

ステップ 2 [脅威の検出（Threat Detection）] ウィンドウで、 [ポートスキャンモード（Portscan mode）] を選択します。

- [無効（Disable）]：脅威検出をオフにします。これは、デフォルトのモードです。[デフォルトに戻す（Revert to Defaults）] をクリックして、この未設定の状態に戻すことができます。

- [検出（Detection）]：ポートスキャン検出を実行しますが、問題に対するアラートのみを送信します。潜在的な攻撃者に対してアクションは実行しません。過剰な誤検出を避けるために、Threat Detection の設定を微調整するまで、最初はこのモードを使用することをお勧めします。
- [防止（Prevention）]：ポートスキャン検出を実行し、特定されたスキャナ、つまりポートスキャンを実行しているホストをアクティブにブロックします。

ステップ 3 [トラフィック選択（Traffic Selection）] オプションを設定します。

トラフィック選択オプションは、モニタリング対象のネットワーク、モニタリング対象の接続タイプ、およびスキャナまたはターゲットホストをモニタリング対象のネットワークから除外するかどうかを決定します。デフォルトでは、システムはすべてのネットワークで許可された接続をモニタリングします。

- [トラフィックの検出（Detection On Traffic）]：ポートスキャン アクティビティをモニタリングする接続タイプ（[許可された（Permitted）]、[拒否された（Denied）]、または [すべて（All）] のトラフィックを選択します。デフォルトは [許可された（Permitted）] です。
- [モニタリング（Monitor）]：ポートスキャンまたはスイープアクティビティをモニタリングするネットワークを定義するネットワークオブジェクトを選択します。デフォルトは、すべてのネットワーク（IPv4 または IPv6）です。このオプションを使用して、スキャンを信頼できないネットワークに制限できます。
- [スキャナを無視（Ignore Scanner）]：モニタリング対象のネットワークの範囲内から、無視する必要があるホストまたはネットワークを定義するネットワークオブジェクトを選択します。たとえば、ネットワークをテストするために独自のスキャナを設定した場合は、スキャナのアドレスを除外して、アドレスに関する不要なレポートを回避できます。モニタリング対象ネットワークの外部にあるアドレスはすでに無視されているため、含めないでください。
- [ターゲットを無視（Ignore Target）]：ターゲット（ポートスキャンまたはスイープの対象）として無視する必要があるホストまたはネットワークを定義するネットワークオブジェクトを選択します。

ステップ 4 [設定（Configuration）] タブをクリックし、スキャン感度レベルを選択します。

事前定義された感度レベル（[低（Low）]、[中（Medium）]、および [高（High）]）を設定することで、ポートスキャンオプションの値を徐々にアグレッシブにできます。たとえば、[低（Low）] を選択すると表示されるポートスキャンイベントが少なくなり、[中（Medium）] または [高（High）] を選択した場合よりも攻撃者を見逃す可能性が高くなります。一方、[高（High）] を選択するとより多くのイベントが表示され、誤検出が増える可能性があります。デフォルトのレベルは [中（Medium）] です。レベルについての詳細は、ポートスキャン検出の事前定義された感度レベル （1943 ページ） を参照してください。

レベルを選択すると、プロトコルセクション内に関連する値（**TCP**、**UDP**、**IP**、および**ICMP**）が表示されます。プリセット値のいずれかを変更するか、スキャンのタイプを無効にすると、感度モードは自動的に [カスタム（Custom）] に変更されます。

各プロトコルセクション内のオプションは次のとおりです。

- [間隔（Interval）]：ポートスキャンまたはポートスイープの設定値を超過する時間範囲（秒単位）。たとえば、90 秒を選択し、TCP ポートスキャンポートの数として 60 を選択した場合、スキャナがポートスキャンと見なされるには、90 秒以内にホスト上の 60 ポートを試行する必要があります。システムは、指定された間隔内にポート、プロトコル、またはホスト（ポートスイープの場合）の数を超えた場合にのみ、イベントを生成します。

  30～600秒の範囲を指定できます。期間が長いほど、ホストがスキャナとして識別される可能性が高くなります。

- [ポートスキャン（TCP/UDP）（Portscan (TCP/UDP)）]：単一のホストに対してポートスキャンをモニタリングするかどうかを選択し、ポートスキャン攻撃として見なされるために間隔内にスキャンする必要があるポートの数を指定します。指定できる範囲は 1 ー 256 です。

- [ポートスイープ（TCP/UDP）（Portsweep (TCP/UDP)）]：複数のホストに対してポートスイープをモニタリングするかどうかを選択し、ポートスイープ攻撃として見なされるために間隔内に特定のポートでスキャンする必要があるホストの数を指定します。指定できる範囲は 1 ー 256 です。

- [プロトコルスキャン（IP）（Protocol Scan (IP)）]：単一のホストに対してプロトコルスキャンをモニタリングするかどうかを選択し、プロトコルスキャン攻撃として見なされるために間隔内にスキャンする必要があるプロトコルの数を指定します。指定できる範囲は 1 ー 255 です。

- [プロトコルスイープ（IP）（Protocol Sweep (IP)）]：複数のホストに対してプロトコルスイープをモニタリングするかどうかを選択し、プロトコルスイープ攻撃として見なされるために間隔内に特定のプロトコルでスキャンする必要があるホストの数を指定します。指定できる範囲は 1 ー 256 です。

- [ホストスイープ（ICMP）（Hostsweep (ICMP)）]：複数のホストに対して ICMP ホストスイープをモニタリングするかどうかを選択し、ホストスイープ攻撃として見なされるために間隔内にスキャンする必要があるホストの数を指定します。指定できる範囲は 1 ー 256 です。

ステップ 5 防止モードを選択した場合は、[防止（Prevention）]タブをクリックし、オプションを設定します。

防止モードでは、ホストは設定された期間中、すべてのプロトコルでネットワークをさらに詳しくスキャンすることを自動的にブロックされます。正当なトラフィックがブロックされないように、検出と防止のパラメータを注意して確認してください。

- [除外（Exclude）]：モニタリング対象ネットワークの範囲内から、自動ブロッキングから除外するホストまたはネットワークを定義するネットワークオブジェクトを選択します。これらのホストがスキャン検出パラメータを超過しても、システムはそれらをブロックしません。

- [期間（Duration）]：自動的にブロックされたスキャナホストがあらゆる種類のトラフィックをデバイスを介して送信できないようにする期間（秒単位）。期間が終了すると、ホス

トは自動的にクリアされ、再びデバイスを介してトラフィックを送信できるようになります。指定できる範囲は 600 ー 2592000 秒です。デフォルトは 3600 秒（1 時間）です。

ホストのブロックを手動で解除する必要がある場合は、ホストをブロックしているファイアウォールに SSH で接続し、**clear threat-detection portscan attacker** コマンドを使用します。

ステップ 6 [OK] をクリックして、脅威検出の設定を保存します。

ステップ 7 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

脅威検出のモニタリング

ここでは、ポートスキャン アクティビティをモニタリングする方法について説明します。

ポートスキャンアラートの表示

ポートスキャンアクティビティは、既存のポートスキャン固有の侵入イベントを通じて警告されます。ジェネレータ ID（GID）122 および SID 1 ～ 27 の Snort ID を持つ侵入イベントが生成されます。これらのイベントの場合、（port_scan）文字列がイベントメッセージの先頭に追加されます。イベントには、アラートをトリガーした統計情報を含むパケットデータとともにパケット情報が含まれます。

ポートスキャンイベントを表示するには、**[分析（Analysis）] > [侵入（Intrusion）] > [イベント（Events）]** に移動します。

ポートスキャンは、侵入ポリシーまたは NAP 設定に関係なく、これらのイベントを発行します。イベントは、関連するプロトコルに設定された時間間隔内に、スキャナがさまざまなタイプのスキャンまたはスイープに設定されたポート/プロトコル/ホストの数を超えた場合にのみ発行されます。1 つのホストからのポートスキャンは、しきい値に達するとすぐに、設定された間隔ごとに 1 つのイベントを生成します。同じホストが同じ間隔で新しいポートスキャンを開始した場合、イベントは報告されません。

次の表に、発生する可能性のあるイベントを示します。

表 *91* : ポートスキャンイベント

ポートスキャン タイプ	侵入イベント
TCP 通常、デコイ、分散スキャン	122:1（port_scan）TCP ポートスキャン
TCP ポートスイープ	122:3（port_scan）TCP ポートスイープ

ポートスキャン タイプ	侵入イベント
TCP 分散型スキャン	122:4（port_scan）TCP 分散型ポートスキャン
IP 通常、デコイ、分散プロトコルスキャン n	122:9（port_scan）IP プロトコル スキャン
IP プロトコルスイープ	122:11（port_scan）IP プロトコルスイープ
IP 分散型スキャン	122:12（port_scan）IP 分散型プロトコル スキャン
UDP 通常、デコイ、分散スキャン	122:17（port_scan）UDP ポートスキャン
UDP ポートスイープ	122:19（port_scan）UDP ポートスイープ
UDP 分散型スキャン	122:20（port_scan）UDP 分散型ポートスキャン
ICMP スイープ	122:25（port_scan）ICMP スイープ
ポートスキャン ブロック	122:100（port_scan）ポートスキャン アクティビティによりホストがブロックされました

ファイアウォールでのポートスキャンのモニタリング

ポートスキャンをモニタリングするには、デバイスCLIにログインして以下のコマンドを使用します。

- **show threat-detection portscan** ［**attacker** ｜ **target** ｜ **shun**］

  スキャナのIPアドレス、回避（ブロック）されたスキャナ、およびスキャンまたはスイープの対象となったホストを表示します。

- **show threat-detection portscan statistics** ［**host** ［*ipv4_address* ｜ *ipv6_address*］］［**protocol** {**tcp** ｜ **udp** ｜ **ip** ｜ **icmp**} ］

  ポートスキャンシステムに関連する統計情報を表示します。ホスト、プロトコル、またはホストとプロトコルを指定して、出力をフィルタ処理して目的の情報を得ることができます。

- **clear threat-detection portscan** ［**attacker** ｜ **target** ｜ **shun**］［*ipv4_address mask* ｜ *ipv6_address/prefix* ］

  スキャナ（攻撃者）または特定されたターゲットのブロックを手動で解除します。すべての攻撃者、ターゲット、または回避されたホストをクリアするには、パラメータを指定せずにコマンドを入力します。

- **clear threat-detection portscan statistics** ［**host** ［*ipv4_address* ｜ *ipv6_address*］］［**protocol** {**tcp** ｜ **udp** ｜ **ip** ｜ **icmp**} ］

  ポートスキャンに関連する統計情報を消去して、このデバイスを介したスキャンの現在の状態をより明確に確認できるようにします。すべての統計情報をクリアするには、パラ

メータを指定せずにコマンドを入力します。または、ホスト、プロトコル、またはホストとプロトコルを指定して、指定された項目のみをリセットします。

ホストのブロック解除

脅威検出を防御モードに設定し、攻撃者ではないことが判明しているホストをシステムがブロックする場合は、期間が終了してホストのブロックが自動的に解除される前に、ホストのブロックを手動で解除できます。

ホストのブロックを手動で解除するには、ホストがブロックされているデバイスのCLIにログインし、**clear threat-detection portscan attack** コマンドを入力します。次に例を示します。

```
> clear threat-detection portscan attacker 10.2.0.100 255.255.255.255
1 tracker object deleted and 1 shun entry removed
```

防止設定の除外リストにホスト IP を追加することを検討してください。

脅威検出の履歴

特長	最小 Firewall Management Center	最小 Firewall Threat Defense	説明
ポートスキャン検出の改善。	7.2	Snort 3 を実行する 7.2	改良されたポートスキャンディテクタを使用すると、ポートスキャンを検出または防止するようにシステムを簡単に設定できます。保護するネットワークを絞り込んだり、感度を設定したりできます。Snort 2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスの場合、ポートスキャン検出には引き続きネットワーク分析ポリシーを使用します。 新規/変更された画面：[脅威検出（Threat Detection）] をアクセス コントロール ポリシーの [詳細（Advanced）] タブに追加しました。 新規/変更されたコマンド：**clear threat-detection portscan**, **show threat-detection portscan**。

第 47 章

エレファントフローの検出

エレファントフローは（合計バイト数が）非常に大きい連続フローであり、ネットワークリンク上で測定されるTCP（または他のプロトコル）フローによって設定されます。デフォルトでは、エレファントフローとは1 GB/10 秒を超えるフローです。これらのフローは、Snort コアでのパフォーマンス拘束の原因となります。エレファントフローはそれほど多くありませんが、一定期間にわたって総帯域幅の不均衡な割合を占める可能性があります。これらのフローは、CPU 使用率の上昇やパケットドロップなどの問題につながる可能性があります。

Firewall Management Center 7.2.0 以降（Snort 3 デバイスのみ）では、エレファントフロー機能を使用して、エレファントフローを検出および修復できます。こうしたアクションはシステムストレスを軽減し、前述の問題を解決するために役立ちます。

- エレファントフローの検出と修復について （1953 ページ）
- インテリジェント アプリケーション バイパスからのエレファントフローのアップグレード （1954 ページ）
- エレファントフローの設定 （1954 ページ）

エレファントフローの検出と修復について

エレファントフロー検出機能を使用して、エレファントフローを検出して修復できます。次の修復アクションを適用できます。

- **エレファントフローをバイパスする**：Snort インスペクションをバイパスするようにエレファントフローを設定できます。このアクションが設定されている場合、Snortはエレファントフローからパケットを受信しません。
- **エレファントフローをスロットルする**：フローにレート制限を適用して、フローの検査を続行できます。フローレートは動的に計算され、フローレートの 10% が削減されます。Snort は、判定結果（フローレートが 10% 少ない QoS フロー）をファイアウォールエンジンに送信します。識別されていないアプリケーションを含むすべてのアプリケーションをバイパスすることを選択した場合、いずれのフローに対してもスロットルアクション（レート制限）を設定できません。

（注） エレファントフロー検出を機能させるには、Snort 3 を検出エンジンにする必要があります。

インテリジェントアプリケーションバイパスからのエレファントフローのアップグレード

バージョン 7.2.0 以降の Snort 3 デバイスでは、インテリジェント アプリケーション バイパス（IAB）は廃止されました。

7.2.0 以降を実行しているデバイスの場合、AC ポリシー（[詳細設定（Advanced Settings）] タブ）の [エレファントフロー設定（Elephant Flow Settings）] セクションでエレファントフロー設定を構成する必要があります。

7.2.0（または以降）へのアップグレード後、Snort 3 デバイスを使用している場合、エレファントフロー構成設定は、[インテリジェントアプリケーションバイパス設定（Intelligent Application Bypass Settings ）] セクションからではなく、[エレファントフロー設定（Elephant Flow Settings ）] セクションから選択されて展開されるため、エレファントフロー構成設定に移行していない場合、次の展開時にデバイスのエレファントフロー構成は失われます。

次の表は、Snort 3 または Snort 2 エンジンを実行しているバージョン 7.2.0 以降およびバージョン 7.1.0 以前に適用できる IAB またはエレファントフロー構成を示しています。

Firewall Management Center	Firewall Threat Defense	エレファントフローまたは IAB 構成
Firewall Management Center 7.0 または 7.1	Snort 2 デバイス	IAB の構成が適用されます。
	Snort 3 デバイス	IAB の構成が適用されます。
Firewall Management Center 7.2.0	Snort 2 デバイス	IAB の構成が適用されます。
	Snort 3 デバイス（7.1.0 以前）	IAB の構成が適用されます。
	Snort 3 デバイス（7.2.0 以降）	エレファントフローの構成が適用されます。

エレファントフローの設定

エレファントフローでアクションを実行するようにエレファントフローを設定できるため、システムの危機、高い CPU 使用率、パケットドロップなどの問題の解決に役立ちます。

注目 エレファントフロー検出は、Snortを介して処理されない、事前フィルタリングされたフロー、信頼されたフロー、または高速転送フローには適用できません。エレファントフローはSnortによって検出されるため、エレファントフロー検出は暗号化されたトラフィックには適用されません。

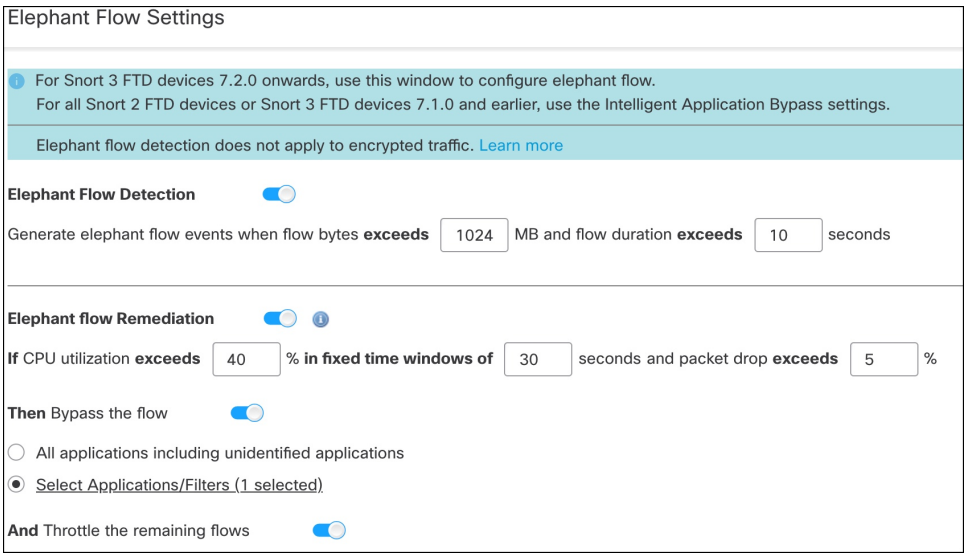
手順

ステップ1 アクセス コントロール ポリシー エディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。次に、[エレファントフロー設定（Elephant Flow Settings ）] の横にある [編集（Edit）]（✎） をクリックします。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

図 *317*：エレファントフロー検出の設定

図 *318*：エレファントフロー検出の設定



ステップ2 [エレファントフロー検出（Elephant Flow Detection）] トグルボタンはデフォルトで有効になっています。フローバイトとフロー期間の値を設定できます。設定した値を超えると、エレファントフローイベントが生成されます。

ステップ3 エレファントフローを修復するには、[エレファントフローの修復（Elephant Flow Remediation）] トグルボタンを有効にします。

ステップ4 エレファントフローの修復基準を設定するには、CPU 使用率 %、固定時間ウィンドウの継続時間、およびパケットドロップ % の値を設定します。

CPU 使用率はエレファントフローごとに計算され、フロー遅延から導出されます。CPU 使用率が設定されたしきい値を超えて、固定時間枠やパケットドロップなどの他の設定も一致した場合、エレファントフロー修復アクションが適用されます。同様に、パケットドロップの計算は、CPU ごとのドロップされたパケット数に基づきます。パケットドロップ率が特定の CPU で設定された値を超えると、修復アクションが適用されます。たとえば、値がデフォルトに設定されているとします。つまり、CPU 使用率が 40%、固定時間枠が 30 秒、パケットドロップが 5% に設定されているとします。特定の CPU で、5% を超えるパケットドロップが検出され、フローごとの CPU 使用率が 30 秒の固定時間枠内で 40% を超えた場合、フローはバイパスまたはスロットリングされます。

ステップ 5 設定された基準を満たしている場合、エレファントフローの修復に対して次のアクションを実行できます。

1. [フローをバイパスする（Bypass the flow）]：選択したアプリケーションまたはフィルタの Snort インスペクションをバイパスするには、このボタンを有効にします。次から選択します。
   - [識別されていないアプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）]：すべてのアプリケーション トラフィックをバイパスするには、このオプションを選択します。このオプションを設定すると、すべてのフローにスロットルアクション（レート制限）を設定できなくなります。
   - [アプリケーション/フィルタの選択（Select Applications/Filters）]：トラフィックをバイパスするアプリケーションまたはフィルタを選択するには、このオプションを選択します。『Cisco Secure Firewall Management Center デバイス設定ガイド』の「**アクセスコントロール ルール**」の章にある「**アプリケーション条件とフィルタの設定**」トピックを参照してください。
2. [フローをスロットルする（Throttle the flow）]：フローにレート制限を適用し、フローの検査を続行するには、このボタンを有効にします。Snort インスペクションをバイパスし、残りのフローをスロットルするアプリケーションまたはフィルタを選択できます。

（注）
スロットルされたエレファントフローからスロットルが自動的に削除されるのは、システムが危機を脱した場合、つまり、Snort パケットドロップのパーセンテージが設定されたしきい値よりも低い場合です。その結果、レート制限も削除されます。

次の Threat Defense コマンドを使用して、スロットルされたエレファントフローからスロットルを手動で削除することもできます。

- **clear efd-throttle <5-tuple/all> bypass**：このコマンドは、スロットルされたエレファントフローからスロットルを削除し、Snort インスペクションをバイパスします。
- **clear efd-throttle <5-tuple/all>**：このコマンドは、スロットルされたエレファントフローからスロットルを削除し、Snort インスペクションを続行します。このコマンドを使用すると、エレファントフローの修復はスキップされます。

  これらのコマンドの詳細については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

（注）
エレファントフローに対するアクション（フローのバイパスとスロットル）の実行は、Cisco Firepower 2100 シリーズ デバイスではサポートされていません。

ステップ 6 [OK] をクリックして、エレファントフロー設定を保存します。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

エレファントフロー設定を構成した後、接続イベントをモニターして、フローが検出、バイパス、またはスロットリングされているかどうかを確認します。これは、接続イベントの [理由（Reason）] フィールドで確認できます。エレファントフロー接続の 3 つの理由は次のとおりです。

- エレファントフロー（Elephant Flow）
- エレファントフローがスロットリングされている（Elephant Flow Throttled）
- エレファントフローが信頼されている（Elephant Flow Trusted）

注目 エレファントフロー検出を有効にしただけでは、エレファントフローの接続イベントは生成されません。接続イベントが別の理由ですでにログに記録されており、フローもエレファントフローである場合、[理由（Reason）] フィールドにはこの情報が含まれます。ただし、すべてのエレファントフローを確実にロギングするには、該当するアクセス制御ルールで接続ロギングを有効にする必要があります。

詳細については、『Cisco Secure Firewall Elephant Flow Detection』を参照してください。

第 48 章

インテリジェント アプリケーション バイパス

次のトピックでは、インテリジェントアプリケーションバイパス（IAB）を使用するようアクセス コントロール ポリシーを設定する方法について説明します。

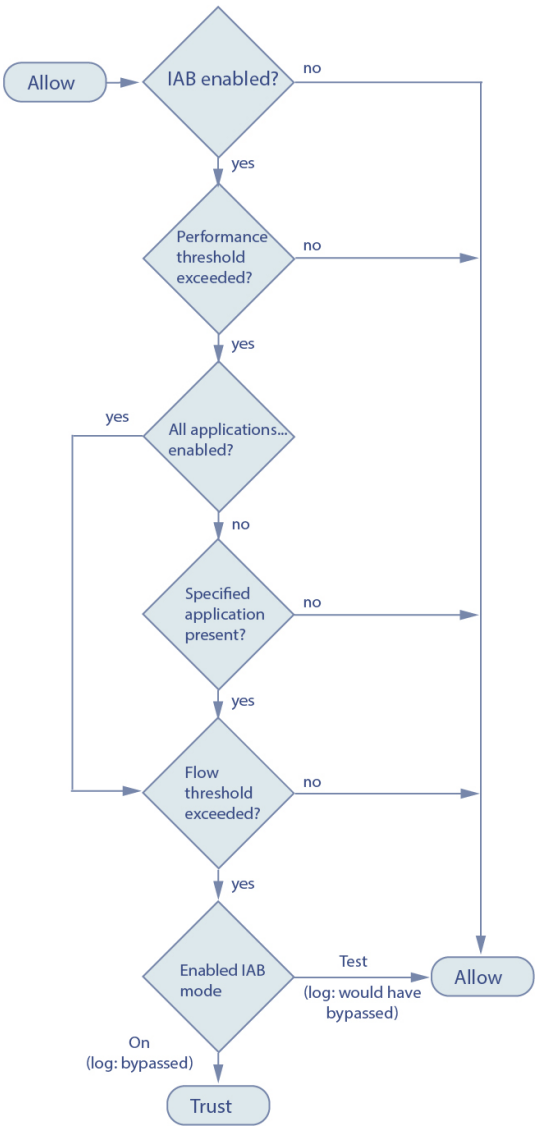
- IAB の概要 （1959 ページ）
- IAB オプション （1960 ページ）
- インテリジェント アプリケーション バイパスの要件と前提条件 （1962 ページ）
- インテリジェント アプリケーション バイパスの設定 （1962 ページ）
- IAB のロギングと分析 （1964 ページ）

IAB の概要

IABは、パフォーマンスとフローのしきい値を超過した場合に追加のインスペクションなしでネットワークを通過する信頼されるアプリケーションを特定します。たとえば、毎晩のバックアップがシステム パフォーマンスに大きく影響する場合、しきい値を超えてもバックアップ アプリケーションが生成したトラフィックを信頼するように設定できます。 オプションで、インスペクション パフォーマンスしきい値を超過したときに、IAB が、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように IAB を設定できます。

システムはトラフィックがディープインスペクションの対象となる前に、アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルトのアクションで許可されたトラフィック上で IAB を実行します。テスト モードでは、しきい値を超過しているかどうか判断することと、しきい値を超過している場合、IAB を実際に有効化している状態（バイパス モードといいます）であればバイパスされたであろうアプリケーション フローを特定することが可能です。

次の図に、IAB の判断決定プロセスの説明を示します。



IAB オプション

状態（State）

IAB を有効または無効にします。

パフォーマンス サンプル インターバル（Performance Sample Interval）

IAB パフォーマンス サンプリング スキャンの間隔を秒で指定します。この間隔で、システムは、IAB パフォーマンスしきい値と比較するためのシステム パフォーマンス測定値を収集します。値を 0 にすると、IAB が無効になります。

バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）

この機能には、相互に排他的な、次の 2 つのオプションがあります。

アプリケーション/フィルタ（Applications/Filters）
バイパス可能なアプリケーションおよびアプリケーション（フィルタ）のセットを指定できるエディタが提供されます。アプリケーションルール条件（817ページ）を参照してください。

未確認アプリケーションを含むすべてのアプリケーション
インスペクション パフォーマンスしきい値を超過すると、アプリケーションのタイプに関係なく、いずれかのフローバイパスしきい値を超過するすべてのトラフィックを信頼します。

パフォーマンスおよびフローのしきい値

少なくとも 1 つのインスペクション パフォーマンスしきい値と 1 つのフロー バイパスしきい値を設定する必要があります。パフォーマンスしきい値を超えると、フローしきい値が検証され、1 つのしきい値を超えた場合には、指定されたトラフィックが信頼されます。複数を有効にする場合は、それぞれ 1 つだけを超過する必要があります。

インスペクション パフォーマンスしきい値は、侵入インスペクションのパフォーマンスの限界を定めるもので、この限界を超えると、フローしきい値のインスペクションがトリガーされます。IAB は、**0** に設定されている検査パフォーマンスしきい値を使用しません。次の 1 つまたは複数のインスペクション パフォーマンスしきい値を設定できます。

ドロップ率（Drop Percentage）

高価な侵入ルール、ファイル ポリシー、圧縮解除などによるパフォーマンスのオーバーロードのためにパケットがドロップされたときの、パケット全体に対する割合としてドロップされた平均パケット数。これは、侵入ルールなどの通常の設定によってドロップされたパケットを参照するものではありません。1 より大きい整数を指定すると、指定されたパーセンテージのパケットがドロップされたときにIABがアクティブ化することに注意が必要です。**1** を指定すると、0 ～ 1 の任意の割合によって IAB がアクティブになります。これにより、少ないパケット数で IAB がアクティブ化します。

プロセッサ使用率（Processor Utilization Percentage）

使用されたプロセッサ リソースの平均比率。

パケット遅延

マイクロ秒単位の平均パケット遅延。

フロー レート（Flow Rate）

1秒あたりのフロー数で測定される、システムによるフロー処理率。このオプションでは、IAB は、フローを件数ではなくレートで測定するように設定されることに注意が必要です。

フローバイパスしきい値はフローの限界を定めるもので、この限界を超えると、IABは、バイパス モードではバイパス可能なアプリケーションを信頼し、テスト モードでは、アプリケーション トラフィックを許可してさらなるインスペクションの対象にします。IABは、**0** に設定

されているフロー バイパスしきい値を使用しません。次の 1 つまたは複数のフロー バイパスしきい値を設定できます。

フローあたりのバイト数（Bytes per Flow）

フローに含めることができる最大キロバイト数。

フローあたりのパケット数（Packets per Flow）

フローに含めることができる最大パケット数。

フロー継続時間（Flow Duration）

フローを開いたままにできる最大秒数。

フロー速度（Flow Velocity）

最大転送速度（KB/秒）。

インテリジェントアプリケーションバイパスの要件と前提条件

モデルのサポート

いずれか（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

インテリジェント アプリケーション バイパスの設定

⚠

注意 すべての展開にIABが必要なわけではありません。IABを使用する展開では、限定的な方法でIAB を使用する場合があります。ネットワーク トラフィック、特にアプリケーション トラフィックと、予測可能なパフォーマンスの問題の原因を含むシステム パフォーマンスの専門知識がない場合は、IABを有効にしないでください。IABをバイパス モードで実行する場合は、指定したトラフィックを信頼することでリスクが生じないことを事前に確認してください。

始める前に

クラシックデバイスの場合は、制御ライセンスが必要です。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。次に、[インテリジェント アプリケーション バイパスの設定（Intelligent Application Bypass Settings）] の隣にある [編集（Edit）]（✎） をクリックします。

ステップ 2 IAB の各オプションを設定します。

- [状態（State）]：IAB を [オフ（Off）] または [オン（On）] に切り替えるか、あるいは [テスト（Test）] モードで有効にします。
- [パフォーマンスサンプル間隔（Performance Sample Interval）]：IAB のパフォーマンス サンプリング スキャン間の時間を秒単位で入力します。IAB を有効にする場合は、テストモードであっても、0 以外の値を入力します。**0** を入力すると、IAB は無効になります。
- [バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）]：次のいずれかを選択します。
  - バイパスされるアプリケーションとフィルタの数をクリックし、トラフィックをバイパスするアプリケーションを指定します。アプリケーション条件とフィルタの設定（1795 ページ）を参照してください。
  - [All applications including unidentified applications] をクリックし、インスペクション パフォーマンスしきい値を超過したときに、IAB が、いずれかのフローバイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように設定します。
- [インスペクション パフォーマンスしきい値（Inspection Performance Thresholds）]：[設定（Configure）] をクリックし、1 つ以上のしきい値を入力します。
- [フローバイパスしきい値（Flow Bypass Thresholds）]：[設定（Configure）] をクリックし、1 つ以上のしきい値を入力します。

少なくとも 1 つのインスペクション パフォーマンスしきい値と 1 つのフロー バイパスしきい値を指定する必要があります。IAB がトラフィックを信頼するには、両方を超過する必要があります。各タイプのしきい値を複数入力した場合は、各タイプの 1 つのみを超過する必要があります。詳細については、IAB オプション （1960 ページ）を参照してください。

ステップ 3 [OK] をクリックして IAB 設定を保存します。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- アプリケーションが検出される前に一部のパケットの通過を許可する必要があるため、これらのパケットを検査するようにシステムを設定する必要があります。

  「トラフィック識別の前に通過するパケットを処理するためのベストプラクティス（2746 ページ）」および「トラフィック識別の前に通過するパケットを処理するためのポリシーの指定 （2747 ページ）」を参照してください。

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

IAB のロギングと分析

IABは、接続ロギングを有効にしたかどうかを問わず、バイパスされたフローやバイパスされることが予想されるフローをロギングする接続終了イベントを強制します。接続イベントは、バイパス モードでバイパスされたフロー、またはテスト モードでバイパスされることが予想されるフローを示します。接続イベントに基づいたカスタムのダッシュボード ウィジェットやレポートでは、バイパスされたフローおよびバイパスされることが予想されるフローの長期的な統計情報を表示できます。

IAB の接続イベント

アクション（Action）

[理由（Reason）]に[インテリジェント アプリケーション バイパス（Intelligent App Bypass）]が含まれる場合：

許可（Allow）：

適用された IAB 設定がテスト モードであり、[アプリケーション プロトコル（Application Protocol）]によって指定されたアプリケーションのトラフィックが、インスペクション用に使用可能のままであることを示します。

信頼する（Trust）：

適用された IAB 設定がバイパス モードであり、[アプリケーション プロトコル（Application Protocol）]によって指定されたアプリケーションのトラフィックが信頼されているため、それ以上インスペクションが行われずにネットワークを通過することを示します。

理由（Reason）

[インテリジェント アプリケーション バイパス（Intelligent App Bypass）] は、IAB がバイパス モードまたはテスト モードでイベントをトリガーしたことを示します。

アプリケーション プロトコル（Application Protocol）

このフィールドには、イベントをトリガーしたアプリケーション プロトコルが表示されます。

例

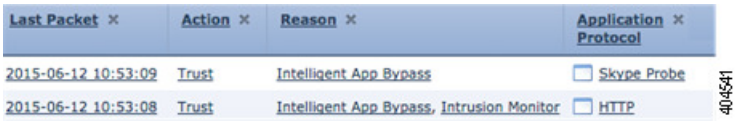
次の省略された図では、一部のフィールドが省かれています。図は、2 つの別個のアクセス コントロール ポリシーの異なる IAB 設定から生成された 2 つの接続イベントの [アクション（Action）]、[理由（Reason）]、および [アプリケーション プロトコル（Application Protocol）] フィールドを示しています。

最初のイベントの場合、[信頼する（Trust）] アクションは、IAB がバイパス モードで有効にされており、Bonjour プロトコル トラフィックが信頼されているため、それ以上インスペクションが行われずに受け渡されることを示します。

2 番目のイベントの場合、[許可（Allow）] アクションは、IAB がテスト モードで有効にされているため、Ubuntu Update Manager トラフィックはさらにインスペクションが行われる必要がありますが、IAB がバイパス モードであればバイパスされることが予想されることを示します。

例

次の省略された図では、一部のフィールドが省かれています。2 番目のイベントのフローは両方とも（[アクション（Action）] : [信頼する（Trust）]、[理由（Reason）] : [インテリジェント アプリケーション バイパス（Intelligent App Bypass）]）をバイパスし、侵入ルール（[理由（Reason）] : [侵入モニター（Intrusion Monitor）]）によって検査されました。[侵入モニター（Intrusion Monitor）] の理由は、[イベントの生成（Generate Events）] に設定された侵入ルールが検出されたが、接続時にエクスプロイトをブロックしなかったことを示しています。この例では、これはアプリケーションが検出される前に発生しました。アプリケーションが検出された後、IAB は、アプリケーションがバイパス可能であると認識し、フローを信頼しました。



IAB のカスタム ダッシュボード ウィジェット

接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム分析ダッシュボード ウィジェットを作成できます。ウィジェットを作成する際には、次の項目を指定します。

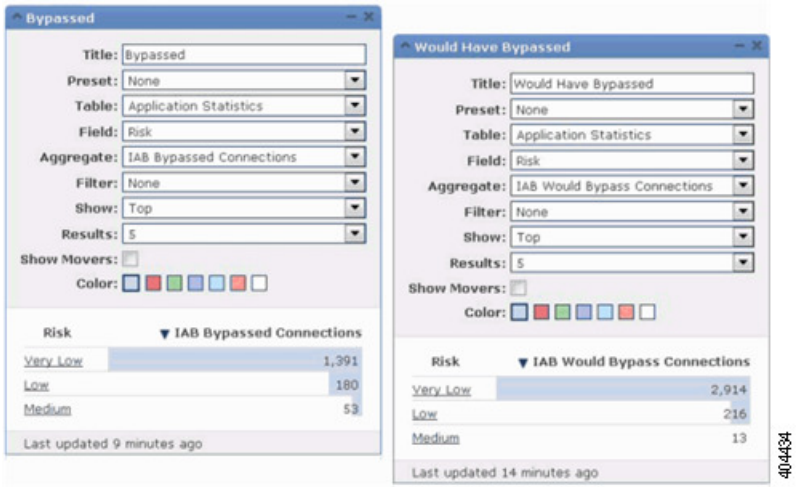
- プリセット（Preset）：なし（None）
- テーブル（Table）：**アプリケーションの統計（Application Statistics）**

- フィールド（Field）：任意（any）
- 集約（Aggregate）：次のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）
- フィールド（Field）：任意（any）

例

次のカスタム分析ダッシュボード ウィジェットの例では、次のようになっています。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーション トラフィックの統計を示しています。.



IAB のカスタム レポート

接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム レポートを作成できます。レポートを作成する際には、次の項目を指定します。

- テーブル（Table）：**アプリケーションの統計（Application Statistics）**
- プリセット（Preset）：なし（None）
- フィールド（Field）：任意（any）

- X 軸（X-Axis）：任意（any）
- Y 軸（Y-Axis）：以下のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）

例

次の図は、2 つのレポートの例の抜粋を示します。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーション トラフィックの統計を示しています。

第 49 章

コンテンツ規制

次のトピックでは、コンテンツ制限機能を使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

- コンテンツ制限について （1969 ページ）
- コンテンツ制限の要件と前提条件 （1971 ページ）
- コンテンツ制限のガイドラインと制限事項 （1971 ページ）
- アクセス コントロール ルールを使用したコンテンツ制限の実施 （1971 ページ）
- DNS シンクホールを使用したコンテンツ制限の実施 （1973 ページ）

コンテンツ制限について

主要な検索エンジンやコンテンツ配信サービスは、検索結果と Web サイトのコンテンツを制限できる機能を提供しています。たとえば学校では、「子どもをインターネットから保護する法律」（CIPA）を順守するために、コンテンツ制限機能を使用します。

コンテンツ制限機能は、検索エンジンやコンテンツ配信サービスで実行する場合には、個々のブラウザやユーザを対象にしか実施できません。このシステムでは、ご使用のネットワーク全体にこれらの機能を拡大できます。

このシステムにより、以下を実施できます。

- セーフサーチ：多くの主要な検索エンジンでサポートされているこのサービスは、ビジネス、行政、および教育の環境で不愉快であると分類されている、露骨なアダルト向けコンテンツを除外します。システムは、サポートされている検索エンジンのホームページへのユーザのアクセス機能は制限しません。

次の 2 つの方法を使用して、これらの機能を実施するようにシステムを設定できます。

方法：アクセス コントロール ルール

コンテンツ制限機能は、検索またはコンテンツ クエリの制限状態を、要求 URI の要素、関連する Cookie、またはカスタム HTTP ヘッダー要素により通信します。システムがトラフィックを処理するときに、これらの要素を変更するためのアクセス コントロール ルールを設定できます。

方法：DNS シンクホール

Google 検索では、セーフサーチのフィルタを課す Google SafeSearch 仮想 IP アドレス（VIP）にトラフィックをリダイレクトするように、システムを設定できます。

次の表では、これらの実施方法の違いについて説明します。

表 *92*：コンテンツ制限方法の比較

属性	方法：アクセス コントロール ルール	方法：DNS シンクホール
サポートされるデバイス（Supported devices）	任意（Any）	Secure Firewall Threat Defense のみ
サポートされる検索エンジン（Search engines supported）	ルールエディタの[アプリケーション（Applications）]タブのタグ付きのすべての `safesearch supported`	Google のみ
サポートされる YouTube 制限付きモード（YouTube Restricted Mode supported）	はい	はい
SSL ポリシーが必要（SSL policy required）	はい	非対応
ホストは IPv4 の使用が必要（Hosts must be using IPv4）	非対応	はい
接続イベント ロギング（Connection event logging）	はい	はい

使用する方法を決定する際には、次の制限事項を考慮します。

- アクセス コントロール ルール方法には SSL ポリシーが必要で、これはパフォーマンスに影響を及ぼします。
- Google セーフサーチ VIP は IPv4 トラフィックのみをサポートします。Google 検索を管理するように DNS シンクホールを設定する場合は、影響を受けるネットワークのすべてのホストが IPv4 を使用している必要があります。

接続イベントの[理由（Reason）]フィールドに、方法に応じて異なる値がログ記録されます。

- アクセス コントロール ルール：[コンテンツの制限（Content Restriction）]
- DNS シンクホール：[DNS ブロック（DNS Block）]

コンテンツ制限の要件と前提条件

モデルのサポート

すべて、または手順に示されているとおり。

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

コンテンツ制限のガイドラインと制限事項

- セーフサーチは Snort 2 でのみサポートされています。
- YouTube と Google は、アクセス制御ルールに実装された YouTubeEDU 機能をサポートしていません。YouTubeEDU を設定するアクセス制御ルールは完全には機能していないため、削除してください。関連する復号ルールも削除できます。

アクセスコントロールルールを使用したコンテンツ制限の実施

次の手順では、コンテンツを制限するアクセス制御ルールを設定する方法について説明します。

（注） アクセス制御ルールでセーフサーチが有効になっている場合、インライン正規化が自動的に有効になります。

手順

ステップ 1 復号ポリシーを作成します。

ステップ 2 セーフサーチトラフィックを処理するためのルールを追加します。

- ルールの [アクション（Action）] として [復号 - 再署名（Decrypt - Resign）] を選択します。
- [アプリケーション（Applications）] で、選択内容を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。
  - セーフサーチ：[カテゴリ：検索エンジン（Category: search engine）] フィルタを追加します。

ステップ 3 追加したルールのルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ステップ 4 アクセス コントロール ポリシーを作成または編集して、復号ポリシーとアクセス コントロール ポリシーを関連付けます。

詳細については、アクセス制御への他のポリシーの関連付け （1765 ページ）を参照してください。

ステップ 5 アクセス コントロール ポリシーに、セーフサーチトラフィックを処理するためのルールを追加します。

- ルールの [アクション（Action）] として [許可（Allow）] を選択します。
- [アプリケーション（Applications）] で、 **セーフサーチ**（ ） のアイコンをクリックし、関連するオプションを設定します。
  - アクセス制御ルールのセーフサーチ オプション （1973 ページ）
- [アプリケーション（Applications）] で、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストのアプリケーション選択を絞り込みます。

  ほとんどの場合、セーフサーチを有効にすると、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに適切な値が入力されます。セーフサーチ機能を有効にしたときに、セーフサーチアプリケーションがすでにリストに含まれている場合、リストへの自動入力は行われません。予期したとおりにアプリケーションが入力を行わない場合は、それらを以下のように手動で追加します。
  - セーフサーチ：[カテゴリ：検索エンジン（Category: search engine）] フィルタを追加します。

詳細については、アプリケーション条件とフィルタの設定（1795 ページ）を参照してください。

ステップ 6 追加したアクセス コントロール ルールに対してルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ステップ 7 システムが制限付きコンテンツをブロックするときに表示する HTTP 応答ページを設定します（HTTP 応答ページの選択 （1838 ページ）を参照）。

ステップ 8 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクセス制御ルールのセーフサーチ オプション

Firepower System は、特定の検索エンジンのセーフサーチ フィルタリングにのみ対応しています。対応している検索エンジンのリストについては、アクセス制御ルール エディタの [アプリケーション（Applications）] タブのアプリケーションにタグ付けされている `safesearch supported` を参照してください。対応していない検索エンジンのリストについては、アプリケーションにタグ付けされている `safesearch` を参照してください。

アクセス制御ルールのセーフサーチを有効にするには、次のパラメータを設定します。

セーフサーチの有効化
このルールに一致するトラフィックのセーフサーチ フィルタリングを有効にします。

対応していない検索トラフィック
対応していない検索エンジンからのトラフィックを処理する場合は、システム上でのアクションを指定します。[ブロック（Block）] または [リセットによるブロック（Block with Reset）] を選択すると、いつ制限されたコンテンツをブロックするかを表示する HTTP 応答ページを設定する必要があります。HTTP 応答ページの選択 （1838 ページ）

DNS シンクホールを使用したコンテンツ制限の実施

通常、DNS シンクホールは、トラフィックを特定のターゲットからそらします。この手順では、Google セーフサーチ仮想 IP アドレス（VIP）にトラフィックをリダイレクトする（つまり、Google と YouTube の検索結果にコンテンツ フィルタを適用する）ように DNS シンクホールを設定する方法について説明します。

Google セーフ サーチは VIP に単一の IPv4 アドレスを使用するため、ホストは IPv4 アドレッシングを使用する必要があります。

⚠

注意 ネットワークにプロキシ サーバーが含まれる場合、Firewall Threat Defense デバイスをプロキシ サーバーとインターネットの間に配置しない限り、この方法でのコンテンツ制限は効果的ではありません。

この手順では、Google 検索のみにコンテンツ制限を適用する方法について説明します。他の検索エンジンには適用できません。

始める前に

この手順は Firewall Threat Defense にのみ適用され、IPS ライセンスが必要です。

手順

ステップ 1 次の URL を使用して、サポートされる Google ドメインのリストを取得します。
https://www.google.com/supported_domains

ステップ 2 ローカル コンピュータにカスタム DNS リストを作成し、次のエントリを追加します。

- Google セーフサーチを適用するには、サポートされる Google ドメインごとにエントリを追加します。
- YouTube 制限モードを適用するには、「youtube.com」エントリを追加します。

カスタム DNS リストは、テキストファイル（.txt）形式にする必要があります。テキストファイルの各行に、先頭ピリオドを除いた状態で、個々のドメイン名を指定する必要があります。たとえば、サポートされるドメインが「.google.com」の場合、「google.com」として指定する必要があります。

ステップ 3 カスタム DNS リストを Firewall Management Center にアップロードします（新しいセキュリティ インテリジェンス リストの Secure Firewall Management Center へのアップロード （1397 ページ）を参照）。

ステップ 4 Google セーフサーチ VIP の IPv4 アドレスを判別します。たとえば、forcesafesearch.google.com で `nslookup` を実行します。

ステップ 5 セーフサーチ VIP のシンクホール オブジェクトを作成します（シンクホール オブジェクトの作成 （1399 ページ）を参照）。

このオブジェクトでは、次の値が使用されます。

- [IPv4 アドレス（IPv4 Address）]：セーフ サーチ VIP アドレスを入力します。
- [IPv6 アドレス（IPv6 Address）]：IPv6 ループバック アドレスを入力します（`::1`）。
- [シンクホールへの接続のログ（Log Connections to Sinkhole）]：[ログ接続（Log Connections）] をクリックします。
- [タイプ（Type）]：[なし（None）] を選択します。

ステップ 6 基本 DNS ポリシーを作成します（基本的な DNS ポリシーの作成 （1871 ページ）を参照）。

ステップ 7 シンクホールの DNS ルールを追加します（DNS ルールの作成と編集 （1874 ページ）を参照）。

このルールでは、

- [有効（Enabled）] チェックボックスをオンにします。
- [アクション（Action）] ドロップダウン リストから [シンクホール（Sinkhole）] を選択します。
- [シンクホール（Sinkhole）] ドロップダウン リストから、作成したシンクホール オブジェクトを選択します。
- 作成したカスタム DNS リストを [DNS] の [選択した項目（Selected Items）] リストに追加します。
- （オプション）[ネットワーク（Networks）] でネットワークを選択し、コンテンツ制限を特定のユーザーに限定します。たとえば、学生ユーザーにコンテンツ制限を限定したい場合、学生を教員とは別のサブネットに割り当て、このルールにそのサブネットを指定します。

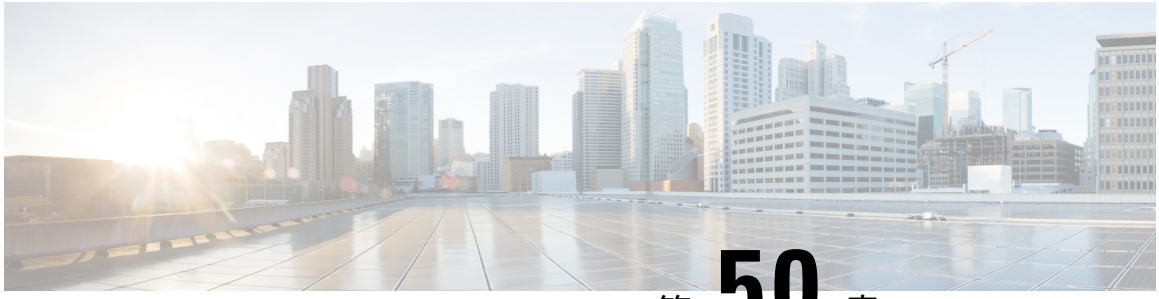
ステップ 8 アクセス コントロール ポリシーと DNS ポリシーを関連付けます（アクセス制御への他のポリシーの関連付け （1765 ページ）を参照）。

ステップ 9 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

第 VIII 部

侵入検知と防御

- ネットワーク分析ポリシーと侵入ポリシーの概要 （1979 ページ）
- 侵入ポリシーの使用を開始するには （2001 ページ）
- ルールを使用した侵入ポリシーの調整 （2013 ページ）
- カスタム侵入ルール （2045 ページ）
- 侵入ポリシーとネットワーク分析ポリシーのレイヤ （2179 ページ）
- ネットワーク資産に応じた侵入防御の調整 （2197 ページ）
- 機密データの検出 （2203 ページ）
- 侵入イベントロギングのグローバル制限 （2219 ページ）
- 侵入防御のパフォーマンスの調整 （2225 ページ）



第 50 章

ネットワーク分析ポリシーと侵入ポリシーの概要

以下のトピックでは、Snort 検査エンジンの概要、およびネットワーク分析ポリシーと侵入ポリシーを示します。

- ネットワーク分析ポリシーと侵入ポリシーの基本 （1979 ページ）
- ポリシーがトラフィックで侵入を検査する方法 （1981 ページ）
- システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー （1987 ページ）
- ネットワーク分析ポリシーと侵入ポリシーのライセンス要件 （1995 ページ）
- ネットワーク分析と侵入ポリシーの要件と前提条件 （1995 ページ）
- ネットワーク分析ポリシーと侵入ポリシーに関するガイドラインと制限事項（1995ページ）
- ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー （1996 ページ）
- 競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

ネットワーク分析ポリシーと侵入ポリシーの基本

ネットワーク分析ポリシーと侵入ポリシーは、システムの侵入検知および防御機能の一部として連携して動作します。

- 侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的にモニタおよび分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。これは「IDS」とも呼ばれます。
- 侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。これは「IPS」とも呼ばれます。

（注）

- Snort 3 および SSL 復号または TLS サーバーアイデンティティを使用している場合は、**防止**モードでネットワーク分析ポリシー（NAP）を構成する必要があります。Snort 3 NAP が検知モードの場合、SSL 機能は動作しません。
- 侵入ポリシー（IPS）とネットワーク分析ポリシー（NAP）を同じ設定にすることを強くお勧めします。IPS が検出モードの場合は、NAP を検出モードに設定します。逆の場合も同様です。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- **ネットワーク分析ポリシー**は、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- **侵入ポリシー**では侵入およびプリプロセッサルール（総称的に「侵入ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別途ネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケットインスペクションを行うことができます。これらによって、ホストとそのデータの可用性、整合性、および機密性を脅かす可能性があるネットワーク トラフィックを検出、警告し、保護することができます。

システムには、同様の名前（Balanced Security and Connectivity など）が付いたいくつかのネットワーク分析ポリシーおよび侵入ポリシーが付属しており、それらは互いに補完しあい、連携して動作します。システム付属のポリシーを使用することで、Talos インテリジェンスグループの経験を活用できます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。

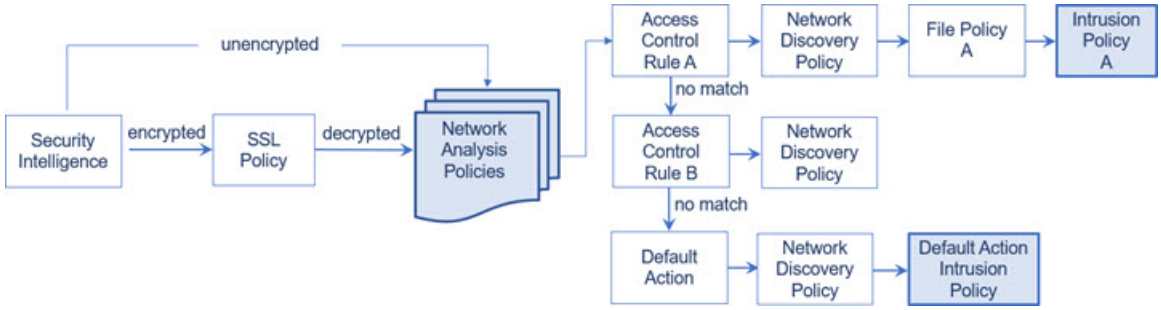
また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタム ポリシーの設定を調整することで、各自に最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Webインターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーション パネルが表示され、右側にさまざまな設定ページが表示されます。

ポリシーがトラフィックで侵入を検査する方法

アクセス コントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図は、インラインの侵入防御およびマルウェア防御 展開におけるトラフィック分析の順序を簡略化して示しています。アクセス コントロール ポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序が示されています。ネットワーク分析ポリシーと侵入ポリシーの選択フェーズは強調表示されています。



インライン展開（つまり、ルーテッド、スイッチド、トランスペアレントインターフェイスまたはインラインインターフェイスのペアを使用して関連設定がデバイスに展開される展開）では、システムは上図のプロセスのほぼすべての段階において、追加のインスペクションなしでトラフィックをブロックすることができます。セキュリティインテリジェンス、SSLポリシー、ネットワーク分析ポリシー、ファイルポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パッシブにパケットを検査するネットワーク検出ポリシーは、トラフィック フローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入およびプリプロセッサイベント（総称して「侵入イベント」と呼ばれることもある）は、パケットまたはそのコンテンツがセキュリティリスクを表す可能性を示しています。

ヒント SSLインスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSLインスペクションが設定されていない場合について、この図は、そのような場合のアクセス コントロール ルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイル インスペクションは無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

単一の接続の場合は、図に示すように、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

復号、正規化、前処理：ネットワーク分析ポリシー

デコードと前処理を実行しないと、プロトコルの相違によりパターンマッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。これらのトラフィック処理タスクは、以下のタイミングでネットワーク分析ポリシーによる処理の対象となります。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた**後**
- 暗号化トラフィックがオプションの SSL ポリシーによって復号された**後**
- ファイルまたは侵入ポリシーによってトラフィックを検査できるようになる**前**

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の 3 つの TCP/IP 層を通ったパケットを復号し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケット デコーダは、パケット ヘッダーやペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーのさまざまな異常動作も検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリプロセッサや侵入ルールによる検査用にパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。

（注） パッシブな展開の場合、シスコでは、ネットワーク分析レベルでインライン正規化を行うのではなく、アクセス コントロール ポリシー レベルで、アダプティブプロファイルの更新を有効にすることを推奨しています。

- ネットワーク層とトランスポート層のさまざまなプリプロセッサは、IP フラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

  トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセス コントロール ポリシーのターゲット デバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケット データを侵入ルールエンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。
- Modbus、DNP3、CIP、および s7commplus SCADA プリプロセッサは、トラフィックの異常を検出し、侵入ルールにデータを提供します。Supervisory Control and Data Acquisition

（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニタ、制御、取得します。

- 一部のプリプロセッサでは、Back Orifice、ポートスキャン、SYN フラッドおよび他のレート ベース攻撃など、特定の脅威を検出できます。

  侵入ポリシーで、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することに注意してください。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックの前処理を制御します。初期段階では、デフォルトで [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致するトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。

（注） ルールアクションが [信頼（Trust）] であるアクセス コントロール ポリシーと、ロギングオプションが無効でアクションが [ファストパス（Fastpath）] であるプレフィルタルールの場合、フロー終了イベントが引き続きシステムで生成されることがわかります。このイベントは、Management Center のイベントページには表示されません。

アクセス コントロール ルール：侵入ポリシーの選択

最初の前処理の後、アクセスコントロールルール（ある場合）はトラフィックを評価します。ほとんどの場合、パケットが一致した最初のアクセス コントロール ルールがそのトラフィックを処理することになります。ユーザは一致したトラフィックをモニタ、信頼、ブロック、または許可することができます。

アクセス コントロール ルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセスコントロール ルールに一致しないトラフィックは、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。デフォルト アクションでは、ディスカバリ データと侵入についても検査できます。

（注） どのネットワーク分析ポリシーによって前処理されるかに**関わらず**、すべてのパケットは、設定されているアクセスコントロールルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。

ポリシーがトラフィックで侵入を検査する方法（1981ページ）の図は、インラインの侵入防御およびマルウェア防御展開でデバイスを通過する、次のようなトラフィックのフローを示しています。

- アクセス コントロール ルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリ データの検査、ファイル ポリシー A による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。
- アクセス コントロール ルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいはファイルまたはマルウェア）について検査されないので、ルールに関連付けられている侵入ポリシーやファイル ポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、この設定を行う必要はありません。
- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションで、一致したトラフィックを許可しています。次に、トラフィックはネットワーク検出ポリシー、さらにその後侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けるときに、必要に応じて、別の侵入ポリシーを使用できます。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。

侵入インスペクション：侵入ポリシー、ルール、変数セット

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、どの侵入ルールおよびプリプロセッサルールを有効にしてどのように設定するかを管理することです。

侵入ルールおよびプリプロセッサルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。

システムには、Talos インテリジェンス グループ によって作成された次のタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）。
- 標準テキスト侵入ルール：ルールの新しいカスタム インスタンスとして保存および変更できます。

- プリプロセッサルール。プリプロセッサと、ネットワーク分析ポリシーのパケットデコーダ検出オプションが関連付けられたルールです。プリプロセッサルールはコピーまたは編集できません。ほとんどのプリプロセッサルールはデフォルトで無効になっています。プリプロセッサを使用してイベントを生成し、インライン展開では、違反パケットをドロップします。 するにはそれらを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理する際には、最初にルール オプティマイザが、基準（トランスポート層、アプリケーションプロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルールエンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが3種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキストルールを記述および追加することで、検出を調整できます。Cisco 推奨機能を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることもできます。

変数セット

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される1つのデフォルト変数セットが含まれています。システム提供の共有オブジェクト ルールと標準テキスト ルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ヒント　システム提供の侵入ポリシーを使用する場合でも、シスコでは、デフォルトセットの主要なデフォルト変数を変更すること**強く**推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。高度なユーザは、1つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。

関連トピック

定義済みデフォルト変数 （1409 ページ）

侵入イベントの生成

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサイベント（まとめて侵入イベントと呼ばれることもあります）を生成します。管理対象デバイスはFirewall Management Centerにイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることができます。

データベース内の各侵入イベントにはイベント ヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケット ベースのイベントの場合、システムは復号されたパケット ヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケット デコーダ、プリプロセッサ、および侵入ルール エンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- （ネットワーク分析ポリシーで設定された）パケット デコーダが 20 バイト（オプションやペイロードのない IP データグラムのサイズ）未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。パケットを検査する侵入ポリシー内の付随するデコーダ ルールが有効な場合、システムは後でプリプロセッサ イベントを生成します。
- IP最適化プリプロセッサが重複する一連のIPフラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈して、付随するプリプロセッサルールが有効な場合、システムはプリプロセッサ イベントを生成します。
- 侵入ルールエンジン内では、ほとんどの標準テキストルールおよび共有オブジェクトルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー

新しいアクセス コントロール ポリシーを作成することは、システムを使用してトラフィック フローを管理するための最初のステップの1つです。デフォルトでは、新しく作成されたアクセス コントロール ポリシーは、システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

図 *319*：新しいアクセス コントロール ポリシー：侵入防御

以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。
- アクセス コントロール ポリシーのデフォルト アクションは、システム付属の Balanced Security and Connectivity 侵入ポリシーによる検査に従って、悪意のないトラフィックをすべて許可します。デフォルトアクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなブロックリストとブロックなしリストのみ）を使用し、SSLポリシーによる暗号化トラフィックの復号や、アクセス コントロール ルールを使用したネットワークトラフィックの特別な処理や検査は実行しません。

侵入防御展開を調整するために実行できるシンプルなステップは、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。システムには、これらのポリシーの複数のペアが提供されています。

または、カスタムポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されているプリプロセッサ オプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティ ニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

システム提供のネットワーク分析ポリシーと侵入ポリシー

システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか付属しています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Talosインテリジェンスグループ のエクスペリエンスを活用することができます。これらのポリシーでは、Talosが侵入ルールおよびプリプロセッサルールの状態、ならびにプリプロセッサおよび他の詳細設定の初期設定も指定しています。

すべてのネットワーク プロファイル、最小トラフィック、または防御ポスチャに対応したシステム付属ポリシーはありません。これらの各ポリシーは一般的なケースとネットワークのセットアップに対応しているため、これらのポリシーに基づいて適切に調整された防御ポリシーを策定することができます。システム付属ポリシーは、変更せずにそのまま使用できますが、カスタム ポリシーのベースとして使用し、カスタム ポリシーを各自のネットワークに合わせて調整することが推奨されます。

ヒント システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。

新しい脆弱性が知られるようになると、Talos が侵入ルールの更新をリリースします（「Snortルールの更新」とも呼ばれます）。これらのルール更新により、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやプリプロセッサルールの新規作成または更新、既存ルールのステータスの変更、デフォルトのポリシー設定の変更が実施されます。ルールアップデートでは、システム付属のポリシーからルールが削除されたり、新しいルールカテゴリが提供されたり、さらにデフォルトの変数セットが変更されることもあります。

ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセス コントロール ポリシーを失効したものとして扱います。変更を有効にするには、更新されたポリシーを再展開する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセス コントロール ポリシーと組み合わせて）自動的に再展開するように、ルールの更新を設定できます。これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセス コントロール ポリシーを再展開する**必要があります**。これにより、現在実行されているものとは異なる、関連するSSLポリシー、ネットワーク分析ポリシー、ファイルポリシーが再展開され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。

システムに付属しているネットワーク分析ポリシーと侵入ポリシーのペアは以下のとおりです。

[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムは Balanced Security and Connectivity のポリシーおよび設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続（すべてのリソースに到達可能な）の方がネットワークインフラストラクチャのセキュリティより優先される組織向けに作られています。この侵入ポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールのみが有効にされます。

[接続性よりもセキュリティを優先（Security over Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性より優先される組織向けに作られています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

[最大検出（Maximum Detection）] ネットワーク分析ポリシーおよび侵入ポリシー

このポリシーは、Security over Connectivity ポリシー以上にネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイト キット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

[アクティブなルールなし（No Rules Active）] 侵入ポリシー

[アクティブなルールなし（No Rules Active）] 侵入ポリシーでは、すべての侵入ルールと侵入ルールのしきい値を除くすべての詳細設定が無効にされます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。

（注） 選択されているシステムから提供されるベース ポリシーによって、ポリシーの設定が異なります。ポリシー設定を表示するには、ポリシーの横にある [編集（Edit）] アイコンをクリックしてから、[ベース ポリシーの管理（Manage Base Policy）] リンクをクリックします。

カスタムネットワーク分析ポリシーと侵入ポリシーの利点

システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーに設定されたプリプロセッサ オプション、侵入ルール、およびその他の詳細設定は、組織のセキュリティ ニーズに十分に対応しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反を重点的に観察できるようになります。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタムポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できる構成要素です。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタム ポリシーには、ポリシーチェーンの根本的な基礎としてシステム付属ポリシーが含まれています。システム付属のポリシーはルールアップデートによって変更される可能性があるので、カスタムポリシーを基本として使用している場合でも、ルールアップデートをインポートするとポリシーに影響が及びます。ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けたポリシーを失効として扱います。

カスタム ネットワーク分析ポリシーの利点

デフォルトでは、1 つのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、侵入ポリシー（および侵入ルールセット）に関係なく、すべてのパケットが同じ設定に基づいてデコードされ、処理されることを意味します。

初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサおよびデコーダを調整できる方法には次のものがあります。

- モニターしているトラフィックに適用されないプリプロセッサを無効にできます。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに Microsoft インターネット インフォメーション サービス（IIS）を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサ オプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

（注） カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、パケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価するために、プリプロセッサを使用する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効なままになります。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートや、Telnet、HTTP、RPC トラフィックを復号するポートを特定できます。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます

（注） カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する**必要があります**。

カスタム侵入ポリシーの利点

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルト アクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。

侵入防御展開をカスタマイズするために、複数の侵入ポリシーを作成し、それぞれがトラフィックを異なる方法で検査するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。

侵入ポリシーの主な機能は、次のように、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効になっていることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。
- Cisco 推奨機能を使用すると、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。
- 必要に応じて、既存のルールの変更や、新しい標準テキスト ルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。
- Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslog ファシリティへのロギングを有効にしたり、イベントデータを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

カスタム ポリシーの制限

前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを処理および検査する、ネットワーク分析ポリシーと侵入ポリシーが相互補完することを設定で許可する場合は、注意する**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1 つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

図 *320*：新しいアクセス コントロール ポリシー：侵入防御

アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効

化されているときに、前処理されたパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web ユーザ インターフェイスではプリプロセッサは無効なままになります。

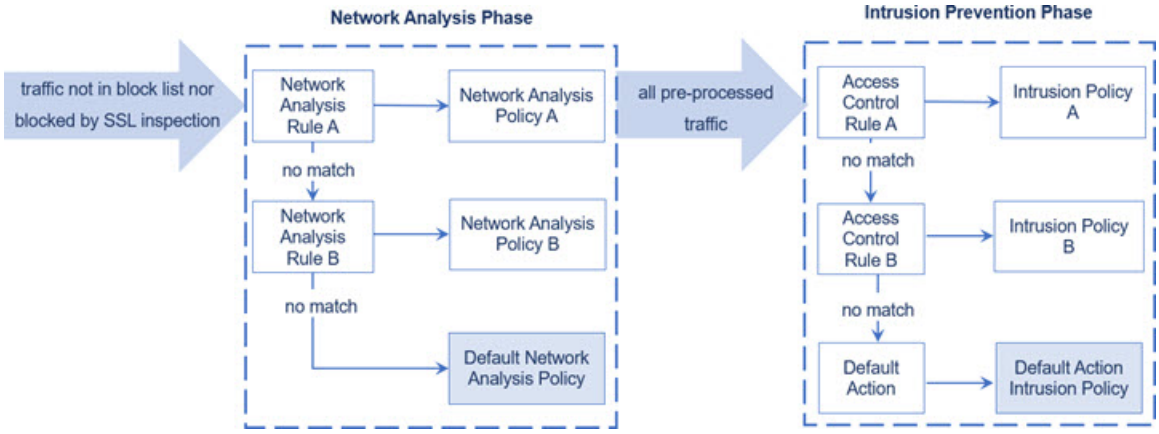
（注） プリプロセッサを無効にするパフォーマンス上の利点を得るには、侵入ポリシーでそのプリプロセッサを必要とするルールが有効になっていないことを確認する**必要があります**。

複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。

ヒント アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。システムの他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれているのではなく、それを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、それら独自のプロセスにおいて引き続きアクセス コントロール ルールと照合されます（つまり、侵入ポリシーにより検査される可能性があります）。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。アクセス コントロール ポリシーを設定するときは、そのポリシーが正しいネットワーク分析ポリシーおよび侵入ポリシーを呼び出して特定のパケットを評価するように、慎重に行う**必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インスペクション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーおよびデフォルト アクションの侵入ポリシーを強調表示しています。



このシナリオでは、アクセス コントロール ポリシーに、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーが設定されています。

- Network Analysis Rule A は、一致するトラフィックを Network Analysis Policy A で前処理します。その後、このトラフィックを Intrusion Policy A で検査されるようにすることができます。
- Network Analysis Rule B は、一致するトラフィックを Network Analysis Policy B で前処理します。その後、このトラフィックを Intrusion Policy B で検査されるようにすることができます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、このトラフィックをアクセス コントロール ポリシーのデフォルト アクションに関連付けられた侵入ポリシーによって検査されるようにすることができます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図では、2 つのアクセス コントロール ルールとデフォルト アクションが含まれるアクセス コントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy A によって検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy B によって検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。トラフィックはその後、デフォルト アクションの侵入ポリシーによって検査されます。

各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整**されません**。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティ ゾーンのトラフィックの処理をポリシー ペアによって制御することを意図している場合に、誤まって、異なるゾーンを使用するように2つのルールの条件を設定したとします。この誤設定により、ト

ラフィックが誤って前処理される可能性があります。したがって、ネットワーク分析ルールおよびカスタム ポリシーを使用した前処理の調整は、**高度な**タスクです。

単一の接続の場合は、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

ネットワーク分析ポリシーと侵入ポリシーのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

ネットワーク分析と侵入ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

ネットワーク分析ポリシーと侵入ポリシーに関するガイドラインと制限事項

- パケットが小さいトラフィックの割合が高いと、Snort のパフォーマンスが低下します。この動作は、すべてのプリプロセッサが無効になっている場合でも見られます。

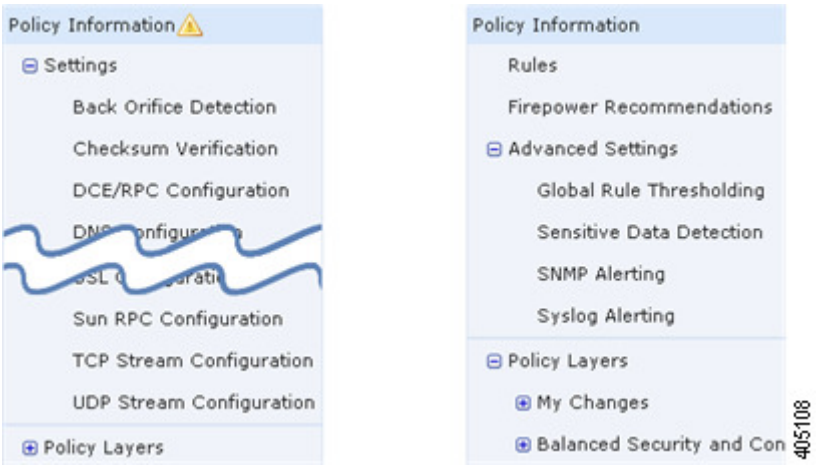
- メモリが不足している Threat Defense デバイスに構成の変更を展開しようとすると、Snort デプロイメントもトリガーされます。その結果、RSS メモリの消費量が高くなります。多数の Snort IPS ルール、ネットワークオブジェクト、およびアクセス制御リストを含む複数の IPS ポリシーなどの大規模な構成をデバイスにデプロイすると、Snort のメモリ使用量にも影響します。構成を最適化することで、このようなメモリの問題を軽減できます。構成を最適化するためのアクセス制御ルールの構成方法に関するベストプラクティスについては、「アクセス制御ルールのベストプラクティス」を参照してください。
- Threat Defense Virtual インスタンスのメモリを増やす場合、追加のメモリを使用するように Snort 3 の構成を再度デプロイする必要があります。

（注） Threat Defense Virtual インスタンスのメモリを増やしても、Snort 3 のメモリ割り当ては自動的に調整されません。構成を再度デプロイして、更新されたリソース制限を Snort 3 に適用する `memory_allocation.lua` などの関連する構成ファイルを再生成する必要があります。

ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー

ネットワーク分析ポリシーと侵入ポリシーは同様の Web インターフェイスを使用して、設定への変更を編集して保存します。

いずれかのタイプのポリシーを編集するときに、Web インターフェイスの左側にナビゲーション パネルが表示されます。次の図は、ネットワーク分析ポリシー（左）および侵入ポリシー（右）のナビゲーション パネルを示しています。



境界線が、ポリシー層との直接対話を使用して構成可能なポリシー設定へのリンク（下側）とポリシー層との直接対話を使用せずに構成可能なポリシー設定へのリンク（上側）にナビゲー

ション パネルを分割します。いずれかの設定ページに移動するには、ナビゲーション パネル内の名前をクリックします。ナビゲーション パネルで影付きで強調表示されている項目は、現在の設定ページを示しています。たとえば、上の図では、[ポリシー情報（Policy Information）] ページがナビゲーション パネルの右側に表示されます。

[ポリシー情報（Policy Information）]

[ポリシー情報（Policy Information）] ページには、一般的に使用される設定の設定オプションが示されます。上記のネットワーク分析ポリシーパネルの図に示すように、ポリシーに未保存の変更がある場合は、ナビゲーションパネルの [ポリシー情報（Policy Information）] の横にポリシー変更アイコン が表示されます。アイコンは、変更を保存すると消えます。

[ルール（Rules）]（侵入ポリシーのみ）

侵入ポリシーの [ルール（Rules）] ページでは、共有オブジェクト ルール、標準テキスト ルール、およびプリプロセッサ ルールのルール ステータスとその他の設定項目を設定できます。

Cisco の推奨事項（侵入ポリシーのみ）

侵入ポリシーの [Ciscoの推奨事項（Cisco Firepower Recommendations）] ページでは、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアントアプリケーションプロトコルを、各アセットを保護するために作成された侵入ルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

[Settings]（ネットワーク分析ポリシー）および [Advanced Settings]（侵入ポリシー）

ネットワーク分析ポリシーの [設定（Settings）] ページでは、プリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。[設定（Settings）] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサの個々の設定ページへのサブリンクが表示されます。

侵入ポリシーの [詳細設定（Advanced Settings）] ページでは、詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスしたりできます。[詳細設定（Advanced Settings）] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。

[Policy Layers]

[ポリシー層（Policy Layers）] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成する階層の要約が表示されます。[ポリシー層（Policy Layers）] リンクを展開すると、ポリシー内の階層に関する概要ページへのサブリンクが表示されます。各階層のサブリンクを展開すると、その階層で有効になっているすべてのルール、プリプロセッサ、または詳細設定の設定ページへのサブリンクがさらに表示されます。

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーや侵入ポリシーを編集するときに、ポリシーに未保存の変更がある場合は、そのことを示すために、ナビゲーションパネルの[ポリシー情報（Policy Information）]の横に**ポリシー変更アイコン**が表示されます。変更をシステムに認識させるには、変更を保存（確定）する必要があります。

（注） 保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを展開する必要があります。保存しないでポリシーを展開すると、最後に保存された設定が使用されます。

編集競合の解決

[ネットワーク分析ポリシー（Network Analysis Policy）]ページ（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policy）]**をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックする）および[侵入ポリシー（Intrusion Policy）]ページ（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**）には、各ポリシーの未保存の変更の有無、および現在ポリシーを編集中のユーザー情報が表示されます。シスコでは、同時に1人だけがポリシーを編集することを推奨します。同時編集を実行すると、次のようになります。

- ネットワーク分析ポリシーまたは侵入ポリシーを編集しているときに、同時に他のユーザが同じポリシーを編集し、ポリシーへの変更を保存した場合、ポリシーを確定すると、他のユーザの変更が上書きされることを警告するメッセージが表示されます。
- 同じユーザーとして複数の Web インターフェイス インスタンス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集中に、1 つのインスタンスの変更を保存すると、他のインスタンスの変更は保存できません。

設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサ ルールとセキュリティ ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ポリシーまたは侵入ポリシーを保存すると、システムが必要な設定を自動的に有効にするか、または次のように無効な設定はトラフィックに影響しないことが警告されます。

- SNMPルールアラートを追加しても、SNMPアラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMPアラートを設定するか、またはルールアラートを無効にしてから、再度保存します。

- 侵入ポリシーに有効なセンシティブ データ ルールが含まれているときに、センシティブ データ プリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効にしてポリシーを保存するように許可するか、またはルールを無効にしてから、再度保存します。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効化しても、まだポリシーを保存できます。ただし、ネットワーク分析ポリシーの Web インターフェイスでプリプロセッサは無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。
- ネットワーク分析ポリシーでインラインモードを無効にしても、インライン正規化プリプロセッサが有効になっている場合は、ポリシーを引き続き保存できます。ただし、正規化設定が無視されることが警告されます。インラインモードを無効化すると他の設定が無視されるので、プリプロセッサは、チェックサム検証やレートベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。

ポリシー変更のコミット、破棄、およびキャッシュ

ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシー エディタを終了した場合、それらの変更はシステムによってキャッシュされます。変更は、システムからログアウトしたり、システム クラッシュが発生したりした場合でもキャッシュされます。システム キャッシュには、ユーザごとに 1 つのネットワーク分析ポリシーと 1 つの侵入ポリシーの未保存の変更しか格納されないため、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。システムは、ユーザが最初のポリシーへの変更を保存せずに別のポリシーを編集したり、侵入ルールの更新をインポートした場合に、キャッシュされた変更内容を破棄します。

ネットワーク分析ポリシー エディタまたは侵入ポリシー エディタの [ポリシー情報（Policy Information）] ページでポリシーの変更内容をコミットまたは破棄できます。

Secure Firewall Management Center 設定では、以下を制御できます。

- ネットワーク分析ポリシーまたは侵入ポリシーへの変更を確定するときに、それに関するコメントの入力を求めるか（または、コメントの入力を必須とするか）
- 変更内容とコメントを監査ログに記録するか

ネットワーク分析または侵入ポリシーの終了

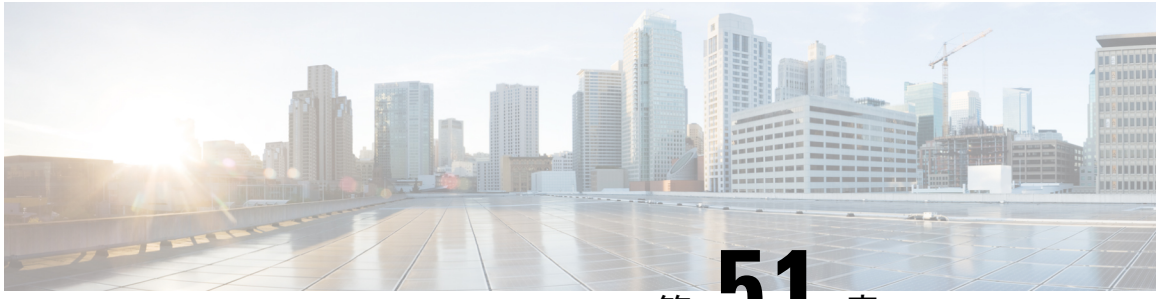
手順

ネットワーク分析、または侵入ポリシーの拡張エディタを終了するには、以下の方法があります。

- キャッシュ：ポリシーを終了し、変更をキャッシュするには、いずれかのメニューを選択するか、別のページへのほかのパスを選択します。終了時に表示される [ページを移動

（Leave page）] をクリックするか、[ページを移動しない（Stay on page）] をクリックして拡張エディタに残ります。

- 破棄：保存されていない変更を破棄するには、[ポリシー情報（Policy Information）] ページの [変更の破棄（Discard Changes）] をクリックし、[OK] をクリックします。
- 保存：ポリシーの変更を保存するには、[ポリシー情報（Policy Information）] ページの [変更の確定（ommit Changes）] をクリックします。プロンプトが表示される場合、コメントを入力し、[OK] をクリックします。



第 51 章

侵入ポリシーの使用を開始するには

ここでは、侵入ポリシーの使用を開始する方法について説明します。

- 侵入ポリシーの基本 （2001 ページ）
- 侵入ポリシーのためのライセンス要件 （2003 ページ）
- 侵入ポリシーの要件と前提条件 （2003 ページ）
- 侵入ポリシーの管理 （2003 ページ）
- カスタム侵入ポリシーの作成 （2005 ページ）
- Snort 2 侵入ポリシーの編集 （2006 ページ）
- 侵入防御を実行するためのアクセスコントロールルール設定 （2007 ページ）
- インライン展開でのドロップ動作 （2009 ページ）
- デュアル システム展開でのドロップ動作 （2010 ページ）
- 侵入ポリシーの詳細設定 （2011 ページ）
- 侵入検知と防御のパフォーマンス最適化 （2012 ページ）

侵入ポリシーの基本

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

各侵入ポリシーの中核となるのは、侵入ルールです。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

システムによって提供されるいくつかの基本的な侵入ポリシーにより、Talos インテリジェンス グループの経験を活用できます。これらのポリシーでは、Talos が侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。

ヒント システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- Cisco推奨機能を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらのアセットを保護するために作成されたルールに関連付ける。
- 外部アラート、センシティブ データの前処理、グローバル ルールのしきい値設定など、さまざまな詳細設定を設定する。
- レイヤを構成要素として使用し、複数の侵入ポリシーを効率的に管理する。

インライン展開では、侵入ポリシーによってトラフィックを変更したりブロックすることができます。

- 廃棄ルールを使用すると、一致したパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサの廃棄ルールを設定するには、そのステータスを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。
- 侵入ルールでは、`replace` キーワードを使用して悪意のあるコンテンツを置き換えることができます。

侵入ルールがトラフィックに影響を与えるようにするには、廃棄ルールおよびコンテンツを置き換えるルールを適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インライン インターフェイス セットを設定する）必要があります。最後に、侵入ポリシーのドロップ動作（[インライン時にドロップ（Drop when Inline）] 設定）を有効にします。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのWebインターフェイスではプリプロセッサは無効のままになります。

注意 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

カスタム侵入ポリシーを設定した後、それを 1 つ以上のアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けることによって、カスタム侵入ポリシーをアクセスコントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わて使用することにより、ホーム ネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセス コントロール ルールと暗号化された接続を照合する際の誤検出が減少し、パフォーマンスが向上します。

侵入ポリシーのためのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

侵入ポリシーの管理

[侵入ポリシー（Intrusion Policy）] ページ（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** **見出し** > **[侵入（Intrusion）]**）では、次に示す情報とともに、現在のカスタム侵入ポリシーを表示できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザー
- [インライン時にドロップ（Drop when Inline）] 設定が有効になっているかどうか。この設定が有効な場合、インライン展開でトラフィックをドロップしたり変更することができます。インライン展開は、ルーテッドインターフェイス、スイッチドインターフェイス、トランスペアレントインターフェイス、あるいはインラインインターフェイスのペアを使用してデバイスに展開される設定です。
- トラフィックの検査に侵入ポリシーを使用しているアクセス コントロール ポリシーとデバイス
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 侵入ポリシーを管理します。

- [比較（Compare）]：**[ポリシーの比較（Compare Policies）]** をクリックします（「ポリシーの比較」を参照）。
- 作成：[ポリシーの作成（Create Policy）] をクリックします。次を参照してください。
  - Snort 2 ポリシーの場合は、カスタム Snort 2 検査ポリシーの作成 （2005 ページ）。
  - Snort 3 ポリシーの場合は、最新バージョンの『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「*Creating a Custom Snort 3 Intrusion Policy*」トピック。
- 削除：削除するポリシーの横にある [削除（Delete）]（）をクリックします。別のユーザが保存していないポリシーの変更がある場合は、システムによって確認と通知のプロンプトが表示されます。[OK] をクリックして確認します。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 編集：次を選択します。
  - [Snort 2バージョン（Snort 2 Version）]。Snort 2 侵入ポリシーの編集 （2006 ページ）を参照してください。
  - [Snort 3バージョン（Snort 3 Version）]。最新バージョンの『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「*Editing Snort 3 Intrusion Policies*」トピックを参照してください。

  代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- エクスポート：別の Secure Firewall Management Center にインポートするために、侵入ポリシーをエクスポートするには、[YouTube EDU]（ ）をクリックします。Cisco Secure Firewall Management Center アドミニストレーション ガイド の 「エクスポート構成」を参照してください。
- [展開（Deploy）]：**[展開（Deploy）]** > **[展開（Deployment）]** をクリックします（設定変更の展開 （172 ページ） を参照）。
- レポート：[レポート（Report）]（ ）をクリックします（現在のポリシーレポートの生成 （192 ページ） を参照）。

カスタム侵入ポリシーの作成

新しい侵入ポリシーを作成する場合は、一意の名前を付けて基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

カスタム Snort 2 検査ポリシーの作成

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[Intrusion Policy] ページに戻るかどうか尋ねられたときに [Cancel] をクリックします。

[侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 [検査モード（Inspection Mode）] を選択します。

選択したアクションによって、侵入ルールでブロックしてアラートを発生させるか（**防御**モード）、またはアラートを発生させるのみにするか（**検出**モード）が決まります。

ステップ 5 [基本ポリシー（Base Policy）] で最初の基本ポリシーを選択します。

システム提供のポリシーまたは別のカスタム ポリシーを基本ポリシーとして使用できます。

ステップ 6 [保存（Save）] をクリックします。

新しいポリシーにはベースポリシーと同じ設定項目が含まれています。

関連トピック

レイヤでの侵入ルール （2189 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

Snort 2 侵入ポリシーの編集

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 設定する侵入ポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 4 ポリシーを編集します。

- 基本ポリシーの変更：[基本ポリシー（Base Policy）] ドロップダウン リストから基本ポリシーを選択します。基本ポリシーの変更 （2183 ページ）を参照してください。
- 詳細設定の構成：ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。侵入ポリシーの詳細設定 （2011 ページ）を参照してください。
- Cisco 推奨ルールの設定：ナビゲーションパネルで **[Cisco推奨事項（Cisco Recommendations）]** をクリックします。Cisco 推奨事項の生成と適用 （2201 ページ）を参照してください。
- インライン展開でのドロップ動作：[インライン時にドロップ（Drop when Inline）] をオンまたはオフにします。インライン展開でのドロップ動作の設定 （2010 ページ）を参照してください。
- 推奨ルール状態によるルールのフィルタ：推奨を生成した後、各推奨タイプの横にある [表示（View）] をクリックします。すべての推奨を表示するには、[推奨される変更の表示（View Recommended Changes）] をクリックします。
- 現在のルール状態によるルールのフィルタ：ルール状態タイプ（イベントを生成する、ドロップしてイベントを生成する）の横にある [表示（View）] をクリックします。侵入ポリシー内の侵入ルール フィルタ （2022 ページ）を参照してください。
- ポリシー階層の管理：ナビゲーション パネルで、[ポリシー層（Policy Layers）] をクリックします。レイヤ管理 （2185 ページ）を参照してください。
- 侵入ルールの管理：[ポリシー情報（Policy Information）] をクリックします。侵入ポリシー内の侵入ルールの表示 （2015 ページ）を参照してください。
- 基本ポリシーの設定の表示：[基本ポリシーの管理（Manage Base Policy）] をクリックします。基本レイヤ （2181 ページ）を参照してください。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

Cisco 推奨事項の生成と適用 （2201 ページ）
レイヤでの侵入ルールの設定 （2191 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

侵入ポリシーの変更

新しい侵入ポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が付与されます。

システムは、ユーザごとに1つのセキュリティ ポリシーをキャッシュします。侵入ポリシーの編集中に、メニューまたは別のページへのパスを選択すると、そのページから移動しても、変更内容はシステム キャッシュに残ります。

侵入防御を実行するためのアクセスコントロールルール設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先のIPアドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトセットにあるデフォルトの変数を変更します。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

システムには複数の侵入ポリシーが付属しています。システム提供の侵入ポリシーを使用することで、Talosインテリジェンスグループの経験を活用できます。これらのポリシーでは、Talosは侵入ルールおよびプリプロセッサ ルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタムポリシーのベースとして使用できます。カスタムポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

接続イベントおよび侵入イベントのロギング

アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成し、そのイベントを Secure Firewall Management Center に保存します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を Secure Firewall Management Center データベースに自動的にロギングします。

関連トピック

定義済みデフォルト変数 （1409 ページ）

アクセス コントロール ルール設定と侵入ポリシー

1 つのアクセス コントロール ポリシーで使用可能な一意の侵入ポリシーの数は、ターゲットデバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲットデバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを展開できません。

侵入防御を実行するアクセス コントロール ルールの設定

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者である必要があります。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、新しいルールを作成するか、既存のルールを編集します。アクセス コントロール ルールのコンポーネント （1778 ページ）を参照してください。

ステップ 2 ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 3 [検査（Inspection）] をクリックします。

ステップ 4 システムによって提供されるまたはカスタムの**侵入ポリシー**を選択するか、またはアクセス コントロール ルールに一致するトラフィックに対する侵入インスペクションを無効にするには [なし（None）] を選択します。

ステップ 5 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット（Variable Set）] ドロップダウン リストから値を選択します。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

ステップ 7 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

変数セット （1406 ページ）
Snort 再起動のシナリオ （162 ページ）

インライン展開でのドロップ動作

実際にトラフィックを変更せず、使用している設定がインライン展開（つまり、ルーテッド、スイッチド、またはトランスペアレントインターフェイス、あるいはインラインインターフェイスペアを使用して、関連する設定がデバイスに展開されている）でどのように機能するかを評価する場合は、ドロップ動作を無効にすることができます。その場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果を確認したら、ドロップ動作を有効化できます。

パッシブ展開またはタップモードでのインライン展開では、ドロップ動作に関わらず、システムはトラフィックに影響を与えることはできません。パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールは [イベントを生成する（Generate Events）] に設定されたルールと同様に動作します。システムは侵入イベントを生成しますが、パケットをドロップすることはできません。

（注） ファイルのブロックアクションにより、ブロックまたは保留中のファイルポリシーによるパケットの判定が発生し、その後、同じパケットで IPS イベントが生成されたとします。その場合、IPS ポリシーが検出モード（IDS）であっても、IPS イベントは Would have dropped ではなく Dropped としてマークされます。

（注） FTP を介してマルウェアの転送をブロックするには、マルウェア防御 を正しく設定するだけでなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーで [インライン時にドロップ（Drop when Inline）] を有効にする必要があります。

侵入イベントを表示する際に、ワークフローにインライン結果を含めることができます。インライン結果は、トラフィックが実際にドロップされたのか、あるいはドロップが想定に過ぎなかったのかを示します。

インライン展開でのドロップ動作の設定

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（ ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ポリシーのドロップ動作を設定します。

- [インライン時にドロップ（Drop when Inline）] チェックボックスをオンにして、侵入ルールのトラフィックへの適用とイベントの生成を許可します。
- [インライン時にドロップ（Drop when Inline）] チェックボックスをオフにすると、侵入ルールのトラフィックへの適用が禁止されますが、イベントは生成されます。

ステップ 4 [変更を確定（Commit Changes）] をクリックして、最後のポリシーの確定以降に、このポリシーに加えた変更を保存します。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

デュアル システム展開でのドロップ動作

ネットワーク内で2つのシステムが連続して接続されている場合、最初のシステムでドロップイベントが発生しても、2番目のシステムでドロップイベントまたは「ドロップ想定」イベントが記録されることは正常です。最初のシステムがファイルの最後のパケットをスキャンするまでにパケットをドロップすることを決定する一方で、2 番目のシステムもトラフィックを調査して「ドロップされる」と識別します。

たとえば、最初のパケットがルールをトリガーする 5 パケット HTTP GET リクエストは、最初のシステムによりブロックされ、最後のパケットのみがドロップされます。2 番目のシステム

は 4 パケットのみを受信し、接続はドロップされますが、2 番目のシステムがセッションをプルーニングしている間に部分的な GET リクエストを最後にフラッシュすると、インライン結果として「ドロップ想定」と同じルールがトリガーされます。

侵入ポリシーの詳細設定

侵入ポリシーの詳細設定を設定するには、特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーション パネルで [詳細設定（Advanced Settings）] を選択すると、ポリシーの詳細設定がタイプ別に一覧表示されます。[詳細設定（Advanced Settings）] ページでは、侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスすることができます。詳細設定を行うには、それを有効にする必要があります。

詳細設定を無効にすると、サブリンクと [編集（Edit）] リンクは表示されなくなりますが、設定は保持されます。侵入ポリシーの一部の設定（センシティブ データ ルール、侵入ルールの SNMP アラート）では、詳細設定を有効化して適切に設定する必要があります。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。

特定の脅威の検出

機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。

特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。

侵入ルールしきい値（Intrusion Rule Thresholds）

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。

外部レスポンス（External Responses）

Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システム ログ（syslog）ファシリティへのロギングを有効にしたり、イベントデータを SNMP トラップサーバーに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。

これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

関連トピック

機密データ検出の基本 （2203 ページ）
グローバル ルールのしきい値の基本 （2219 ページ）

侵入検知と防御のパフォーマンス最適化

Firepower システムを使用して侵入検知および防御を実行するものの検出データを利用する必要がない場合は、以下の説明に従って新しい検出を無効にしてパフォーマンスを最適化できます。

始める前に

このタスクを実行するには、次のいずれかのユーザーロールが必要です。

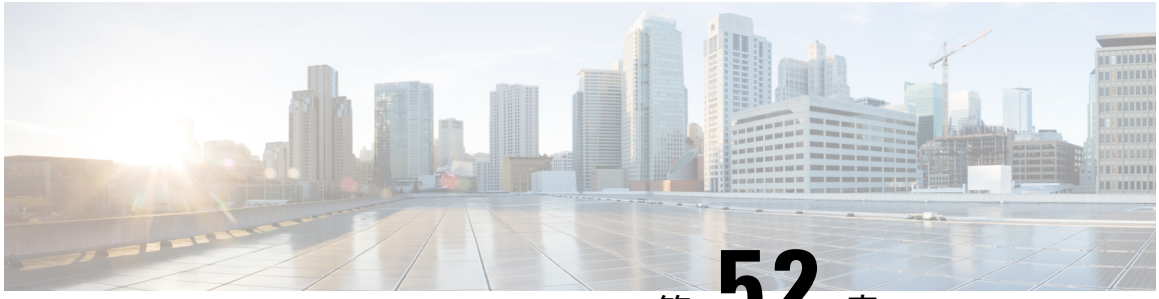
- アクセス制御用の管理者、アクセス管理者、またはネットワーク管理者。
- ネットワーク検出用の管理者または検出管理者。

手順

ステップ 1 ターゲット デバイスに導入したアクセス コントロール ポリシーと関連付けられたルールを変更または削除します。そのデバイスに関連付けられたアクセス制御ルールはいずれも、ユーザ、アプリケーション、または URL の条件を指定できません（アクセスコントロールルールの作成および編集 （1788 ページ）を参照）。

ステップ 2 ターゲット デバイスのネットワーク検出ポリシーからすべてのルールを削除します（ネットワーク検出ルールの設定 （2661 ページ）を参照）。

ステップ 3 変更された設定をターゲットデバイスに導入します（設定変更の展開 （172ページ）を参照）。



第 52 章

ルールを使用した侵入ポリシーの調整

ここでは、ルールを使用して侵入ポリシーを調整する方法について説明します。

- 侵入ルールの調整の基本 （2013 ページ）
- 侵入ルールのタイプ （2014 ページ）
- 侵入ルールのライセンス要件 （2015 ページ）
- 侵入ルールの要件と前提条件 （2015 ページ）
- 侵入ポリシー内の侵入ルールの表示 （2015 ページ）
- 侵入ポリシー内の侵入ルール フィルタ （2022 ページ）
- 侵入ルールの状態 （2031 ページ）
- 侵入ポリシーの侵入イベント通知フィルタ （2033 ページ）
- 動的侵入ルール状態 （2040 ページ）
- 侵入ルールコメントの追加 （2043 ページ）

侵入ルールの調整の基本

侵入ポリシーの [ルール（Rules）] ページを使用して、共有オブジェクトルール、標準テキストルール、およびプリプロセッサルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。また、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスでは無効化されたままになりますが、システムは自動的に現在の設定を使用します。

侵入ルールのタイプ

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムは、ネットワーク トラフィックを分析し、各ルールで指定された基準でパケットを比較し、データ パケットがルールで指定されたすべての基準を満たしている場合、ルールがトリガーされます。

侵入ポリシーには以下の構成要素があります。

- 侵入ルール。共有オブジェクト ルールと標準テキスト ルールに分割されます。
- プリプロセッサルール。パケットデコーダの検出オプション、またはシステムに付属のプリプロセッサの 1 つに関連付けられます。

次の表に、以上のルール タイプの属性を要約します。

表 *93 :* 侵入ルールのタイプ

タイプ（Type）	ジェネレータ ID（GID）	[Snort ID]（SID）	ソース（Source）	コピーの可否	編集の可否
共有オブジェクト ルール	3	1000000 未満	Talos インテリジェンス グループ	○	制限付き
標準テキスト ルール	1（グローバル ドメインまたはレガシー GID）	1000000 未満	Talos	○	制限付き
	1000～2000（子孫ドメイン）	1000000 以上	ユーザが作成またはインポート	○	○
プリプロセッサ ルール	デコーダまたはプリプロセッサに固有	1000000 未満	Talos	×	×
		1000000 以上	オプション設定時にシステムにより生成	×	×

Talos によって作成されたルールを変更して保存することはできませんが、変更されたルールのコピーをカスタム ルールとして保存することはできます。ルールで使用される変数またはルール ヘッダー情報（送信元と宛先のポートや IP アドレスなど）を変更できます。

Talos によって作成されるルールには、各デフォルト侵入ポリシー内でデフォルトのルール状態が割り当てられます。ほとんどのプリプロセッサルールがデフォルトで無効になっているため、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を行わせる場合は、これらのルールを有効にする必要があります。

マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタムルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバルドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。

侵入ルールのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入ルールの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

侵入ポリシー内の侵入ルールの表示

侵入ポリシー内のルールの表示方法を調整したり、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを表示している間、以下を実行できます。

- 侵入ポリシー内のルール フィルタの設定（2030ページ）の説明に従ってルールをフィルタリングします。
- ソートの基準とするカラムの一番上のタイトルをクリックすることによって、ルールをソートします。
- 侵入ルール詳細の表示（2018ページ）の説明に従って、侵入ルールの詳細を表示します。
- [ポリシー（Policy）] ドロップダウン リストから階層を選択することによって、異なるポリシー階層のルールを表示します。

[侵入ルール（Intrusion Rules）] ページの列

[侵入ルール（Intrusion Rules）] ページでは、メニュー バーおよび列ヘッダーに同じアイコンが使用されます。たとえば、[ルール状態（Rule State）] メニューでは、ルールリストの [ルール状態（Rule State）] カラムと同じ [イベントの生成（Generate Events）] が使用されます。

表 94 : [Rules] ページの列

見出し	説明
GID	ルールのジェネレータ ID（GID）を表す整数。
SID	ルールの固有識別子として機能する [Snort ID]（SID）を表す整数。 カスタム ルールの場合、SID は 1000000 以上です。
メッセージ	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。

見出し	説明
イベントを生成する（Generate Events）	ルールのルール状態。 • ドロップおよびイベントの生成 • イベントを生成する • 無効 無効なルールのアイコンは、トラフィックをドロップせずにイベントを生成するように設定されたルールのアイコンのグレー表示されたバージョンです。また、ルールのルール状態アイコンをクリックすると、ルール状態を変更できます。
Cisco 推奨ルール状態	ルールの Cisco 推奨ルール状態。
イベント フィルタ	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。
動的状態	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。
エラー（ ）	ルールに対して設定されたアラート（現在は SNMP アラートのみ）。
コメント（ ）	ルールに追加されたコメント。

レイヤのドロップダウンリストを使用して、ポリシー内の他のレイヤの[ルール（Rules）]ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの[ルール（Rules）]ページと、元は`My Changes`という名前だったポリシー階層の [ルール（Rules）] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。ドロップダウンリストには、読み取り専用の基本ポリシーの[ルール（Rules）]ページも表示されます。

侵入ルールの詳細

[ルールの詳細（Rule Detail）] ビューで、ルールドキュメント、Cisco の推奨事項、およびルールオーバーヘッドを確認できます。また、ルール固有の機能を表示および追加できます。

表 *95 :* ルールの詳細

項目	説明
要約	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこの行が表示されます。
ルール状態（Rule State）	ルールの現在のルール状態。ルール状態が設定された階層も示します。

項目	説明
Cisco の推奨事項（Cisco Recommendation）	Cisco の推奨事項が生成されている場合は、推奨されるルール状態を表すアイコンがあります。[侵入ルール（Intrusion Rules）]ページの列（2016ページ）を参照してください。ルールを有効にすることが推奨されている場合、システムは推奨事項をトリガーしたネットワーク アセットまたは設定も示します。
ルールのオーバーヘッド（Rule Overhead）	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。脆弱性にマップされていないローカル ルールにはオーバーヘッドが割り当てられていません。
しきい値	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。
抑制（Suppressions）	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。
動的状態（Dynamic State）	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。
アラート（Alerts）	このルールに設定されている SNMP アラートと、ルールのアラートを追加するための機能。
説明	このルールに追加されたコメントと、ルールのコメントを追加するための機能。
資料	Talos インテリジェンス グループによって提供される現在のルールのルール ドキュメント。必要に応じて、[ルール ドキュメンテーション（Rule Documentation）]をクリックして、ルールの詳細を表示します。

侵入ルール詳細の表示

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ペインで [ルール（Rules）] をクリックします。

ステップ 4 ルールの詳細を表示したいルールをクリックし、ページの下部にある [詳細の表示（Show details）] をクリックします。
侵入ルールの詳細（2017 ページ）で説明されているように、ルールの詳細が表示されます。

ステップ 5 ルールの詳細から、以下を設定できます。

- アラート：侵入ルールの SNMP アラートの設定 （2021 ページ）を参照してください。
- コメント：侵入ルールへのコメントの追加 （2022 ページ）を参照してください。
- ダイナミック ルールの状態：[ルール詳細（Rule Details）] ページからの動的ルール状態の設定 （2020 ページ）を参照してください。
- しきい値：侵入ルールのしきい値の設定 （2019 ページ）を参照してください。
- 抑制：侵入ルールの抑制の設定 （2020 ページ）を参照してください。

侵入ルールのしきい値の設定

[ルールの詳細（Rule Detail）] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

無効な値を入力するとフィールドに [復元（Revert）] が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[しきい値（Thresholds）] の横にある [追加（Add）] をクリックします。

ステップ 2 [タイプ（Type）] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベントインスタンス数に通知を制限する場合は、[制限（Limit）] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値（Threshold）] を選択します。
- 指定されたイベントインスタンス数に達した後で、期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

ステップ 3 [追跡対象（Track By）] ドロップダウンリストから、[送信元（Source）] または [宛先（Destination）] を選択し、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

ステップ 4 [カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5 [秒数（Seconds）] フィールドに、イベント インスタンスを追跡する期間（秒数）を指定する数値を入力します。

ステップ 6 [OK] をクリックします。

ヒント
[イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加すると、イベントフィルタの数が表示されます。

侵入ルールの抑制の設定

侵入ポリシーのルールに対して 1 つ以上の抑制を設定できます。

無効な値を入力するとフィールドに[復元（Revert）] アイコンが表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[抑制（Suppressions）] の横にある [追加（Add）] をクリックします。

ステップ 2 [抑制タイプ（Suppression Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール（Rule）] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] を選択します。

ステップ 3 抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに IP アドレス、アドレス ブロック、またはそれらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルトアクション変数セットでネットワーク変数を指定または列挙することもできます。

ステップ 4 [OK] をクリックします。

ヒント
抑制するルールの横にある [イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加した場合は、フィルタ上の数字がフィルタの数を示します。

[ルール詳細（Rule Details）] ページからの動的ルール状態の設定

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに [復元（Revert）] が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[動的状態（Dynamic State）] の横にある [追加（Add）] をクリックします。

ステップ 2 [追跡対象（Track By）] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元（Source）] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先（Destination）] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール（Rule）] を選択します。

ステップ 3 [追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。

ステップ 4 [レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドで、しきい値として使用するルール一致の数を指定します。
- [秒（Seconds）] フィールドで、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5 [新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを選択します。

ステップ 6 [タイムアウト（Timeout）] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を入力します。

ステップ 7 [OK] をクリックします。

ヒント

[動的状態（Dynamic State）] カラムのルールの横に動的状態（）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、フィルタ上の数字がフィルタの数を示します。

侵入ルールの SNMP アラートの設定

[ルールの詳細（Rule Detail）] ページで、ルールの SNMP アラートを設定できます。

手順

侵入ルールの詳細で、[アラート（Alerts）] の横にある [SNMP アラートの追加（Add SNMP Alert）] をクリックします。

ヒント

[アラート（Alerting）] カラムのルールの横にアラート **エラー**（） が表示されます。ルールに複数のアラートを追加した場合は、アラートの数が表示されます。

侵入ルールへのコメントの追加

手順

ステップ 1 侵入ルールの詳細で、[コメント（Comments）] の横の [追加（Add）] をクリックします。

ステップ 2 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 3 [OK] をクリックします。

ヒント

システムは [コメント（Comments）] カラムのルールの横に **コメント**（） を表示します。ルールに複数のコメントを追加した場合は、コメント上の数字がコメントの数を示します。

ステップ 4 ルール コメントを削除するには、ルール コメント セクションで [削除（Delete）] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

侵入ポリシー内の侵入ルール フィルタ

[ルール（Rules）] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[ルール（Rules）] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

侵入ルール フィルタの注意事項

作成したフィルタが [フィルタ（Filter）] テキストボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、**[ルール コンテンツ（Rule Content）] > [GID]** の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

[カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、[プリプロセッサ（Preprocessor）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタパネルを表示するには、**表示アイコン** をクリックします。

フィルタパネルを非表示にするには、**非表示アイコン** をクリックします。

侵入ポリシー ルール フィルタ構築のガイドライン

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには複数のレベルが設定されているので、それを展開して個別のルールにドリルダウンできます。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の点に注意してください。

- キーワード（[ルール設定（Rule Configuration）]、[ルール コンテンツ（Rule Content）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）]）以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開されて使用可能なキーワードが一覧表示されます。

  基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

  そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

  たとえば、フィルタ パネルの **[ルール設定（Rule Configuration）] > [推奨（Recommendation）]** で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキストボックスに追加されます。その後で、**[ルール設定（Rule Configuration）] > [推奨**

（**Recommendation**）] で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

- キーワード（[カテゴリ（Category）]、[分類（Classifications）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[優先度（Priority）]、および [ルール アップデート（Rule Update）]）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

  このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[カテゴリ（Category）] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [ルール コンテンツ（Rule Content）] の下の [参照（Reference）] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタパネルで **[ルールコンテンツ（Rule Content）]** > **[参照（Reference）]** > **[CVE ID]** の順にクリックすると、ポップアップウィンドウが開いて CVE ID を指定するよう求められます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキストボックスに追加されます。別の例では、フィルタパネルで **[ルールコンテンツ（Rule Content）]** > **[参照（Reference）]** の順にクリックすると、ポップアップウィンドウが開いて、参照を指定するよう求められます。「`2007`」と入力すると、「`Reference:"2007"`」がフィルタ テキストボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[Microsoft 脆弱性（Microsoft Vulnerabilities）] で [MS00-006] をクリックすると、フィルタが「`Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、**[ルール コンテンツ（Rule Content）]** > **[GID]** の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

- [カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数

の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,app-detect"`」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールを [dos] カテゴリによってフィルタ処理する場合や [High] 優先度でフィルタ処理する場合は、DOS Cisco 試行ルール（SID 1545）が表示されます。

（注） Talos インテリジェンス グループ がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[ルール（Rules）] ページのルールは、共有オブジェクト ルール（ジェネレータ ID 3）または標準テキスト ルール（ジェネレータ ID 1、グローバル ドメインまたはレガシー GID（1000 ～ 2000）、子孫ドメイン）のいずれかになります。次の表に、さまざまなルール フィルタの説明を示します。

表 *96 :* ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Rule Configuration	ルールの設定に基づいてルールを検索します。	いいえ	グループ	キーワード
Rule Content	ルールの内容に基づいてルールを検索します。	いいえ	グループ	キーワード
Category	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。	はい	キーワード	引数
Classifications	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。	いいえ	キーワード	引数
Microsoft Vulnerabilities	Microsoft セキュリティ情報番号に従ってルールを検索します。	はい	キーワード	引数
Microsoft Worms	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	はい	キーワード	引数

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Platform Specific	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
Preprocessors	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成し、インライン展開では、違反パケットをドロップします。するためには、そのオプションに関連付けられたプリプロセッサ ルールを有効にする必要があることに注意してください。	はい	グループ	サブグループ
Priority	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカルルール（つまり、ユーザーがインポートまたは作成したルール）は優先度グループに表示されないことに注意してください。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
Rule Update	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	いいえ	キーワード	引数

侵入ルール構成フィルタ

[ルール（Rules）]ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[推奨と一致しない（Does not match recommendation）] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの **[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、**[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

侵入ルール コンテンツ フィルタ

[Rules] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [Rule Content] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力が促されます。「`1045`」と入力すると、「`SID:"1045"`」がフィルタ テキスト ボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「`1044`」に変更すると、フィルタが「`SID:"1044"`」に変更されます。

表 *97:* ルール コンテンツ フィルタ

フィルタ	検索するルールの内容
メッセージ	メッセージ フィールドで指定された文字列を含む。
SID	指定された SID がある。
GID	指定された GID がある。
参照	参照フィールドで指定された文字列を含む。また、特定のタイプの参照および指定された文字列でフィルタリングすることもできます。
操作	`alert` または `pass` から開始する。
プロトコル	選択されたプロトコルを含む。
方向（Direction）	ルールに、指定された方向設定が含まれているかどうかに基づく。
ソース IP	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または `$HOME_NET` や `$EXTERNAL_NET` などの変数を使用してフィルタ処理できます。

フィルタ	検索するルールの内容
宛先 IP（Destination IP）	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できます。
ソース ポート	指定された送信元ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
接続先ポート（Destination port）	指定された宛先ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
ルールのオーバーヘッド	選択されたルールのオーバーヘッドがある。
メタデータ	一致するキーと値のペアを含むメタデータがある。たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「metadata:"service http"」と入力します。

侵入ルール カテゴリ

Firepower システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[ルール（Rules）] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールの数を表示できます。

（注） Talos インテリジェンス グループ がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

侵入ルールのフィルタ コンポーネント

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[ルール（Rules）] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[ルール（Rules）] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキストボックスに表示されます。キーワードのカンマ区切りの複数の引数は [カテゴリ（Category）] と [優先度（Priority）] のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、および除外文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および[SID]の各フィールドで指定された単語が検索されます。

`gid`キーワードと`sid`キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

`keyword:"argument"`

ここで、Keyword は侵入ルール フィルタ グループ内のキーワードのいずれかで、argument は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの[メッセージ（Message）]フィールド、[Snort ID]（SID）、およびジェネレータ ID（GID）を検索します。たとえば、文字列 `123` は、ルール メッセージ内の文字列 `"Lotus123"` や `"123mania"` などを返し、`SID 6123` や `SID 12375` なども返します。部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列`ADMIN`、`admin`、または`Admin`はすべて、「`admin`」、「`CFADMIN`」、「`Administrator`」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されるフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタリングの結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

侵入ルール フィルタの使用

侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたフィルタは、ルールデータベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内のルール フィルタの設定

[ルール（Rules）]ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキストメニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

すべてのフィルタのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（ ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 次に示す方法を個別に使用したり、組み合わせて使用することでフィルタを作成します。

- [フィルタ（Filter）] テキスト ボックスに値を入力して、Enter キーを押します。
- 事前定義されたキーワードのいずれかを展開します。たとえば、[ルール設定（Rule Configuration）] をクリックします。
- キーワードをクリックして、プロンプトが表示されたら引数の値を指定します。次に例を示します。

- [ルール設定（Rule Configuration）] の下で、[ルール状態（Rule State）] をクリックし、ドロップダウンリストから [イベントの生成（Generate Events）] を選択して、[OK] をクリックします。
- [ルール設定（Rule Configuration）] の下で、[コメント（Comment）] をクリックし、フィルタ条件として使用するコメント テキストの文字列を入力して、[OK] をクリックします。
- [カテゴリ（Category）] の下で、[アプリ検出（app-detect）] をクリックします。システムは、これを引数の値として使用します。

- キーワードを展開して、引数の値をクリックします。たとえば、[ルール状態（Rule State）] を展開して、[イベントの生成（Generate Events）] をクリックします。

侵入ルールの状態

侵入ルールの状態により、個々の侵入ポリシー内のルールを有効または無効にできるだけでなく、モニタ対象の条件によってルールがトリガーされたときにシステムが実行するアクションを指定できます。

各デフォルト ポリシーの侵入ルールとプリプロセッサ ルールのデフォルト状態は、Talos インテリジェンスグループが設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。Talos がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合もあります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルトポリシー（または基礎となるデフォルトポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

侵入ルールを作成すると、そのルールは、ポリシーの作成時に使用されたデフォルトポリシー内のルールのデフォルト状態を継承します。

侵入ルールの状態オプション

侵入ポリシーでは、ルールの状態を次の値に設定できます。

イベントを生成する（Generate Events）

システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。悪意のあるパケットはその対象に到達しますが、イベント ロギングによって通知されます。

ドロップおよびイベントの生成（Drop and Generate Events）

システムで特定の侵入試行を検出して、その攻撃を含むパケットをドロップし、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットはその対象に到達せず、イベント ロギングによって通知されます。

このルール状態に設定されたルールはイベントを生成しますが、パッシブ展開ではパケットをドロップしないことに注意してください。システムがパケットをドロップするには、侵入ポリシーで[インライン時にドロップ（Drop when Inline）] も有効にして、デバイスインラインを展開する必要があります。

無効（Disable）

システムで一致するトラフィックを評価しない場合。

（注） [イベントを生成する（Generate Events）] または [ドロップおよびイベントの生成（Drop and Generate Events）] オプションのいずれかを選択すると、ルールが有効になります。[無効（Disable）] を選択すると、ルールが無効になります。

シスコでは、侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨しています。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルールセットを調整してください。

侵入ルール状態の設定

侵入ルール状態は、ポリシー固有です。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント
このページには、有効なルールの総数、[イベントを生成する（Generate Events）] に設定された有効なルールの総数、および[ドロップしてイベントを生成する（Drop and Generate Events）] に設定された有効なルールの総数が表示されます。また、パッシブ展開では、[Drop and Generate Events] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

ステップ 3 ナビゲーションウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルール状態を設定する 1 つ以上のルールを選択します。

ステップ 5 次のいずれかを実行します。

- **[Rule State]** > **[Generate Events]**
- **[Rule State]** > **[Drop and Generate Events]**
- **[Rule State]** > **[Disable]**

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

侵入ポリシーの侵入イベント通知フィルタ

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

侵入イベントしきい値

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。共有オブジェクトのルール、標準テキスト ルール、またはプリプロセッサ ルールごとにしきい値を設定できます。

侵入イベントしきい値の設定

しきい値を設定するには、最初にしきい値のタイプを指定します。

表 *98 :* しきい値設定オプション

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[Seconds] と [Count] のカウンタをリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
Both	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定します。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。

表 *99 : IP* しきい値設定オプション

オプション	説明
ソース（Source）	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
Destination	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *100* : インスタンス/時間のしきい値設定オプション

オプション	説明
カウント	しきい値を満たすために必要な、追跡するIPアドレス単位で指定された期間単位のイベントインスタンスの数。
Seconds	カウントがリセットされるまでの秒数。しきい値タイプを [制限（limit）] に、トラッキングを [送信元IP（Source IP）] に、[カウント（count）] を [10] に、[秒（seconds）] を [10] に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒間に 7 つのイベントしか発生しなかった場合は、システムがそれらのイベントを記録して表示します。最初の 10 秒間に 40 のイベントが発生した場合は、システムが 10 のイベントを記録して表示してから 10 秒後にカウントを再開します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。

ヒント 侵入イベントのパケット ビューでしきい値を追加することもできます。

関連トピック

detection_filter キーワード （2161 ページ）

侵入イベントしきい値の追加と変更

侵入ポリシーの1つ以上の特定のルールにしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに1つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

また、侵入ポリシーに関係したすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

無効な値を入力するとフィールドに**復元**が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ヒント 複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 しきい値を設定するルールを選択します。

ステップ 5 [イベントのフィルタリング（Event Filtering）] > [しきい値（Threshold）] を選択します。 >

ステップ 6 [タイプ（Type）] ドロップダウン リストからしきい値のタイプを選択します。

ステップ 7 [追跡対象（Track By）] ドロップダウンリストから、イベントインスタンスが [送信元（Source）] IP アドレスまたは [宛先（Destination）] IP アドレスのどちらによって追跡されるかを選択します。

ステップ 8 [カウント（Count）] フィールドに値を入力します。

ステップ 9 [秒（Seconds）] フィールドに値を入力します。

ステップ 10 [OK] をクリックします。

ヒント
[イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加した場合は、フィルタ上の数字がイベントフィルタの数を示します。

ステップ 11 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

グローバル ルールのしきい値の基本 （2219 ページ）

侵入イベントしきい値の表示と削除

ルールに関する既存のしきい値設定を表示または削除することができます。[Rules Details] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

侵入ポリシーによって記録されるすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。

ステップ 5 選択した各ルールのしきい値を削除するには、**[イベントフィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）]** の順に選択します。

ステップ 6 [OK] をクリックします。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

グローバル ルールのしきい値の基本 （2219 ページ）

侵入ポリシー抑制の設定

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを伝送しているメールサーバが存在する場合は、そのメールサーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入ポリシー抑制タイプ

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。

ヒント　侵入イベントのパケット ビュー内から抑制を追加できます。また、侵入ルール エディタ ページ（**[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**）や任意の侵入イベント ページ（イベントが侵入ルールによってトリガーされた場合）で右クリック コンテキスト メニューを使用して、抑制設定にアクセスすることもできます。

関連トピック

detection_filter キーワード （2161 ページ）

特定のルールの侵入イベントの抑制

侵入ポリシーのルールに関連する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2つの抑制が競合している場合は、最初の抑制のアクションが実行されます。

無効な値を入力するとフィールドに [復元（Revert）] が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1　**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

ステップ 2　編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3　[ナビゲーション（navigation）] パネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4　抑制条件を設定する 1 つまたは複数のルールを選択します。

ステップ 5　**[イベント フィルタリング（Event Filtering）]** > **[抑制（Suppression）]** を選択します。

ステップ 6　[抑制タイプ（Suppression Type）] を選択します。

ステップ 7　抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

ステップ 8　[OK] をクリックします。

ヒント
抑制するルールの横にある [イベントフィルタリング（Event Filtering）] カラムのルールの横に [イベントフィルタ（Event Filter）] が表示されます。ルールに複数のイベントフィルタを追加した場合は、フィルタ上の数字がイベントフィルタの数を示します。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

抑制条件の表示と削除

既存の抑制条件を表示または削除することもできます。たとえば、メールサーバーが悪用のように見えるパケットを普段から送信しているという理由で、そのメール サーバーの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメール サーバーが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] パネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 抑制を表示または削除する 1 つまたは複数のルールを選択します。

ステップ 5 次の選択肢があります。

- ルールのすべての抑制を削除するには、**[イベントフィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）]**を選択します。
- 特定の抑制設定を削除するには、ルールをクリックして、[詳細の表示（Show Details）] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [削除（Delete）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

動的侵入ルール状態

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レートベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

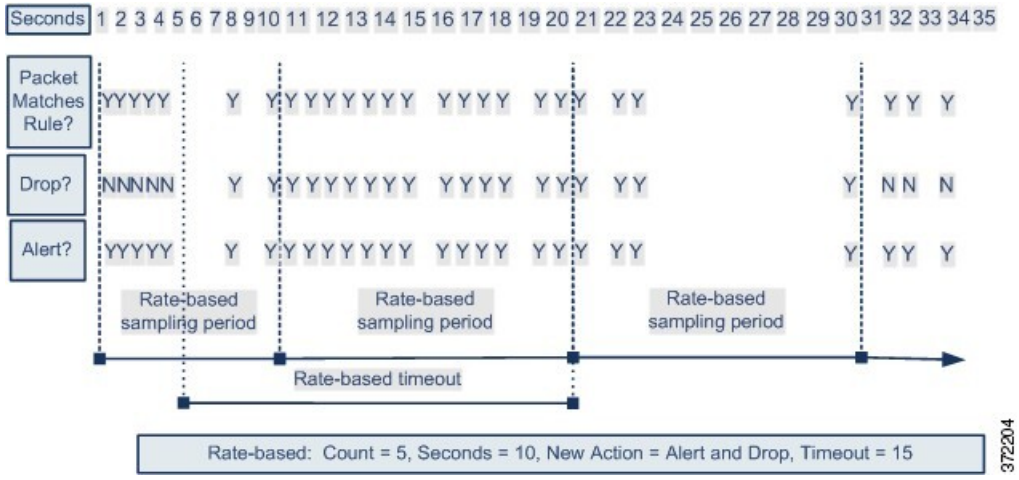
侵入ポリシーにレートベースのフィルタを含めることにより、一定期間においてルールの一致が過剰に発生した時点を検出できます。インライン展開された管理対象デバイス上でこの機能を使用して、指定された時刻のレートベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

レートベースの攻撃防止は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値を超えている場合は、新しいアクションが続行されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[イベントを生成する（Generate Events）] に戻ります。



ダイナミックな侵入ルール状態の設定

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（[イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、および [無効（Disable）] の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[イベントを生成する（Generate Events）] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レートベースの基準が設定されているルールに一致した場合、それらのルールが当初 [イベントのドロップおよび生成（Drop and Generate Events）] に設定されていないとしても、レート アクションがアクティブである期間は、パケットがドロップされる場合があります。

（注） レート ベース アクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。

同じルールに複数のレート ベース フィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレートベースのフィルタ アクション

が競合している場合は、最初のレートベースのフィルタのアクションが実行されることに注意してください。

[ルール（Rule）] ページからの動的ルール状態の設定

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに**復元**が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

（注） 動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 動的ルール状態を追加する 1 つまたは複数のルールを選択します。

ステップ 5 **[動的状態（Dynamic State）] > [レート ベースのルール状態の追加（Add Rate-Based Rule State）]** を選択します。

ステップ 6 [追跡対象（Track By）] ドロップダウンリストから値を選択します。

ステップ 7 [Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストのアドレスを入力します。単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。

ステップ 8 [レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドに値を入力します。
- [秒（Seconds）] フィールドに値を入力します。

ステップ 9 [新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを指定します。

ステップ 10 [タイムアウト（Timeout）] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[Timeout] フィールドを空白のままにします。

ステップ 11 [OK] をクリックします。

ヒント
[動的状態（Dynamic State）] 列のルールの横に [動的状態（Dynamic State）] が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、フィルタ上の数字がフィルタの数を示します。

ヒント
ルールのセットに対する動的ルール設定を削除するには、[ルール（Rules）]ページでルールを選択して、**[動的状態（Dynamic State）] > [レート ベースの状態の削除（Remove Rate-Based States）]** を選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[詳細の表示（Show Details）] をクリックしてから、削除するレート ベースのフィルタのそばにある [削除（Delete）] をクリックします。

ステップ 12 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

侵入ルールコメントの追加

侵入ポリシーのルールにコメントを追加できます。このようにして追加されたコメントはポリシー専用のコメントとなります。よって、ある侵入ポリシーのルールに追加したコメントは、他の侵入ポリシーでは表示されません。追加したコメントは、侵入ポリシーの [ルール（Rules）] ページ上の [ルールの詳細（Rule Details）] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [編集（Edit）] ページで [ルール コメント（Rule Comment）] をクリックしてコメントを表示することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] パネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 コメントを追加する 1 つまたは複数のルールを選択します。

ステップ 5 [コメント（Comments）] > [ルールコメントの追加（Add Rule Comment）] を選択します。 >

ステップ 6 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 7 [OK] をクリックします。

ヒント

システムは [コメント（Comments）] カラムのルールの横に **コメント**（） を表示します。ルールに複数のコメントを追加した場合は、コメント上の数字がコメントの数を示します。

ステップ 8 必要に応じて、コメントの横にある [削除（Delete）] をクリックし、ルールのコメントを削除します。

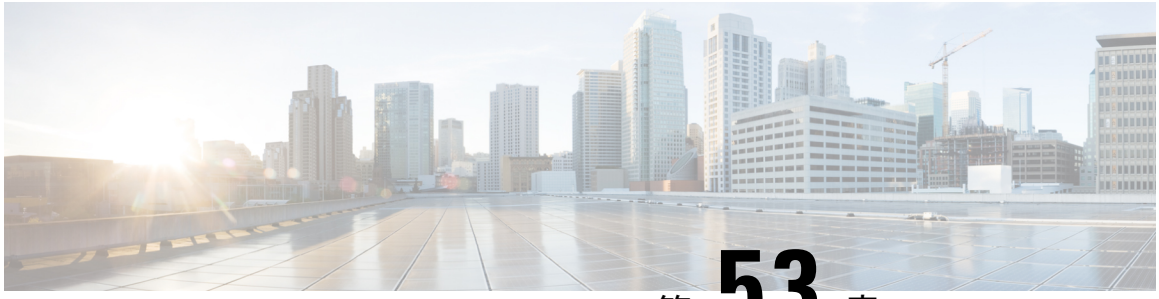
侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。



第 53 章

カスタム侵入ルール

以下のトピックでは、侵入ルール エディタの使用方法について説明します。

- カスタム侵入ルールの概要 （2045 ページ）
- 侵入ルールエディタのライセンス要件 （2046 ページ）
- 侵入ルールエディタの要件と前提条件 （2046 ページ）
- ルールの詳細 （2047 ページ）
- カスタム ルールの作成 （2060 ページ）
- ルールの検索 （2066 ページ）
- 侵入ルール エディタ ページでのルールのフィルタリング （2068 ページ）
- 侵入ルールのキーワードと引数 （2072 ページ）

カスタム侵入ルールの概要

侵入ルールは、ネットワークの脆弱性を不正利用する試みを検出するために使用するキーワードや引数です。ネットワーク トラフィックの分析では、パケットを各ルールで指定した条件と比較します。パケットのデータがルールで指定したすべての条件に一致すると、そのルールがトリガーされます。アラート ルールであれば、侵入イベントが生成されます。通過ルールであれば、トラフィックを無視します。インライン展開の廃棄ルールでは、システムがパケットを破棄してイベントを生成します。侵入イベントは、Secure Firewall Management Center の Web インターフェイスから表示して評価できます。

システムの侵入ルールには、共有オブジェクト ルールと標準テキスト ルールの 2 種類があります。Talos インテリジェンス グループ では、共有オブジェクト ルールを使うことにより、従来の標準テキスト ルールではできなかった方法で脆弱性に対する攻撃を検出できます。共有オブジェクト ルールを作成することはできません。独自の侵入ルールを作成する場合は、標準テキスト ルールを作成します。

発生する可能性のあるイベントのタイプを調整するために、カスタム標準テキスト ルールを作成することができます。このマニュアルでは特定のエクスプロイトの検出を目的とするルールについて説明することもありますが、優秀なルールのほとんどは、特定の既知のエクスプロイトではなく既知の脆弱性を悪用しようとするトラフィックをターゲットとすることに注意してください。ルールを作成してルールのイベント メッセージを指定することにより、攻撃とポリシー回避を示唆するトラフィックをより簡単に識別できます。

カスタム侵入ポリシーでカスタム標準テキストルールを有効にすると、一部のルールキーワードと引数では、トラフィックを特定の方法で最初に復号または前処理する必要があることに留意してください。この章では、前処理を制御するネットワーク分析ポリシーで設定する必要があるオプションについて説明します。注意点として、必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

注意 作成した侵入ルールを実稼働環境で使用する前に、制御されたネットワーク環境で必ずテストしてください。不適切に作成された侵入ルールは、システムのパフォーマンスに重大な影響を与える可能性があります。

（注） Snort を使用してカスタム侵入ルールを作成できます。ただし、カスタム侵入ルールの調整と障害対応のサポートは現在利用できません。

侵入ルールエディタのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入ルールエディタの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

ルールの詳細

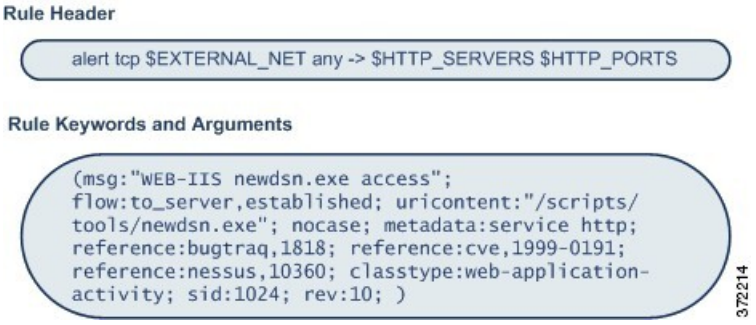
すべての標準テキスト ルールには、ルール ヘッダーとルール オプションという 2 つの論理セクションが含まれています。ルール ヘッダーの内容は次のとおりです。

- ルールのアクションまたはタイプ
- プロトコル
- 送信元および宛先の IP アドレスとネットマスク
- 送信元から宛先へのトラフィック フローを示す方向インジケータ
- 送信元ポートと宛先ポート

ルール オプション セクションの内容は次のとおりです。

- イベント メッセージ
- キーワードとそのパラメータおよび引数
- ルールをトリガーとして使用するためにパケットのペイロードが一致する必要があるパターン
- パケットのどの部分をルール エンジンで検査するかの指定

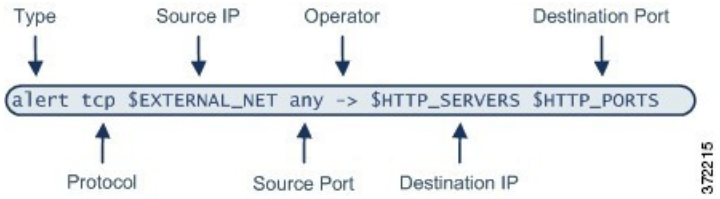
次の図に、ルールの構成要素を示します。



ルールのオプション セクションは、カッコで囲まれたセクションであることに注意してください。侵入ルール エディタは、標準テキスト ルールの作成を支援する使いやすいインターフェイスを備えています。

侵入ルール ヘッダー

すべての標準テキスト ルールおよび共有オブジェクト ルールに、パラメータと引数を含むルール ヘッダーがあります。ルール ヘッダーの構成要素を以下に示します。



次の表では、上記のルール ヘッダーの各部分について説明します。

表 *101* : ルール ヘッダーの値

ルール ヘッダーのコンポーネント	値の例	機能
操作	`alert`	トリガー時に侵入イベントを生成します。
プロトコル	`tcp`	TCP トラフィックのみをテストします。
送信元 IP アドレス	`$EXTERNAL_NET`	内部ネットワーク上に存在しないホストから送られてきたトラフィックをテストします。
送信元ポート	`any`	発信元ホスト上の任意のポートから送られてきたトラフィックをテストします。
演算子	`->`	（このネットワーク上の Web サーバーに向かう）外部トラフィックをテストします。
宛先 IP アドレス	`$HTTP_SERVERS`	この内部ネットワーク上の Web サーバとして指定された任意のホストに送られるトラフィックをテストします。
宛先ポート	`$HTTP_PORTS`	この内部ネットワーク上の HTTP ポートに送られるトラフィックをテストします。

（注） 前述の例では、ほとんどの侵入ルールの場合と同様に、デフォルト変数が使用されています。

関連トピック

変数セット （1406 ページ）

侵入ルール ヘッダー アクション

各ルールヘッダーには、パケットがルールをトリガーとして使用したときにシステムで行われるアクションを指定するパラメータが 1 つ含まれています。アクションが *alert* に設定されたルールは、それをトリガーとして使用したパケットに対する侵入イベントを生成し、そのパケットの詳細をログに記録します。アクションが *pass* に設定されたルールは、それをトリガーとして使用したパケットに関するイベントを生成せず、そのパケットの詳細も記録しません。

（注） インライン展開において、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールは、それをトリガーとして使用したパケットに対する侵入イベントを生成します。また、パッシブ展開で廃棄ルールを適用した場合は、ルールがアラートルールとして機能します。

デフォルトでは、パス ルールがアラート ルールをオーバーライドします。パス ルールを作成することで、アラート ルールを無効にする代わりに、パス ルールで定義された基準を満たすパケットが特定の状況でアラート ルールをトリガーとして使用しないことを指定できます。たとえば、ユーザ "anonymous" として FTP サーバにログインする試行を検索するルールをアクティブのままにする必要があるとします。ただし、1 つ以上の正式な匿名 FTP サーバがネットワークに存在する場合、そのような特定のサーバで匿名ユーザにより最初のルールがトリガーとして使用されないことを指定するパス ルールを作成し、アクティブにすることができます。

侵入ルール エディタで、[アクション（Action）] リストからルール タイプを選択します。

侵入ルール ヘッダー プロトコル

各ルール ヘッダーで、ルールにより検査されるトラフィックのプロトコルを指定する必要があります。次のネットワーク プロトコルを分析対象として指定できます。

- ICMP（Internet Control Message Protocol）
- インターネット プロトコル（IP）

（注） プロトコルが `ip` に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。

- 伝送制御プロトコル（TCP）
- ユーザー データグラム プロトコル（UDP）

TCP、UDP、ICMP、IGMP など、IANA によって割り当てられたすべてのプロトコルを検査するには、プロトコル タイプとして **IP** を使用します。

（注） 現在のところ、IP ペイロード内の次のヘッダー（TCP ヘッダーなど）でパターンを照合するルールを作成することはできません。代わりに、最後にデコードされたプロトコルからコンテンツ照合が始まります。次善策として、ルール オプションを使用して TCP ヘッダー内のパターンを照合できます。

侵入ルール エディタで、[プロトコル（Protocol）] リストからプロトコル タイプを選択します。

関連トピック

侵入ルール ヘッダー プロトコル （2049 ページ）

侵入ルール ヘッダーの方向

ルールによる検査対象となるパケットが進むべき方向を、ルールヘッダー内で指定できます。以下の表は、それらのオプションを示しています。

表 *102 :* ルール ヘッダー内の方向オプション

使用するフィルタ	テスト対象
指向性	指定された送信元 IP アドレスから指定された宛先 IP アドレスに向かうトラフィックのみ
双方向	指定された送信元 IP アドレスと宛先 IP アドレスの間を移動するすべてのトラフィック

侵入ルール ヘッダーの送信元と宛先の IP アドレス

パケット検査の対象を、特定の IP アドレスから発信されたパケットまたは特定の IP アドレスに向かうパケットに制限すると、システムが実行しなければならないパケット検査の量が減ります。さらに、ルールをより具体化し、送信元および宛先 IP アドレスが疑わしい動作を示していないパケットに対してルールがトリガーとして使用される可能性をなくすと、誤検出も減ります。

ヒント　システムは IP アドレスのみを認識し、送信元/宛先 IP アドレスのホスト名を受け入れません。

侵入ルール エディタの [送信元 IP（Source IPs）] フィールドと [宛先 IP（Destination IPs）] フィールドで、送信元および宛先の IP アドレスを指定します。

標準テキスト ルールの作成時には、必要に応じて、さまざまな方法で IPv4 アドレスと IPv6 アドレスを指定できます。単一の IP アドレス、`any`、IP アドレス リスト、CIDR 表記、プレフィクス長、またはネットワーク変数を指定できます。加えて、1 つの特定の IP アドレスまたは IP アドレスのセットを除外するよう指定できます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

侵入ルールの IP アドレスの構文

次の表では、送信元と宛先の IP アドレスを指定するさまざまな方法を要約します。

表 *103 :* 送信元/宛先 *IP* アドレスの構文

指定する項目	指定内容	例
任意の IP アドレス	任意	任意

指定する項目	指定内容	例
1 つの特定の IP アドレス	その IP アドレス 同じルール内に IPv4 と IPv6 の送信元アドレスと宛先アドレスを混在させないでください。	`192.168.1.1` `2001:db8::abcd`
IP アドレスのリスト	複数の IP アドレスをカンマで区切り、それを大カッコ（`[]`）で囲む	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP アドレスのブロック	IPv4 CIDR ブロックまたは IPv6 アドレス プレフィクス表記	`192.168.1.0/24` `2001:db8::/32`
特定の 1 つの IP アドレスまたはアドレス セットを除くすべて	拒否する IP アドレスの前に付ける「`!`」記号	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
特定の 1 つ以上の IP アドレスを除く、IP アドレスブロック内のすべて	アドレス ブロックの後に、否定されるアドレスのリストまたはブロック	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
ネットワーク変数で定義された IP アドレス	`$` で始まる大文字の変数名 プリプロセッサルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。	`$HOME_NET`
IP アドレス変数で定義されたアドレスを除く、すべての IP アドレス	大文字の変数名の前に `!$` を付ける	`!$HOME_NET`

以下の説明では、いくつかの IP アドレス入力方法に関する追加情報を提供します。

任意の IP アドレス

任意の IPv4 または IPv6 アドレスを示す「`any`」という単語を、ルールの送信元 IP アドレスまたは宛先 IP アドレスとして指定できます。

たとえば、次のルールでは [Source IPs] フィールドと [Destination IPs] フィールドで引数 **any** を使用して、任意の IPv4 または IPv6 の送信元または宛先アドレスを持つパケットを評価します。

```
alert tcp any any -> any any
```

また、任意の IPv6 アドレスを示すために `::` を指定することもできます。

複数の IP アドレス

次の例に示すように、カンマを使って複数の IP アドレスを区切り、オプションで、非拒否リストを大カッコで囲むことにより、個別の IP アドレスを列挙できます。

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4 アドレスと IPv6 アドレスのいずれかだけを列挙することも、任意に組み合わせて列挙することもできます（次の例を参照）。

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

以前のソフトウェア リリースでは IP アドレス リストを大カッコで囲む必要がありましたが、現在ではこれが必須でないことに注意してください。また、オプションで、リストを入力するときに各カンマの前または後にスペースを含めることができます。

（注） 否定リストは、大カッコで囲む必要があります。

また、IPv4 クラスレス ドメイン間ルーティング（CIDR）表記または IPv6 プレフィクス長を使用してアドレス ブロックを指定することもできます。次に例を示します。

- 192.168.1.0/24 は、サブネット マスク 255.255.255.0 の 192.168.1.0 ネットワーク内の IPv4 アドレス、つまり 192.168.1.0 ～ 192.168.1.255 を指定します。
- 2001:db8::/32 は、プレフィクス長 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレス、つまり 2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を指定します。

ヒント IP アドレスのブロックを指定する必要があるが、CIDR またはプレフィクス長表記を単独で使ってそれを表現できない場合は、1 つの IP アドレス リスト内でいくつかの CIDR ブロックとプレフィクス長を使用できます。

IP アドレスの否定

特定の IP アドレスを否定するために感嘆符（!）を使用できます。つまり、1 つ以上の特定の IP アドレスを除く、すべての IP アドレスに一致させることができます。たとえば、`!192.168.1.1` は 192.168.1.1 以外の任意の IP アドレスを、`!2001:db8:ca2e::fa4c` は 2001:db8:ca2e::fa4c 以外の任意の IP アドレスを指定します。

一連の IP アドレスを拒否するには、大かっこで囲んだ IP アドレスのリストの前に「!」記号を付けます。たとえば、`![192.168.1.1,192.168.1.5]` は 192.168.1.1 と 192.168.1.5 を除くすべての IP アドレスを定義します。

（注） IP アドレスのリストを否定するには、大カッコを使用する必要があります。

否定文字と一緒にIPアドレス リストを使用する場合は注意が必要です。たとえば、192.168.1.1と 192.168.1.5 を除くすべてのアドレスと一致させるために `[!192.168.1.1,!192.168.1.5]` を使用した場合、システムはこの構文を「192.168.1.1 以外のすべて、**または** 192.168.1.5 以外のすべて」と解釈します。

192.168.1.5 は 192.168.1.1 ではなく、192.168.1.1 は 192.168.1.5 ではないため、この両方の IP アドレスが `[!192.168.1.1,!192.168.1.5]` という IP アドレス値に一致します。つまり、実質的に「`any`」を使用するのと同じです。

代わりに `![192.168.1.1,192.168.1.5]` を使用してください。システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致します。

論理的に言って、`any` を除外（negation）と同時に使用できないことに注意してください。any を除外すると「アドレスなし」を意味することになります。

関連トピック

変数セット （1406 ページ）

侵入ルール ヘッダーの送信元および宛先ポート

侵入ルール エディタの [送信元ポート（Source Port）] フィールドと [宛先ポート（Destination Port）] フィールドで、送信元および宛先ポートを指定します。

侵入ルールのポート構文

Firepower System では、特定のタイプの構文を使用して、ルール ヘッダーで使用されるポート番号を定義できます。

（注） プロトコルが `ip` に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。

次の例に示すように、カンマでポートを区切ることによって、ポートのリストを指定できます。

```
80, 8080, 8138, 8600-9000, !8650-8675
```

オプションで、次の例に示すように、ポート リストを大カッコで囲むこともできます（以前のソフトウェア バージョンではこれが必須でしたが、現在は必須ではありません）。

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

なお、次の例に示すように、ポート リストの否定を大カッコで囲む**必要がある**ことに注意してください。

```
![20, 22, 23]
```

次の表に、使用可能な構文を要約します。

表 *104 :* 送信元/宛先ポート構文

指定する項目	指定内容	例
任意のポート	任意	任意
1 つの特定のポート	そのポート番号	80
ポートの範囲	範囲内の最初のポート番号と最後のポート番号をダッシュでつなぐ	80-443
1 つの特定のポートに等しい、またはより小さいすべてのポート	ポート番号の前にダッシュを付ける	-21
1 つの特定のポートに等しい、またはより大きいすべてのポート	ポート番号の後ろにダッシュを付ける	80-
1 つの特定のポートまたはポート範囲を除く、すべてのポート	否定する場合には、ポート、ポート リスト、ポート範囲の前に文字 ! を付けます。 否定が「ポートなし」を示す場合を除いて、すべてのポート宛先に論理上、否定を使用できる点にご注意ください。	!20
ポート変数で定義されるすべてのポート	$ の後ろに英大文字の変数名	$HTTP_PORTS
ポート変数で定義されるポートを除く、すべてのポート	大文字の変数名の前に !$ を付ける	!$HTTP_PORTS

侵入イベント詳細

標準のテキスト ルールを作成するときには、ルールでエクスプロイト試行を検出する対象となる脆弱性についてのコンテキスト情報を含めることができます。また、脆弱性データベースへの外部参照を含めたり、組織内でイベントに設定するプライオリティを定義したりすることもできます。アナリストがイベントを認識すると、そのプライオリティ、エクスプロイト、および既知の対策についての情報をすぐに入手できます。

メッセージ

ルールのトリガー時にメッセージとして表示される、意味のあるテキストを指定できます。メッセージを読むと、ルールで攻撃試行を検出する対象となった脆弱性の特性をすぐに理解できます。中カッコ（{}）を除く、印字可能な任意の標準ASCII文字を使用できます。システムは、メッセージ全体を囲んでいる引用符を取り除きます。

ヒント　ルール メッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

侵入ルール エディタでイベント メッセージを定義するには、[メッセージ（Message）] フィールドにイベント メッセージを入力します。

分類（Classification）

ルールごとに、イベントのパケット表示に含める攻撃分類を指定できます。次の表に、それぞれの分類の名前と番号を示します。

表 *105* : ルールの分類

番号（Number）	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生
[6]	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス拒否が試行された
8	successful-dos	サービス拒否が発生
9	attempted-user	ユーザ特権の獲得が試行された
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功
18	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された

番号（Number）	分類名	説明
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された
19	system-call-detect	システム コールが検出された
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス拒否攻撃の検出
25	non-standard-protocol	非標準プロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
36	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント
32	inappropriate-content	不適切な内容が検出された
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側 exploit 試行
38	file-format	既知の悪意のあるファイルまたはファイルベースのエクスプロイト

カスタム分類

定義したルールによって生成されるイベントのパケット表示記述の内容をもっとカスタマイズする必要がある場合には、カスタム分類を作成できます。

引数	説明
分類名	分類の名前。40 文字を超える文字を使用すると、ページが読みにくくなります。<>()\'"&$; 文字および空白文字はサポートされていません。
分類の説明	分類の説明。英数字とスペースを使用できます。<>()\'"&$; 文字はサポートされていません。
[プライオリティ（Priority）]	[高（High）]、[中（medium）]、または [低（low）]。

カスタム プライオリティ

デフォルトでは、ルールのイベント分類からルールのプライオリティが派生します。ただし、`priority` キーワードをルールに追加し、高、中、または低のプライオリティを選択することで、ルールの分類優先度を上書きすることができます。たとえば、Web アプリケーション攻撃を検出するルールに高プライオリティを割り当てるには、`priority` キーワードをルールに追加して、プライオリティとして [高（high）] を選択します。

カスタム参照

`reference` キーワードを使用すると、イベントに関する外部 Web サイトや追加情報への参照を追加できます。参照を追加すると、アナリストは参照情報をすぐに利用できるため、パケットがルールをトリガーとして使用した理由を特定するのに役立ちます。次の表に、既知のエクスプロイトや攻撃についてのデータを提供する外部システムをいくつか示します。

表 *106 :* 外部攻撃識別システム

システム ID（System ID）	説明	ID の例
`bugtraq`	[Bugtraq] ページ	`8550`
`cve`	共通脆弱性（CVE）ID	`2020-9607`
`mcafee`	[McAfee] ページ	`98574`
`url`	Web サイト参照	`www.example.com?exploit=14`
`msb`	Microsoft セキュリティ情報	`MS11-082`
`nessus`	[Nessus] ページ	`10039`

システム ID（System ID）	説明	ID の例
`secure-url`	セキュア Web サイト参照（https://...）	`intranet/exploits/exploit=14` 任意のセキュア Web サイトで `secure-url` を使用できることに注意してください。

次のように、参照値を入力して参照を指定します。

```
id_system,id
```

ここで、id_system はプレフィックスとして使用されるシステム、id は CVE ID 番号、Arachnids ID、または URL（`http://`なし）です。

たとえば、CVE-2020-9607 で文書化されている Adobe Acrobat および Reader の問題を指定するには、次の値を入力します。

```
cve,2020-9607
```

参照をルールに追加するときには、次の点に注意してください。

- カンマの後ろにスペースを入力しないでください。
- システム ID に大文字を使用しないでください。

関連トピック

カスタム分類の追加 （2058 ページ）
イベント優先順位の定義 （2059 ページ）
イベント参照の定義 （2059 ページ）

カスタム分類の追加

手順

ステップ 1 ルールの作成または編集時に、[分類（Classification）] ドロップダウンリスト（**[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）] > [ルールの作成（Create Rules）] > [分類の編集（Edit Classifications）]**）から [分類の編集（Edit Classifications）] を選択します。

代わりに [分類の表示（View Classifications）] が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 侵入イベント詳細 （2054 ページ） の説明に従い、[分類名（Classification Name）] と [分類の説明（Classification Description）] を入力します。

ステップ 3 [優先度（Priority）] ドロップダウン リストから分類の優先度を選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [完了（Done）] をクリックします。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2061 ページ）または 既存のルールの変更 （2062 ページ） を参照してください。

関連トピック

カスタム ルールの作成 （2060 ページ）

イベント優先順位の定義

手順

ステップ 1 ルールの作成または編集時に、[検出オプション（Detection Options）] ドロップダウン リストから [優先順位（priority）] を選択します。

ステップ 2 [Add Option] をクリックします。

ステップ 3 [優先順位（priority）] ドロップダウン リストから値を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2061 ページ）または 既存のルールの変更 （2062 ページ） を参照してください。

関連トピック

カスタム ルールの作成 （2060 ページ）

イベント参照の定義

手順

ステップ 1 ルールの作成または編集時に、[検出オプション（Detection Options）] ドロップダウン リストから [参照（reference）] を選択します。

ステップ 2 [Add Option] をクリックします。

ステップ 3 侵入イベント詳細 （2054 ページ）の説明に従って、[参照（reference）] フィールドに値を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2061 ページ）または 既存のルールの変更 （2062 ページ） を参照してください。

関連トピック

カスタム ルールの作成 （2060 ページ）

カスタム ルールの作成

カスタム侵入ルールは以下の方法で作成できます。

- 独自の標準テキスト ルールを作成する
- 既存の標準テキスト ルールを新規ルールとして保存する
- システムが提供する共有オブジェクト ルールを新規ルールとして保存する
- ローカル ルール ファイルをインポートする

作成方法に関わらず、システムはカスタム ルールをローカル ルールに分類して保存します。

カスタム侵入ルールを作成すると、システムは一意のルール番号（番号の形式は`GID:SID:Rev`）を割り当てます。この番号には次の要素が含まれます。

GID

ジェネレータ ID。すべての標準テキスト ルールでは、この値は 1（グローバル ドメインまたはレガシー GID）または 1000 ～ 2000（子孫ドメイン）です。共有オブジェクト ルールを新規ルールとして保存する場合、値は 1 です。

SID

[Snort ID]。ルールがシステム ルールのローカル ルールであるかどうかを示します。新しいルールを作成すると、システムは次に使用可能なローカル ルール SID 番号を割り当てます。

ローカル ルールの SID 番号は 1000000 から始まり、新しいローカル ルールにつき番号が 1 ずつ増えます。

Rev

改訂番号。新しいルールのリビジョン番号は 1 です。カスタム ルールを変更するたびに、リビジョン番号が 1 ずつ増えます。

カスタム標準テキスト ルールでは、ルール ヘッダー設定、ルール キーワード、およびルール引数を設定できます。特定のプロトコルを使用する、特定の IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルール ヘッダーを設定できます。

システムが提供する標準テキスト ルールまたは共有オブジェクト ルールのカスタム ルールで変更できるルール ヘッダー情報は、送信元と宛先ポートと IP アドレスなどの情報に限られます。ルール キーワードやルール引数は変更できません。

共有オブジェクトルールのヘッダー情報を変更して変更内容を保存すると、ルールの新しいインスタンスが作成され、ジェネレータ ID（GID） 1（グローバル ドメイン）または 1000 ～ 2000（子孫ドメイン）、およびカスタム ルールとして次に使用可能な SID が割り当てられます。システムは、共有オブジェクト ルールの新しいインスタンスを予約済み `soid` キーワードにリンクします。これにより、新しく作成したルールが Talos インテリジェンスグループ 作成のルールにマップされます。ユーザーが作成した共有オブジェクト ルールのインスタンスは削除できますが、Talos が作成した共有オブジェクト ルールは削除できません。

新規ルールの作成

手順

ステップ 1 **[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**を選択します。

ステップ 2 [Create Rule] をクリックします。

ステップ 3 [メッセージ（Message）] フィールドに値を入力します。

ステップ 4 次の各ドロップダウン リストから値を選択します。

- **[分類（Classification）]**
- **操作**
- **[Protocol]**
- **方向（Direction）**

ステップ 5 次のフィールドに値を入力します。

- **[送信元 IP（Source IPs）]**
- **[宛先 IP（Destination IPs）]**
- **送信元ポート（Source Port）**
- **宛先ポート（Destination Port）**

これらのフィールドに値を指定しない場合、システムは値 [すべて（any）] を使用します。

ステップ 6 [検出オプション（Detection Options）] ドロップダウン リストから値を選択します。

ステップ 7 [Add Option] をクリックします。

ステップ 8 追加したキーワードの引数を入力します。

ステップ 9 必要に応じて、手順 6 ～ 8 を繰り返します。

ステップ 10 複数のキーワードを追加した場合、以下を実行できます。

- キーワードの並べ替え：移動するキーワードの横にある上矢印または下矢印をクリックします。
- キーワードの削除：そのキーワードの横にある [X] をクリックします。

ステップ 11 [新規として保存（Save As New）] をクリックします。

次のタスク

- 該当する侵入ポリシー内の新規または変更されたルールを有効にします。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

既存のルールの変更

システム提供のルールと先祖ドメインに属しているルールは、新しいカスタム ルールとしてローカル ルール カテゴリに保存してから変更できます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

  編集するポリシーの横にある [Snort2バージョン（Snort 2 Version）] をクリックし、[ルール（Rules）] をクリックします。

- **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]**を選択します。

ステップ 2 変更するルールを見つけます。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを検索します。ルールの検索 （2066 ページ）を参照してください。
- ルールが属しているグループにフィルタを適用します。フィルタリング ルール （2071 ページ）を参照してください。

ステップ 3 ルールの横にある [編集（Edit）]（✎） をクリックします。検索結果の場合はルールメッセージをクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ルール タイプに応じて、ルールを変更します。

（注）
共有オブジェクト ルールのプロトコルは変更しないでください。これを変更すると、ルールの効果がなくなる可能性があります。

ステップ 5 次の選択肢があります。

- カスタム ルールを編集していて、そのルールの現在のバージョンを上書きする場合は、[保存（Save）] をクリックします。

- システム提供のルールまたは先祖ドメインに属しているルールを編集している場合や、カスタム ルールを編集しているときに変更を新しいルールとして保存する場合は、[新規に保存（Save As New）] をクリックします。

次のタスク

- システム提供のルールの代わりにローカルで変更したルールを使用するには、侵入ルールの状態（2031 ページ）の手順に従ってシステム提供のルールを非アクティブ化してから、ローカル ルールをアクティブ化します。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

ルールの検索 （2066 ページ）
侵入ルール エディタ ページでのルールのフィルタリング （2068 ページ）

ルール ドキュメンテーションの表示

[ルールの編集（Rule Edit）] ページから、Talos インテリジェンスグループ によって提供されるルール ドキュメンテーションを表示できます。 表示中に、**[ルールドキュメンテーション（Rule Documentation）]** およびその他の外部参照をクリックして、Talos によって提供される追加情報を表示できます。[コンテキスト エクスプローラ（Context Explorer）] をクリックして、ルールによって生成されたイベントのコンテキスト情報を表示することもできます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

  編集するポリシーの横にある [Snort2バージョン（Snort 2 Version）] をクリックし、[ルール（Rules）] をクリックします。

- **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]**を選択します。

ステップ 2 表示するルールを探します。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを検索します。ルールの検索 （2066 ページ）を参照してください。
- ルールが属しているグループにフィルタを適用します。フィルタリング ルール （2071 ページ）を参照してください。

ステップ 3 ルールの横にある [編集（Edit）]（✎） をクリックします。検索結果の場合はルールメッセージをクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [ドキュメントの表示（View Documentation）] をクリックします。

ステップ 5 状況に応じて、次のいずれかのリンクをクリックします。

- [ルール ドキュメンテーション（Rule Documentation）]：ルール固有の詳細を表示します。
- [その他の外部参照（Other external references）]：利用可能な外部参照に関する情報については、キーワードフィルタリング（2069ページ）および侵入イベント詳細（2054ページ）の「カスタム リファレンス」を参照してください。
- [コンテキストエクスプローラ（Context Explorer）]：コンテキスト エクスプローラでのルールのコンテキストデータの表示に関する情報については、Cisco Secure Firewall Management Center アドミニストレーション ガイド の侵入情報セクションを参照してください。

ヒント
外部リンクを選択するとドキュメンテーションのポップアップ ウィンドウが閉じます。ルールを変更せずにルール編集ページを終了するには、任意のメニュー パスを選択します。

侵入ルールへのコメントの追加

任意の侵入ルールにコメントを追加できます。コメントにより、環境や条件の説明と、ルールやルールが検出する悪意あるプログラム、スクリプト（エクスプロイト）やポリシー違反の詳細を示すことができます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

  編集するポリシーの横にある [Snort2バージョン（Snort 2 Version）] をクリックし、[ルール（Rules）] をクリックします。

- **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]**を選択します。

ステップ 2 注釈を付けるルールを探します。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを検索します。ルールの検索（2066 ページ）を参照してください。
- ルールが属するグループをフィルタします。フィルタリング ルール（2071 ページ）を参照してください。

ステップ 3 ルールの横にある [編集（Edit）]（） をクリックします。検索結果の場合はルールメッセージをクリックします。

代わりに [表示（View）]（） がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 4 [Rule Comment] をクリックします。

ステップ 5 テキスト ボックスにコメントを入力します。

ステップ 6 [コメントを追加（Add a Comment）] をクリックします。

ヒント
また、侵入イベントのパケット ビューで、ルール コメントを追加して表示することもできます。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2061 ページ）または 既存のルールの変更 （2062 ページ） を参照してください。

関連トピック

ルールの検索 （2066 ページ）

カスタム ルールの削除

侵入ポリシーで現在有効になっていないカスタム ルールを削除することができます。システムにより提供されている標準テキスト ルールおよび共有オブジェクト ルールは削除できません。

削除されたルールは削除済みカテゴリに保存されます。削除済みのルールを、新しいルールの基準として使用することができます。侵入ポリシーの [Rules] ページには削除済みカテゴリが表示されないため、削除したカスタム ルールを有効にすることはできません。

ヒント カスタム ルールには、変更されたヘッダー情報で保存する共有オブジェクト ルールが含まれます。また、これらはローカル ルール カテゴリに保存され、1（グローバル ドメインまたはレガシー GID）または 1000 ～ 2000（子孫ドメイン）の GID を使用してリストされます。変更した共有オブジェクト ルールは削除できますが、元の共有オブジェクト ルールは削除できません。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

  編集するポリシーの横にある [Snort2バージョン（Snort 2 Version）] をクリックし、[ルール（Rules）] をクリックします。

- **[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**を選択します。

ステップ 2 次の 2 つの選択肢があります。

- すべてのローカル ルールを削除します：[ローカル ルールの削除（Delete Local Rules）] をクリックし、[OK] をクリックします。
- 1 つのルールを削除します：[ルールのグループ化基準（Group Rules By）] ドロップダウンから [ローカルルール（Local Rules）] を選択し、削除するルールの隣にある [削除（Delete）]（） をクリックし、[OK] をクリックして削除を確認します。

関連トピック

侵入ルールの状態 （2031 ページ）

ルールの検索

システムには、数千もの標準テキストルールが用意されています。また、Talos インテリジェンスグループは新しい脆弱性およびエクスプロイトが見つかったときのルールを追加を継続します。特定のルールを簡単に検索して、そのルールをアクティブ化、非アクティブ化、または編集することができます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

  編集するポリシーの横にある [Snort2バージョン（Snort 2 Version）] をクリックし、[ルール（Rules）] をクリックします。

- **[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**を選択します。

ステップ 2 ツールバーで [検索（Search）] をクリックします。

ステップ 3 検索条件を追加します。

ステップ 4 [検索（Search）] をクリックします。

次のタスク

- 見つかったルール（システムルールの場合はルールのコピー）を表示または編集する場合は、ハイパーリンクが付いたルールメッセージをクリックします。詳細については、新規ルールの作成（2061ページ）または既存のルールの変更（2062ページ）を参照してください。

侵入ルールの検索条件

次の表には、利用可能な検索オプションについて説明しています。

表 *107*：ルール検索規則

オプション	説明
署名 ID	[Snort ID]（SID）に基づいて 1 つのルールを検索するには、SID 番号を入力します。複数のルールを検索するには、SID番号リストをカンマで区切って入力します。このフィールドは、80 文字以内です。
ジェネレータ ID	標準テキストルールを検索するには、[1]を選択します。共有オブジェクトのルールを検索するには、[3] を選択します。
メッセージ	特定のメッセージを含むルールを検索するには、ルール メッセージの 1 つの単語を [Message] フィールドに入力します。たとえば、DNS exploitを検索するには「`DNS`」と入力し、バッファオーバーフロー exploit を検索するには「`overflow`」と入力します。
Protocol	特定のプロトコルのトラフィックを評価するルールを検索には、プロトコルを選択します。プロトコルを選択しない場合、検索結果にはすべてのプロトコルのルールが含まれます。
送信元ポート	指定したポートから送信されたパケットを検査するルールを検索するには、送信元ポート番号またはポート関連変数を入力します。
宛先ポート	特定のポートに向けて送られるパケットを検査するルールを検索するには、宛先ポート番号またはポート関連変数を入力します。
送信元 IP	指定した IP アドレスから送信されたパケットを検査するルールを検索するには、送信元 IP アドレスまたは IP アドレス関連の変数を入力します。
宛先 IP	指定した IP アドレスに向けて送られるパケットを検査するルールを検索するには、宛先 IP アドレスまたは IP アドレス関連の変数を入力します。
キーワード	特定のキーワードを検索するには、キーワード検索オプションを使用できます。キーワードを選択して、検索するキーワード値を入力します。特定値以外の任意の値に一致させるには、キーワードの前に疑問符（`!`）を入力します。
Category	特定のカテゴリ内のルールを検索するには、[Category] リストからカテゴリを選択します。
Classification	特定の分類が設定されたルールを検索するには、[Classification] リストから分類名を選択します。

オプション	説明
Rule State	特定のポリシー内のルールや特定のルール状態を検索するには、最初のルール状態リストからポリシーを選択し、第2のリストから状態を選択して、イベントの作成、イベントのドロップ、作成、無効に設定されたルールを検索します。

侵入ルール エディタ ページでのルールのフィルタリング

侵入ルール エディタ ページ上でルールをフィルタリングして、ルールのサブセットを表示することができます。たとえば、あるルールまたはその状態を変更したいが、数千ものルールの中からそれを見つけるのが困難な場合に、この機能が役立つことがあります。

フィルタを入力すると、1 つ以上の一致するルールを含むフォルダがページに表示され、一致するルールがない場合はメッセージが表示されます。

フィルタリング ガイドライン

フィルタには、特殊なキーワードとその引数、文字列、引用符で囲んだリテラル文字列、さらに複数のフィルタ条件を区切るスペースを含めることができます。ただし、正規表現、ワイルドカード文字、および否定文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。`gid`キーワードと`sid`キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

フィルタ処理前の元のページで 1 つのフォルダを展開すると、その後のフィルタ処理でそのフォルダ内の一致が返されるときにフォルダが展開したままになります。探しているルールが多数のルールを含むフォルダ内に存在する場合には、これが役立つことがあります。

1 つのフィルタを後続の別のフィルタで制約することはできません。入力されたフィルタは、ルールデータベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、侵入ルール エディタ ページでは、リストがフィルタ処理されているかどうかに関わらず、リスト内のルールを編集できます。また、ページのコンテキスト メニューの任意のオプションを使用することもできます。

ヒント すべてのサブグループ内のルールの合計数が多い場合は、フィルタリングに長い時間がかかることがあります。これは、個別のルールの数がかなり少なくても、1 つのルールが複数のカテゴリに出現することがあるためです。

キーワード フィルタリング

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

```
keyword:argument
```

ここで、keyword は次の表のいずれかのキーワード、argument はキーワードに関連する特定のフィールドで検索される単一の、大文字/小文字を区別しない英数字文字列です。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` によって SID 3080 のみが返されます。

ヒント 部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

次の表に、ルールのフィルタ処理に使用できる特定のフィルタリング キーワードと引数を示します。

表 *108*：ルール フィルタ キーワード

キーワード	説明	例
`arachnids`	ルール参照内の Arachnids ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`arachnids:181`
`bugtraq`	ルール参照内の Bugtraq ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`bugtraq:2120`
`cve`	ルール参照内の CVE 番号全体またはその一部分に基づいて 1 つ以上のルールを返します。	`cve:2003-0109`
`gid`	引数 `1` は標準のテキスト ルールを返します。引数 `3` は共有オブジェクト ルールを返します。	`gid:3`
`mcafee`	ルール参照内の McAfee ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`mcafee:10566`
`msg`	ルールの [メッセージ（Message）] フィールド（イベント メッセージとも呼ばれる）の全体またはその一部分に基づいて 1 つ以上のルールを返します。	`msg:chat`
`nessus`	ルール参照内の Nessus ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`nessus:10737`
`ref`	ルール参照内またはルールの [メッセージ（Message）] フィールド内の単一の英数字文字列の全体または一部分に基づいて、1 つ以上のルールを返します。	`ref:MS03-039`

キーワード	説明	例
sid	正確な [Snort ID] を持つルールを返します。	sid:235
url	ルール参照内の URL 全体またはその一部分に基づいて 1 つ以上のルールを返します。	url:faqs.org

関連トピック

イベント参照の定義 （2059 ページ）
侵入イベント詳細 （2054 ページ）

文字列フィルタリング

各ルールフィルタに1つ以上の英数字文字列を含めることができます。文字列により、ルールの [メッセージ（Message）] フィールド、[Snort ID] ID（SID）、およびジェネレータ ID が検索されます。たとえば、文字列 `123` を指定すると、ルール メッセージ内の文字列「`Lotus123`」や「`123mania`」などが返され、さらに、SID 6123、SID 12375 なども返されます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はすべて、「`admin`」、「`CFADMIN`」、「`Administrator`」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの2つの文字列 `overflow` と `attempt` で構成されるフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

関連トピック

侵入イベント詳細 （2054 ページ）

キーワードと文字列の組み合わせによるフィルタリング

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタリングの結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

フィルタリング ルール

[侵入ルール（Intrusion Rules）]ページで、ルールをサブセットにフィルタ処理すると、より簡単に特定のルールを見つけることができます。その後で、いずれかのページ機能を使用できます。これには、コンテキスト メニューで使用可能な機能の選択も含まれます。

編集する特定のルールを見つけるのに、規則のフィルタリングはとても役立ちます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

  編集するポリシーの横にある [Snort2バージョン（Snort 2 Version）] をクリックし、[ルール（Rules）] をクリックします。

- **[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**を選択します。

ステップ 2 フィルタリングする前に、次の選択を行います。

- 該当のルール グループを展開します。複数のルール グループにも、展開できるサブグループがあります。

  また、ルールがどのグループに含まれているか予想できる場合は、フィルタ処理前の元のページでそのグループを展開しておくと便利な場合があります。その後のフィルタ処理でそのフォルダ内の一致した結果が返されるとき、およびフィルタ [クリア（Clear）]（✕）をクリックしてフィルタ処理前のページに戻ったときに、グループが展開されたままになります。

- [グループ ルール（Group Rules By）] ドロップダウンリストから別のグループ メソッドを選択します。

ステップ 3 [グループルール（Group Rules By）] リストで [フィルタ（filter）]（🔍） の横にあるテキストボックスにフィルタ制約を入力します。

ステップ 4 Enter を押します。

（注）

フィルタ [クリア（Clear）]（✕） をクリックして、現在のフィルタ処理されたリストをクリアします。

侵入ルールのキーワードと引数

ルール言語では、キーワードを組み合わせることによってルールの動作を指定できます。キーワードとそれに関連する値（引数と呼ばれる）は、ルールエンジンによって検査されるパケットおよびパケット関連値をシステムがどのように評価するかを決定します。Firepower システムでは現在、コンテンツ マッチング、プロトコル固有のパターンマッチング、状態固有のマッチングなどのインスペクション機能を実行するためのキーワードがサポートされています。キーワードあたり最大100個の引数を定義し、互換性のある任意の数のキーワードを組み合わせて非常に具体的なルールを作成できます。これにより、誤検出や検出漏れの可能性が減少し、受け取った侵入情報に集中的に取り組むことができます。

また、パッシブ展開でadaptive profile updatesを使用すると、ルール メタデータとホスト情報に基づいて特定のパケットに対するアクティブ ルール処理を動的に調整できます。

ここに記載されているキーワードは、ルールエディタの検出オプションとして表示されます。

関連トピック

アダプティブ プロファイルについて （2933 ページ）

content キーワードと protected_content キーワード

`content` キーワードまたは `protected_content` キーワードを使用すると、パケット内から検出するコンテンツを指定できます。

ほとんどの場合、`content` または `protected_content` キーワードの後ろに修飾子を付けて、コンテンツを検索すべき場所、検索で大文字/小文字を区別するかどうか、およびその他のオプションを指定する必要があります。

ルールでイベントがトリガーとして使用されるためには、すべてのコンテンツマッチングが真でなければならないことに注意してください。つまり、各コンテンツマッチングは相互にAND関係にあります。

また、インライン展開では、有害なコンテンツを照合した後でそれを同じ長さの独自のテキスト文字列に置き換えるルールをセットアップできることにも注意してください。

content

`content` キーワードを使用すると、ルールエンジンはパケットペイロードまたはストリームでその文字列を検索します。たとえば、いずれかの `content` キーワードの値として `/bin/sh` と入力した場合、ルール エンジンはパケット ペイロード内で文字列 `/bin/sh` を検索します。

ASCII 文字列、16 進コンテンツ（バイナリ バイト コード）、またはその両方の組み合わせを使用してコンテンツを照合できます。キーワード値の中で 16 進コンテンツをパイプ文字（|）で囲みます。たとえば、`|90C8 C0FF FFFF|/bin/sh` のように 16 進コンテンツと ASCII コンテンツを混在させることができます。

1つのルール内で複数のコンテンツマッチングを指定できます。これを行うには、`content` キーワードの追加のインスタンスを使用します。コンテンツマッチングごとに、ルールをトリガー

として使用させるにはパケットペイロードまたはストリームでコンテンツ一致が見つからなければならないことを指定できます。

⚠

注意 **Not** オプションが選択された 1 つの content キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。

protected_content

protected_content キーワードを使用すると、ルール引数を設定する前に、検索コンテンツ文字列をエンコードすることができます。キーワードを設定する前に、ルール作成者がハッシュ関数（SHA-512、SHA-256、または MD5）を使用して文字列をエンコードします。

content キーワードの代わりに protected_content キーワードを使用した場合でも、ルール エンジンがパケットペイロードまたはストリームの中で文字列を検索する方法に違いはなく、ほとんどのキーワードオプションが想定どおりに機能します。次の表は、protected_content キーワードオプションと content キーワードオプションの間の例外的な相違点を要約しています。

表 *109 : protected_content* オプションの例外

オプション	説明
Hash Type	protected_content ルール キーワードの新しいオプション。
[大文字小文字の区別なし（Case Insensitive）]	サポート対象外
Within	サポート対象外
Depth	サポート対象外
Length	protected_content ルール キーワードの新しいオプション。
高速パターンマッチ機能を使用（Use Fast Pattern Matcher）	サポート対象外
Fast Pattern Matcher Only	サポート対象外
Fast Pattern Matcher Offset and Length	未サポート

Cisco では、protected_content キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルール内の protected_content キーワードの前に content キーワードを配置します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの Use Fast Pattern Matcher 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

注意 **Not** オプションが選択された 1 つの `protected_content` キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。

関連トピック

カスタム ルールの作成 （2060 ページ）
基本コンテンツおよび protected_content キーワードの引数 （2074 ページ）
replace キーワード （2086 ページ）

基本コンテンツおよび protected_content キーワードの引数

`content` または `protected_content` キーワードを変更するパラメータを使用すると、コンテンツ検索の位置や大文字/小文字の区別を制約できます。`content` または `protected_content` キーワードを変更するオプションを設定して、検索対象となるコンテンツを指定します。

[大文字小文字の区別なし（Case Insensitive）]

（注） このオプションは `protected_content` キーワードの設定では**サポートされません**。

ASCII 文字列でコンテンツ一致を検索するときに大文字/小文字の区別を無視するようルールエンジンに指示できます。検索で大文字と小文字を区別しないようにするには、コンテンツ検索の指定時に [大文字小文字の区別なし（Case Insensitive）] をオンにします。

ハッシュ タイプ（Hash Type）

（注） このオプションは `protected_content` キーワードで**のみ**設定できます。

[ハッシュ タイプ（Hash Type）] ドロップダウンを使用して、検索文字列のエンコードに使用されたハッシュ関数を特定します。`protected_content` 検索文字列のハッシュ方式として、SHA-512、SHA-256、および MD5 がサポートされています。選択したハッシュ タイプとハッシュされたコンテンツの長さが一致しない場合、システムはルールを保存**しません**。

自動的に Cisco 設定のデフォルト値が選択されます。[デフォルト（Default）] が選択される場合、ルールに特定のハッシュ関数は含まれず、SHA-512 がハッシュ関数であると見なされます。

Raw Data

[raw データ（Raw Data）] オプションを使用すると、ルール エンジンは、正規化されたペイロードデータ（ネットワーク分析ポリシーによってデコードされたデータ）を分析する前にオリジナルのパケット ペイロードを分析します。引数値は使用されません。正規化の前に、ペイ

ロード内の Telnet ネゴシエーション オプションを検査するために Telnet トラフィックを分析する場合に、このキーワードを使用できます。

同じ `content` または `protected_content` キーワードで、**Raw Data** オプションを HTTP コンテンツ オプションと一緒に使用することはできません。

ヒント HTTP トラフィックで raw データを検査するかどうか、また、どの程度の量の raw データを検査するかを決定するため、HTTP 検査プリプロセッサの [クライアント フローの深さ（Client Flow Depth）] オプションと [サーバー フローの深さ（Server Flow Depth）] オプションを設定することができます。

注

指定したコンテンツと一致しないコンテンツを検索するには、[一致しない（Not）] オプションを選択します。[一致しない（Not）] オプションが選択された `content` または `protected_content` キーワードを含むルールを作成する場合には、そのルール内に、[一致しない（Not）] オプションが選択されていない別の `content` または `protected_content` キーワードを 1 つ以上含める必要があります。

注意 `content` または `protected_content` キーワードに対して **Not** オプションを選択した場合は、そのキーワードだけを含むルールを作成しないでください。侵入ポリシーの効果がなくなる可能性があります。

たとえば、SMTP ルール 1:2541: 9 に 3 つの `content` キーワードが含まれており、そのうちの 1 つで [一致しない（Not）] オプションが選択されているとします。[一致しない（Not）] オプションが選択されているキーワード以外のすべての `content` キーワードを削除すると、このルールに基づくカスタム ルールが無効になります。このようなルールを侵入ポリシーに追加すると、そのポリシーの効果がなくなる可能性があります。

ヒント 同じ `content` キーワードで、[Not] チェック ボックスと [Use Fast Pattern Matcher] チェック ボックスを同時に選択することはできません。

コンテンツ（content）および保護コンテンツ（protected_content）キーワード検索位置

検索位置オプションを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

許可された組み合わせ：content 検索位置の引数

次のように、2 つの `content` 位置ペアのいずれかを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして検索する場合は、**Offset** と **Depth** を一緒に使用します。
- 現在の検索位置を基準にして検索する場合は、**Distance** と **Within** を一緒に使用します。

ペアに含まれるオプションのどちらか 1 つだけを指定した場合は、そのペアのもう 1 つのオプションのデフォルトが想定されます。

Offset および **Depth** オプションと、**Distance** および **Within** オプションを混合することはできません。たとえば、**Offset** と **Within** をペアにすることはできません。1 つのルール内で任意の数の位置オプションを使用できます。

位置が指定されない場合は、**Offset** と **Depth** のデフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の `byte_extract` 変数を使用して位置オプションの値を指定することもできます。

ヒント 1 つのルール内で任意の数の位置オプションを使用できます。

関連トピック

byte_extract キーワード （2092 ページ）

許可された組み合わせ：protected_content 検索位置の引数

次のように、必須の **Length** `protected_content` 位置オプションを **Offset** または **Distance** 位置オプションと組み合わせて使用すると、指定されたコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして、保護された文字列を検索するには、**Length** と **Offset** を一緒に使用します。
- 現在の検索位置を基準にして、保護された文字列を検索するには、**Length** と **Distance** を一緒に使用します。

ヒント 1 つのキーワード設定内で [オフセット（Offset）] オプションと [距離（Distance）] オプションを併用することはできませんが、1 つのルール内では任意の数の位置オプションを使用できます。

位置が指定されない場合は、デフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の `byte_extract` 変数を使用して位置オプションの値を指定することもできます。

関連トピック

byte_extract キーワード （2092 ページ）

content および protected_content の検索位置の引数

奥行

（注） このオプションは、content キーワードを設定する場合に**のみ**サポートされます。

オフセット値の先頭からの（またはオフセットが設定されていない場合はパケットペイロード先頭からの）コンテンツ検索の最大の深さをバイト単位で指定します。

たとえば、ルールのコンテンツ値が cgi-bin/phf、offset 値が 3、depth 値が 22 である場合、ルール ヘッダーで指定されたパラメータを満たすパケット内で、cgi-bin/phf 文字列との一致の検索がバイト位置 3 から始まり、22 バイト処理した後（バイト位置 25 で）停止します。

指定したコンテンツの長さ以上の、最大65535バイトまでの値を指定する必要があります。値 0 は指定できません。

デフォルトの深さは、「パケットの末尾まで検索」です。

距離（Distance）

以前に見つかったコンテンツ一致から数えて、指定されたバイト数の後に出現する後続のコンテンツ一致を見つけるようルール エンジンに指示します。

Distance（距離）カウンタはバイト 0 から始まるため、最後に見つかったコンテンツ一致から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 4 を指定した場合、5 番目のバイトから検索が始まります。

-65535 ～ 65535 バイトを値として指定できます。負の Distance 値を指定した場合は、検索を開始するバイト位置がパケットの先頭から外れる可能性があります。実際にはパケットの第 1 バイトから検索が開始されますが、計算ではパケットの外側のバイトも考慮されます。たとえば、パケット内の現在の位置が第 5 バイトで、次のコンテンツ ルール オプションで Distance 値 -10 および Within 値 20 が指定された場合、検索はペイロードの先頭から開始され、[Within] オプションが 15 に調整されます。

デフォルトの距離は 0 で、これは最後のコンテンツ一致の後のパケット内の現在位置という意味です。

長さ（Length）

（注） このオプションは protected_content キーワードを設定する場合に**のみ**サポートされます。

Length protected_content キーワードオプションは、ハッシュされていない検索文字列の長さをバイト単位で示します。

たとえば、コンテンツ Sample1 を使ってセキュア ハッシュを生成した場合には、**Length** 値として 7 を使用します。このフィールドに値を入力することは**必須**です。

Offset

パケット ペイロードの先頭を基準とする、コンテンツの検索を開始するパケット ペイロード内の位置をバイト単位で指定します。65535 ～ 65535 バイトを値として指定できます。

オフセット カウンタはバイト 0 から始まるため、パケット ペイロードの先頭から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 7 を指定した場合は、8 番目のバイトから検索が始まります。

デフォルトのオフセットは 0 で、これはパケットの先頭を意味します。

Within

（注） このオプションは、`content` キーワードを設定する場合に**のみ**サポートされます。

[次の範囲内（Within）] オプションを使用すると、ルールをトリガーとして使用させるには、最後に見つかったコンテンツ一致の末尾以降、指定のバイト数以内に次のコンテンツ一致が発生する必要があることを指示できます。たとえば **Within** 値として `8` を指定した場合、次のコンテンツ一致がパケット ペイロードの次の 8 バイト以内に発生する必要があります。発生しない場合は、ルールをトリガーとして使用する基準が満たされません。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定できます。

[次の範囲内（Within）] のデフォルトは「パケットの末尾まで検索」です。

概要：HTTP content および protected_content キーワードの引数

HTTP `content` または `protected_content` キーワード オプションを使用すると、HTTP Inspect プリプロセッサによってデコードされた HTTP メッセージ内の一致コンテンツを検索する位置を指定できます。

次の 2 つのオプションは、HTTP 応答内のステータス フィールドを検索します。

- **HTTP ステータス コード（HTTP Status Code）**
- **HTTP ステータス メッセージ（HTTP Status Message）**

ルール エンジンは未加工の正規化されていないステータス フィールドを検索しますが、ここでは、他の Raw HTTP フィールドと正規化された HTTP フィールドを併用する際に考慮すべき制限についての説明を簡略化するために、これらのオプションが別個に列挙されていることに注意してください。

次の 5 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で正規化フィールドを検索します。

- **HTTP URI**
- **HTTP メソッド（HTTP Method）**
- **HTTP ヘッダー（HTTP Header）**
- **HTTP Cookie**

- **HTTP クライアント ボディ（HTTP Client Body）**

次の 3 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で未加工の（正規化されていない）非ステータス フィールドを検索します。

- **HTTP Raw URI**
- **HTTP Raw ヘッダー（HTTP Raw Header）**
- **HTTP Raw Cookie**

HTTP `content` オプションを選択する場合は、次のガイドラインに従ってください。

- HTTP `content` オプションは TCP トラフィックにのみ適用されます。
- パフォーマンスへの悪影響を避けるために、指定したコンテンツが出現する可能性のあるメッセージ部分だけを選択してください。

  たとえば、ショッピング カート メッセージの場合のように大きな cookie がトラフィックに含まれている可能性がある場合は、HTTP cookie ではなく HTTP ヘッダーの中で指定のコンテンツを検索することができます。

- HTTP Inspect プリプロセッサの正規化機能を活用し、パフォーマンスを向上させるには、作成するすべての HTTP 関連ルールの中に少なくとも 1 つの `content` または `protected_content` キーワードを含め、それに対して **HTTP URI**、**HTTP Method**、**HTTP Header**、または **HTTP Client Body** オプションを選択します。

- HTTP `content` または `protected_content` キーワード オプションと組み合わせて `replace` キーワードを使用することはできません。

単一の正規化された HTTP オプションまたはステータス フィールドを指定できます。または、複数の正規化 HTTP オプションとステータス フィールドを任意に組み合わせて、コンテンツ領域をマッチング対象にすることもできます。ただし、HTTP フィールド オプションを使用する場合には次の制限事項に注意してください。

- 同じ `content` または `protected_content` キーワード内で、**Raw Data** オプションと HTTP オプションを一緒に使用することはできません。

- 未加工 HTTP フィールド オプション（**HTTP Raw URI**、**HTTP Raw Header**、または **HTTP Raw Cookie**）と、それぞれに対応する正規化されたオプション（**HTTP URI**、**HTTP Header**、または **HTTP Cookie**）を同じ `content` または `protected_content` キーワード内で一緒に使用することはできません。

- **Use Fast Pattern Matcher** を、次の 1 つ以上の HTTP フィールド オプションと組み合わせて選択することはできません。

  [HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、[HTTP Raw Cookie]、[HTTP Cookie]、[HTTP メソッド（HTTP Method）]、[HTTP ステータス メッセージ（HTTP Status Message）]、[HTTP ステータス コード（HTTP Status Code）]

ただし、次のいずれかの正規化フィールドを検索するために高速パターンマッチ機能を使用する `content` または `protected_content` キーワードでは、上記のオプションを含めることができます。

HTTP URI、**HTTP Header**、または **HTTP Client Body**

たとえば、**HTTP Cookie**、**HTTP Header**、および **Use Fast Pattern Matcher** を選択した場合、ルールエンジンは HTTP cookie と HTTP 見出しの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP 見出しにのみ適用されます。

- 制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、侵入ルールエディタにルールを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。

関連トピック

content キーワードの高速パターン マッチ機能の引数 （2083 ページ）

HTTP コンテンツと protected_content キーワードの引数

HTTP URI

正規化された要求URIフィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI（U）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

（注） パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理されたHTTP要求パケットをルールエンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP Raw URI

正規化された要求URIフィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI（U）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

（注） パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理されたHTTP要求パケットをルールエンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP メソッド

（URI で識別されるリソースに対して行う GET や POST などのアクションを特定する）要求メソッド フィールド内のコンテンツ一致を検索するには、このオプションを選択します。

HTTP Header

HTTP 要求内の（cookie を除く）正規化されたヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと `pcre` キーワードの HTTP 見出し（H）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

HTTP Raw Header

HTTP 要求内の（cookie を除く）raw ヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと `pcre` キーワードの HTTP 未加工見出し（D）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

HTTP Cookie

正規化された HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP cookie（C）オプションを一緒に使用して、同じコンテンツを検索することはできません。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP Raw Cookie

未加工 HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP 未加工 cookie（K）オプションを一緒に使用して同じコンテンツを検索することはできません。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP Client Body

HTTP クライアント要求内のメッセージ本文でコンテンツ一致を検索するには、このオプションを選択します。

このオプションが機能するためには、HTTP Inspect プリプロセッサの [HTTP クライアント ボディの抽出の深さ（HTTP Client Body Extraction Depth）] オプションで 0 ～ 65535 の値を指定する必要があることに注意してください。

HTTP ステータス コード（HTTP Status Code）

HTTP 応答内の 3 桁のステータス コードでコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。

HTTP Status Message

HTTP 応答のステータス コードに付加されるテキスト記述の中でコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。

関連トピック

PCRE 修飾子のオプション （2101 ページ）
サーバー レベルの HTTP 正規化オプション （2798 ページ）

概要：content キーワードによる高速パターン マッチ機能

（注） これらのオプションは、`protected_content` キーワードの設定では**サポートされません**。

高速パターン マッチ機能は、パケットをルール エンジンに渡す前に、評価するルールをすばやく決定します。この初期決定により、パケット評価で使用されるルール数が大幅に減るため、パフォーマンスが向上します。

デフォルトで、高速パターンマッチ機能は、ルールで指定された最長のコンテンツをパケットで検索します。これは、不必要なルール評価をできるだけ減らすためです。次の例のようなルール フラグメントがあるとします。

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

ほとんどすべての HTTP クライアント要求にはコンテンツ `GET` が含まれていますが、コンテンツ `/exploit.cgi` を含む要求は稀です。`GET` を高速パターン コンテンツとして使用した場合、ルール エンジンはほとんどのケースでこのルールを評価し、一致はほとんど検出されないでしょう。しかし、`/exploit.cgi` を使用するとほとんどのクライアントの `GET` 要求は評価されないため、パフォーマンスが向上します。

指定されたコンテンツが高速パターン マッチ機能で検出された場合にのみ、ルール エンジンはパケットをルールに照らして評価します。たとえば、ルール内の 1 つの `content` キーワードでコンテンツ `short` を指定し、別のキーワードで `longer`、さらに 3 番目のキーワードで `longest` を指定した場合、高速パターン マッチ機能はコンテンツ `longest` を使用し、ルール エンジンがペイロード内で `longest` を検出した場合にのみ、ルールが評価されます。

content キーワードの高速パターン マッチ機能の引数

Use Fast Pattern Matcher

使用する高速パターンマッチ機能の短い検索パターンを指定するには、このオプションを使用します。理論的には、指定したパターンの方が最長パターンよりもパケット内で見つかる可能性が低いため、より的を絞って対象のエクスプロイトを識別できます。

Use Fast Pattern Matcher と他のオプションを同じ `content` キーワード内で選択する場合は、次の制限事項に注意してください。

- ルールごとに 1 回だけ、**Use Fast Pattern Matcher** を指定できます。
- **Use Fast Pattern Matcher** と **Not** を組み合わせて選択した場合は、**Distance**、**Within**、**Offset**、および **Depth** を使用できません。
- Use Fast Pattern Matcher を、次のいずれかの HTTP フィールド オプションと組み合わせて選択することはできません。

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message**、または **HTTP Status Code**

  ただし、次のいずれかの正規化フィールドを検索するために高速パターンマッチ機能を使用する `content` キーワードでは、上記のオプションを含めることができます。

  HTTP URI、**HTTP Header**、または **HTTP Client Body**

たとえば、**HTTP Cookie**、**HTTP Header**、および **Use Fast Pattern Matcher** を選択した場合、ルール エンジンは HTTP cookie と HTTP 見出しの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP 見出しにのみ適用されます。

未加工 HTTP フィールド オプション（[HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、または [HTTP raw クッキー（HTTP Raw Cookie）]）と、それぞれに対応する正規化されたオプション（[HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP クッキー（HTTP Cookie）]）を同じ `content` キーワード内で一緒に使用できないことに注意してください。

制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、ルールエンジンにパケットを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。

- オプションで、**Use Fast Pattern Matcher** を選択した場合には **Fast Pattern Matcher Only** または **Fast Pattern Matcher Offset and Length** を選択することもできますが、この両方は選択できません。
- Base64 データの検査時には高速パターン マッチ機能を使用できません。

Fast Pattern Matcher Only

このオプションを使用すると、`content` キーワードをルール オプションとしてではなく、高速パターン マッチ機能オプションとしてのみ使用できます。指定したコンテンツをルール エンジンで評価する必要がない場合、このオプションを使ってリソースを節約できます。たとえば、ペイロード内のいずれかの場所にコンテンツ `12345` が存在することだけを必要とするルールがあるとします。高速パターンマッチ機能でパターンが検出された場合に、ルール内の追加のキーワードに照らしてパケットを評価できます。パターン `12345` が含まれているかどうかを判断するために、ルール エンジンがパケットを再評価する必要はありません。

指定されたコンテンツに関連する他の条件がルールに含まれている場合は、このオプションを使用しないでください。たとえば、別のルール条件で `abcd` が `1234` の前に出現するかどうかを判断する場合には、このオプションを使ってコンテンツ `1234` を検索しないでください。**Fast Pattern Matcher Only** を指定すると、指定されたコンテンツがルール エンジンによって検索されないため、このケースではルール エンジンが相対的な位置を判断できません。

このオプションを使用するときには、次の条件に注意してください。

- 指定されたコンテンツは位置に依存しない、つまり、ペイロードのどこにでも出現する可能性があるため、位置オプション（**Distance**、**Within**、**Offset**、**Depth**、**Fast Pattern Matcher Offset and Length**）を使用することはできません。
- このオプションを **Not** と組み合わせて使用することはできません。
- このオプションを **Fast Pattern Matcher Offset and Length** と組み合わせて使用することはできません。
- 大文字/小文字を区別しない方法ですべてのパターンが高速パターン マッチ機能に挿入されるため、指定したコンテンツは「大文字/小文字の区別なし」として扱われます。これ

は自動的に処理されるため、このオプションの選択時に **Case Insensitive** を選択する必要はありません。

- **Fast Pattern Matcher Only** オプションを使用する `content` キーワードの直後に、現在の検索位置を基準にして検索位置を設定する次のキーワードを続けないようにしてください。
  - `isdataat`
  - `pcre`
  - `content`（**Distance** または **Within** が選択されている場合）
  - `content`（**HTTP URI** が選択されている場合）
  - `asn1`
  - `byte_jump`
  - `byte_test`
  - `byte_math`
  - `byte_extract`
  - `base64_decode`

Fast Pattern Matcher Offset and Length

[高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] オプションを使用すると、検索するコンテンツの一部分を指定できます。これにより、パターンが非常に長く、ルールの一致の可能性を判断するのにパターンの一部分だけで十分な場合に、メモリ消費を抑えることができます。高速パターンマッチ機能によってルールが選択されたときに、パターン全体がルールに照らして評価されます。

次の構文に従い、検索を開始する位置（オフセット）およびコンテンツ内をどれほど検索するか（長さ）をバイト単位で指定することにより、高速パターンマッチ機能で使用する部分を決定します。

```
offset,length
```

たとえば、次のコンテンツに対して

```
1234567
```

次のようにオフセットと長さのバイト数を指定した場合、

```
1,5
```

高速パターン マッチ機能はコンテンツ `23456` のみを検索します。

このオプションを [Fast Pattern Matcher Only] と一緒に使用できないことに注意してください。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2078 ページ）

base64_decode キーワードと base64_data キーワード （2176 ページ）

replace キーワード

インライン導入で replace キーワードを使用すると、指定したコンテンツ、または Cisco SSL アプライアンスによって検出された SSL トラフィック内のコンテンツを置き換えることができます。

replace キーワードを使用するには、content キーワードを使って特定の文字列を検索するカスタムの標準テキスト ルールを作成します。その後、replace キーワードを使用して、コンテンツを置き換える文字列を指定します。置換値とコンテンツ値は同じ長さである必要があります。

（注） protected_content キーワード内でハッシュされたコンテンツを置き換えるために replace キーワードを使用することは**できません**。

オプションで、以前の Firepower システム ソフトウェア バージョンとの下位互換性を維持するために、置換文字列を引用符で囲むことができます。引用符を含めない場合は、それらが自動的にルールに追加されるため、構文的に正しいルールになります。置換テキストの一部として先行引用符または後続引用符を含めるには、次の例に示すように、バックスラッシュを使ってエスケープする必要があります。

```
"replacement text plus \"quotation\" marks""
```

1 つのルール内に複数の replace キーワードを含めることができますが、content キーワードごとに 1 つずつしか含めることができません。ルールによって検出されたコンテンツの最初のインスタンスだけが置き換えられます。

次に、replace キーワードの使用例を示します。

- エクスプロイトを含んでいる着信パケットをシステムが検出した場合、有害な文字列を無害な文字列に置き換えることができます。このテクニックは、有害なパケットを単に破棄するよりも効果的である場合があります。破棄されたパケットを攻撃者が単に再送信し続け、やがてネットワーク防御を通り抜けるか、ネットワークを氾濫させるという攻撃シナリオがあります。パケットを破棄する代わりに別の文字列に置換することで、脆弱ではないターゲットに対して攻撃が実行されたと攻撃者に思い込ませることができます。
- （たとえば Web サーバーの）脆弱なバージョンが稼働しているかどうかを調べる偵察攻撃が懸念される場合は、発信パケットを検出して、バナーを独自のテキストに置換できます。

（注） 置換ルールを使用するインライン侵入ポリシー内でルール状態が[イベントを生成する（Generate Events）] に設定されていることを確認してください。ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合はパケットが破棄され、コンテンツが置き換えられません。

文字列置換プロセスでは、宛先ホストがエラーなしでパケットを受信できるように、パケットチェックサムがシステムによって自動的に更新されます。

`replace` キーワードは、HTTP 要求メッセージの `content` キーワード オプションと組み合わせて使用できないことに注意してください。

関連トピック

content キーワードと protected_content キーワード （2072 ページ）
概要：HTTP content および protected_content キーワードの引数 （2078 ページ）

byte_jump キーワード

`byte_jump` キーワードは、指定されたバイト セグメントで定義されるバイト数を計算し、指定したオプションに応じて、指定されたバイト セグメントの末尾から、パケット ペイロードの先頭または末尾から、あるいは最後のコンテンツ一致に対して相対的なポイントから順方向に、パケット内でそのバイト数だけスキップします。パケットの特定のバイト セグメントが、パケット内の可変データに含まれるバイト数を示す場合には、これが役立ちます。

次の表では、`byte_jump` キーワードで必要な引数を説明します。

表 *110 : byte_jump* の必須引数

引数	説明
Bytes	パケットから抽出するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 0 ～ 10 ですが、次の制限があります。 • `From End` 引数とともに使用すると、バイト数は 0 になることがあります。Bytes が 0 の場合、抽出された値は 0 です。 • 1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。

引数	説明
Offset	ペイロード内で処理を開始するバイト数。`offset` カウンタはバイト 0 から始まるため、パケットペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にジャンプさせるバイト数から 1 を差し引いて `offset` 値を計算してください。 -65535 ～ 65535 バイトを指定できます。 また、既存の `byte_extract` 変数または `byte_math` 結果を使用してこの引数の値を指定することもできます。

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 *111 : byte_jump* の追加のオプション引数

引数	説明
相対的	最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Align	変換されたバイト数を、次の 32 ビット境界に切り上げます。
Multiplier	ルール エンジンで最終的な `byte_jump` 値を算出するために、パケットから得られた `byte_jump` 値に掛ける値を示します。 つまり、ルール エンジンは、指定されたバイト セグメントで定義されるバイト数だけスキップする代わりに、Multiplier 引数で指定される整数を乗算したバイト数だけスキップします。
Post Jump Offset	他の `byte_jump` 引数を適用した後に、順方向または逆方向にスキップするバイト数（-65535 ～ 65535）。正の値は順方向にスキップし、負の値は逆方向にスキップします。無効にするには、フィールドを空白のままにするか、`0` を入力します。 **DCE/RPC** 引数を選択すると、一部の `byte_jump` 引数が適用されないことに注意してください。
From Beginning	ルール エンジンが、パケット内の現在の位置からではなく、パケット ペイロードの先頭からペイロード内の指定されたバイト数をスキップする必要があることを示します。
From End	ジャンプは、バッファの最後のバイトのすぐ後のバイトから実行されます。

引数	説明
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

バイト数を `byte_extract` キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *112 : byte_jump* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_jump` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_jump` を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義します。

表 *113 :* 番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_jump` に設定した場合、

- Bytes = 4

- Offset = 12
- Relative enabled
- Align enabled

ルール エンジンは、最後に見つかったコンテンツ一致から 13 バイト後に出現する 4 つのバイトで記述される数値を計算して、そのバイト数だけパケット内を順方向にスキップします。たとえば、ある特定のパケット内で計算される 4 つのバイトが `00 00 00 1F` である場合、ルール エンジンはこれを 31 に変換します。`align` が指定されている（次の 32 ビット境界まで移動するようエンジンに指示する）ため、ルール エンジンはパケット内を 32 バイト先までスキップします。

あるいは、次のような値を `byte_jump` に設定した場合、

- Bytes = 4
- Offset = 12
- From Beginning enabled
- Multiplier = 2

ルール エンジンは、パケットの先頭から 13 バイト後に出現する 4 つのバイトで記述される数値を計算します。その後、その数値に 2 を掛けてスキップする総バイト数を計算します。たとえば、ある特定のパケット内で計算される 4 つのバイトが `00 00 00 1F` である場合、ルール エンジンはこれを 31 に変換し、それに 2 を掛けて 62 にします。[From Beginning] が有効になっているため、ルール エンジンはパケット内の最初の 63 バイトをスキップします。

関連トピック

byte_extract キーワード （2092 ページ）
DCE/RPC キーワード （2131 ページ）

byte_test キーワード

`byte_test` キーワードは、指定されたバイト セグメントを Value 引数およびその演算子に対してテストします。

次の表に、`byte_test` キーワードで必要な引数を説明します。

表 *114 : byte_test* の必須引数

引数	説明
Bytes	パケットから計算するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 1 ～ 10 です。ただし、1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。

引数	説明
値	テストする値（演算子を含む）。 サポート対象演算子：<、>、=、!、&、^、!>、!<、!=、!&、または !^。 たとえば !1024 と指定した場合、byte_test は指定された数値を変換し、それが 1024 と等しくなければイベントが生成されます（他のすべてのキーワード パラメータが一致する場合）。 「!」と「!=」は等価であることに注意してください。 また、既存の byte_extract 変数または byte_math 結果を使用してこの引数の値を指定することもできます。
Offset	ペイロード内で処理を開始するバイト数。offset カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にカウントするバイト数から 1 を差し引いて offset 値を計算してください。 既存の byte_extract 変数または byte_math result 変数を使用して、この引数の値を指定することができます。

次の表に示す引数を使用すると、システムで byte_test 引数がどのように使用されるかをさらに定義できます。

表 *115 : byte_test* の追加のオプション引数

引数	説明
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。
Relative	最後に見つかったパターン一致を基準にしてオフセットを計算します。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを byte_test キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *116 : byte_test* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。

引数	説明
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_test` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_test` を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のストリングデータをシステムがどのように表示するかを定義できます。

表 *117 : byte-test* の番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_test` に指定した場合、

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative enabled

ルールエンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9バイト後に出現する 4 つのバイトで記述される数値を計算し、その計算値が 128 バイトを超えた場合に、ルールがトリガーとして使用されます。

関連トピック

byte_extract キーワード （2092 ページ）
DCE/RPC キーワード （2131 ページ）

byte_extract キーワード

`byte_extract` キーワードを使用すると、指定したバイト数をパケットから変数の中に読み込むことができます。後で、その変数を、同じルール内で他の検出キーワードの特定の引数の値として使用できます。

たとえば、パケット データに含まれるバイト数が特定のバイト セグメントで記述されている場合、パケットからデータ サイズを抽出するには、これが役立ちます。たとえば、特定のバイト セグメントにおいて、後続データが 4 バイト構成であると記述されている場合、データ サイズ 4 バイトを抽出して変数値として使用できます。

`byte_extract` を使用するとき、1 つのルール内で最大 2 つの異なる変数を同時に作成できます。`byte_extract` 変数を何回でも再定義できます。同じ変数名と別の変数定義を使って新しい `byte_extract` キーワードを入力した場合、その前の変数定義がオーバーライドされます。

次の表に、`byte_extract` キーワードで必要な引数について説明します。

表 *118 : byte_extract* の必須引数

引数	説明
Bytes to Extract	パケットから抽出するバイト数。 1、2、または4以外のバイト数を指定する場合は、番号タイプ（16進数、8 進数、または 10 進数）を指定する必要があります。
Offset	ペイロード内でデータの抽出を開始するバイト数。-65535 ～ 65535 バイトを指定できます。オフセット カウンタはバイト0から始まるため、順方向に数えるバイト数から1を差し引いてオフセット値を計算してください。たとえば、順方向に8バイト数えるには7を指定します。ルール エンジンは、パケット ペイロードの先頭から（**Relative** も一緒に指定した場合は最後に見つかったコンテンツ一致の後から）順方向に数えます。負の数は、**Relative** も指定した場合にのみ指定できます。 既存の `byte_math` の結果を使用して、この引数の値を指定することもできます。
Variable Name	他の検出キーワードの引数で使用する変数名。英数字の文字列を指定できます（ただし文字で始まる必要があります）。

抽出対象のデータを見つける方法をさらに詳しく定義するには、次の表に示す引数を使用できます。

表 *119 : byte_extract* の追加のオプション引数

引数	説明
Multiplier	パケットから抽出された値の乗数。0 ～ 65535 を指定できます。乗数を指定しない場合のデフォルト値は 1 です。
Align	抽出された値を、最も近い 2 バイトまたは 4 バイト境界に調整します。**Multiplier** も一緒に選択した場合、システムはこの調整の前に乗数を適用します。
Relative	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致の末尾を基準にして **Offset** を計算します。

引数	説明
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes to Extract 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを `byte_extract` キーワードでどのように計算するか定義するには、次の表の中から引数を選択できます。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *120 : byte_extract* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_extract` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_extract` を使用することもできます。

データを読み取るときの数値タイプを ASCII 文字列として指定できます。パケット内のストリング データをシステムがどのように認識するかを定義するには、次の表のいずれかの引数を選択できます。

表 *121 : byte_extract* の番号タイプ引数

引数	説明
Hexadecimal String	抽出されたストリング データを 16 進形式で読み取ります。
Decimal String	抽出されたストリング データを 10 進形式で読み取ります。
Octal String	抽出されたストリング データを 8 進形式で読み取ります。

たとえば、`byte_extract` の値を次のように指定した場合、

- Bytes to Extract = 4

- Variable Name = var
- Offset = 8
- Relative = enabled

ルールエンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9バイト後に出現する、4 バイトで表現される数値を `var` という名前の変数の中に読み込みます。後でこの変数を、特定のキーワード引数の値としてルール内で指定できます。

`byte_extract` キーワードで定義した変数を指定できるキーワード引数を、次の表に列挙します。

表 *122 : byte_extract* 変数を使用できる引数

キーワード	引数
content	Depth、Offset、Distance、Within
byte_jump	Offset
byte_test	Offset、Value
byte_math	RValue、Offset
isdataat	Offset

関連トピック

DCE/RPC プリプロセッサ （2768 ページ）
DCE/RPC キーワード （2131 ページ）
基本コンテンツおよび protected_content キーワードの引数 （2074 ページ）
byte_jump キーワード （2087 ページ）
byte_test キーワード （2090 ページ）
パケット特性 （2156 ページ）

byte_math キーワード

`byte_math` キーワードは、抽出された値と指定された値または既存の変数の算術演算を実行し、その結果を新しい結果変数に格納します。結果の変数は、他のキーワードの引数として使用することができます。

ルール内で複数の `byte_math` キーワードを使用して、複数の byte_math 操作を実行できます。

次の表で、`byte_math` キーワードで必要な引数について説明します。

表 *123 : byte_math* の必須引数

引数	説明
Bytes	パケットから計算するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 1 ～ 10 です。 • 演算子が +、-、*、または / の場合、バイト数は 1 ー 10 になります。 • 演算子が << または >> の場合、バイト数は 1 ー 4 になります。 • 1、2、または4以外のバイト数を指定する場合は、番号タイプ（16進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。
Offset	ペイロード内で処理を開始するバイト数。`offset` カウンタはバイト 0 から始まるため、パケットペイロードの先頭、または最後に見つかったコンテンツ一致（Relative を指定した場合）から順方向にジャンプさせるバイト数から 1 を差し引いて `offset` 値を計算してください。 -65535 ～ 65535 バイトを指定できます。 ここでは、`byte_extract` 変数を指定することもできます。
演算子	+、-、*、/、<<、または >>
RValue	演算子に続く値。これは、符号なし整数または `byte_extract` から渡される変数です。
Result Variable	`byte_math` の計算結果が格納される変数の名前。この変数は、他のキーワードの引数として使用することができます。 この値は符号なし整数として格納されます。 この変数名には次の条件があります。 • 英数字を使用する必要がある • 先頭を数字にすることはできない • Microsoft のファイル名/変数名の規則でサポートされている特殊文字を含めることができる • 特殊文字のみの名前にすることはできない

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 *124 : byte_math* の追加のオプション引数

引数	説明
相対的	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

バイト数を `byte_math` キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *125 : byte_math* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_math` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_math` を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義します。

表 *126 :* 番号タイプ引数

引数	説明
Hexadecimal String	ストリング データを 16 進形式で表現します。
Decimal String	ストリング データを 10 進形式で表現します。
Octal String	ストリング データを 8 進形式で表現します。

たとえば、次のような値を byte_math に設定した場合、

- Bytes = 2
- Offset = 0
- Operator = *
- RValue = height
- Result Variable = area

ルール エンジンは、パケット内の最初の 2 バイトに記述された番号を抽出し、RValue（既存の変数 height を使用）を乗じて新しい変数 area を作成します。

表 *127 : byte_math* 変数を使用できる引数

キーワード	引数
byte_jump	Offset
byte_test	Offset、Value
byte_extract	Offset
isdataat	Offset

概要：pcre キーワード

pcre キーワードを使用すると、指定されたコンテンツをパケット ペイロード内で検査するために Perl 互換正規表現（PCRE）を使用できます。PCRE を使用すると、同じ内容のわずかなバリエーションにそれぞれ一致する複数のルールを作成する手間が省けます。

正規表現は、さまざまな方法で表現されることのあるコンテンツを検索する場合に役立ちます。パケットのペイロード内でコンテンツを検索するときには、コンテンツがさまざまな属性を持つ可能性があることを考慮すべき場合があります。

侵入ルールで使われる正規表現構文は完全な正規表現ライブラリのサブセットであり、完全なライブラリ内のコマンドで使用される構文とはいくつかの点で異なることに注意してください。侵入ルール エディタを使用して pcre キーワードを追加するときには、次の形式で完全な値を入力します。

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

引数の説明

- 「!」は否定オプションです（正規表現に**一致しない**パターンを照合する場合に使用します）。
- /pcre/ は Perl 互換正規表現です。
- ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。

また、次の表に示す文字をエスケープする必要があることに注意してください。これにより、パケット ペイロード内で特定のコンテンツを検索するために PCRE でこれらの文字を使用した場合、ルール エンジンがそれを正しく解釈するようになります。

表 *128* : エスケープする *PCRE* 文字

エスケープする必要のある文字	バックスラッシュを使用した場合	16進コードを使用した場合
#（ナンバー記号）	\#	\x23
;（セミコロン）	\;	\x3B
|（縦棒）	\\|	\x7C
：（コロン）	\:	\x3A

`m?regex?` を使用することもできます。ここで、`?` は「/」以外のデリミタです。正規表現内でスラッシュと一致させる必要があり、バックスラッシュを使ってそれをエスケープしたくない場合には、これを使用できます。たとえば、`m?`regex`? ismxAEGRBUIPHDMCKSY` を使用できます。ここで regex は Perl 互換正規表現、`ismxAEGRBUIPHDMCKSY` は修飾子オプションの任意の組み合わせです。

ヒント 必要に応じて、Perl 互換正規表現を引用符で囲むことができます。たとえば、pcre_expression は "pcre_expression" となります。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザーのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルール エディタで表示すると、引用符が表示されません。

PCRE の構文

`pcre` キーワードでは、標準の Perl 互換正規表現（PCRE）構文を使用できます。以下の項では、この構文について説明します。

ヒント ここでは PCRE で使用可能な基本的な構文について説明しますが、Perl および PCRE 専用のオンライン リファレンスやブックで、さらに詳しい情報を参照することもできます。

メタ文字

メタ文字は正規表現内で特別な意味を持つリテラル文字です。メタ文字を正規表現内で使用するときは、その前にバックスラッシュを付けて「エスケープする」必要があります。

次の表に、PCRE で使用可能なメタ文字について説明し、それぞれの例を示します。

表 *129 : PCRE* メタ文字

メタ文字	説明	例
。	改行以外の任意の文字と一致します。修飾オプションとして s が使用されている場合は、改行文字も含まれます。	abc. は、abcd、abc1、abc# などと一致します。
*。	ある文字または式の 0 回以上の出現と一致します。	abc* は、abc、abcc、abccc、abcccccc などと一致します。
?	ある文字または式の 0 回または 1 回の出現と一致します。	abc? は abc に一致します。
+	ある文字または式の 1 回以上の出現と一致します。	abc+ は、abc、abcc、abccc、abcccccc などと一致します。
()	式をグループ化します。	(abc)+ は、abc、abcabc、abcabcabc などと一致します。
{}	ある文字または式の一致回数の限度を指定します。下限と上限を設定する場合には、下限と上限をカンマで区切ります。	a{4,6} は、aaaa、aaaaa、または aaaaaa と一致します。 (ab){2} は abab と一致します。
[]	文字クラスを定義できます。セットの中で記述される任意の文字または文字の組み合わせに一致します。	[abc123] は、a または b または c などと一致します。
^	文字列の先頭でコンテンツを照合します。また、文字クラスの中で否定としても使用されます。	^in は、info 内の “in” と一致しますが、bin では一致しません。[^a] は、a を含まない任意の文字列と一致します。
$	文字列の末尾でコンテンツを照合します。	ce$ は、announce 内の “ce” と一致しますが、cent では一致しません。
|	OR 式を示します。	(MAILTO|HELP) は、MAILTO または HELP と一致します。
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\. はピリオドと一致し、* はアスタリスクと一致し、\\ はバックスラッシュと一致します。\d は数字と一致し、\w は英数字と一致します。

文字クラス

文字クラスには、英字、数字、英数字、および空白文字があります。大カッコで囲んで独自の文字クラスを作成できます。また、事前定義のクラスをさまざまな文字タイプのショートカットとして使用することもできます。追加の修飾子なしで文字クラスを使用すると、1 つの文字クラスは 1 桁または 1 文字に一致します。

次の表に、PCRE で使用できる事前定義の文字クラスの説明と例を示します。

表 *130 : PCRE* 文字クラス

文字クラス	説明	文字クラスの定義
\d	数字（桁）と一致します。	[0-9]
\D	数字以外の任意の文字と一致します。	[^0-9]
\w	英数字（語）と一致します。	[a-zA-Z0-9_]
\W	英数字以外の任意の文字と一致します。	[^a-zA-Z0-9_]
\s	スペース、復帰、タブ、改行、および改ページを含む空白文字と一致します。	[\r\t\n\f]
\S	空白文字以外の任意の文字と一致します。	[^ \r\t\n\f]

PCRE 修飾子のオプション

pcre キーワードの値の中で正規表現構文を指定した後、修飾オプションを使用できます。これらの修飾子は、Perl、PCRE、および Snort 固有の処理機能を実行します。修飾子は、常に PCRE 値の末尾に、次の形式で出現します。

```
/pcre/ismxAEGRBUIPHDMCKSY
```

ここで、ismxAEGRBUPHMC には、次の表に示す任意の修飾オプションを含めることができます。

ヒント　オプションで、正規表現と修飾オプションを引用符で囲むことができます（たとえば "/pcre/ismxAEGRBUIPHDMCKSY"）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザーのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルール エディタで表示すると、引用符が表示されません。

次の表に、Perl 処理機能を実行するために使用できるオプションを説明します。

表 *131 : Perl* 関連の正規表現後オプション

オプション	説明
i	正規表現で大文字と小文字を区別しないようにします。
s	ドット文字（.）は、改行または \n 文字を除くすべての文字を表します。オプションとして "s" を使用すると、これをオーバーライドして、改行文字を含むすべての文字をドット文字に一致させることができます。

オプション	説明
m	デフォルトで、1 つの文字列は複数文字からなる単一行として扱われ、^ と $ は特定の文字列の先頭および末尾に一致します。オプションとして "m" を使用すると、^ および $ はバッファの先頭または末尾だけでなく、バッファ内の改行文字の直前または直後のコンテンツとも一致します。
x	エスケープされた（バックスラッシュが先行する）場合、および文字クラスに含まれる場合を除き、空白データ文字がパターン内に出現してもそれを無視します。

次の表に、正規表現の後ろに使用できる PCRE 修飾子の説明を示します。

表 *132 : PCRE* 関連の正規表現後オプション

オプション	説明
A	文字列の先頭でパターンが一致する必要があります（正規表現で ^ を使用した場合と同じ）。
E	対象の文字列の末尾でのみ一致するように $ を設定します（E を伴わない $ は、それが改行である場合には最後の文字の直前とも一致しますが、他の改行文字の直前とは一致しません）。
G	デフォルトでは、* + と ? は「最長マッチ」を実行します。つまり、複数の一致が見つかった場合は最も長い一致が選択されます。G 文字を使用するとこの動作が変更され、常に最初の一致がこれらの文字で選択されます。ただし後ろに疑問符（?）が続く場合を除きます。たとえば、*? +? と ?? は G 修飾子を使った構造内で最長マッチを実行し、疑問符が付いていない *、+、または ? は最長マッチではありません。

次の表に、正規表現の後ろに使用できる Snort 固有の修飾子の説明を示します。

.

表 *133 : Snort* 固有の正規表現後の修飾子

オプション	説明
R	ルールエンジンで見つかった最後の一致の末尾を基準にして、一致するコンテンツを検索します。
B	プリプロセッサによってデコードされる前のデータ内のコンテンツを検索します（このオプションは、`content` または `protected_content` キーワードで `Raw Data` 引数を使用する場合と似ています）。

オプション	説明
U	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP URI** オプションを一緒に使用して、同じコンテンツを検索することはできません。 パイプライン処理された HTTP 要求パケットには複数の URI が含まれていることに注意してください。U オプションを含む PCRE 式を使用すると、ルールエンジンは、パイプライン処理された HTTP 要求パケット内の最初の URI でのみコンテンツ一致を検索します。パケット内のすべての URI を検索するには、**HTTP URI** を選択して `content` または `protected_content` キーワードを使用します。U オプションを含む PCRE 式を一緒に使用するかどうかは問いません。
I	HTTP Inspect プリプロセッサによってデコードされた raw HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Raw URI** オプションを一緒に使用して、同じコンテンツを検索することはできません。
P	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージ本文の中でコンテンツを検索します。
H	HTTP Inspect プリプロセッサによってデコードされた HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Header** オプションを一緒に使用して、同じコンテンツを検索することはできません。
D	HTTP Inspect プリプロセッサによってデコードされた未加工の HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Raw Header** オプションを一緒に使用して、同じコンテンツを検索することはできません。
M	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージのメソッドフィールド内のコンテンツを検索します。メソッドフィールドは、URI で識別されるリソースに対して実行すべきアクション（GET、PUT、CONNECT など）を特定します。

オプション	説明
C	HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の正規化済みコンテンツを検索します。さらに、プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[Inspect HTTP Cookies] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または `protected_content` キーワードの **HTTP Cookie** オプションを一緒に使用して、同じコンテンツを検索することはできません。 • `Cookie:` 見出し名と `Set-Cookie:` 見出し名、見出し行の先行スペース、および見出し行の終わりを示す `CRLF` は cookie の一部としてではなく、見出しの一部として検査されます。
K	HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の未加工コンテンツを検索します。さらに、プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[Inspect HTTP Cookies] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または `protected_content` キーワードの **HTTP Raw Cookie** オプションを一緒に使用して、同じコンテンツを検索することはできません。 • `Cookie:` 見出し名と `Set-Cookie:` 見出し名、見出し行の先行スペース、および見出し行の終わりを示す `CRLF` は cookie の一部としてではなく、見出しの一部として検査されます。
S	HTTP 応答内の 3 桁のステータス コードを検索します。
Y	HTTP 応答内のステータス コードに付加されるテキスト記述を検索します。

（注） UオプションとRオプションを組み合わせて使用しないでください。パフォーマンスの問題が発生する可能性があります。また、他のHTTPコンテンツ オプション（I、P、H、D、M、C、K、S または Y）と組み合わせて U オプションを使用しないでください。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2078 ページ）

PCRE のキーワード値の例

次に、pcre で入力できる値の例を示し、それぞれの例で何が一致するかを説明します。

- **/feedback[(\d{0,1})]?\.cgi/U**

この例では、URI データにのみ配置された、feedback の後に 0 個または 1 個の数字、さらに .cgi が続くインスタンスをパケット ペイロード内で検索します。

この例は以下のものと一致します。

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

この例は、以下のものとは**一致しません**。

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi

- **/^ez(\w{3,5})\.cgi/iU**

この例では、先頭の ez の後に 3 ～ 5 文字の単語、さらに .cgi が続く文字列をパケット ペイロード内で検索します。この検索では大文字と小文字を区別せず、URI データだけを検索します。

この例は以下のものと一致します。

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

この例は、以下のものとは**一致しません**。

- ezez.cgi
- fez.cgi
- abcezboard.cgi
- ezboardman.cgi

- **/mail(file|seek)\.cgi/U**

この例では、URI データ内の mail の後に file と seek のどちらかが続くインスタンスをパケット ペイロードで検索します。

この例は以下のものと一致します。

- mailfile.cgi
- mailseek.cgi

この例は、以下のものとは**一致しません**。

- MailFile.cgi
- mailfilefile.cgi

- **m?http\\x3a\x2f\x2f.*(\n|\t)+?U**

この例では、任意の数の文字の後ろにある、HTTP 要求内のタブまたは改行文字を示す URI コンテンツをパケット ペイロード内で検索します。この例では、式で m?regex? を使用して、http\:\/\/ を使用しないようにしています。コロンの前にバックスラッシュがあることに注意してください。

この例は以下のものと一致します。

- http://www.example.com?scriptvar=x&othervar=\n\..\..
- http://www.example.com?scriptvar=\t

この例は、以下のものとは**一致しません**。

- ftp://ftp.example.com?scriptvar=&othervar=\n\..\..
- http://www.example.com?scriptvar=|/bin/sh -i|

- **m?http\\x3a\x2f\x2f.*=\|.*\|+?sU**

この例では、（改行を含む）任意の数の文字の後に 1 つの等号、さらに任意の数の文字または空白を含むパイプ文字が続くという構成の URL をパケット ペイロード内で検索します。この例では、式で m?regex? を使用して、http\:\/\/ を使用しないようにしています。

この例は以下のものと一致します。

- http://www.example.com?value=|/bin/sh/ -i|
- http://www.example.com?input=|cat /etc/passwd|

この例は、以下のものとは**一致しません**。

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

この例では、MAC アドレスをパケット ペイロード内で検索します。コロン文字がバックスラッシュでエスケープされていることに注意してください。

metadata キーワード

`metadata` キーワードを使用すると、記述情報をルールに追加できます。また、`metadata` キーワードを `service` 引数とともに使用すると、ネットワーク トラフィック内のアプリケーションとポートを特定することができます。追加する情報を使用して、要件に適合するルールを編成または識別することができ、追加する情報や `service` 引数についてルールを検索することができます。

システムは次の形式の引数に基づいてメタデータを検証します。

key value

ここで、*key* と *value* は、スペースで区切られた記述の組み合わせです。これは、Cisco 提供のルールにメタデータを追加するために Talos インテリジェンス グループ VRT で使用されている形式です。

または、次の形式を使用することもできます。

key = *value*

たとえば、*key value* 形式で次のようにカテゴリとサブカテゴリを使用し、作成者と日付によってルールを識別できます。

```
author SnortGuru_20050406
```

1 つのルール内で複数の `metadata` キーワードを使用できます。また、以下の例に示すように、単一の `metadata` キーワード内で複数の *key value* 引数をカンマで区切ることもできます。

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,
revised_by SnortUser1_20070123
```

使用できる形式は *key value* と *key*=*value* だけに限定されません。ただし、これらの形式に基づく検証に起因する制限事項を把握しておく必要があります。

注意すべき制限のある文字

次の文字制限に注意してください。

- セミコロン（;）またはコロン（:）を使用しないでください。

- システムはカンマを、複数の *key value* 引数または *key=value* 引数の区切り文字であると解釈します。次に例を示します。

  key value,*key value*,*key value*

- システムは等号（=）または余白文字を、*key* と *value* の間の区切り文字であると解釈します。次に例を示します。

  key value

  key=value

その他のすべての文字が使用可能です。

注意すべき予約済みメタデータ

`metadata` キーワードでは、次の単語を単一の引数として、または *key value* 引数内の *key* として使用しないでください。これらは Talos 用に予約されています。

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

（注） ローカル ルールを適切に機能させるために制限付きメタデータをどうしても追加する必要がある場合は、サポート担当にお問い合わせください。

影響レベル 1

`metadata` キーワードでは、次に示す予約済み *key value* 引数を使用できます。

```
impact_flag red
```

この *key value* 引数は、インポートしたローカル ルールまたは侵入ルール エディタを使って作成したカスタム ルールに関する影響フラグを赤（レベル 1）に設定します。

「送信元または宛先のホストがウイルス、トロイの木馬、その他の有害ソフトウェアによって侵害されている可能性があることを、ルールをトリガーしているパケットが示している」と Talos が判断した場合、Talos は Cisco 提供のルールに `impact_flag red` 引数を含めます。

サービス メタデータ

システムは、ネットワークのホストで動作しているアプリケーションを検出し、ネットワーク トラフィックにアプリケーション プロトコル情報を挿入します。これは、検出ポリシーの設定に関係なく実行されます。TCP または UDP ルールで `metadata` キーワード `service` 引数を使用して、ネットワーク トラフィックのアプリケーション プロトコルとポートを照合することが

できます。ルールで 1 つ以上の `service` アプリケーション引数を単一のポート引数と組み合わせることができます。

サービス アプリケーション

`metadata` キーワードとともに `service` を *key* として、アプリケーションを *value* として使用し、パケットを識別されたアプリケーションプロトコルと一致させることができます。たとえば、次に示す `metadata` キーワード内の *key value* 引数は、ルールを HTTP トラフィックに関連付けます。

```
service http
```

複数のアプリケーションをカンマで区切って指定することもできます。次に例を示します。

```
service http, service smtp, service ftp
```

注意 侵入ルールでサービス メタデータを使用するためには、適応型プロファイルの設定（2937 ページ） で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする**必要があります**。

次の表に、`service` キーワードとともに使用される最も一般的なアプリケーション値を示します。

（注） 表にないアプリケーションを特定することが難しい場合は、サポートにお問い合わせください。

表 *134 : service* 値

値	説明
`cvs`	Concurrent Versions System（バージョン管理システム）
`dcerpc`	分散コンピューティング環境/リモート プロシージャ コール システム
`dns`	Domain Name System; ドメイン ネーム システム
`finger`	Finger ユーザー情報プロトコル
`FTP`	File Transfer Protocol
`ftp-data`	ファイル転送プロトコル（データ チャネル）
`http`	Hypertext Transfer Protocol
`imap`	Internet Message Access Protocol
`isakmp`	Internet Security Association and Key Management Protocol
`mysql`	My Structured Query Language（構造化照会言語）

値	説明
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS セッション サービス
nntp	Network News Transfer Protocol
oracle	Oracle Net Services
shell	OS Shell
pop2	Post Office Protocol バージョン 2
pop3	Post Office Protocol バージョン 3
smtp	Simple Mail Transfer Protocol
snmp	簡易ネットワーク管理プロトコル
ssh	セキュア シェル ネットワーク プロトコル
sunrpc	Sun リモート プロシージャ コール プロトコル
telnet	Telnet ネットワーク プロトコル
tftp	Trivial File Transfer Protocol
x11	X Window システム

サービス ポート

Metadata キーワードとともに service を *key* として、指定したポート引数を *value* として使用し、ルールがアプリケーションと組み合わせてポートを照合する方法を定義できます。

次の表の任意のポート値を、ルールごとに 1 つ指定できます。

表 *135 : service* ポート値

値	説明
`else-ports` または `unknown`	次の条件のいずれかが満たされるとルールが適用されます。 • パケット アプリケーションが既知で、ルール アプリケーションと一致する。 • パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。 `else-ports` および `unknown` の値では、`service` がポート修飾子なしでアプリケーションプロトコルを指定する場合にシステムで使用されるデフォルトの動作が生成されます。
`and-ports`	パケットアプリケーションが既知で、ルールアプリケーションと一致し、パケット ポートがルール ヘッダーのポートと一致する場合、ルールが適用されます。アプリケーションを指定しないルールで `and-ports` を使用することはできません。
`or-ports`	次の条件のいずれかが満たされるとルールが適用されます。 • パケット アプリケーションが既知で、ルール アプリケーションと一致する。 • パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。 • パケット アプリケーションはルール アプリケーションと一致せず、パケット ポートはルール ポートと一致する。 • ルールはアプリケーションを指定せず、パケット ポートはルール ポートと一致する。

次の点に注意してください。

- `service` アプリケーション引数を `service and-ports` 引数とともに含める必要があります。
- ルールで上記の表の値が複数指定されている場合、ルールの一番最後にある値が適用されます。
- ポートおよびアプリケーション引数は任意の順序にすることができます。

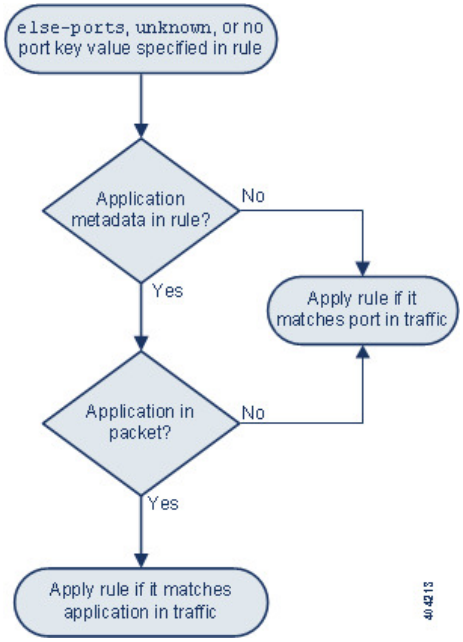
`and-ports` 値を除き、1 つ以上の `service` アプリケーション引数の有無にかかわらず、`service` ポート引数を含めることができます。次に例を示します。

```
service or-ports, service http, service smtp
```

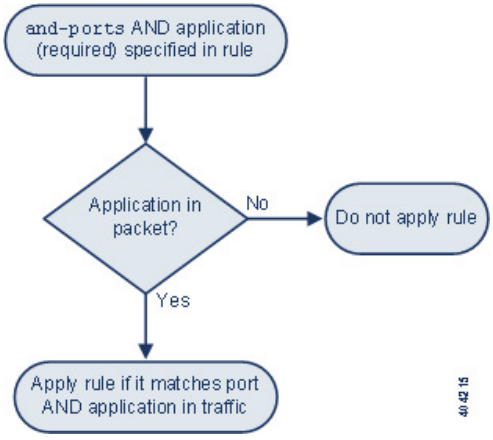
トラフィックのアプリケーションとポート

次の図は、侵入ルールでサポートされるアプリケーションとポートの組み合わせ、およびパケット データにこれらのルール制約を適用した結果を示しています。

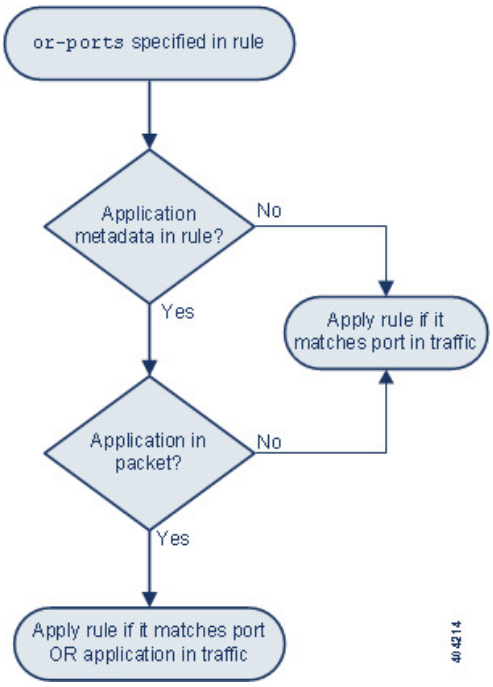
ホスト アプリケーション プロトコル else 送信元/宛先ポート：



ホスト アプリケーション プロトコル and 送信元/宛先ポート：



ホスト アプリケーション プロトコル **or** 送信元/宛先ポート：



一致する例

`metadata` キーワードを `service` 引数とともに使用した次のサンプル ルールを、一致するデータおよび一致しないデータの例とともに示します。

- `alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)`

一致する例	一致しない例
• TCP ポート 80 経由の HTTP トラフィック • TCP ポート 8080 経由の HTTP トラフィック • TCP ポート 80 経由の SMTP トラフィック • TCP ポート 8080 経由の SMTP トラフィック	• ポート 80 または 8080 の POP3 トラフィック • ポート 80 または 8080 の不明なアプリケーション トラフィック • ポート 9999 の HTTP トラフィック

- `alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)`

一致する例	一致しない例
• あらゆるポートの HTTP トラフィック • ポート 80 の SMTP トラフィック • ポート 8080 の SMTP トラフィック • ポート 80 および 8080 の不明なアプリケーションのトラフィック	• 80 または 8080 以外のポートの非 HTTP および非 SMTP トラフィック

- 次のいずれかの規則：
  - `alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service unknown, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service http;)`

一致する例	一致しない例
• あらゆるポートの HTTP トラフィック • パケット アプリケーションが不明な場合はポート 80 • パケット アプリケーションが不明な場合はポート 8080	• ポート 80 または 8080 の SMTP トラフィック • ポート 80 または 8080 の POP3 トラフィック

メタデータ検索のガイドライン

`metadata` キーワードを使用するルールを検索するには、ルールの [検索（Search）] ページで `metadata` キーワードを選択して、オプションで、メタデータの一部分を入力します。たとえば次のように入力できます。

- `search` と入力すると、*key* として `search` が使用されているすべてのルールが表示されます。
- `search http` と入力すると、*key* として `search`、*value* として `http` がそれぞれ使用されているすべてのルールが表示されます。
- `author snortguru` と入力すると、*key* として `author`、*value* として `SnortGuru` がそれぞれ使用されているすべてのルールが表示されます。
- `author s` と入力すると、*key* として `author`、さらに *value* として `SnortGuru`、`SnortUser1`、`SnortUser2` などの語が使用されているすべてのルールが表示されます。

ヒント *key* と *value* の両方を検索するときには、ルール内の *key value* 引数で使用されているのと同じ接続演算子（等号 [=] または空白文字）を検索で使用してください。*key* の後に等号（=）と空白文字のどちらを入力するかに応じて、異なる結果が検索で返されます。

なお、メタデータ追加のために使用する形式とは無関係に、システムはメタデータ検索語を *key value* または *key*=*value* 引数の全部または一部として解釈します。たとえば、次に示すメタデータは *key value* または *key*=*value* 形式に従っていませんが、有効なメタデータです。

```
ab cd ef gh
```

ただし、この例に含まれる各スペースは *key* と *value* の間の区切り文字としてシステムで解釈されます。次に示す並列語や単一語を検索で使用すると、この例のメタデータを含むルールを正しく検出できます。

```
cd ef
ef gh
ef
```

一方、次の検索を使用した場合、単一の *key value* 引数としてシステムによって解釈されるため、ルールを検出できません。

```
ab ef
```

関連トピック

ルールの検索 （2066 ページ）

IP ヘッダー値

キーワードを使用すると、パケットの IP ヘッダーの中で攻撃やセキュリティ ポリシー違反の可能性を識別できます。

fragbits

`fragbits` キーワードは、IP 見出し内のフラグメント ビットと予約ビットを検査します。パケットごとに、予約ビット、More Fragments ビット、および Don't Fragment ビットを任意に組み合わせて検査できます。

表 *136 : Fragbits* 引数の値

引数	説明
R	予約ビット
M	More Fragments ビット

引数	説明
D	Don’t Fragment ビット

`fragbits` キーワードを使ってルールを微調整するために、次の表に示す演算子をルール内の引数値の後ろに指定できます。

表 *137 : Fragbit* 演算子

演算子	説明
プラス記号（**+**）	パケットは、指定されたすべてのビットと一致する必要があります。
アスタリスク（*****）	パケットは、指定されたどのビットと一致することもできます。
感嘆符（**!**）	指定されたどのビットも設定されていない場合、パケットが基準を満たします。

たとえば、（他のビットの有無とは無関係に）少なくとも予約済みビットが設定されたパケットに対してイベントを生成するには、`fragbits` 値として `R+` を使用します。

id

`id` キーワードは、キーワード引数で指定される値に照らしてIP見出しフラグメント識別フィールドを検査します。一部のサービス拒否ツールやスキャナは、このフィールドを、容易に検出できる特定の番号に設定します。たとえば、Synscanポートスキャンを検出するSID 630では、`id` 値が `39426`（スキャナから伝送されるパケットのID番号として使われる静的な値）に設定されます。

（注） `id` 引数値は数値でなければなりません。

ipopts

`IPopts` キーワードを使用すると、指定されたIP見出しオプションをパケット内で検索できます。次の表に、使用可能な引数値を示します。

表 *138 : IPoption* 引数

引数	説明
rr	経路を記録
eol	リストの末尾
nop	オペレーションなし
ts	タイム スタンプ

引数	説明
sec	IP セキュリティ オプション
lsrr	厳密でない送信元ルーティング
ssrr	厳密な送信元ルーティング
satid	ストリーム識別子

アナリストが最も頻繁に監視するのは、厳密な送信元ルーティングと厳密でない送信元ルーティングです。これらのオプションは送信元 IP アドレスのスプーフィングを示している可能性があるためです。

ip_proto

`ip_proto` キーワードを使用すると、キーワードの値として指定された IP プロトコルを含むパケットを識別できます。IP プロトコルは 0 ～ 255 の数値として指定できます。これらの番号を、<、>、または ! 演算子と組み合わせることができます。たとえば、ICMP 以外のプロトコルを使用しているトラフィックを検査するには、`ip_proto` キーワードの値として `!1` を使用します。1 つのルール内で `ip_proto` キーワードを複数回にわたって使用できます。ただし、ルール エンジンはキーワードの複数インスタンスをブール和関係（AND）と解釈することに注意してください。たとえば、`ip_proto:!3; ip_proto:!6` を含むルールを作成した場合、このルールは GGP プロトコルおよび TCP プロトコルを使用するトラフィックを無視します。

tos

一部のネットワークでは、ネットワーク上を移動するパケットの優先度を設定するタイプオブサービス（ToS）値が使用されます。`tos` キーワードを使用すると、キーワードの引数で指定された値に照らしてパケットの IP 見出し ToS 値を検査できます。`tos` キーワードを使用するルールは、ToS が指定の値に設定され、しかもルール内の残りの基準を満たすパケットに対してトリガーとして使用されます。

（注） `tos` の引数値は数値でなければなりません。

[ToS] フィールドは IP ヘッダー プロトコルでは非推奨になり、[Differentiated Services Code Point (DSCP)] フィールドに置き換えられています。

ttl

パケットの存続可能時間（time-to-live、ttl）値は、パケットが破棄される前に生成できるホップ数を示します。`ttl` キーワードを使用すると、キーワードの引数として指定された値または値の範囲に照らしてパケットの IP 見出し ttl 値を検査できます。`ttl` キーワード パラメータを 0 や 1 などの低い値に設定すると役立つことがあります。これは、低い存続可能時間値がトレースルートや侵入回避の試みを示している場合があるためです。（ただし、このキーワードの適

切な値は、管理対象デバイスの配置やネットワークトポロジによって異なります）。次のように構文を使用します。

- TTL 値に特定の 1 つの値を設定するには、0 ～ 255 の整数を使用します。値の前に等号（=）を付けることもできます（たとえば 5 または =5 を指定できます）。
- TTL 値の範囲を指定するには、ハイフン（-）を使用します（たとえば、0-2 は 0 ～ 2 のすべての値、-5 は 0 ～ 5 のすべての値、5- は 5 ～ 255 のすべての値をそれぞれ指定します）。
- 特定の値より大きい TTL 値を指定するには、「大なり」記号（>）を使用します（たとえば、>3 は 3 より大きいすべての値を指定します）。
- 特定の値以上の TTL 値を指定するには、「大なりイコール」記号（>=）を使用します（たとえば、>=3 は 3 以上のすべての値を指定します）。
- 特定の値より小さい TTL 値を指定するには、「小なり」記号（<）を使用します（たとえば、<3 は 3 より小さいすべての値を指定します）。
- 特定の値以下の TTL 値を指定するには、「小なりイコール」記号（<=）を使用します（たとえば、<=3 は 3 以下のすべての値を指定します）。

ICMP ヘッダー値

Firepower システムでサポートされるキーワードを使用すると、ICMP パケット ヘッダー内の攻撃やセキュリティ ポリシー違反を識別できます。なお、ほとんどの ICMP タイプおよびコードを検出する事前定義ルールがあることに注意してください。既存のルールを有効にするか、既存のルールに基づいてローカル ルールを作成することを考慮してください。ICMP ルールを最初から作成するよりも、ニーズを満たすルールを見つける方が時間の節約になる可能性があります。

icmp_id と icmp_seq

ICMP の識別番号とシーケンス番号は、ICMP 応答と ICMP 要求を関連付けるうえで役立ちます。通常のトラフィックでは、これらの値はパケットに動的に割り当てられます。一部のコバート チャネルおよび Distributed Denial of Server（DDoS）プログラムは、静的な ICMP ID およびシーケンス値を使用します。次のキーワードを使用すると、静的な値を含む ICMP パケットを識別できます。

キーワード	定義（Definition）
icmp_id	ICMP エコー要求または応答パケットの ICMP ID 番号を検査します。ICMP ID 番号に対応する数値を `icmp_id` キーワードの引数として使用します。
icmp_seq	`icmp_seq` キーワードは、ICMP エコー要求または応答パケットの ICMP シーケンスを検査します。ICMP シーケンス番号に対応する数値を `icmp_seq` キーワードの引数として使用します。

itype

itype キーワードを使用して、特定の ICMP メッセージ タイプ値を含むパケットを検索します。有効な ICMP タイプ値と無効な ICMP タイプ値のいずれかを指定して、さまざまなタイプのトラフィックを検査できます。たとえば、サービス拒否攻撃やフラッディング攻撃を発生させるために攻撃者が範囲外の ICMP タイプ値を設定することがあります。

「小なり」（<）と「大なり」（>）を使用して itype 引数値の範囲を指定できます。

次に例を示します。

- <35
- >36
- 3<>55

icode

ICMP メッセージには、宛先が到達不能である場合の詳細を示すコード値が含まれることがあります。

icode キーワードを使用すると、特定の ICMP コード値を含むパケットを識別できます。有効な ICMP コード値と無効な ICMP コード値のいずれかを指定することにより、さまざまなタイプのトラフィックを検査できます。

「小なり」（<）と「大なり」（>）を使用して icode 引数値の範囲を指定できます。

次に例を示します。

- 35 より小さい値を検索するには <35 と指定します。
- 36 より大きい値を検索するには >36 と指定します。
- 3 ～ 55 の間にある値を検索するには、3<>55 と指定します。

ヒント icode キーワードと itype キーワードを一緒に使用すると、両方に一致するトラフィックを識別できます。たとえば、ICMP 宛先到達不能コード タイプと ICMP ポート到達不能コード タイプを含む ICMP トラフィックを特定するには、値 3 の itype キーワード（宛先到達不能）と、値 3 の icode キーワード（ポート到達不能）を指定します。

TCP ヘッダー値とストリーム サイズ

Firepower システムでは、パケットの TCP ヘッダーと TCP ストリーム サイズを使って試行される攻撃を識別するためのキーワードを使用できます。

ack

`ack` キーワードを使用すると、パケットの TCP 確認応答番号と特定の値を比較できます。パケットの TCP 確認応答番号が、`ack` キーワードに指定された値と一致した場合に、ルールがトリガーとして使用されます。

`ack` の引数値は数値でなければなりません。

フラグ（Flags）

`flags` キーワードを使用すると、複数の TCP フラグを任意に組み合わせて指定できます。検査対象のパケットでこれらが設定されている場合、ルールがトリガーとして使用されます。

（注） 従来、`flags` の値として `A+` を使用していたケースでは、代わりに `flow` キーワードおよび値 `established` を使用してください。一般に、フラグのすべての組み合わせが検出されるようにするには、フラグの使用時に `flow` キーワードおよび値 `stateless` を使用する必要があります。

次の表に示す `flags` キーワードの値を確認または無視することができます。

表 *139 : flags* の引数

引数	TCP フラグ
Ack	データを確認応答します。
Psh	このパケットでデータが送信される必要があります。
Syn	新しい接続。
Urg	パケットに緊急データが含まれています。
Fin	接続が閉じられました。
Rst	接続が異常終了しました。
CWR	ECN 輻輳ウィンドウが減少しました。旧 R1 引数（下位互換性を維持するために引き続きサポートされています）。
ECE	ECN エコー。旧 R2 引数（下位互換性を維持するために引き続きサポートされています）。

`flags` キーワードを使用する場合、複数のフラグに対する照合方法をシステムに指示するための演算子を使用できます。次の表に、これらの演算子の説明を示します。

表 *140 : flags* と一緒に使用する演算子

演算子	説明	例
all	パケットは、指定されたすべてのフラグを含んでいる必要があります。	`Urg` と `all` を選択すると、パケットが緊急フラグを含んでいる必要があること、および他のフラグが含まれる可能性があることを指定できます。
any	パケットは、指定された任意のフラグを含むことができます。	`Ack`、`Psh`、および `any` を選択すると、ルールをトリガーとして使用するためには `Ack` と `Psh` のどちらか（または両方）のフラグが設定される必要があること、およびパケット内で他のフラグも設定されている可能性があることを指定できます。
not	パケットは、指定されたフラグセットを**含んではなりません**。	`Urg` と `not` を選択すると、このルールをトリガーとして使用するパケットに関して緊急フラグが設定**されない**ことを指定できます。

flow

`flow` キーワードを使用すると、セッション特性に基づいてルールで検査されるパケットを選択できます。`flow` キーワードを使用することで、ルールの適用対象となるトラフィック フロー方向を指定して、クライアントフローとサーバーフローのどちらかにルールを適用できます。`flow` キーワードによるパケット検査の方法を指定するには、分析すべきトラフィックの方向、検査するパケットの状態、およびパケットが再構築ストリームの一部かどうかを設定できます。

ルールの処理時に、パケットのステートフルインスペクションが実行されます。ステートレストラフィック（セッション コンテキストが確立されていないトラフィック）を TCP ルールで無視するには、`flow` キーワードをルールに追加して、そのキーワードで **Established** 引数を選択する必要があります。UDP ルールでステートレス トラフィックを無視するには、`flow` キーワードをルールに追加して、**Established** 引数と方向引数のどちらか（または両方）を選択する必要があります。これにより、TCP または UDP ルールでパケットのステートフル インスペクションが実行されます。

方向引数を追加した場合、ルール エンジンは、指定された方向と一致するフローを伴う確立された状態のパケットだけを検査します。たとえば、TCP または UDP 接続が検出されたときトリガーとして使用されるルールに、`flow` キーワードおよび `established` 引数と `From Client` 引数を 追加した場合、ルール エンジンはクライアントから送信されたパケットだけを検査します。

ヒント パフォーマンスを最大にするには、必ず TCP ルールまたは UDP セッション ルールに `flow` キーワードを含めてください。

次の表に、`flow` キーワードで指定できるストリーム関連引数の説明を示します。

表 *141 : flow* の状態関連引数

引数	説明
Established	確立された接続でトリガーとして使用されます。
Stateless	ストリーム プロセッサの状態に関係なくトリガーとして使用されます。

次の表に、`flow` キーワードで指定できる方向オプションの説明を示します。

表 *142 : flow* の方向引数

引数	説明
To Client	サーバー応答でトリガーとして使用されます。
To Server	クライアント応答でトリガーとして使用されます。
From Client	クライアント応答でトリガーとして使用されます。
From Server	サーバー応答でトリガーとして使用されます。

`From Server` と `To Client` の機能が同じであること、および `To Server` と `From Client` の機能も同じであることに注意してください。これらのオプションは、ルールに文脈と読みやすさを加味するために提供されています。たとえば、サーバーからクライアントへの攻撃を検出するよう設計されたルールを作成する場合は、`From Server` を使用します。一方、クライアントからサーバーへの攻撃を検出するように設計されたルールを作成する場合は、`From Client` を使用します。

次の表に、`flow` キーワードで指定できるストリーム関連引数の説明を示します。

表 *143 : flow* のストリーム関連引数

引数	説明
Ignore Stream Traffic	再構築されたストリーム パケットでトリガーとして使用されません。
Only Stream Traffic	再構築されたストリーム パケットでのみトリガーとして使用されます。

たとえば、`flow` キーワードの値として `To Server, Established, Only Stream Traffic` を使用すると、ストリームプリプロセッサで再構築された、確立済みセッションでクライアントからサーバーに移動するトラフィックを検出できます。

seq

`seq` キーワードを使用すると、静的なシーケンス番号値を指定できます。パケットのシーケンス番号が、指定された引数と一致する場合、そのキーワードを含むルールがトリガーとして使

用されます。このキーワードはあまり使用されませんが、静的シーケンス番号付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

window

`window` キーワードを使用すると、特定の TCP ウィンドウ サイズを指定できます。このキーワードを含むルールは、指定された TCP ウィンドウ サイズのパケットが検出されるたびにトリガーされます。このキーワードはあまり使用されませんが、静的 TCP ウィンドウ サイズ付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

stream_size

次に示す形式で、`stream_size` キーワードとストリーム プリプロセッサを組み合わせて使用すると、TCP ストリームのサイズをバイト単位で特定できます。

```
direction,operator,bytes
```

ここで、bytes はバイト数です。引数内の各オプションをカンマ（,）で区切る必要があります。

次の表は、`stream_size` キーワードで指定できる大文字/小文字を区別しない方向オプションを示しています。

表 *144 : stream_size* キーワードの方向引数

引数	説明
client	指定されたストリーム サイズに一致するクライアントからのストリームでトリガーとして使用されます。
server	指定されたストリーム サイズに一致するサーバーからのストリームでトリガーとして使用されます。
both	指定されたストリーム サイズに一致するクライアントからのトラフィックとサーバーからのトラフィックの両方によってトリガーとして使用されます。 たとえば `both, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバーからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。
either	指定されたストリーム サイズに一致するクライアントまたはサーバーからのトラフィック（どちらか先に出現した方）によってトリガーとして使用されます。 たとえば `both, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバーからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。

次の表に、`stream_size` キーワードで使用できる演算子の説明を示します。

表 *145 : stream_size* キーワードの引数演算子

演算子	説明
=	等しい
!=	等しくない
>	より大きい
<	より小さい
>=	以上
<=	以下

たとえば、クライアントからサーバーに移動する 5001216 バイト以上の TCP ストリームを検出するには、`stream_size` キーワードの引数として `client, >=, 5001216` を使用できます。

stream_reassembly キーワード

`stream_reassemble` キーワードを使用すると、接続での検査対象トラフィックがルールの条件と一致した場合に、1 つの接続の TCP ストリーム再構築を有効/無効にすることができます。オプションで、このキーワードを 1 つのルール内で複数回使用することができます。

ストリーム再構築を有効または無効にするには、次の構文を使用します。

```
enable|disable, server|client|both, option, option
```

次の表に、`stream_reassemble` キーワードで使用できるオプション引数の説明を示します。

表 *146 : stream_reassemble* のオプション引数

引数	説明
noalert	ルールで他にどの検出オプションが指定されているかに関係なく、イベントを生成しません。
fastpath	一致の検出時に残りの接続トラフィックを無視します。

たとえば、次のルールは、HTTP 応答で 200 OK ステータス コードが検出される接続に対してイベントを生成せずに、TCP クライアント側ストリーム再構築を無効にします。

```
alert tcp any 80 -> any any (flow:to_client, established; content: “200 OK”;
stream_reassemble:disable, client, noalert
```

SSL キーワード

SSL ルール キーワードを使用すると、Secure Sockets Layer（SSL）プリプロセッサを呼び出し、暗号化セッションのパケットから SSL のバージョンとセッション状態に関する情報を抽出できます。

SSL または Transport Layer Security（TLS）を使用する暗号化セッションを確立するためにクライアントとサーバーが通信するとき、ハンドシェイク メッセージが交換されます。セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL プリプロセッサは、特定のハンドシェイク フィールドから状態とバージョンの情報を抽出します。ハンドシェイク内の 2 つのフィールドは、セッション暗号化に使われる SSL または TLS のバージョンとハンドシェイクのステージを示します。

ssl_state

`ssl_state` キーワードを使用すると、暗号化されたセッションの状態情報と照合することができます。同時に使用される複数の SSL バージョンを検査するには、1 つのルール内で複数の `ssl_version` キーワードを使用します。

ルールで `ssl_state` キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL 状態情報を検査します。

たとえば、チャレンジ長が非常に長く、データが多すぎる `ClientHello` メッセージを送信することによってサーバー上のバッファ オーバーフローを引き起そうとする攻撃者の試みを検出するには、`ssl_state` キーワードと引数 `client_hello` を使用し、異常に大きなパケットを検査することができます。

SSL 状態に関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、引数として `client_hello` および `server_hello` を指定すると、システムは `client_hello` または `server_hello` のどちらかを含むトラフィックに照らしてルールを評価します。

次のように、引数を除外することもできます。

```
!client_hello, !unknown
```

接続が一連の状態のそれぞれに到達したことを確認するには、ssl_state ルール オプションを使用する複数のルールを使う必要があります。`ssl_state` キーワードは、次の識別子を引数として受け入れます。

表 *147: ssl_state* の引数

引数	目的
`client_hello`	クライアントが暗号化セッションを要求する、メッセージ タイプ `ClientHello` のハンドシェイク メッセージを照合します。
`server_hello`	クライアントからの暗号化セッション要求に対してサーバーが応答する、メッセージ タイプ `ServerHello` のハンドシェイク メッセージを照合します。

引数	目的
client_keyx	サーバーからのキーの受信を確認するためにクライアントがサーバーにキーを伝送する、メッセージ タイプ ClientKeyExchange のハンドシェイク メッセージを照合します。
server_keyx	サーバーからのキーの受信を確認するためにクライアントがサーバーにキーを伝送する、メッセージ タイプ ServerKeyExchange のハンドシェイク メッセージを照合します。
unknown	任意のハンドシェイク メッセージ タイプを照合します。

ssl_version

ssl_version キーワードを使用すると、暗号化されたセッションのバージョン情報と照合することができます。ルールで ssl_version キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL バージョン情報を検査します。

たとえば、SSL バージョン 2 にバッファ オーバーフロー脆弱性があることがわかっている場合、ssl_version キーワードで sslv2 引数を使用して、その SSL バージョンを使用するトラフィックを識別できます。

SSL バージョンに関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、SSLv2 を使用していない暗号化トラフィックを識別するには、ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2 をルールに追加できます。このルールは、SSL バージョン 3、TLS バージョン 1.0、TLS バージョン 1.1、または TLS バージョン 1.2 を使用するトラフィックを評価します。

ssl_version キーワードは、次の SSL/TLS バージョン識別子を引数として受け入れます。

表 *148: ssl_version* の引数

引数	目的
sslv2	Secure Sockets Layer（SSL）バージョン 2 を使用してエンコードされたトラフィックを照合します。
sslv3	Secure Sockets Layer（SSL）バージョン 3 を使用してエンコードされたトラフィックを照合します。
tls1.0	Transport Layer Security（TLS）バージョン 1.0 を使用してエンコードされたトラフィックを照合します。
tls1.1	Transport Layer Security（TLS）バージョン 1.1 を使用してエンコードされたトラフィックを照合します。
tls1.2	Transport Layer Security（TLS）バージョン 1.2 を使用してエンコードされたトラフィックを照合します。

appid キーワード

パケットからアプリケーションプロトコル、クライアントアプリケーション、Webアプリケーションを特定するために `appid` キーワードを使用できます。たとえば、ある脆弱性をもつことが知られている特定のアプリケーションを検出することを考えます。

侵入ルールの `appid` キーワードの中で、[AppID の設定（Configure AppID）] をクリックし、検出するアプリケーションを 1 つまたは複数選択します。

使用可能なアプリケーションの参照

条件の作成を初めて開始するときは、[使用可能なアプリケーション（Available Applications）] リストは制約されておらず、システムが検出するすべてのアプリケーションをページごとに 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関する概要情報と参照可能なインターネット検索リンクを含むポップアップウィンドウを表示するには、アプリケーションの横にある**情報**（ ）をクリックします。

アプリケーション フィルタの使用

照合するアプリケーションを見つけやすくするために、[Available Applications] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します。フィルタを適用すると、[Available Applications] リストが更新されます。便宜上、システムは**ロック解除アイコン**を使用して、復号されたトラフィック（暗号化されているトラフィックまたは暗号化されていないトラフィックではなく）でのみ識別できるアプリケーションをマークします。

（注） [アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション（Available Applications）] リストを検索した場合、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使って結合されます。

アプリケーションの選択

アプリケーションを 1 つだけ選択するには、そのアプリケーションを選択し、[ルールへの追加（Add to Rule）] をクリックします。フィルタで限定されている現在の表示のすべてのアプリケーションを選択するには、右クリックして [すべて選択（Select All）] を選択します。

アプリケーション層プロトコル値

アプリケーション層プロトコル値の正規化と検査はほとんどがプリプロセッサによって実行されますが、種々のプリプロセッサオプションを使用して、アプリケーション層値をさらに検査できます。

RPC キーワード

rpc キーワードは、TCP または UDP パケットでオープン ネットワーク コンピューティング リモート プロシージャ コール（ONC RPC）サービスを識別します。これにより、ホスト上の RPC プログラムの識別試行を検出することができます。ネットワークで実行中のいずれかの RPC サービスを悪用できるかどうか判断するために、侵入者は RPC ポートマッパーを使用できます。また、ポートマッパーを使用せずに RPC を実行中の他のポートへのアクセスを試みることもできます。次の表に、rpc キーワードで使用できる引数を列挙します。

表 *149 : rpc* キーワードの引数

引数	説明
application	RPC アプリケーション番号
手順	呼び出される RPC プロシージャ
version	RPC バージョン

rpc キーワードの引数を指定するには、次の構文を使用します。

```
application,procedure,version
```

ここで、application は RPC アプリケーション番号、procedure は RPC プロシージャ番号、version は RPC バージョン番号です。rpc キーワードのすべての引数を指定する必要があります。引数のいずれかを指定できない場合は、アスタリスク（*）で置き換えてください。

たとえば、任意のプロシージャまたはバージョンの RPC ポートマッパー（100000 という番号で示される RPC アプリケーション）を検索するには、引数として 100000,*,* を使用します。

ASN.1 キーワード

asn1 キーワードを使用すると、さまざまな有害エンコードを検索しながら、パケットまたはパケットの一部分をデコードできます。

次の表に、asn1 キーワードの引数について説明します。

表 *150 : asn.1* キーワードの引数

引数	説明
Bitstring Overflow	無効な、リモートで悪用可能なビットストリング エンコードを検出します。

引数	説明
Double Overflow	標準バッファより大きい二重 ASCII エンコードを検出します。これは Microsoft Windows の悪用可能な機能であることが知られていますが、現時点でどのサービスが悪用可能であるかは不明です。
Oversize Length	指定された引数より大きい ASN.1 タイプ長を検出します。たとえば Oversize Length を 500 に設定した場合、500 を上回る ASN.1 タイプによってルールがトリガーとして使用されます。
Absolute Offset	パケット ペイロードの先頭からの絶対オフセットを設定します（offset カウンタがバイト 0 から始まることに注意してください）。たとえば SNMP パケットをデコードするには、Absolute Offset を 0 に設定し、Relative Offset を設定しません。Absolute Offset として正または負の値が可能です。
Relative Offset	これは、最後に見つかったコンテンツ一致、`pcre`、または `byte_jump` からの相対オフセットです。コンテンツ "foo" の直後の ASN.1 シーケンスをデコードするには、Relative Offset を 0 に設定し、Absolute Offset を設定しません。Relative Offset として正または負の値が可能です。（オフセット カウンタが 0 から始まることに注意してください。）

たとえば、Microsoft ASN.1 ライブラリにおける既知の脆弱性ではバッファ オーバーフローが発生し、攻撃者は特別に細工した認証パケットを使ってその状態を悪用できます。システムが asn.1 データをデコードするとき、パケット内の exploit コードは、システム レベル特権付きでホスト上で動作したり、DoS 状態を引き起したりすることができます。次のルールは、`asn1` キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|";
nocase; offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length 100,
relative_offset 54;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、ポート 445 を使用する $HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみルールを実行します。その後、ルールは特定の位置にある特定のコンテンツを検査します。最後に、ルールは `asn1` キーワードを使用して、ビットストリング エンコードと二重 ASCII エンコードを検出し、最後に見つかったコンテンツ一致の末尾から 55 バイト目以降、長さ 100 バイトを超える asn.1 タイプ長を識別します（`offset` カウンタがバイト 0 から始まることに注意してください。）

urilen キーワード

`urilen` キーワードと HTTP Inspect プリプロセッサを組み合わせて使用すると、特定の長さ、最大長を下回る、最小長を上回る、または指定された範囲内の URI を HTTP トラフィック内で検査できます。

HTTP Inspectプリプロセッサがパケットを正規化して検査した後、ルールエンジンはルールに照らしてそのパケットを評価し、urilen キーワードで指定された長さ条件に URI が一致するかどうか判断します。このキーワードを使用すると、URI長の脆弱性をエクスプロイトしようとする試みを検出できます。たとえばバッファ オーバーフローを発生させて、攻撃者が DoS 状態を引き起こしたり、システム レベル特権付きでホスト上でコードを実行したりしようと試みる可能性があります。

ルール内で urilen キーワードを使用するときには、次の点に注意してください。

- 必ずflow:establishedキーワードおよび他の1つ以上のキーワードを組み合わせて、urilen キーワードを使用してください。
- ルール プロトコルは常に TCP です。
- ターゲット ポートは常に HTTP ポートです。

URI 長を指定するときには、10 進のバイト数、「小なり」（<）、および「大なり」（>）を使用します。

次に例を示します。

- 5 バイト長の URI を検出するには、5 を指定します。
- 5 バイト長を下回る URI を検出するには、< 5（1 つの空白文字で区切る）を指定します。
- 5 バイト長を上回る URI を検出するには、> 5（1 つの空白文字で区切る）を指定します。
- 3 ～ 5 バイト長の URI を検出するには、3 <> 5（<> の前後に空白文字を 1 つずつ含む）を指定します。

たとえば、Novell の eDirectory バージョン 8.8 に付属のサーバー モニタリングおよび診断ユーティリティ iMonitor バージョン 2.4 に脆弱性があることが知られています。長すぎる URI を含むパケットはバッファ オーバーフローを発生させるため、攻撃者はシステム レベル特権付きでホスト上で動作したり、DoS 状態を引き起こしたりできる特別に細工したパケットを使ってその状態をエクスプロイトできます。次のルールは、urilen キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

上記のルールの場合、任意のポートおよび$EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、$HTTP_PORTS 変数で定義されたポートを使用して、$HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバーへの TCP 接続が確立された時点でのみ、パケットがルールに照らして評価されます。ルールは、urilen キーワードを使用して、長さ 8192 バイトを超える URI を検出します。最後に、ルールはURIを検索して、大文字/小文字を区別しない特定のコンテンツ /nds/ を探します。

関連トピック

侵入ルール ヘッダー プロトコル （2049 ページ）
侵入ルール ヘッダーの送信元および宛先ポート （2053 ページ）
定義済みデフォルト変数 （1409 ページ）

DCE/RPC キーワード

次の表で説明する 3 つの DCE/RPC キーワードを使用して、DCE/RPC セッション トラフィックのエクスプロイトをモニターできます。これらのキーワードを含むルールを処理するとき、システムは DCE/RPC プリプロセッサを呼び出します。

表 *151 : DCE/RPC* キーワード

使用するフィルタ	使用方法	検出対象
`dce_iface`	単独	特定の DCE/RPC サービスを特定するパケット
`dce_opnum`	`dce_iface` の後ろ	特定の DCE/RPC サービス オペレーションを特定するパケット
`dce_stub_data`	`dce_iface` + `dce_opnum` の後ろ	特定の処理要求または応答を定義するスタブ データ

表に示されているように、`dce_opnum` の前に必ず `dce_iface` を配置し、`dce_stub_data` の前に必ず `dce_iface` + `dce_opnum` を配置する必要があることに注意してください。

また、これらの DCE/RPC キーワードを他のルール キーワードと組み合わせて使用することもできます。DCE/RPC ルールでは、**DCE/RPC** の引数が選択された状態で `byte_jump`、`byte_test`、`byte_extract` の各キーワードを使用することに注意してください。

シスコでは、DCE/RPC キーワードを含むルールに 1 つ以上の `content` キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の `content` キーワードが含まれている場合は、`content` キーワードの [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

次のケースでは、DCE/RPC バージョンおよび隣接ヘッダー情報を一致コンテンツとして使用できます。

- ルールに他の `content` キーワードが含まれていない
- ルールにもう 1 つ `content` キーワードが含まれているが、DCE/RPC バージョンおよび隣接情報が、他方の content よりも特有のパターンを表している

  たとえば、DCE/RPC バージョンおよび隣接情報は通常、1 バイトのコンテンツよりも特有です。

次に示すバージョンおよび隣接情報コンテンツ一致のいずれか 1 つを使用して、ルール限定を終了する必要があります。

- コネクション型 DCE/RPC ルールでは、コンテンツ `|05 00 00|`（メジャー バージョン 05、マイナー バージョン 00、および要求 PDU（プロトコル データ ユニット）タイプ 00 ）を使用します。
- コネクションレス型 DCE/RPC ルールでは、コンテンツ `|04 00|`（バージョン 04、要求 PDU タイプ 00）を使用します。

いずれの場合も、DCE/RPC プリプロセッサで完了済みの処理を繰り返すことなく高速パターンマッチ機能を呼び出すために、ルール内の最後のキーワードとしてバージョンおよび隣接情報の `content` キーワードを配置してください。ルールの末尾に配置される `content` キーワードは、高速パターン マッチ機能を呼び出す手段として使われるバージョン コンテンツに当てはまりますが、ルール内の他のコンテンツ一致には必ずしも当てはまらないことに注意してください。

関連トピック

DCE/RPC プリプロセッサ （2768 ページ）
content キーワードと protected_content キーワード （2072 ページ）
content キーワードの高速パターン マッチ機能の引数 （2083 ページ）
概要：byte_jump および byte_test キーワード
byte_extract キーワード （2092 ページ）

dce_iface

`dce_iface` キーワードを使用すると、特定の DCE/RPC サービスを識別できます。

オプションで、`dce_iface` キーワードを `dce_opnum` キーワードおよび `dce_stub_data` キーワードと組み合わせて使用すると、検査する DCE/RPC トラフィックをさらに限定することができます。

固定型 16 バイト Universally Unique Identifier（UUID）は、それぞれの DCE/RPC サービスに割り当てられるアプリケーション インターフェイスを識別します。たとえば、UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 は、srvsvc サービスとしても知られる DCE/RPC lanmanserver サービスを識別します。このサービスは、ピアツーピア プリンタ、ファイル、および SMB 名前付きパイプを共有するためのさまざまな管理機能を提供します。DCE/RPC プリプロセッサは UUID および関連する見出し値を使用して DCE/RPC セッションを追跡します。

インターフェイス UUID は、次のように、ハイフンで区切られた 5 つの 16 進文字列で構成されます。

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

次に示す netlogon インターフェイスの UUID のように、ハイフンを含む UUID 全体を入力することで、インターフェイスを指定します。

```
12345678-1234-abcd-ef00-01234567cffb
```

UUID 内の最初の 3 つの文字列はビッグ エンディアン バイト順で指定される必要があることに注意してください。通常、公開されたインターフェイス リストやプロトコル アナライザには UUID が正しいバイト順で表示されますが、それを入力する前に UUID バイト順を変更しなけ

ればならない場合もあります。次に示すメッセンジャー サービス UUID の場合、リトル エンディアン バイト順の最初の 3 つの文字列を含む未加工 ASCII テキストで表示されることがあります。

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

この同じ UUID を `dce_iface` キーワードに指定するには、次のようにハイフンを挿入し、最初の 3 つの文字列をビッグ エンディアン バイト順で配置できます。

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

1 つの DCE/RPC セッションに複数のインターフェイスへの要求を含めることができますが、1 つのルールには 1 つの `dce_iface` キーワードだけを含めてください。追加のインターフェイスを検出するには、追加のルールを作成します。

DCE/RPC アプリケーション インターフェイスにはインターフェイス バージョン番号も割り当てられます。オプションで、インターフェイス バージョンを指定できます。その際、バージョンが指定値に等しい、等しくない、指定値より小さい、または大きいことを示す演算子を使用します。

TCP セグメンテーションや IP フラグメンテーションに加えて、コネクション型とコネクションレス型の両方の DCE/RPC をフラグメント化することができます。通常、先頭以外の DCE/RPC フラグメントを指定のインターフェイスに関連付けるのはあまり効率的ではありません。このようにすると、多数の誤検出が発生する可能性があります。ただし、柔軟性を維持するために、オプションで、指定されたインターフェイスに照らしてすべてのフラグメントを評価できます。

次の表に、`dce_iface` キーワードの引数を要約します。

表 *152*：*dce_iface* の引数

引数	説明
Interface UUID	DCE/RPC トラフィック内で検出対象となる特定のサービスのアプリケーション インターフェイスを識別する、ハイフンを含む UUID。指定されたインターフェイスに関連付けられた任意の要求がインターフェイス UUID に一致します。
バージョン	オプションで、アプリケーション インターフェイス バージョン番号 0 ～ 65535 と、検出対象のバージョンが指定値より大きい（>）、小さい（<）、等しい（=）、または等しくない（!）を示す演算子。
All Fragments	オプションで、関連するすべての DCE/RPC フラグメント内のインターフェイスの照合、およびインターフェイス バージョン（指定されている場合）での照合を有効にします。この引数はデフォルトで無効になっています。これは、最初のフラグメントまたはフラグメント化されていないパケット全体が指定のインターフェイスに関連付けられている場合にのみ、キーワードが一致することを意味します。この引数を有効にすると、誤検出が発生する可能性があることに注意してください。

dce_opnum キーワード

dce_opnum キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、DCE/RPC サービスが提供する 1 つ以上の特定のオペレーションを識別するパケットを検出できます。

クライアント関数呼び出しは、DCE/RPC 仕様で「オペレーション」と呼ばれる特定のサービス関数を要求します。オペレーション番号（opnum）はDCE/RPCヘッダー内の特定のオペレーションを識別します。エクスプロイトは特定のオペレーションを標的にすることがあります。

たとえばUUID 12345678-1234-abcd-ef00-01234567cffb は、数十種類のオペレーションを提供する netlogon サービスのインターフェイスを識別します。その 1 つがオペレーション 6（NetrServerPasswordSet オペレーション）です。

オペレーション用のサービスを識別するには、dce_opnum キーワードの前に dce_iface キーワードを指定する必要があります。

特定のオペレーションを示す1 つの 10 進数値（0 ～ 65535 の範囲）、ハイフンで区切られたオペレーション範囲、またはカンマ区切りのオペレーション/範囲リストを任意の順序で指定できます。

次の例は、すべて有効な netlogon オペレーション番号を表しています。

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data キーワード

dce_stub_data キーワードをDCE/RPCプリプロセッサと組み合わせて使用すると、他のルールオプションとは無関係に、スタブ データの先頭からインスペクションを開始するようルールエンジンに指示できます。dce_stub_data キーワードの後に続くパケット ペイロードルール オプションは、スタブ データ バッファを基準にして適用されます。

DCE/RPC スタブ データは、クライアント プロシージャ コールと DCE/RPC ランタイム システム（DCE/RPC の中核をなすルーチンとサービスを提供するメカニズム）の間のインターフェイスを提供します。DCE/RPCエクスプロイトは、DCE/RPCパケットのスタブ データ部分で識別されます。スタブデータは特定のオペレーションまたは関数呼び出しに関連付けられているため、必ず dce_stub_data の前に dce_iface と dce_opnum を指定して、関連するサービスとオペレーションを識別してください。

dce_stub_data キーワードには引数がありません。

SIP キーワード

4 つの SIP キーワードを使用すると、SIP セッション トラフィックでエクスプロイトを監視できます。

SIP プロトコルはサービス拒否（DoS）攻撃に対して脆弱であることに注意してください。このような攻撃に対処するルールでは、レート ベースの攻撃防御を活用できます。

sip_header キーワード

sip_header キーワードを使用すると、抽出された SIP 要求または応答ヘッダーの先頭から検査を開始し、検査対象をヘッダー フィールドに限定することができます。

sip_header キーワードには引数がありません。

次の例のルール フラグメントは SIP ヘッダーを指し示し、CSeq ヘッダー フィールドに一致します。

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

関連トピック

動的侵入ルール状態 （2040 ページ）
レート ベースの攻撃防御 （2921 ページ）

sip_body キーワード

sip_body キーワードを使用すると、抽出された SIP 要求または応答メッセージ本文の先頭から検査を開始し、検査対象をメッセージ本文に限定することができます。

sip_body キーワードには引数がありません。

次の例のルール フラグメントは SIP メッセージ本文を指し示し、抽出された SDP データの c（接続情報）フィールド内の特定の IP アドレスに一致します。

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

ルールが SDP コンテンツの検索だけに限定されないことに注意してください。SIP プリプロセッサはメッセージ本文全体を抽出し、それをルール エンジンで使用できるようにします。

sip_method キーワード

各 SIP 要求内の *method* フィールドは要求の目的を識別します。sip_method キーワードを使用すると、SIP 要求の中で特定のメソッドを検査することができます。複数のメソッドはカンマで区切ります。

次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。複数のメソッドをカンマで区切ることができます。

今後、新しいSIPメソッドが定義される可能性があるため、カスタムメソッド、つまり現在定義されているSIPメソッド以外のメソッドを指定することもできます。可能なフィールド値はRFC 2616で定義されています。=、(、) などの制御文字と区切り文字を除いて、すべての文字を使用できます。除外されている区切り文字の完全なリストについては、RFC 2616 を参照してください。指定されたカスタムメソッドがトラフィックで検出されると、システムはパケット ヘッダーを検査しますが、メッセージは検査されません。

現在定義されている 21 個のメソッドと追加の 11 個のメソッドを含む、最大 32 個のメソッドがシステムでサポートされます。未定義のメソッドを設定した場合、システムはそれを無視します。合計 32 個のメソッドには、SIP プリプロセッサのオプション [検査するメソッド（Methods to Check）] を使って指定されるメソッドが含まれることに注意してください。

否定を使用する場合は、1 つのメソッドだけを指定できます。次に例を示します。

```
!invite
```

ただし、1 つのルール内の複数の `sip_method` キーワードが **AND** 演算で結合されることに注意してください。たとえば、`invite` と `cancel` を除くすべての抽出されたメソッドを検査するには、次のような 2 つの除外付き `sip_method` キーワードを使用します。

```
sip_method: !invite
sip_method: !cancel
```

Cisco では、`sip_method` キーワードを含むルールに 1 つ以上の `content` キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の `content` キーワードが含まれている場合は、`content` キーワードの [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

関連トピック

SIP プリプロセッサのオプション （2819 ページ）
content キーワードと protected_content キーワード （2072 ページ）
content キーワードの高速パターン マッチ機能の引数 （2083 ページ）

sip_stat_code キーワード

各 SIP 応答内の 3 桁のステータス コードは、要求されたアクションの結果を示します。`sip_stat_code` キーワードを使用すると、SIP 応答の中で特定のステータス コードを検査することができます。

1 桁の応答タイプ番号 1 ～ 9、特定の 3 桁の番号 100 ～ 999、またはこれらを任意に組み合わせたカンマ区切りリストを指定できます。リスト内のいずれか 1 つの番号が SIP 応答内のコードに一致する場合、そのリストが一致します。

次の表に、指定可能な SIP ステータス コード値の説明を示します。

表 *153 : sip_stat_code* の値

検出対象	指定する内容	例	検出結果
1 つの特定のステータス コード	3 桁のステータス コード	189	189
指定された 1 桁で始まる 3 桁のコード	1 桁	1	1xx、つまり 100、101、102 など

検出対象	指定する内容	例	検出結果
値のリスト	特定のコードおよび 1 桁を任意に組み合わせてカンマで区切る	222, 3	222 および 300、301、302 など

また、ルールに content キーワードが含まれているかどうかに関係なく、sip_stat_code キーワードを使って指定された値を検索するためにルール エンジンが高速パターン マッチ機能を使用しないことにも注意してください。

GTP キーワード

3 つの GSRP トンネリング プロトコル（GTP）キーワードを使用すると、GTP バージョン、メッセージタイプ、および情報要素をコマンドチャネル内で検査できます。contentやbyte_jumpなどの他の侵入ルール キーワードと組み合わせて GTP キーワードを使用することはできません。gtp_info または gtp_type キーワードを使用するそれぞれのルールで、gtp_version キーワードを使用する**必要があります**。

gtp_version キーワード

gtp_version キーワードを使用すると、GTP 制御メッセージの中で GTP バージョン 0、1、または 2 を検査することができます。

定義されているメッセージタイプと情報要素はGTPバージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、gtp_version を使用する必要があります。値として 0、1、または 2 を指定できます。

gtp_type キーワード

それぞれの GTP メッセージは、数値と文字列で構成されるメッセージ タイプによって識別されます。gtp_type キーワードを使用すると、特定の GTP メッセージ タイプのトラフィックを検査できます。定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、gtp_version も使用する必要があります。

次の例に示すように、メッセージ タイプとして定義済みの 10 進数値、定義済み文字列、あるいはどちらか（または両方）を任意に組み合わたカンマ区切りリストを指定できます。

```
10, 11, echo_request
```

リスト内のそれぞれの値または文字列を照合するとき、システムは OR 演算を使用します。値と文字列を列挙する順序は重要ではありません。リスト内のいずれか1つの値または文字列の一致により、キーワードが一致します。認識されない文字列または範囲外の値を含むルールを保存しようとすると、エラーが発生します。

表に示されているように、GTP バージョンに応じて、同じメッセージ タイプの値が異なる場合があることに注意してください。たとえば sgsn_context_request メッセージ タイプの値は GTPv0 と GTPv1 では 50 ですが、GTPv2 では 130 です。

パケット内のバージョン番号に応じて、gtp_type キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードがメッセージ タイプ値 50 と一致しますが、GTPv2 パケットでは値 130 と一致します。パケット内のメッセージ タイプ値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

メッセージタイプに整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP メッセージ タイプごとにシステムで認識される定義済みの値と文字列を示します。

表 *154 : GTP* メッセージ タイプ

値	バージョン 0	バージョン 1	バージョン 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	該当なし
5	node_alive_response	node_alive_response	該当なし
6	redirection_request	redirection_request	該当なし
7	redirection_response	redirection_response	なし
16	create_pdp_context_request	create_pdp_context_request	該当なし
17	create_pdp_context_response	create_pdp_context_response	該当なし
	update_pdp_context_request	update_pdp_context_request	該当なし
19	update_pdp_context_response	update_pdp_context_response	該当なし
20	delete_pdp_context_request	delete_pdp_context_request	該当なし
21	delete_pdp_context_response	delete_pdp_context_response	該当なし
22	create_aa_pdp_context_request	init_pdp_context_activation_request	該当なし
23	create_aa_pdp_context_response	init_pdp_context_activation_response	-
24	delete_aa_pdp_context_request	N/A	なし
25	delete_aa_pdp_context_response	N/A	なし
26	error_indication	error_indication	該当なし

値	バージョン 0	バージョン 1	バージョン 2
27	pdu_notification_request	pdu_notification_request	なし
36	pdu_notification_response	pdu_notification_response	該当なし
29	pdu_notification_reject_request	pdu_notification_reject_request	該当なし
30	pdu_notification_reject_response	pdu_notification_reject_response	該当なし
31	該当なし	supported_ext_header_notification	該当なし
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	N/A	なし	change_notification_request
39	N/A	なし	change_notification_response
48	identification_request	identification_request	該当なし
49	identification_response	identification_response	該当なし
50	sgsn_context_request	sgsn_context_request	該当なし
51	sgsn_context_response	sgsn_context_response	該当なし
52	sgsn_context_ack	sgsn_context_ack	該当なし
53	該当なし	forward_relocation_request	該当なし
54	該当なし	forward_relocation_response	該当なし
55	該当なし	forward_relocation_complete	なし
56	該当なし	relocation_cancel_request	該当なし
57	該当なし	relocation_cancel_response	該当なし
58	該当なし	forward_srns_contex	該当なし
59	該当なし	forward_relocation_complete_ack	なし
60	該当なし	forward_srns_contex_ack	該当なし

値	バージョン 0	バージョン 1	バージョン 2
64	N/A	なし	modify_bearer_command
65	N/A	なし	modify_bearer_failure_indication
66	N/A	なし	delete_bearer_command
67	N/A	なし	delete_bearer_failure_indication
68	N/A	なし	bearer_resource_command
69	N/A	なし	bearer_resource_failure_indication
70	該当なし	ran_info_relay	downlink_failure_indication
71	N/A	なし	trace_session_activation
72	N/A	なし	trace_session_deactivation
73	N/A	なし	stop_paging_indication
95	N/A	なし	create_bearer_request
96	該当なし	mbms_notification_request	create_bearer_response
97	該当なし	mbms_notification_response	update_bearer_request
98	該当なし	mbms_notification_reject_request	update_bearer_response
99	該当なし	mbms_notification_reject_response	delete_bearer_request
100	該当なし	create_mbms_context_request	delete_bearer_response
101	該当なし	create_mbms_context_response	delete_pdn_request
102	該当なし	update_mbms_context_request	delete_pdn_response
103	該当なし	update_mbms_context_response	該当なし
104	該当なし	delete_mbms_context_request	該当なし
105	該当なし	delete_mbms_context_response	該当なし
112	該当なし	mbms_register_request	該当なし
113	該当なし	mbms_register_response	該当なし
114	該当なし	mbms_deregister_request	該当なし
115	該当なし	mbms_deregister_response	該当なし
116	該当なし	mbms_session_start_request	該当なし

値	バージョン 0	バージョン 1	バージョン 2
117	該当なし	mbms_session_start_response	該当なし
118	該当なし	mbms_session_stop_request	該当なし
119	該当なし	mbms_session_stop_response	該当なし
120	該当なし	mbms_session_update_request	該当なし
121	該当なし	mbms_session_update_response	なし
128	該当なし	ms_info_change_request	identification_request
129	該当なし	ms_info_change_response	identification_response
130	N/A	なし	sgsn_context_request
131	N/A	なし	sgsn_context_response
132	N/A	なし	sgsn_context_ack
133	N/A	なし	forward_relocation_request
134	N/A	なし	forward_relocation_response
135	N/A	なし	forward_relocation_complete
136	N/A	なし	forward_relocation_complete_ack
137	N/A	なし	forward_access
138	N/A	なし	forward_access_ack
139	N/A	なし	relocation_cancel_request
140	N/A	なし	relocation_cancel_response
141	N/A	なし	configuration_transfer_tunnel
149	N/A	なし	detach
150	N/A	なし	detach_ack
151	N/A	なし	cs_paging
152	N/A	なし	ran_info_relay
153	N/A	なし	alert_mme
154	N/A	なし	alert_mme_ack
155	N/A	なし	ue_activity

値	バージョン 0	バージョン 1	バージョン 2
156	N/A	なし	ue_activity_ack
160	N/A	なし	create_forward_tunnel_request
161	N/A	なし	create_forward_tunnel_response
162	N/A	なし	suspend
163	N/A	なし	suspend_ack
164	N/A	なし	resume
165	N/A	なし	resume_ack
166	N/A	なし	create_indirect_forward_tunnel_request
167	N/A	なし	create_indirect_forward_tunnel_response
168	N/A	なし	delete_indirect_forward_tunnel_request
169	N/A	なし	delete_indirect_forward_tunnel_response
170	N/A	なし	release_access_bearer_request
171	N/A	なし	release_access_bearer_response
176	N/A	なし	downlink_data
177	N/A	なし	downlink_data_ack
179	N/A	なし	pgw_restart
180	N/A	なし	pgw_restart_ack
200	N/A	なし	update_pdn_request
201	N/A	なし	update_pdn_response
211	N/A	なし	modify_access_bearer_request
212	N/A	なし	modify_access_bearer_response
231	N/A	なし	mbms_session_start_request
232	N/A	なし	mbms_session_start_response
233	N/A	なし	mbms_session_update_request
234	N/A	なし	mbms_session_update_response
235	N/A	なし	mbms_session_stop_request

値	バージョン 0	バージョン 1	バージョン 2
236	N/A	なし	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	該当なし
241	data_record_transfer_response	data_record_transfer_response	該当なし
254	該当なし	end_marker	該当なし
255	pdu	pdu	N/A

gtp_info キーワード

1 つの GTP メッセージには多数の情報要素が含まれることがあり、それぞれの要素は定義済み数値および定義済み文字列によって識別されます。`gtp_info` キーワードを使用すると、指定された情報要素の先頭から検査を開始し、検査対象を指定の情報要素に限定することができます。定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、このキーワードを使用するときには、`gtp_version` も使用する必要があります。

情報要素に対して定義された 10 進数値と定義された文字列のどちらでも指定できます。単一の値または文字列を指定することも、1 つのルール内で複数の `gtp_info` キーワードを使って複数の情報要素を検査することもできます。

1 つのメッセージに同じタイプの複数の情報要素が含まれている場合は、すべてが照合対象として検査されます。情報要素が無効な順序で出現する場合は、最後のインスタンスだけが検査されます。

GTP バージョンに応じて、同じ情報要素の値が異なる場合があることに注意してください。たとえば `cause` 情報要素の値は GTPv0 と GTPv1 では 1 ですが、GTPv2 では 2 です。

パケット内のバージョン番号に応じて、`gtp_info` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードが情報要素値 1 と一致しますが、GTPv2 パケットでは値 2 と一致します。パケット内の情報要素値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

情報要素に整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP 情報要素ごとにシステムで認識される値と文字列を示します。

表 *155 : GTP* 情報要素

値	バージョン 0	バージョン 1	バージョン 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	復旧
4	tlli	tlli	該当なし

値	バージョン 0	バージョン 1	バージョン 2
5	p_tmsi	p_tmsi	該当なし
6	qos	N/A	なし
8	recording_required	recording_required	該当なし
9	authentication	authentication	該当なし
11	map_cause	map_cause	該当なし
12	p_tmsi_sig	p_tmsi_sig	該当なし
13	ms_validated	ms_validated	該当なし
18	復旧	復旧	該当なし
15	selection_mode	selection_mode	なし
16	flow_label_data_1	teid_1	該当なし
17	flow_label_signalling	teid_control	該当なし
	flow_label_data_2	teid_2	該当なし
19	ms_unreachable	teardown_ind	該当なし
20	該当なし	nsapi	該当なし
21	該当なし	ranap	該当なし
22	該当なし	rab_context	該当なし
23	該当なし	radio_priority_sms	-
24	N/A	radio_priority	該当なし
25	該当なし	packet_flow_id	該当なし
26	該当なし	charging_char	該当なし
27	該当なし	trace_ref	なし
36	該当なし	trace_type	該当なし
29	該当なし	ms_unreachable	該当なし
71	N/A	なし	apn
72	N/A	なし	ambr
73	N/A	なし	ebi

値	バージョン 0	バージョン 1	バージョン 2
74	N/A	なし	ip_addr
75	N/A	なし	mei
76	N/A	なし	msisdn
77	N/A	なし	indication
78	N/A	なし	pco
79	N/A	なし	paa
80	N/A	なし	bearer_qos
80	N/A	なし	flow_qos
82	N/A	なし	rat_type
83	N/A	なし	serving_network
84	N/A	なし	bearer_tft
85	N/A	なし	tad
86	N/A	なし	uli
87	N/A	なし	f_teid
88	N/A	なし	tmsi
89	N/A	なし	cn_id
90	N/A	なし	s103pdf
91	N/A	なし	s1udf
92	N/A	なし	delay_value
93	N/A	なし	bearer_context
94	N/A	なし	charging_id
95	N/A	なし	charging_char
96	N/A	なし	trace_info
97	N/A	なし	bearer_flag
99	N/A	なし	pdn_type
100	N/A	なし	pti

値	バージョン 0	バージョン 1	バージョン 2
101	N/A	なし	drx_parameter
103	N/A	なし	gsm_key_tri
104	N/A	なし	umts_key_cipher_quin
105	N/A	なし	gsm_key_cipher_quin
106	N/A	なし	umts_key_quin
107	N/A	なし	eps_quad
108	N/A	なし	umts_key_quad_quin
109	N/A	なし	pdn_connection
110	N/A	なし	pdn_number
111	N/A	なし	p_tmsi
112	N/A	なし	p_tmsi_sig
113	N/A	なし	hop_counter
114	N/A	なし	ue_time_zone
115	N/A	なし	trace_ref
116	N/A	なし	complete_request_msg
117	N/A	なし	guti
118	N/A	なし	f_container
119	N/A	なし	f_cause
120	N/A	なし	plmn_id
121	N/A	なし	target_id
123	N/A	なし	packet_flow_id
124	N/A	なし	rab_contex
125	N/A	なし	src_rnc_pdcp
126	N/A	なし	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode

値	バージョン 0	バージョン 1	バージョン 2
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	該当なし
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	該当なし	qos	node_type
136	該当なし	authentication_qu	fqdn
137	該当なし	tft	ti
138	該当なし	target_id	mbms_session_duration
139	該当なし	utran_trans	mbms_service_area
140	該当なし	rab_setup	mbms_session_id
141	該当なし	ext_header	mbms_flow_id
142	該当なし	trigger_id	mbms_ip_multicast
143	該当なし	omc_id	mbms_distribution_ack
144	該当なし	ran_trans	rfsp_index
145	該当なし	pdp_context_pri	uci
146	該当なし	addi_rab_setup	csg_info
147	該当なし	sgsn_number	csg_id
148	該当なし	common_flag	cmi
149	該当なし	apn_restriction	service_indicator
150	該当なし	radio_priority_lcs	detach_type
151	該当なし	rat_type	ldn
152	該当なし	user_loc_info	node_feature
153	該当なし	ms_time_zone	mbms_time_to_transfer
154	該当なし	imei_sv	throttling

値	バージョン 0	バージョン 1	バージョン 2
155	該当なし	camel	arp
156	該当なし	mbms_ue_context	epc_timer
157	該当なし	tmp_mobile_group_id	signalling_priority_indication
158	該当なし	rim_routing_addr	tmgi
159	該当なし	mbms_config	mm_srvcc
160	該当なし	mbms_service_area	flags_srvcc
161	該当なし	src_rnc_pdcp	nmbr
162	該当なし	addi_trace_info	該当なし
163	該当なし	hop_counter	該当なし
164	該当なし	plmn_id	該当なし
165	該当なし	mbms_session_id	該当なし
166	該当なし	mbms_2g3g_indicator	該当なし
167	該当なし	enhanced_nsapi	該当なし
168	該当なし	mbms_session_duration	該当なし
169	該当なし	addi_mbms_trace_info	該当なし
170	該当なし	mbms_session_repetition_num	該当なし
171	該当なし	mbms_time_to_data	該当なし
173	該当なし	bss	該当なし
174	該当なし	cell_id	該当なし
175	該当なし	pdu_num	該当なし
177	該当なし	mbms_bearer_capab	該当なし
178	該当なし	rim_routing_disc	該当なし
179	該当なし	list_pfc	該当なし
180	該当なし	ps_xid	該当なし
181	該当なし	ms_info_change_report	該当なし
182	該当なし	direct_tunnel_flags	該当なし

値	バージョン 0	バージョン 1	バージョン 2
183	該当なし	correlation_id	該当なし
184	該当なし	bearer_control_mode	該当なし
185	該当なし	mbms_flow_id	該当なし
186	該当なし	mbms_ip_multicast	該当なし
187	該当なし	mbms_distribution_ack	該当なし
188	該当なし	reliable_inter_rat_handover	該当なし
189	該当なし	rfsp_index	該当なし
190	該当なし	fqdn	該当なし
191	該当なし	evolved_allocation1	該当なし
192	N/A	evolved_allocation2	該当なし
193	該当なし	extended_flags	該当なし
194	該当なし	uci	該当なし
195	該当なし	csg_info	該当なし
196	該当なし	csg_id	該当なし
197	該当なし	cmi	該当なし
198	該当なし	apn_ambr	該当なし
199	該当なし	ue_network	該当なし
200	該当なし	ue_ambr	該当なし
201	該当なし	apn_ambr_nsapi	該当なし
202	該当なし	ggsn_backoff_timer	該当なし
203	該当なし	signalling_priority_indication	該当なし
204	該当なし	signalling_priority_indication_nsapi	該当なし
205	該当なし	high_bitrate	該当なし
206	該当なし	max_mbr	該当なし
251	charging_gateway_addr	charging_gateway_addr	該当なし
255	private_extension	private_extension	private_extension

SCADA キーワード

ルールエンジンは Modbus、DNP3、CIP、および S7Commplus のルールを使用して特定のプロトコルフィールドにアクセスします。

Modbus キーワード

Modbus キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせて使用することもできます。

modbus_data

`modbus_data` キーワードを使用すると、Modbus 要求または応答内の [Data] フィールドの先頭を指し示すことができます。

modbus_func

`modbus_func` キーワードを使用すると、Modbus アプリケーション層要求または応答見出し内の [Function Code（機能コード）] フィールドを照合できます。Modbus 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、Modbus機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 *156 : Modbus* 機能コード

値	文字列
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
	report_slave_id

値	文字列
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

modbus_unit

modbus_unit キーワードを使用すると、Modbus 要求または応答ヘッダー内の [Unit ID] フィールドで 1 つの 10 進数値を照合できます。

DNP3 キーワード

DNP3 キーワードを単独で使用することも、content や byte_jump など他のキーワードと組み合わせて使用することもできます。

dnp3_data

dnp3_data キーワードを使用すると、再構築された DNP3 アプリケーション層フラグメントの先頭を指し示すことができます。

DNP3 プリプロセッサが、リンク層フレームをアプリケーション層フラグメントに再構築します。dnp3_data キーワードは、各アプリケーション層フラグメントの先頭を指し示します。他のルール オプションは、16 バイトごとにデータを分離してチェックサムを追加せずに、フラグメント内の再構築されたデータを照合することができます。

dnp3_func

dnp3_func キーワードを使用すると、DNP3 アプリケーション層要求または応答ヘッダー内の [機能コード（Function Code）] フィールドを照合できます。DNP3 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、DNP3 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 *157 : DNP3* 機能コード

値	文字列
0	confirm
1	read
2	write

値	文字列
3	select
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
	start_appl
	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file

値	文字列
31	activate_config
32	authenticate_req
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

dnp3_ind

`dnp3_ind` キーワードを使用すると、DNP3 アプリケーション層応答ヘッダー内の [Internal Indications] フィールド内のフラグを照合できます。

1 つの既知のフラグ、または次の例のようなカンマ区切りのフラグ リストを示す文字列を指定できます。

```
class_1_events, class_2_events
```

複数のフラグを指定した場合、キーワードはリスト内の任意のフラグと一致します。いくつかのフラグの組み合わせを検出するには、1 つのルール内で `dnp3_ind` キーワードを複数回使用します。

定義済みの DNP3 内部通知フラグとしてシステムによって認識される文字列構文を以下に示します。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

dnp3_obj

`dnp3_obj` キーワードを使用すると、要求または応答内の DNP3 オブジェクト ヘッダーを照合できます。

DNP3 データは、アナログ入力やバイナリ入力など、さまざまなタイプの一連の DNP3 オブジェクトで構成されます。各タイプは、それぞれ 10 進数値で識別されるグループ を使って区別されます（アナログ入力グループ、バイナリ入力グループなど）。各グループ内のオブジェクト

は、それぞれオブジェクト データ形式を指定するオブジェクト バリエーション によってさらに区別されます（16 ビット整数、32 ビット整数、短精度浮動小数点など）。また、オブジェクト バリエーションの各タイプは 10 進数値でも識別可能です。

オブジェクト 見出しを識別する際には、オブジェクト 見出し グループのタイプを示す 10 進数値とオブジェクト バリエーションのタイプを示す 10 進数値を指定します。この 2 つの組み合わせによって DNP3 オブジェクトの特定のタイプが定義されます。

CIP および ENIP のキーワード

次のキーワードを単体でまたは組み合わせて使用すると、CIP プリプロセッサで検出された CIP および ENIP トラフィックに対する攻撃を識別するカスタム侵入ルールを作成できます。設定可能なキーワードについては、許容範囲内の単一の整数を指定します。詳細については、CIP プリプロセッサ （2857 ページ）を参照してください。

表 *158*：

対象キーワード	照合先	範囲
`cip_attribute`	CIP メッセージの [オブジェクト クラス/インスタンス属性（Object Class/Instance Attribute）] フィールド。定義された 1 つの整数値を指定します。	0 ～ 65535
`cip_class`	CIP メッセージの [オブジェクト クラス（Object Class）] フィールド。定義された 1 つの整数値を指定します。	0 ～ 65535
`cip_conn_path_class`	接続パスのオブジェクト クラス。1 つの整数値を指定します。	0 ～ 65535
`cip_instance`	CIP メッセージの [インスタンス ID（Instance ID）] フィールド。1 つの整数値を指定します。	0 ～ 4284927295
`cip_req`	サービス要求メッセージ。	該当なし
`cip_rsp`	サービス応答メッセージ。	該当なし
`cip_service`	CIP サービス要求メッセージの [サービス（Service）] フィールド。1 つの整数値を指定します。	0 ～ 127
`cip_status`	CIP サービス応答メッセージの [ステータス（Status）] フィールド。1 つの整数値を指定します。	0 ～ 255
`enip_command`	EthNet/IP ヘッダーのコマンド コード。1 つの整数値を指定します。	0 ～ 65535

対象キーワード	照合先	範囲
enip_req	EthNet/IP 要求メッセージ。	該当なし
enip_rsp	EthNet/IP 応答メッセージ。	N/A

S7Commplus キーワード

S7Commplusプリプロセッサが検出したトラフィックに対する攻撃を識別するカスタム侵入ルールを作成するには、S7Commplus キーワードを単体で使用するか、または組み合わせて使用します。設定可能なキーワードについては、許容範囲内の既知の単一の値か、または単一の整数を指定します。詳細については、「S7Commplusプリプロセッサ（2862ページ）」を参照してください。

次の点に注意してください。

- 同じルール内の複数の S7commplus キーワードは、AND 演算されます。
- 同じルールで複数の `s7commplus_func` キーワードまたは `s7commplus_opcode` キーワードを使用すると、ルールが無効になり、トラフィックに一致しなくなります。これらのキーワードで複数の値を検索するには、複数のルールを作成します。

s7commplus_content

S7Commplus侵入ルールで `content` キーワードまたは `protected_content` キーワードを使用する前に、`s7commplus_content` キーワードを使用して、カーソルをパケットペイロードの先頭に配置します。詳細については、content キーワードと protected_content キーワード（2072 ページ）を参照してください。

s7commplus_func

`s7commplus_func` キーワードを使用して、S7Commplus ヘッダー内の次の値の 1 つと照合します。

- explore
- createobject
- deleteobject
- setvariable
- getlink
- setmultivar
- getmultivar
- beginsequence
- endsequence
- invoke

- getvarsubstr
- 0x0 ～ 0xFFF

  数式では追加の値を使用できることに注意してください。

s7commplus_opcode

s7commplus_opcode キーワードを使用して、S7Commplus ヘッダー内の次の値の 1 つと照合します。

- request
- response
- 通知
- response2
- 0x0 ～ 0xFF

  数式では追加の値を使用できることに注意してください。

パケット特性

特定のパケット特性を持つパケットに対してのみイベントを生成するルールを作成できます。

dsize

dsize キーワードはパケット ペイロード サイズを検査します。「大なり」演算子と「小なり」演算子（<、>）を使って値の範囲を指定することができます。次の構文をに従って範囲を指定できます。

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

たとえば、400 バイトを超えるパケット サイズを指定するには、dtype 値として >400 を使用します。500 バイト未満のパケット サイズを指定するには、<500 を使用します。400 ～ 500 バイトのパケットに対してルールをトリガーとして使用するよう指定するには、400<>500 を使用します。

⚠

注意 dsize キーワードは、プリプロセッサによってデコードされる前のパケットを検査します。

isdataat

isdataat キーワードは、ペイロード内の特定の位置にデータが存在することを確認するよう、ルール エンジンに指示します。

次の表に、isdataat キーワードで使用可能な引数を列挙します。

表 *159 : isdataat* の引数

引数	タイプ	説明
Offset	必須	ペイロード内の特定の位置。たとえば、パケット ペイロード内のバイト位置 50 にデータが出現することを検査するには、オフセット値として `50` を指定します。`!` 修飾子は `isdataat` 検査の結果を否定します。特定量のデータがペイロードに存在しない場合は警告が出されます。 また、既存の `byte_extract` 変数または `byte_math` 結果を使用してこの引数の値を指定することもできます。
Relative	任意	最後に見つかったコンテンツ一致を基準にして相対的な位置を計算します。相対位置を指定する場合は、カウンタがバイト 0 から始まることに注意してください。最後に見つかったコンテンツ一致から順方向に移動するバイト数から 1 を差し引いて位置を計算します。たとえば、最後に見つかったコンテンツ一致から 9 バイト後にデータが出現すべきことを指定するには、相対オフセットとして `8` を指定します。
Raw Data	オプション	Firepower システム プリプロセッサによるデコードやアプリケーション層の正規化が行われる前の、元のパケット ペイロードにデータが配置されていることを指定します。前のコンテンツ一致が未加工パケット データ内に存在していた場合は、この引数を **Relative** と一緒に使用できます。

たとえば、`foo` というコンテンツを検索するルールで `isdataat` の値が次のように指定される場合、

- Offset = !10
- Relative = enabled

ルール エンジンが `foo` の後ろからペイロード末尾までに 10 バイトを検出しない場合、システムは警告を出します。

sameip

`sameip` キーワードは、パケットの送信元 IP アドレスと宛先 IP アドレスが同じであることを検査します。このキーワードは引数を受け入れません。

fragoffset

`fragoffset` キーワードは、フラグメント化されたパケットのオフセットを検査します。一部の exploit（WinNuke サービス拒否攻撃など）では、特定のオフセットを持つ手動生成されたパケット フラグメントが使われるため、このキーワードが役立ちます。

たとえば、フラグメント化されたパケットのオフセットが 31337 バイトかどうかを検査するには、`fragoffset` 値として `31337` を指定します。

`fragoffset` キーワードの引数を指定するときには、次の演算子を使用できます。

表 *160 : fragoffset* キーワードの引数演算子

演算子	説明
!	not
>	より大きい
<	より小さい

否定（!）演算子を < や > と組み合わせて使用できないことに注意してください。

cvs

cvs キーワードは、Concurrent Versions System（CVS）トラフィック内で不正な形式の CVS エントリを検査します。攻撃者は不正な形式のエントリを使用して、ヒープ オーバーフローを強制的に発生させ、CVS サーバー上で有害コードを実行することができます。このキーワードを使用すると、2 つの既知の CVS 脆弱性 CVE-2004-0396（CVS 1.11.x ～ 1.11.15 と 1.12.x ～ 1.12.7）および CVS-2004-0414（CVS 1.12.x ～ 1.12.8 と 1.11.x ～ 1.11.16）に対する攻撃を識別できます。cvs キーワードは、正しい形式のエントリであることを検査して、不正な形式のエントリが検出された場合はアラートを生成します。

CVS が動作するポートをルールに含める必要があります。さらに、トラフィックが発生する可能性のあるポートを TCP ポリシー内のストリーム再構築用のポート リストに追加することで、CVS セッションの状態を保持できるようにする必要があります。ストリーム再構築が行われるクライアント ポートのリストには、TCP ポート 2401（pserver）と 514（rsh）が含まれています。ただし、サーバーが xinetd サーバー（つまり pserver）として動作する場合は、任意の TCP ポート上で動作できることに注意してください。すべての非標準ポートを、ストリーム再構築の [クライアント ポート（Client Ports）] リストに追加します。

関連トピック

byte_extract キーワード （2092 ページ）
TCP ストリームのプリプロセス オプション （2895 ページ）

アクティブ応答のキーワード

resp キーワードおよび **react** キーワードにより、2 つの方法でアクティブ応答を開始できます。パケットがどちらかのキーワードを含む侵入ルールをトリガーとして使用すると、その侵入ルールにより、1 つのアクティブ応答が開始します。アクティブ応答のキーワードは、トリガーとして使用された TCP ルールに応答して TCP 接続を閉じるために、またはトリガーとして使用された UDP ルールに応答して UDP セッションを閉じるために、アクティブ応答を開始します。侵入廃棄ルールでのアクティブ応答（2867 ページ）を参照してください。（攻撃者がアクティブ応答を無視または回避するよう選択する可能性があるなど）さまざまな理由で、アクティブ応答はファイアウォールの代わりとして想定されていません。

アクティブ応答は、ルーテッド展開またはトランスペアレント展開を含むインライン展開でサポートされます。たとえば、インライン展開での react キーワードに応答して、システムは接続の両端用のトラフィックに TCP リセット（RST）パケットを直接挿入でき、通常はこれに

よって接続が閉じます。アクティブ応答は、パッシブ展開ではサポートされていないか、または適していません。

アクティブ応答は戻って来ることがあるため、システムは TCP リセットによる TCP リセットの開始を許可しません。これにより、アクティブ応答が無限に続くことを防止できます。また、システムは、標準的な慣行に従って ICMP 到達不能パケットによる ICMP 到達不能パケットの開始を許可しません。

侵入ルールがアクティブ応答をトリガーとして使用した後、TCP 接続で追加のトラフィックを検出するよう、TCP ストリーム プリプロセッサを設定できます。追加のトラフィックが検出されると、プリプロセッサは、指定された最大値まで、追加のアクティブ応答を接続またはセッションの両端に送信します。トランスポート/ネットワーク プリプロセッサの詳細オプション（2868 ページ）の「**アクティブ応答の最大数（Maximum Active Responses）**」および「**最小応答時間（秒）（Minimum Response Seconds）**」を参照してください。

関連トピック

侵入廃棄ルールでのアクティブ応答 （2867 ページ）

resp キーワード

`resp` キーワードを使用すると、ルール ヘッダーで TCP プロトコルと UDP プロトコルのどちらが指定されているかに基づいて、TCP 接続または UDP セッションにアクティブに（能動的に）応答できます。

キーワード引数を使用すると、パケットの方向、および TCP リセット（RST）パケットと ICMP 到達不能パケットのどちらをアクティブ応答として使用するかを指定できます。

任意の TCP リセット引数または ICMP 到達不能引数を使用して、TCP 接続を閉じることができます。UDP セッションを閉じるには、ICMP 到達不能引数だけを使用する必要があります。

また、さまざまな TCP リセット引数を使用することで、パケットの送信元、宛先、またはその両方にアクティブ応答を送ることができます。すべての ICMP 到達不能引数はパケット送信元に送られます。ICMP ネットワーク、ホスト、またはポートのどの到達不能パケットを使用するか（または 3 つすべてを使用するか）を指定できます。

ルールがトリガーとして使用されたときに Firepower システムで実行されるアクションを正確に指定するために、`resp` キーワードで使用できる引数を次の表に列挙します。

表 *161 : resp* 引数

引数	説明
reset_source	ルールをトリガーとして使用したパケットを送信元エンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_snd` を指定することもできます。
reset_dest	ルールをトリガーとして使用したパケットの宛先であるエンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_rcv` を指定することもできます。

引数	説明
reset_both	送信側エンドポイントと受信側エンドポイントの両方に TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_all` を指定することもできます。
icmp_net	送信側に ICMP ネットワーク到達不能メッセージを送ります。
icmp_host	送信側に ICMP ホスト到達不能メッセージを送ります。
icmp_port	送信側に ICMP ポート到達不能メッセージを送ります。この引数は、UDP トラフィックを終了するために使われます。
icmp_all	送信側に次の ICMP メッセージを転送します。 • ネットワーク到達不能 • ホスト到達不能 • ポート到達不能

たとえば、ルールがトリガーとして使用されたときに接続の両側をリセットするようルールを設定するには、`resp` キーワードの値として `reset_both` を使用します。

次のように、カンマ区切りのリストを使用して複数の引数を指定できます。

```
argument,argument,argument
```

react キーワード

`react` キーワードを使用すると、パケットがルールをトリガーとして使用した時点でデフォルト HTML ページを TCP 接続クライアントに送信できます。HTML ページの送信後に、システムは TCP リセット パケットを使って接続の両端へのアクティブ応答を開始します。`react` キーワードは UDP トラフィックのアクティブ応答をトリガーとして使用しません。

オプションで、次の引数を指定できます。

```
msg
```

`msg` 引数を使用する `react` ルールがパケットによってトリガーとして使用されると、HTML ページにルール イベント メッセージが表示されます。

`msg` 引数を指定しない場合、HTML ページには次のメッセージが含まれます。

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

（注） アクティブ応答は戻されることがあるため、HTML 応答ページによって react ルールがトリガーとして使用されないようにしてください（結果としてアクティブ応答が無限に続く可能性があります）。Cisco では、react ルールを十分にテストしてから実稼動環境でアクティブにするよう推奨しています。

関連トピック

ルールの詳細 （2047 ページ）

detection_filter キーワード

detection_filter キーワードを使用すると、指定された時間内に指定された数のパケットがルールをトリガーとして使用しない限り、ルールでイベントが生成されないようにすることができます。これにより、早すぎるタイミングでルールがイベントを生成することを回避できます。たとえば、数秒間にログイン試行が 2 ～ 3 回失敗することは想定の範囲内ですが、同じ時間内に多数の試行が発生した場合はブルートフォース アタックを示唆している可能性があります。

detection_filter キーワードの必須の引数は、送信元/宛先のどちらの IP アドレスをシステムで追跡するか、イベントをトリガーすめたに検出基準が満たされるべき回数、およびカウントの継続時間を定義します。

イベントのトリガーを遅らせるには、次の構文を使用します。

```
track by_src/by_dst, count count, seconds number_of_seconds
```

track 引数は、ルールの検出基準を満たすパケット数をカウントするときに、パケットの送信元 IP アドレスと宛先 IP アドレスのどちらを使用するかを指定します。システムでイベント インスタンスを追跡する方法を指定するには、次の表の中から引数値を選択します。

表 *162 : detection_filter* の追跡引数

引数	説明
by_src	送信元 IP アドレスによる検出基準カウント。
by_dst	宛先 IP アドレスによる検出基準カウント。

count 引数は、ルールでイベントを生成するために、指定された時間内に指定された IP アドレスのルールをトリガーすべきパケットの数を指定します。

seconds 引数は、ルールでイベントを生成するために、指定された数のパケットがルールをトリガーすべき時間枠を秒数で指定します。

パケット内でコンテンツ foo を検索するルールが、次の引数を含む detection_filter キーワードを使用するとします。

```
track by_src, count 10, seconds 20
```

この例のルールは、特定の送信元 IP アドレスから 20 秒以内に 10 個のパケットで foo を検出するまでは、イベントを生成しません。システムが最初の 20 秒以内に foo を含むパケットを 7 つしか検出しなかった場合は、イベントが生成されません。しかし、最初の 20 秒間で foo が 40 回出現した場合は、ルールで 30 個のイベントが生成され、20 秒が経過するとカウントが再開されます。

しきい値と detection_filter キーワードの比較

detection_filter キーワードは、非推奨の threshold キーワードに代わるものです。threshold キーワードは、下位互換性を維持するために引き続きサポートされていますが、侵入ポリシー内で設定されるしきい値と同じ機能です。

detection_filter キーワードは、パケットがルールをトリガーとして使用する前に適用される検出機能です。ルールは、指定されたパケット カウントの前に検出されたトリガー パケットに関してイベントを生成しません。また、インライン展開では、パケットを破棄するようルールで設定されていても、そのようなパケットを破棄しません。逆に、指定されたパケット カウントの後に出現する、ルールをトリガーとして使用するパケットに関してルールはイベントを生成します。また、インライン展開でパケットを破棄するよう設定されている場合は、そのようなパケットを破棄します。

しきい値は、検出アクションを発生させないイベント通知機能です。これは、パケットがイベントをトリガーとして使用した後に適用されます。インライン展開において、パケットを破棄するよう設定されたルールは、ルールしきい値とは無関係に、ルールをトリガーとして使用するすべてのパケットを破棄します。

侵入ポリシー内で detection_filter キーワードを侵入イベントしきい値、侵入イベント抑制、および Rate-Based 攻撃防御機能と任意に組み合わせて使用できることに注意してください。また、侵入ポリシー内の侵入イベントしきい値機能と組み合わせて非推奨の threshold キーワードを使用するインポートされたローカル ルールを有効にした場合、ポリシー検証が失敗することに注意してください。

関連トピック

侵入イベントしきい値 （2033 ページ）
侵入ポリシー抑制の設定 （2037 ページ）
[ルール（Rule）] ページからの動的ルール状態の設定 （2042 ページ）

tag キーワード

ホストまたはセッションに関する追加のトラフィックをログに記録するようシステムに指示するには、tag キーワードを使用します。tag キーワードを使って検出するトラフィックのタイプと量を指定するときには、次の構文を使用します。

```
tagging_type, count, metric, optional_direction
```

次の 3 つの表に、その他の使用可能な引数について説明します。

2 つのタイプのタグ機能から選択できます。次の表に、これらのタグ機能の説明を示します。侵入ルールでルール見出しオプションのみを設定した場合、session タグ引数タイプによって、

同じセッションからのパケットが別のセッションからのパケットのように記録されることに注意してください。同じセッションからのパケットをまとめてグループ化するには、同じ侵入ルール内で 1 つ以上のルール オプション（`flag` キーワードや `content` キーワードなど）を設定します。

表 *163 : tag* の引数

引数	説明
session	ルールをトリガーとして使用したセッション内のパケットをログに記録します。
host	ルールをトリガーとして使用したパケットを送信したホストからのパケットをログに記録します。ホストからのトラフィックのみ（`src`）、またはホストへのトラフィックのみ（`dst`）を記録する方向修飾子を追加できます。

ログに記録するトラフィック量を指定するには、次の引数を使用します。

表 *164 :* カウント引数

引数	説明
count	ルールがトリガーとして使用された後にログに記録するパケット数または秒数。 この単位を指定するには、count 引数の後に測定基準引数を使用します。

次の表の中から、トラフィックの時間または量ごとにログで使用する測定基準を選択してください。

⚠

注意 高帯域ネットワークでは、1 秒あたり数千パケットが発生する可能性があり、多数のパケットにタグを付けるとパフォーマンスに重大な影響が及ぶ可能性があるため、必ずネットワーク環境に合わせてこの設定を調整してください。

表 *165 :* ログの測定基準引数

引数	説明
packets f f	ルールのトリガー後に、カウントで指定されるパケット数をログに記録します。
seconds	ルールのトリガー後に、カウントで指定される秒数の間、トラフィックを記録します。

たとえば、次の `tag` キーワード値を使用するルールがトリガーとして使用された場合、

```
host, 30, seconds, dst
```

次の30秒間にクライアントからホストに送信されるすべてのパケットがログに記録されます。

flowbits キーワード

状態名をセッションに割り当てるには、flowbitsキーワードを使用します。すでに名前が付けられた状態に基づいてセッション内の後続パケットを分析することにより、システムは単一セッション内で複数のパケットに及ぶエクスプロイトを検出して警告を出すことができます。

flowbits状態名は、セッションの特定部分でパケットに割り当てられるユーザー定義のラベルです。パケットの内容に基づいてパケットに状態名を付けると、警告の必要のないパケットと有害なパケットを区別しやすくなります。管理対象デバイスごとに最大 1024 個の状態名を定義できます。たとえば、ログイン成功後にのみ発生することがわかっている有害パケットについて警告するには、flowbitsキーワードを使用して、初期ログイン試行を構成するパケットを除去することにより、有害パケットに焦点を絞ることができます。このような機能を実装するには、まず、セッション内のすべてのログイン確立済みパケットにlogged_in 状態のラベルを付けるルールを作成した後、2 番目のルールを作成し、最初のルールで設定された状態を持つパケットを検査してそのようなパケットだけを処理する flowbits をそのルールに含めます。

オプションの *group name* を使用すると、状態のグループに状態名を含めることができます。1つの状態名は複数のグループに属することができます。グループに関連付けられていない状態は相互排他的ではないため、トリガーとして使用されたルールがグループに関連付けられていない状態を設定した場合、現在設定されている他の状態には影響がありません。

flowbits キーワードのオプション

次の表に、flowbitsキーワードで使用できる演算子、状態、およびグループのさまざまな組み合わせについて説明します。なお、状態名には、英数字、ピリオド（.）、アンダースコア（_）、およびダッシュ（-）を含めることができます。

表 *166 : flowbits* のオプション

演算子	状態オプション	グループ	説明
set	state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
set	state_name&state_name	オプション	パケットに関する、指定された複数の状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
setx	state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
setx	state_name&state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。

演算子	状態オプション	グループ	説明
unset	state_name	グループなし	パケットに関する指定された状態を解除します。
unset	state_name&state_name	グループなし	パケットに関する指定された状態を解除します。
unset	all	入力必須	指定されたグループ内のすべての状態を解除します。
toggle	state_name	グループなし	指定された状態が設定されている場合はそれを解除し、指定された状態が解除されている場合にはそれを設定します。
toggle	state_name&state_name	グループなし	指定された複数の状態が設定されている場合はそれらを解除し、指定された複数の状態が解除されている場合はそれらを設定します。
toggle	all	入力必須	指定されたグループ内で設定されているすべての状態を解除し、指定されたグループ内で解除されているすべての状態を設定します。
isset	state_name	グループなし	指定された状態がパケット内で設定されているかどうかを判別します。
isset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されているかどうかを判別します。
isset	state_name|state_name	グループなし	指定されたいずれかの状態がパケット内で設定されているかどうかを判別します。
isset	any	入力必須	指定されたグループ内で、いずれかの状態が設定されているかどうかを判別します。
isset	all	入力必須	指定されたグループ内で、すべての状態が設定されているかどうかを判別します。
isnotset	state_name	グループなし	指定された状態がパケット内で設定されていないかどうかを判別します。
isnotset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されていないかどうかを判別します。
isnotset	state_name|state_name	グループなし	指定されたいずれかの状態が、パケット内で設定されていないかどうかを判別します。
isnotset	any	入力必須	パケット内でいずれかの状態が設定されていないかどうかを判別します。

演算子	状態オプション	グループ	説明
isnotset	all	入力必須	パケット内ですべての状態が設定されていないかどうかを判別します。
reset	（状態なし）	オプション	すべてのパケットのすべての状態を解除します。グループが指定されている場合、グループ内のすべての状態を解除します。
noalert	（状態なし）	グループなし	イベント生成を抑制するには、これを他の演算子と組み合わせて使用します。

flowbits キーワードの使用に関するガイドライン

flowbits キーワードを使用するときには、次の点に注意してください。

- setx 演算子を使用する場合、指定した状態は、指定したグループ以外のグループに属することができません。
- setx 演算子を複数回定義して、それぞれのインスタンスで別々の状態と同じグループを指定できます。
- setx 演算子を使用してグループを指定する場合、そのグループに対して set、toggle、unset 演算子を使用することはできません。
- isset 演算子と isnotset 演算子は、指定された状態がグループに含まれるかどうかに関係なく、その状態を評価します。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループ**指定のない** isset または isnotset 演算子を含むルールを有効にした場合、対応する状態名とプロトコルに関する flowbits 割り当て（set、setx、unset、toggle）に影響する 1 つ以上のルールを有効にしないと、対応する状態名の flowbits 割り当てに影響するすべてのルールが有効になります。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループを**指定した** isset 演算子または isnotset 演算子を含むルールを有効にした場合、flowbits 割り当て（set、setx、unset、toggle）に影響し、対応するグループ名を定義するすべてのルールもまた有効になります。

flowbits キーワードの例

この項では、flowbits キーワードを使用する 3 つの例を示します。

flowbits キーワードの例：state_name を使用した設定

これは、state_name を使用した flowbits 設定の例です。

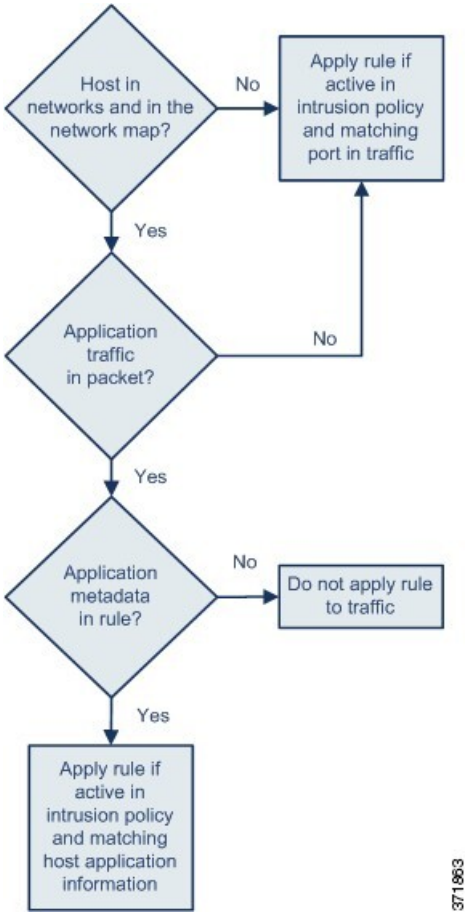
CVE ID 2000-0284 に記述されている IMAP 脆弱性について考えてみます。この脆弱性は、IMAP の実装（具体的には LIST、LSUB、RENAME、FIND、および COPY コマンド）で見られます。ただし、攻撃者がこの脆弱性を悪用するには、IMAP サーバにログインする必要があります。IMAP サーバからの LOGIN 確認とそれに続く exploit は必然的に別々のパケットに存在するため、この exploit を検出する非フロー ベースのルールを作成するのは困難です。`flowbits` キーワードを使って一連のルールを作成すると、ユーザが IMAP サーバにログイン済みかどうかを追跡し、ログイン済みの場合は、いずれかの攻撃が検出された時点でイベントを生成できます。ユーザがログイン済みでない場合、攻撃によって脆弱性が悪用されることはないため、イベントが生成されません。

下記の 2 つのルール フラグメントはこの例を示しています。最初のルール フラグメントは IMAP サーバーからの IMAP ログイン確認を検索します。

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK

LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

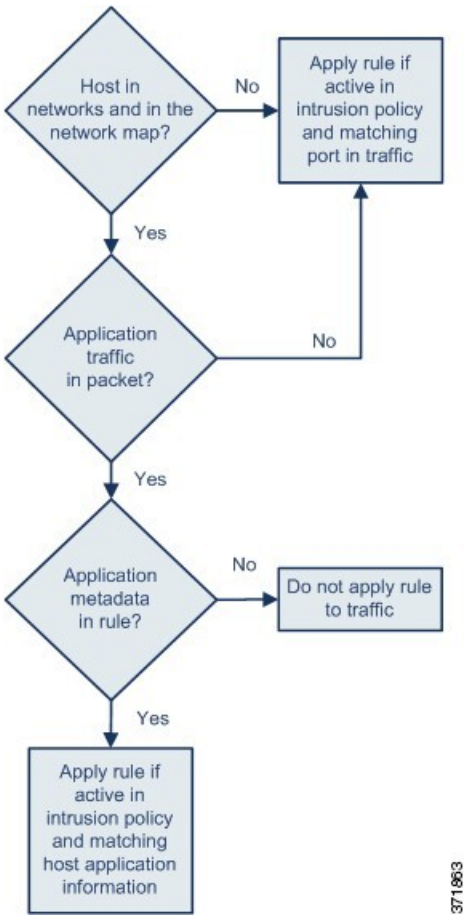


`flowbits:set` は `logged_in` 状態を設定しますが、`flowbits:noalert` がアラートを抑制することに注意してください。これは、IMAP サーバー上で多数の無害なログイン セッションが見つかる可能性があるためです。

次のルール フラグメントは LIST 文字列を検索しますが、セッション内の先行パケットの結果として logged_in 状態が設定済みでない限り、イベントを生成しません。

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



この場合、最初のフラグメントを含むルールが先行パケットによってトリガーとして使用した場合、2 番目のフラグメントを含むルールがトリガーとして使用し、イベントを生成します。

flowbits キーワードの例：誤検出イベントを引き起こす設定

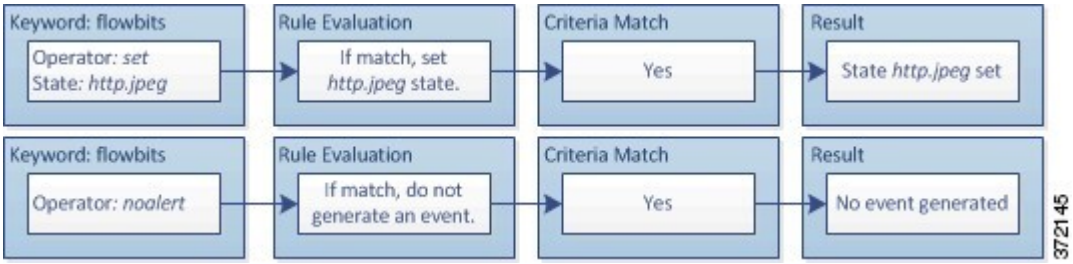
後続パケット内コンテンツが、効力を失った状態を持つルールに一致することによって誤検出イベントが発生する可能性があります。複数のルールで設定された複数の状態名をグループに含めることでこれを回避できます。次の例は、複数の状態名をグループに含めない場合に誤検出が発生する可能性があることを示しています。

1 つのセッションで次の 3 つのルール フラグメントがこの順序でトリガーとして使用される場合を考えてみます。

```
(msg:"JPEG transfer";
```

```
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

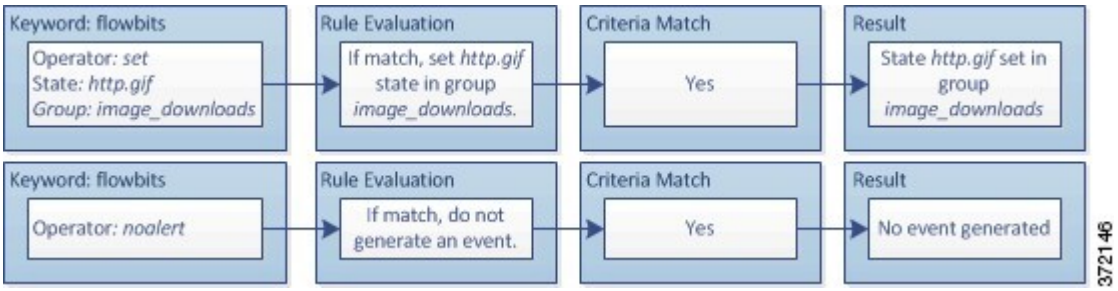


最初のルール フラグメント内の content キーワードと pcre キーワードが JPEG ファイル ダウンロードに一致し、flowbits:set,http.jpeg が http.jpeg flowbits ステートを設定し、flowbits:noalert はルールでのイベント生成を抑制します。イベントが生成されない理由は、このルールの目的がファイル ダウンロードを検出して flowbits 状態を設定することだからです。これにより、1 つ以上のコンパニオン ルールで状態名を検査して有害コンテンツを探し、有害コンテンツが検出された時点でイベントを生成できます。

次のルール フラグメントは、上記の JPEG ファイル ダウンロードに続く GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

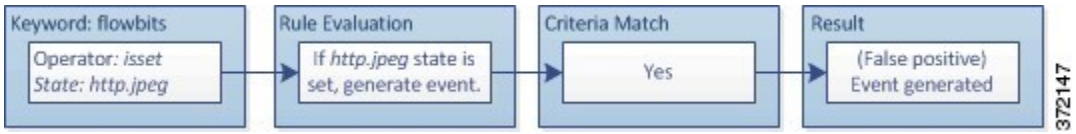


2 番目のルール内の content キーワードと pcre キーワードは GIF ファイル ダウンロードを照合し、flowbits:set,http.jpg は http.jpg flowbit ステートを設定し、flowbits:noalert はルールでのイベント生成を抑制します。最初のルール フラグメントで設定された http.jpeg 状態が不要になっても引き続き設定されていることに注意してください。これは、後続の GIF ダウンロードが検出されたときに JPEG ダウンロードが既に終了しているはずであるためです。

次に示す 3 番目のルール フラグメントは最初のルール フラグメントのコンパニオンです。

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"?/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。



3 番目のルール フラグメントでは、もはや無意味になった `http.jpeg` ステートが設定されていることを `flowbits:isset,http.jpeg` が判別し、`content` と `pcre` は（GIF ファイルでは無害でも）JPEG ファイル内では有害とみなされるコンテンツを照合します。3 番目のルール フラグメントによって、JPEG ファイル内に存在しないエクスプロイトに関する誤検出イベントが生成されます。

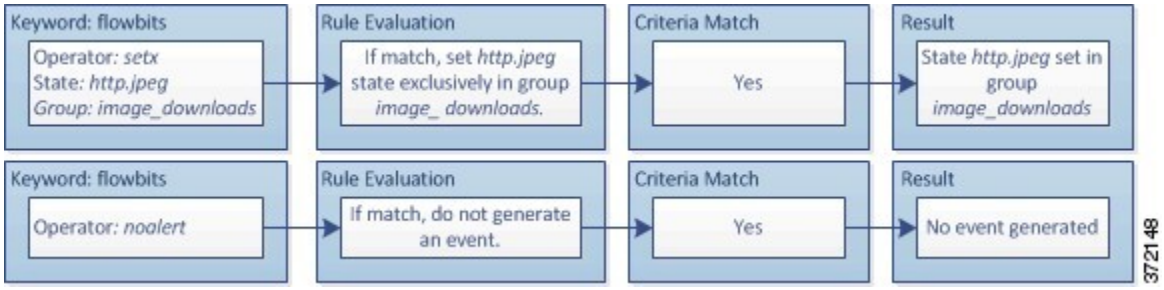
flowbits キーワードの例：誤検出イベントを防ぐための設定

次の例は、状態名をグループに含めて `setx` 演算子を使用することで、どのように誤検出を防止できるかを示しています。

前の例とほぼ同じケースを考えます。ただし、最初の 2 つのルールで、同じ状態グループに 2 つの異なる状態名が含まれるようになった点が異なります。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

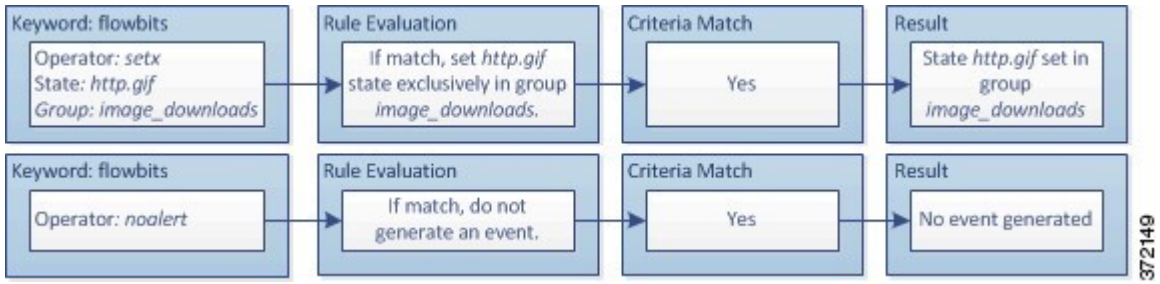


最初のルール フラグメントが JPEG ファイル ダウンロードを検出すると、`flowbits:setx,http.jpeg,image_downloads` キーワードが `flowbits` 状態を `http.jpeg` に設定し、その状態を `image_downloads` グループに含めます。

その後、次のルールが後続の GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

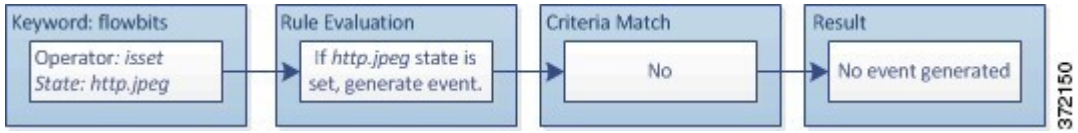


2 番目のルール フラグメントが GIF ダウンロードに一致すると、`flowbits:setx,http.jpg,image_downloads` キーワードが `http.jpg flowbits` ステートを設定し、グループ内の他のステートである `http.jpeg` を解除します。

次に示す 3 番目のルール フラグメントで誤検出は発生しません。

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"/?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



`flowbits:isset,http.jpeg` が false であるため、ルール エンジンはルールの処理を停止し、イベントは生成されません。こうして、GIF ファイル内のコンテンツが JPEG ファイルに関するエクスプロイト コンテンツと一致した場合でも誤検出が回避されます。

http_encode キーワード

`http_encode` キーワードを使用すると、HTTP URI、HTTP ヘッダー内の非 cookie データ、HTTP 要求ヘッダー内の cookie、HTTP 応答内の set-cookie データのいずれかにおいて、正規化前の HTTP 要求または応答内のエンコード タイプに基づいてイベントを生成できます。

HTTP 応答と HTTP cookie を検査し、`http_encode` キーワードを使用しているルールに一致したものを返すように、HTTP Inspect プリプロセッサを設定する必要があります。

また、侵入ルール内の `http_encode` キーワードで特定のエンコード タイプによってイベントがトリガーとして使用されるようにするには、HTTP Inspect プリプロセッサ設定で個々の特定のエンコード タイプのデコード オプションとアラート オプションの両方を有効にする必要があります。

次の表は、このオプションでイベントを生成できる、HTTP URI、ヘッダー、cookie、set-cookie のエンコード タイプを説明しています。

表 *167 : http_encode* エンコード タイプ

エンコード タイプ	説明
utf8	HTTP Inspect プリプロセッサによるデコードで UTF-8 エンコード タイプが有効になっている場合、指定された場所で UTF-8 エンコードを検出します。
double_encode	HTTP Inspect プリプロセッサによるデコードで二重エンコード タイプが有効になっている場合、指定された場所で二重エンコードを検出します。
non_ascii	非 ASCII 文字が検出されても、検出されたエンコード タイプが有効になっていない場合に、指定された場所で非 ASCII 文字を検出します。
uencode	HTTP Inspect プリプロセッサによるデコードで Microsoft %u エンコード タイプが有効になっている場合、指定された場所で Microsoft %u エンコードを検出します。
bare_byte	HTTP Inspect プリプロセッサによるデコードで空白バイト エンコード タイプが有効になっている場合、指定された場所で空白バイト エンコードを検出します。

関連トピック

HTTP Inspect プリプロセッサ （2796 ページ）
サーバー レベルの HTTP 正規化オプション （2798 ページ）

http_encode キーワードの構文

エンコーディングの場所

HTTP URI、ヘッダー、または set-cookie などの Cookie で指定されたエンコーディング タイプを検索するかどうかを指定します。

エンコード タイプ

次のいずれかの形式を使用して、1 つ以上のエンコード タイプを指定します。

```
encode_type
encode_type|encode_type|encode_type...
```

ここで、`encode_type` は次のいずれかです。

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

否定（!）演算子と OR（|）演算子を一緒に使用できないことに注意してください。

http_encode キーワードの例：2 つの http_endcode キーワードを使用した 2 つのエンコーディングの検索

次に、同じルールで 2 つの `http_encode` キーワードを使用して、UTF-8 および Microsoft IIS %u エンコーディングの HTTP URI を検索する例を示します。

最初に、`http_encode` キーワードを使用します。

- **エンコーディングの場所**：`HTTP URI`
- **エンコーディングのタイプ**：`utf8`

次に、追加の `http_encode` キーワードを使用します。

- **エンコーディングの場所**：`HTTP URI`
- **エンコーディングのタイプ**：`uencode`

概要：file_type および file_group キーワード

`file_type` と `file_group` キーワードを使用すると、タイプとバージョンに基づいて、FTP、HTTP、SMTP、IMAP、POP3、NetBIOS-ssn（SMB）を介して伝送されるファイルを検出できます。1 つの侵入ルール内で複数の `file_type` キーワードや `file_group` キーワードを使用**しない**でください。

ヒント 脆弱性データベース（VDB）を更新すると、最新のファイル タイプ、バージョン、グループが侵入ルール エディタに表示されます。

（注） システムは、`file_type` および `file_group` キーワードに値を代入するためにプリプロセッサを自動的に有効にすることはしません。

`file_type` または `file_group` キーワードに一致するトラフィックに対してイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、特定のプリプロセッサを有効にする**必要があります**。

表 *168 : file_type* および *file_group* の侵入イベントの生成

プロトコル	必要なプリプロセッサまたはプリプロセッサ オプション
FTP	FTP/Telnet プリプロセッサおよび [TCP ペイロードの正規化（Normalize TCP Payload）] インライン正規化プリプロセッサ オプション
HTTP	HTTP トラフィックでの侵入イベントを生成する HTTP Inspect プリプロセッサ。

プロトコル	必要なプリプロセッサまたはプリプロセッサ オプション
SMTP	HTTP トラフィックでの侵入イベントを生成する SMTP プリプロセッサ
IMAP	IMAP プリプロセッサ
POP3	POP プリプロセッサ
NetBIOS-ssn（SMB）	DCE/RPC プリプロセッサおよび [SMB ファイル インスペクション（SMB File Inspection）] DCE/RPC プリプロセッサ オプション

関連トピック

FTP/Telnet デコーダ （2787 ページ）
インライン正規化プリプロセッサ （2872 ページ）
HTTP Inspect プリプロセッサ （2796 ページ）
SMTP プリプロセッサ （2833 ページ）
IMAP プリプロセッサ （2826 ページ）
POP プリプロセッサ （2829 ページ）
DCE/RPC プリプロセッサ （2768 ページ）

file_type キーワードと file_group キーワード

file_type

`file_type` キーワードを使用すると、トラフィック内で検出対象となるファイルのタイプとバージョンを指定できます。ファイル タイプ引数（**JPEG** や **PDF** など）は、トラフィックで検出するファイルの形式を識別します。

（注） 同じ侵入ルール内で `file_type` キーワードを別の `file_type` キーワードまたは `file_group` キーワードと一緒に**使用しないでください**。

デフォルトでは **Any Version** が選択されますが、一部のファイル タイプではバージョン オプション（たとえば PDF バージョン **1.7**）を選択することにより、トラフィックで検出対象となる特定のファイル タイプ バージョンを識別できます。

file_group

`file_group` キーワードを使用すると、トラフィック内で検出する類似のファイル タイプからなる Cisco 定義のグループを選択できます（**マルチメディア**、**オーディオ**など）。また、ファイル グループには、グループ内の各ファイル タイプに関する Cisco 定義のバージョンも含まれています。

（注） 同じ侵入ルール内で file_group キーワードを別の file_group キーワードまたは file_type キーワードと一緒に使用**しない**でください。

file_data キーワード

file_data キーワードは、content、byte_jump、byte_test、pcre などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。file_data キーワードが指し示すデータのタイプは、検出されるトラフィックによって決まります。file_data キーワードを使用すると、次のペイロード タイプの先頭を指し示すことができます。

- HTTP 応答本文

  HTTP 応答パケットを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。HTTP Inspect プリプロセッサが HTTP 応答本文データを検出した場合に、file_data キーワードが一致します。

- 非圧縮 gzip ファイル データ

  HTTP 応答本文内の非圧縮 gzip ファイルを検査するには、HTTP Inspect プリプロセッサを有効にする必要があり、さらに HTTP 応答を検査して HTTP 応答本文内の gzip 圧縮ファイルを復元するようプリプロセッサを設定する必要があります。詳細については、サーバレベルの HTTP 正規化オプション [HTTP 応答の検査（Inspect HTTP Responses）] および [圧縮データの検査（Inspect Compressed Data）] を参照してください。file_data キーワードは、HTTP Inspect プリプロセッサが HTTP 応答本文内で非圧縮 gzip データを検出した場合に一致します。

- 正規化された JavaScript

  正規化された JavaScript データを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。file_data キーワードは、HTTP Inspect プリプロセッサが応答本文データ内で JavaScript を検出した場合に一致します。

- SMTP ペイロード

  SMTP ペイロードを検査するには、SMTP プリプロセッサを有効にする必要があります。file_data キーワードは、SMTP プリプロセッサが SMTP データを検出した場合に一致します。

- SMTP、POP、または IMAP トラフィック内のエンコードされた電子メール添付ファイル

  SMTP、POP、または IMAP トラフィック内の電子メール添付ファイルを検査するには、それぞれ SMTP、POP、または IMAP プリプロセッサを単独で、または任意に組み合わせて有効にする必要があります。その後、有効にしたプリプロセッサごとに、デコード対象のそれぞれの添付ファイル エンコード タイプをデコードするようプリプロセッサが設定されていることを確認する必要があります。プリプロセッサごとに設定可能な添付ファイ

ル デコード オプションは、[Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted Printable 復号の深さ（Quoted-Printable Decoding Depth）]、および [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] です。

1 つのルール内で複数の `file_data` キーワードを使用できます。

関連トピック

HTTP Inspect プリプロセッサ （2796 ページ）
サーバーレベルの HTTP 正規化オプション （2798 ページ）
SMTP プリプロセッサ （2833 ページ）
IMAP プリプロセッサ （2826 ページ）

pkt_data キーワード

`pkt_data` キーワードは、`content`、`byte_jump`、`byte_test`、`pcre` などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。

正規化された FTP、Telnet、または SMTP トラフィックが検出された場合、`pkt_data` キーワードは、正規化されたパケット ペイロードの先頭を指します。その他のトラフィックが検出された場合、`pkt_data` キーワードは、未加工の TCP または UDP ペイロードの先頭を指します。

侵入ルールで検査するために、該当するトラフィックをシステムで正規化するには、次の正規化オプションを有効にする必要があります。

- 検査のために FTP トラフィックを正規化するには、FTP & Telnet プリプロセッサの [FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape codes within FTP commands）] オプションを有効にします。
- 検査のために Telnet トラフィックを正規化するには、FTP & Telnet プリプロセッサの Telnet の [正規化（Normalize）] オプションを有効にします。
- 検査のために SMTP トラフィックを正規化するには、SMTP プリプロセッサの [正規化（Normalize）] オプションを有効にします。

1 つのルール内で複数の `pkt_data` キーワードを使用できます。

関連トピック

クライアントレベルの FTP オプション （2792 ページ）
Telnet オプション （2787 ページ）
SMTP プリプロセッサのオプション （2833 ページ）

base64_decode キーワードと base64_data キーワード

`base64_decode` キーワードと `base64_data` キーワードを組み合わせて使用すると、指定したデータを Base64 データとしてデコードおよび検査するようルール エンジンに指示できます。たと

えば HTTP PUT および POST 要求内の Base64 エンコード HTTP 認証要求見出しと Base64 エンコード データを検査する場合に、これが役立つ可能性があります。

これらのキーワードは特に、HTTP 要求内の Base64 データをデコードして検査するうえで役立ちます。また、長いヘッダー行を複数行に拡張するために HTTP で使われるのと同じ方法でスペース文字やタブ文字を使用する SMTP などのプロトコルでも、これらを使用できます。この行拡張（折り返しとも言う）を使用するプロトコル内に行拡張が存在しない場合、後続スペース/タブを伴わない復帰または改行が出現した箇所で検査が終了します。

base64_decode

`base64_decode` キーワードは、パケット データを Base64 データとしてデコードするようルール エンジンに指示します。オプションの引数を使用すると、デコードするバイト数と、デコードを開始するデータ内の位置を指定できます。

`base64_decode` キーワードは 1 つのルール内で 1 回だけ使用可能です。また、少なくとも 1 つの `base64_data` キーワードのインスタンスの前にこれを配置する必要があります。

Base64 データをデコードする前に、ルール エンジンは、複数行にわたって折り返された長いヘッダーを元どおりに広げます。ルール エンジンが次のいずれかに遭遇するとデコードが終了します。

- ヘッダー行の末尾
- デコード対象として指定されたバイト数
- パケットの末尾

次の表に、`base64_decode` キーワードで使用可能な引数の説明を示します。

表 *169 : base64_decode* のオプション引数

引数	説明
Bytes	デコードするバイト数を指定します。これを指定しない場合、ヘッダー行の末尾またはパケット ペイロード末尾のどちらかが先に出現するまでデコードが続行されます。ゼロ以外の正の値を指定できます。
Offset	パケットペイロードの先頭を基準にしたオフセットを決定します。さらに **Relative** も指定した場合は、現在の検査位置を基準にしたオフセットを決定します。ゼロ以外の正の値を指定できます。
Relative	現在の検査位置を基準にして検査することを指定します。

base64_data

`base64_data` キーワードは、`base64_decode` キーワードを使ってデコードされた Base64 データを検査するための参照を提供します。`base64_data` キーワードは、デコードされた Base64 データの先頭から検査を開始するよう設定します。オプションで、`content` や `byte_test` などの他のキーワードで使用可能な位置引数を使用して、検査位置をさらに指定することもできます。

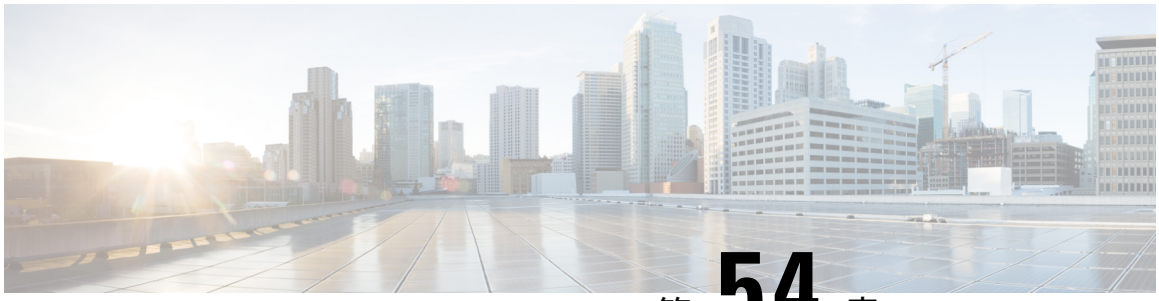
base64_decode キーワードを使用した後に base64_data キーワードを 1 回以上使用する必要があります。オプションで、base64_data を複数回使用して、デコードされた Base64 データの先頭に戻ることができます。

Base64 データを検査するときには、次の点に注意してください。

- 高速パターン マッチ機能は使用できません。
- 中間的な HTTP コンテンツ引数を使ってルール内で Base64 検査を中断する場合は、Base64 データをさらに検査する前に、別の base64_data キーワードをルールに挿入する必要があります。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2078 ページ）
content キーワードの高速パターン マッチ機能の引数 （2083 ページ）



第 54 章

侵入ポリシーとネットワーク分析ポリシーのレイヤ

以下のトピックでは、侵入ポリシーおよびネットワーク分析ポリシーでレイヤ（層）を使用する方法について説明します。

- レイヤの基本 （2179 ページ）
- ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤのライセンス要件 （2180ページ）
- ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤの要件と前提条件 （2180ページ）
- レイヤ スタック （2180 ページ）
- レイヤ管理 （2185 ページ）

レイヤの基本

多数の管理対象デバイスが存在する大規模な組織では、さまざまな部署や事業部門、場合によってはさまざまな企業の固有のニーズをサポートするために、多数の侵入ポリシーやネットワーク分析ポリシーが存在することがあります。両方のポリシータイプでの設定はレイヤと呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーおよびネットワーク分析ポリシーのレイヤは、原則的に同じ方法で動作します。ポリシー タイプの作成および編集は、レイヤを意識せずに行えます。ポリシー設定を変更でき、ポリシーにユーザー レイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は *My Changes* という名前が付けられています）に含められます。また、最大200までレイヤを追加して、それらのレイヤで設定を任意に組み合わせて構成することもできます。ユーザー レイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザー レイヤを同じタイプの他のポリシーと共有できます。

ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

レイヤ スタック

レイヤ スタックは、次の各レイヤから構成されています。

ユーザ レイヤ

ユーザ設定可能なレイヤです。ユーザ設定可能なレイヤは、コピー、マージ、移動、または削除を行うことができます。また、任意のユーザ設定可能なレイヤが同じタイプの他のポリシーと共有されるように設定することもできます。このレイヤには、最初にMy Changesという名前が付けられた自動生成されたレイヤが含まれています。

組み込み型レイヤ

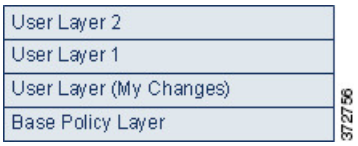
読み取り専用の基本ポリシー レイヤです。このレイヤ内のポリシーは、システムによって提供されるポリシー、または自分で作成したカスタム ポリシーにできます。

ネットワーク分析ポリシーまたは侵入ポリシーには、デフォルトでは基本ポリシー レイヤと My Changes レイヤが含まれています。ユーザ レイヤは必要に応じて追加できます。

各ポリシー レイヤには、ネットワーク分析ポリシー内のすべてのプリプロセッサまたは侵入ポリシー内のすべての侵入ルールと詳細設定の完全な設定が含まれます。最下部の基本ポリシー レイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれます。上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次の高いレイヤから設定を継承します。システムはレイヤをフラット化します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント 侵入またはネットワークの分析ポリシーは、基本ポリシーのデフォルト設定のみに基づいて作成できます。侵入ポリシーの場合に、モニタ対象ネットワークの特定のニーズに合わせて侵入ポリシーを調整したいときは、Firepower のルール状態の推奨を使用することもできます。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤの他に、2 つの追加のユーザ設定可能なレイヤ *User Layer 1* と *User Layer 2* も含まれているレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能なレイヤそれぞれがスタックの最上位レイヤとして最初に配置されるため、図内の User Layer 2 が最後に追加されたもので、このスタックの最上位になっていることに注目してください。



ルール更新にポリシーの変更を許可しているかどうかに関わらず、ルール更新での変更は、レイヤで行った変更を上書きしません。これは、ルール更新での変更が、基本ポリシー レイヤのデフォルト設定を決定する基本ポリシーで行われるためです。変更は常により上位のレイヤに加えられ、その変更によって、ルール更新が基本ポリシーに加えた変更が上書きされます。

基本レイヤ

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更は My Changes レイヤに保存され、基本ポリシーの設定を上書きしますが変更はしません。

システム提供の基本ポリシー

Firepower システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか提供されています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Talos インテリジェンス グループのエクスペリエンスを活用することができます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよ

び他の詳細設定の初期設定も提供します。これらのシステムによって提供されるポリシーをそのまま使用したり、カスタム ポリシーのベースとして使用することができます。

システムによって提供されるポリシーをベースとして使用する場合、ルール更新をインポートすると、基本ポリシー内の設定が変更される場合があります。ただし、カスタム ポリシーを設定して、これらの変更内容がシステム提供の基本ポリシーに自動的に反映されないようにすることもできます。これにより、ルール更新とは関係ないスケジュールで、システム提供の基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によって My Changes または他のレイヤの設定が変更または上書きされることはありません。

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。

カスタム基本ポリシー

カスタム ポリシーを基本（ベース）として使用することができます。カスタム ポリシーの設定を調整することで、最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

別のポリシーのベースとして使用するカスタムポリシー変更すると、変更内容はこのベースを使用するポリシーのデフォルト設定として自動的に使用されます。

また、ポリシーはすべて、システムが提供するポリシーをポリシーチェーンにおける最終的なベースとしているため、たとえカスタム基本ポリシーを使っていても、ルールが更新されればポリシーに影響する可能性があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がその基本ポリシーを変更することが許可されている場合は、ポリシーが影響を受ける可能性があります。

基本ポリシーがどのように変更されたかに関わらず（ルール更新による変更でも、基本ポリシーとして使用するカスタムポリシーを変更でも）、ユーザーの基本ポリシーに対する変更によって My Changes やその他のレイヤの設定が変更または上書きされることはありません。

基本ポリシーに対するルール更新の影響

ルール更新をインポートすると、システム提供の侵入ポリシー、アクセス コントロール ポリシー、ネットワーク分析ポリシーが変更されます。ルール更新には次の要素が含まれる場合があります。

- 変更されたネットワーク分析プリプロセッサの設定
- 変更された侵入ポリシーおよびアクセス コントロール ポリシーの詳細設定
- 新規または更新された侵入ルール
- 既存のルールの変更された状態
- 新しいルール カテゴリとデフォルト変数

ルール更新により、既存のルールがシステム提供のポリシーから削除される場合もあります。

デフォルト変数とルール カテゴリに対する変更はシステム レベルで処理されます。

システム提供のポリシーを侵入またはネットワーク分析の基本ポリシーとして使用するときは、ルール更新が基本ポリシー（この場合はシステムによって提供されるポリシーのコピー）を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステム提供のポリシーに対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、ポリシー内の設定が決定されます。ただし、ルール更新では、ポリシー内で行った変更は上書きされません。

ルール更新による基本ポリシーの変更を許可しない場合は、1 つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新による基本の侵入ポリシーの変更が許可されているかどうかに関係なく、Talos が削除した侵入ルールが常に削除されます。

ネットワーク トラフィックに変更を再展開するまで、現在展開されている侵入ポリシー ルールは次のように動作します。

- 無効になっている侵入ルールは無効のままになります。
- [イベントを生成する（Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない限り、ルール更新でカスタム基本ポリシーは変更されません。

- ルール更新が親ポリシーのシステムによって提供される基本ポリシー（つまり、カスタム基本ポリシーの起源となるポリシー）を変更することを許可している。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、ルール更新で以前に無効になっていた侵入ルールを有効にして、親の侵入ポリシー内のルール状態を変更していない場合は、親ポリシーを保存したときに、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルール更新でデフォルトのプリプロセッサ設定を変更し、親のネットワーク分析ポリシーの設定を変更していない場合は、変更された設定は親ポリシーを保存したときに基本ポリシーに渡されます。

基本ポリシーの変更

別のシステム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 必要な侵入ポリシーの行にある [編集（Edit）]（✎） をクリックします。

ステップ 4 [ベースポリシー（Base Policy）] ドロップダウンリストからベースポリシーを選択します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

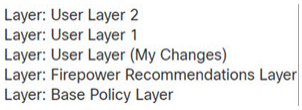
関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

Cisco 推奨レイヤ

侵入ポリシーでルール状態の推奨を生成する場合は、その推奨に基づいてルール状態を自動的に変更するかどうかを選択できます。

下記の図に示すように、推奨されたルール状態を使用すると、侵入ポリシーの基本レイヤのすぐ上に読み取り専用の組み込み Cisco 推奨レイヤが挿入されます。



このレイヤは侵入ポリシー固有のものです。

それ以後、推奨されたルール状態を使用しないことを選択すると、Cisco 推奨レイヤは削除されます。このレイヤは手動で削除できませんが、推奨されるルール状態を使用するかどうかを選択することで、サービスを追加したり削除することができます。

Cisco推奨レイヤを追加すると、ナビゲーションパネルの [ポリシー階層（Policy Layers）]の下に Cisco 推奨リンクが追加されます。このリンクから Cisco 推奨レイヤページの読み取り専用

ビューにアクセスして、[ルール（Rules）]ページの推奨でフィルタリングされたビューを読み取り専用モードで表示できます。

推奨されたルール状態を使用すると、ナビゲーションパネルの Cisco 推奨リンクの下に [ルール（Rules）] サブリンクも追加されます。[ルール（Rules）] サブリンクから、Cisco 推奨レイヤの [ルール（Rules）] ページの読み取り専用画面にアクセスできます。このビューでは次の点に注意してください。

- 状態列にルール状態のアイコンがない場合、状態は基本ポリシーから継承されます。
- このビューまたは他の [ルール（Rules）] ページビューの Cisco 推奨列にルール状態のアイコンがない場合、このルールに対する推奨は存在しません。

関連トピック

ネットワーク資産に応じた侵入防御の調整 （2197 ページ）

レイヤ管理

[ポリシー層（Policy Layers）] ページには、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤスタックの単一ページの概要が示されます。このページでは、共有レイヤおよび非共有レイヤの追加、レイヤのコピー、マージ、移動、および削除、各レイヤの概要ページへのアクセス、各レイヤ内の有効、無効、および上書きされている設定の設定ページへのアクセスを行うことができます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤに最上位の（つまり効果的な）プリプロセッサまたは詳細設定が含まれているか（機能名別に）
- 侵入ポリシーで、状態がレイヤで設定されている侵入ルールの数、および各ルール状態に設定されているルールの数

[ポリシー層（Policy Layers）] ページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

各レイヤのサマリーにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能の状態	機能名
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示

機能の状態	機能名
下位レイヤから継承される	表示されない

最大200のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、ポリシーで最上位レイヤとして表示されます。初期状態はすべての機能に対して[継承（Inherit）]で、侵入ポリシーでは、イベントのフィルタリング、動的状態、またはルール アクションのアラートは設定されません。

レイヤをポリシーに追加する際は、ユーザが設定可能なレイヤに一意の名前を指定します。その名前は後で変更できます。また、必要に応じて、レイヤを編集する際に表示される説明を追加あるいは変更することもできます。

レイヤはコピーすることも、[ユーザ レイヤ（User Layers）]ページ内での表示位置を上下に移動することもできます。また、初期の My Changes レイヤを含め、ユーザ レイヤを削除することも可能です。次の考慮事項に注意してください。

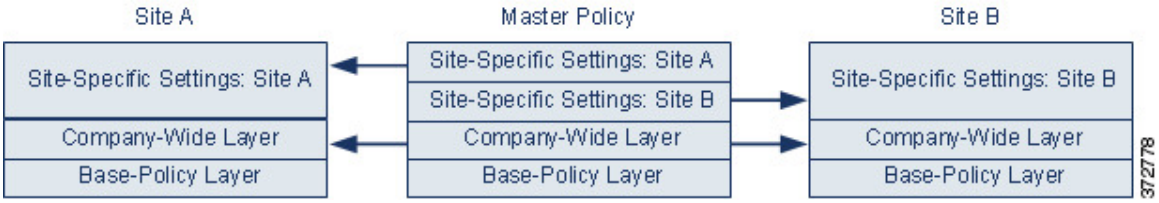
- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、初期状態ではそのレイヤは共有されませんが、必要に応じて、後から共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

ユーザ設定可能なレイヤの直下に、別のユーザ設定可能なレイヤをマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルール、または詳細設定が含まれていた場合、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。他のポリシーに追加できる共有可能なレイヤを作成するポリシーでは、共有可能なレイヤのすぐ上に非共有レイヤのある共有可能なレイヤをマージできますが、共有可能なレイヤの直下には非共有レイヤのある共有可能なレイヤをマージすることはできません。別のポリシーに作成した共有レイヤを追加するポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。非共有レイヤをその下の共有レイヤとマージすることはできません。

共有レイヤ

共有レイヤとは、あるポリシー内で作成して共有を許可し、別のポリシーに追加されたレイヤのことです。共有可能レイヤとは、共有が許可されているレイヤのことです。

以下の図に示すプライマリポリシーの例では、全社的レイヤと、サイト A およびサイト B に固有のレイヤを作成し、これらのサイト固有のレイヤの共有を許可しています。その上で、これらのサイト固有のレイヤを共有レイヤとしてサイト A とサイト B のポリシーに追加しています。



プライマリポリシーの全社的なレイヤには、サイト A とサイト B に適用される設定が含まれる一方、サイト固有のレイヤには各サイトに固有の設定が含まれています。たとえば、ネットワーク分析ポリシーの場合、サイト A にはモニタ対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクションプリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、サイト A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、サイト B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のプライマリポリシーでフラット化された設定値そのものがトラフィックをモニターするのに役立つわけではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシー階層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、ネットワーク、さらにはユーザごとにポリシーのレイヤを定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できるように設定できます。共有可能レイヤ内の設定を変更し、変更をコミットすると、そのレイヤを共有するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシーの機能設定のみを変更できます。

別のポリシーに追加しているレイヤの共有を無効にすることはできません。まずレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

基本ポリシーが共有するレイヤが作成されたカスタムポリシーである場合、ポリシーに共有レイヤを追加することはできません。追加した場合、ポリシーで依存関係が循環することになります。

レイヤの管理

手順

ステップ 1 Snort 2 ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] をクリックします。

ステップ 2 [ポリシー層（Policy Layers）] ページでは、次に示す管理アクションを実行できます。

- 別のポリシーからの共有レイヤの追加：[ユーザーレイヤ（User Layers）] の横にある [共有レイヤの追加（Add Shared Layer）] [追加（Add）] (＋) をクリックし、[共有レイヤの追加（Add Shared Layer）] ドロップダウンリストからレイヤを選択して、[OK] をクリックします。
- 非共有レイヤの追加：[ユーザーレイヤ（User Layers）] の横にあるレイヤの追加[追加（Add）] (＋)をクリックし、[名前（Name）] を入力して、[OK] をクリックします。
- レイヤの説明の追加または変更：レイヤの横にある[編集（Edit）]（✎）をクリックして、[説明（Description）] を追加または変更します。
- 別のポリシーとのレイヤの共有の許可：レイヤの横にある[編集（Edit）]（✎）をクリックして、[共有（Sharing）] チェックボックスをオフにします。
- レイヤの名前の変更：レイヤの横にある[編集（Edit）]（✎）をクリックして、[名前（Name）] を変更します。
- レイヤのコピー：レイヤの[コピー（Copy）]（⧉）をクリックします。
- レイヤの削除：レイヤの[削除（Delete）]（🗑）をクリックして、[OK] をクリックします。
- 2 つのレイヤのマージ：2 つのレイヤの上部の**マージ**（⧉）をクリックして、[OK] をクリックします。
- レイヤの移動：レイヤサマリ内の任意の空いている場所をクリックし、**位置矢印**が移動するレイヤの上または下の行を指すまでドラッグします。

ステップ 3 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

レイヤ間のナビゲーション

手順

ステップ 1 Snort 2 ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] をクリックします。Snort 2 ポリシーにアクセスするには、[ポリシー（Policies）] > [侵入（Intrusion）]

> [侵入ポリシー（Intrusion Policies）] タブ を選択し、編集するポリシーに対して [Snort 2] をクリックします。 > >

ステップ 2 レイヤの移動は、次のいずれかのアクションで実行できます。

- プリプロセッサ ページまたは詳細設定ページにアクセスする：レイヤ レベルのプリプロセッサまたは詳細設定の設定ページにアクセスするには、そのレイヤに対応する行の機能名をクリックします。基本ポリシーおよび共有レイヤでは、設定ページは読み取り専用です。
- ルールページにアクセスする：ルールの状態タイプでフィルタ処理されたレイヤレベルのルール設定ページにアクセスする場合は、レイヤの概要で [イベントのドロップおよび生成（Drop and Generate Events）]、[イベントの生成（Generate Events）]、または [無効化（Disabled）] をクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。
- [ポリシー情報ページ（Policy Information）]ページを表示する：[ポリシー情報ページ（Policy Information）] ページを表示するには、ナビゲーション ウィンドウで [ポリシーの概要（Policy Summary）] をクリックします。
- レイヤの概要ページを表示する：レイヤの概要ページを表示するには、レイヤに対応する行のレイヤ名をクリックするか、ユーザーレイヤの横にある [編集（Edit）]（ ） をクリックします。[表示（View）]（ ） をクリックして、共有レイヤの読み取り専用サマリーページにアクセスすることもできます。

ステップ 3 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

レイヤでの侵入ルール

レイヤの [ルール（Rules）] ページで個々のレイヤ設定を表示することも、[ルール（Rules）] ページのポリシー ビューですべての設定の最終的な効果を表示することもできます。[ルール（Rules）]ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[ルール（Rules）] ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 *170 :* レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルール状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。 基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を [継承（Inherit）] に設定します。侵入ポリシーの [ルール（Rules）] ページは、すべてのルール設定の最終的な効果を示す複合ビューであるため、このページでの作業中にルールの状態を [継承（Inherit）] に設定することはできないことに注意してください。
1	しきい値 SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。
1 つ以上	抑制 レートベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。
1 つ以上	コメント	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。

たとえば、あるレイヤでルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）] に設定し、それよりも上位のレイヤで [無効（Disabled）] に設定した場合、侵入ポリシーの [ルール（Rules）] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[ルール（Rules）] ページには、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレートベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

特定のレイヤの各 [ルール（Rules）] ページの色分けでは、有効状態が上位レイヤ、下位レイヤ、現在のレイヤのどれに該当するのかが次の色で示されます。

- 赤：上位レイヤでの有効状態
- 黄色：下位レイヤでの有効状態
- 陰影なし：現在のレイヤでの有効状態

侵入ポリシーの [ルール（Rules）] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。

レイヤでの侵入ルールの設定

侵入ポリシーでは、すべてのユーザー設定可能なレイヤのルールに対して、ルール状態、イベント フィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [ルール（Rules）] ページの設定を、侵入ポリシーの [ルール（Rules）] ページの設定と同じように追加します。

手順

ステップ 1 Snort 2 侵入ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 変更するポリシー階層を展開します。

ステップ 3 変更するポリシー レイヤのすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを使用した侵入ポリシーの調整 （2013 ページ） に示されている任意の設定を変更します。

ヒント
編集可能なレイヤから個々の設定を削除するには、そのレイヤの [ルール（Rules）] ページでルール メッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [Delete] をクリックして [OK] を 2 回クリックします。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

複数のレイヤからのルール設定の削除

侵入ポリシーの複数のレイヤから、特定のタイプのイベント フィルタ、動的状態、またはアラートを同時に削除できます。システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。後者の場合、そのレイヤから設定が削除され、設定タイプの削除が停止されます。

共有レイヤまたは基本ポリシーに指定されたタイプの設定があり、ポリシーの最上位レイヤが編集可能である場合は、ルールの残りの設定とルール状態がその編集可能なレイヤにコピーされます。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

（注） 共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。

手順

ステップ 1 Snort 2 侵入ポリシーの編集中に、ナビゲーションパネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。Snort 2 ポリシーにアクセスするには、[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policies）] タブ を選択し、編集するポリシーに対して [Snort 2] をクリックします。 > >

ヒント
また、任意のレイヤの [ルール（Rules）] ページでレイヤのドロップダウンリストから [ポリシー（Policy）] を選択するか、[ポリシー情報（Policy Information）] ページの [ルールの管理（Manage Rules）] をクリックすることもできます。

ステップ 2 複数の設定を削除するルールを選択します。

- 特定の選択（Choose specific）：特定のルールを選択するには、各ルールの横にあるチェックボックスをオンにします。
- すべて選択（Choose all）：現在のリストのルールをすべて選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 3 次のいずれかのオプションを選択します。

- **[イベントのフィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）]**
- **[イベントのフィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）]**
- **[動的状態（Dynamic State）] > [レート ベースのルール状態の削除（Remove Rate-Based Rule States）]**
- **[アラート（Alerting）] > [SNMP アラートの削除（Remove SNMP Alerts）]**

（注）
共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

カスタム基本ポリシーからのルール変更の受け入れ

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーが別のカスタム ポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、または SNMP アラートを削除する場合、および
- 基本ポリシーとして使用する他のカスタム ポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

手順

ステップ 1 Snort 2 侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 [個人用の変更（My Changes）] を展開します。

ステップ 3 [個人用の変更（My Changes）] のすぐ下にある [ルール（Rules）] リンクをクリックします。

ステップ 4 設定を受け入れるルールを選択します。次の選択肢があります。

- [特定ルールの選択（Choose specific rules）]：特定のルールを選択するには、各ルールの横にあるチェックボックスをチェックします。
- [すべてのルールを選択（Choose all rules）]：現在のリストのすべてのルールを選択する場合は、列の最上部にあるチェックボックスをチェックします。

ステップ 5 [ルール状態（Rule State）] ドロップダウン リストから、[継承（Inherit）] を選択します。

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

レイヤでのプリプロセッサと詳細設定

ネットワーク分析ポリシーでプリプロセッサを設定するときと、侵入ポリシーで詳細詳細を設定するときのメカニズムは同様です。プリプロセッサの有効化および無効化はネットワーク分析の [設定（Settings）] ページで行うことができ、侵入ポリシーの詳細設定の有効化および無効化は侵入ポリシーの [詳細設定（Advanced Settings）] ページで行うことができます。これらのページでは、すべての関連機能の有効な状態の概要も示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤでは無効になっていて上位レイヤでは有効になっている場合、[設定（Settings）] ページにはプリプロセッサが有効であるとして表示されます。これらのページで行った変更は、ポリシーの最上位レイヤに表示されます。Back Orifice プリプロセッサにはユーザ設定可能なオプションがないことに注意してください。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリ ページの設定ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。ナビゲーション パネルの [ポリシー層（Policy Layers）] の下のレイヤの名前を選択することによって、別のレイヤのサマリー ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、その機能の設定ページへのサブリンクがナビゲーションパネルのレイヤの名前の下に表示され、[編集（Edit）]（）がそのレイヤのサマリーページの機能の横に表示されます。レイヤで機能を無効にしたり、[継承（Inherit）] に設定した場合はこれらは表示されません。

プリプロセッサまたは詳細設定の状態（有効または無効）を設定すると、下位レイヤでのその機能の状態と構成設定が上書きされます。プリプロセッサまたは詳細設定についてその状態と設定を基本ポリシーまたは下位レイヤから継承する場合、状態を [継承（Inherit）] に設定します。[設定（Settings）] または [詳細設定（Advanced Settings）] ページで操作するときには、[継承（Inherit）] の選択項目は使用できないことに注意してください。また、現在有効にされている機能を継承すると、ナビゲーション パネルではその機能のサブリンクが表示されなくなり、設定ページではその機能の編集アイコンが表示されなくなることにも注意してください。

システムは、機能が有効にされている最上位レイヤの設定を使用します。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、あるレイヤでネットワーク分析 DCE/RPC プリプロセッサを有効にして変更し、それより上位のレイヤでプリプロセッサを有効にするが変更はしない場合、システムは上位レイヤのデフォルト設定を使用します。

各レイヤのサマリページは次のようにカラーコード化されており、有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤのいずれにあるかが示されます。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[設定（Settings）] および [詳細設定（Advanced Settings）] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラーコーディングを使用しません。

層のプリプロセッサと詳細の設定

手順

ステップ 1 Snort 2 ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] を展開し、変更するレイヤの名前をクリックします。

ステップ 2 次の選択肢があります。

- 層の名前を変更します。
- 説明を追加または変更します。
- [共有（Sharing）] チェックボックスをオンまたはオフにして、層を別のポリシーと共有できるようにするかどうかを指定します。
- 有効にしたプリプロセッサ/詳細設定の設定ページにアクセスするには、[編集（Edit）]（）または機能のサブリンクをクリックします。
- 現在の層のプリプロセッサ/詳細設定を無効にするには、機能の横にある [無効化（Disabled）] をクリックします。
- 現在の層のプリプロセッサ/詳細設定を有効にするには、機能の横にある [有効化（Enabled）] をクリックします。
- 現在の層の下にある最上位レイヤの設定からプリプロセッサ/詳細設定の状態および構成を継承するには、[継承（Inherit）] をクリックします。

ステップ 3 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

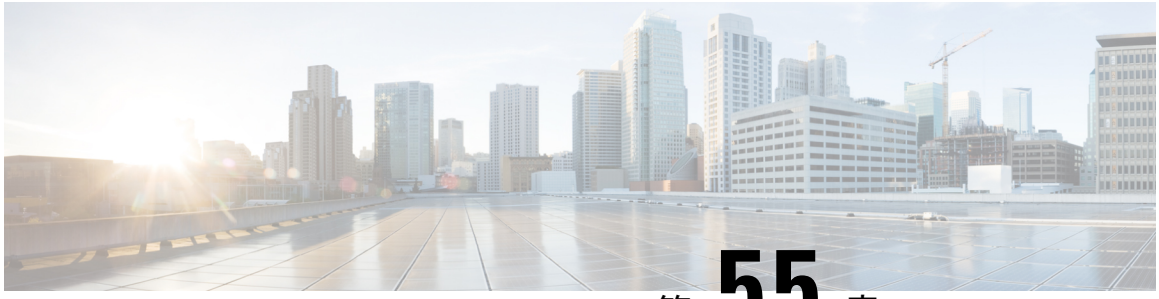
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）



第 55 章

ネットワーク資産に応じた侵入防御の調整

以下のトピックでは、Cisco 推奨ルールの使用方法について説明します。

- シスコ推奨ルールについて （2197 ページ）
- Cisco 推奨のデフォルト設定 （2198 ページ）
- Cisco 推奨事項の詳細設定 （2200 ページ）
- Cisco 推奨事項の生成と適用 （2201 ページ）
- スクリプト検出 （2202 ページ）

シスコ推奨ルールについて

侵入ルールの推奨事項を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらのアセットを保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

システムは、侵入ポリシーごとに個別の推奨事項のセットを作成します。これにより、通常、標準テキストルールと共有オブジェクトルールのルール状態の変更が推奨されます。ただし、プリプロセッサおよびデコーダのルールの変更も推奨されます。

ルール状態の推奨事項を生成する場合は、デフォルト設定を使用するか、詳細設定を指定できます。詳細設定では次の操作が可能です。

- システムが脆弱性をモニタするネットワーク上のホストを再定義する。
- ルール オーバーヘッドに基づき、システムが推奨するルールに影響を与える。
- ルールを無効にする推奨事項を生成するかどうかを指定する。

推奨事項をすぐに使用するか、推奨事項（および影響を受けるルール）を確認してから受け入れることができます。

推奨ルール状態を使用することを選択すると、読み取り専用のシスコ推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されます。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。

システムは、手動で設定されたルール状態を変更しません。

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる。
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる。

ヒント　侵入ポリシー レポートには、推奨状態と異なるルール状態を持つルールのリストを含めることができます。

推奨が絞り込まれた [ルール（Rules）] ページを表示している最中に、あるいは、ナビゲーション パネルまたは [ポリシー情報（Policy Information）] ページから [ルール（Rules）] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[ルール（Rules）] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。

（注）　Talos インテリジェンスグループ は、システム提供のポリシーでの各ルールの適切な状態を決定します。システムによって提供されるポリシーをベースポリシーとして使用し、システムがルールをシスコの推奨ルール状態に設定できるようにすると、侵入ポリシーのルールは、シスコが推奨するネットワークアセットの設定と一致します。

Cisco 推奨のデフォルト設定

Cisco 推奨を生成すると、システムがネットワーク資産に関連付けられた脆弱性から保護するルールの基本ポリシーを検索して、その基本ポリシー内のルールの現在の状態を特定します。システムによってルールの状態が推奨されますが、自身で設定する場合はルールを推奨される状態に設定します。

システムによって次の基本的な分析が実行され、推奨が生成されます。

表 *171* : 脆弱性に基づく ルール状態推奨

検出された資産がルールにより保護されるか	基本ポリシー ルール状態	推奨ルール状態
はい	無効	イベントを生成する（Generate Events）
	イベントを生成する（Generate Events）	イベントを生成する（Generate Events）
	ドロップおよびイベントの生成	ドロップおよびイベントの生成（Drop and Generate Events）
いいえ	任意	無効

表の次の点に注意してください。

- ベース ポリシーでルールが無効になっているか、または[イベントの生成（Generate Events）]に設定されている場合、推奨される状態は常に[イベントの生成（Generate Events）]です。

  たとえば、ベース ポリシーが [アクティブなルールなし（No Rules Active）] の場合（すべてのルールが無効になっている）、[ドロップしてイベントを生成する（Drop and Generate Events）] は推奨されません。

- [ドロップしてイベントを生成する（Drop and Generate Events）] は、ベース ポリシーですでに[ドロップしてイベントを生成する（Drop and Generate Events）]に設定されているルールにのみ推奨します。

  ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定して、そのルールを無効にするか、またはベース ポリシーで [イベントの生成（Generate Events）] に設定した場合は、ルールの状態を手動でリセットする必要があります。

Cisco 推奨ルールの詳細設定を変更せずに推奨を生成する場合は、システムが検出対象のネットワーク全体のすべてのホストのルール状態の変更を推奨します。

デフォルトで、システムは、オーバーヘッドが低または中のルールに対してのみ推奨を生成し、ルールを無効にする推奨を生成します。

システムは、Impact Qualification 機能を使用して無効にされた脆弱性に基づく侵入ルールのルール状態を推奨しません。

システムは、常に、ホストにマップされたサードパーティの脆弱性に関連付けられたローカル ルールを有効にするように推奨します。

マップされていないローカル ルールに対する状態推奨は生成されません。

関連トピック

サードパーティ製品のマッピング （2599 ページ）

Cisco 推奨事項の詳細設定

推奨とルール状態とのすべての差をポリシー レポートに含める（Include all differences between recommendations and rule states in policy reports）

デフォルトで、侵入ポリシー レポートには、ポリシーで有効になっているルール、つまり、[イベントを生成する（Generate Events）] と [ドロップしてイベントを生成する（Drop and Generate Events）] のいずれかに設定されているルールが表示されます。また、[すべての差を含める（Include all differences）] オプションを有効にすると、推奨されている状態が保存されている状態と異なるルールが一覧表示されます。ポリシー レポートの詳細については、設定の展開について （155 ページ）を参照してください。

検査対象のネットワーク（Networks to Examine）

モニタ対象のネットワークまたは推奨について検査する個々のホストを指定します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

指定したホスト内のアドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされます。

ホスト情報に基づいて特定のパケットのアクティブ ルール処理を動的に適応させる場合は、adaptive profile updates を有効にすることもできます。

推奨しきい値（ルール オーバーヘッドの指定）（Recommendation Threshold (By Rule Overhead)）

選択したしきい値をオーバーヘッドが超える侵入ルールが推奨または自動的に有効にされないようにします。

オーバーヘッドは、システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率に基づいています。オーバーヘッドが高いルールを許可すると、通常、より多くの推奨が生成されるようになりますが、システム パフォーマンスに影響を及ぼす可能性があります。[侵入ルール（Intrusion Rules）] ページのルール詳細ビューでルールのオーバーヘッドの評価を確認できます。

ただし、ルールを無効にする推奨ではルール オーバーヘッドが考慮されません。また、ローカル ルールは、サードパーティの脆弱性にマップされていない限り、オーバーヘッドがないものと見なされます。

特定の設定のオーバーヘッド評価のルールについて推奨を生成した場合でも、別のオーバーヘッドの推奨を生成してから、再び元のオーバーヘッド設定の推奨を生成することができます。推奨を生成する回数や生成時に使用する異なるオーバーヘッド設定の数に関係なく、同じルールセットについては、推奨を生成するたびに、オーバーヘッド設定ごとに同じルール状態の推奨が生成されます。たとえば、オーバーヘッドを「中」に設定して推奨を生成し、次に「高」にして推奨を生成してから、再び「中」にして推奨を生成することができます。ネットワーク上のホストとアプリケーションが変更されていなければ、オーバーヘッドが「中」の推奨は、どちらも、そのルール セットに対して同じになります。

ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）

Cisco の推奨に基づいて侵入ルールを無効にするかどうかを指定します。

ルールを無効にする推奨を受け入れると、ルールの適用範囲が制限されます。ルールを無効にする推奨を無視すると、ルールの適用範囲が拡大されます。

関連トピック

アダプティブプロファイルの更新とシスコの推奨ルール （2935 ページ）

Cisco 推奨事項の生成と適用

Cisco の推奨事項の使用を開始または停止する場合、ネットワークのサイズと侵入ルールセットに応じて、数分かかる場合があります。

始める前に

- Cisco の推奨事項には、次の要件があります。
  - Threat Defense ライセンス：IPS
  - 従来のライセンス：保護
  - ユーザの役割 ～ 管理者 または 侵入管理者
- 手順を開始する前に、ネットワーク検出ポリシーを設定します。Cisco の推奨事項が適切になるように、ネットワーク検出ポリシーを設定して内部ホストを定義します。ネットワーク検出のカスタマイズ （2658 ページ）を参照してください。

手順

ステップ 1 Snort 2 侵入ポリシーエディタのナビゲーションウィンドウで、[Cisco推奨事項（Cisco Recommendations）] をクリックします。

ステップ 2 （オプション）詳細設定を設定します。Cisco 推奨事項の詳細設定 （2200 ページ）を参照してください。

ステップ 3 推奨事項を生成して適用します。

- **推奨事項の生成および使用（Generate and Use Recommendations）**：推奨事項を生成して、一致するようにルール状態を変更します。これまでに推奨事項を生成したことがない場合にのみ使用できます。
- **推奨事項の生成（Generate Recommendations）**：推奨事項を使用しているかどうかに関係なく、新しい推奨事項を生成しますが、一致するようにルールの状態を変更しません。
- **推奨事項の更新（Update Recommendations）**：推奨事項を使用している場合は、推奨事項を生成してルールの状態を一致するように変更します。それ以外の場合は、ルールの状態を変更することなく、新しい推奨事項を生成します。

- **推奨事項の使用（Use Recommendations）**：ルールの状態を未実装の推奨事項に一致するように変更します。
- **推奨事項を使用しない（Do Not Use Recommendations）**：推奨事項の使用を停止します。推奨事項の適用前にルールの状態を手動で変更した場合、ルールの状態は指定した値に戻ります。それ以外の場合、ルールの状態はデフォルト値に戻ります。

推奨事項の生成時に、システムは推奨される変更の概要を表示します。システムによって状態の変更が推奨されるルールのリストを表示するには、新しく提案されたルール状態の横にある[表示（View）] をクリックします。

ステップ 4 実装した推奨事項を評価して調整します。

ほとんどの Cisco の推奨事項を承認する場合でも、ルールの状態を手動で設定することで、推奨事項を個別に上書きできます。侵入ルール状態の設定（2032 ページ）を参照してください。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

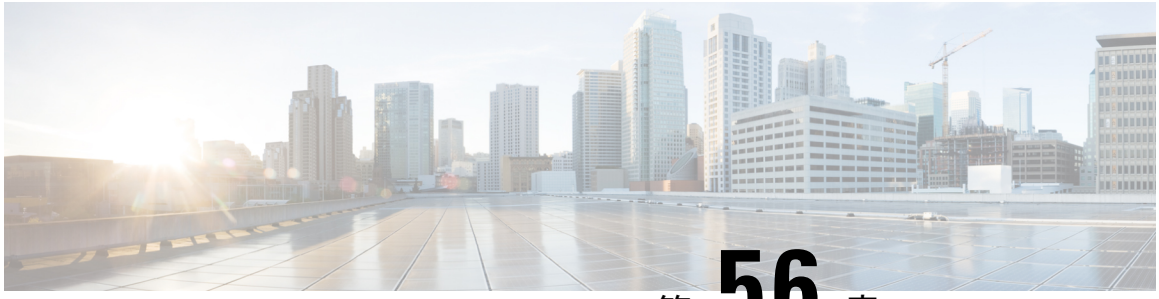
次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

スクリプト検出

スクリプト検出は、部分的な検査で Snort ブロックの手遅れになった侵入による障害を防ぎます。HTML ファイルがクライアントとサーバーの間で転送されるときに、これらのファイルに悪意のあるスクリプト（攻撃を開始するための JavaScript など）が含まれている可能性があります。このような悪意のあるスクリプトが検出された場合、部分的な検査により任意の IPS ルールを悪意のあるスクリプトと照合することができ、インスペクタが検査と検出を通じてそのデータセグメントをフラッシュします。悪意のあるファイルが宛先に到達することはありません。この機能は、HTTP/1 と HTTP/2 の両方のトラフィックをサポートしています。

この機能はデフォルトで常に有効になっています。オフにするには、**`http_inspect.script_detection=true`** を false に設定します。



第 56 章

機密データの検出

ここでは、機密データ検出とその設定方法について説明します。

- 機密データ検出の基本 （2203 ページ）
- グローバル センシティブ データ検出オプション （2205 ページ）
- 個別のセンシティブ データ タイプのオプション （2205 ページ）
- システム提供のセンシティブ データのタイプ （2206 ページ）
- 機密データの検出のライセンス要件 （2207 ページ）
- 機密データの検出の要件と前提条件 （2208 ページ）
- センシティブ データ検出の設定 （2208 ページ）
- 監視対象のアプリケーション プロトコルおよび機密データ （2210 ページ）
- モニター対象のアプリケーション プロトコルの選択 （2210 ページ）
- 特別なケース：FTP トラフィックでのセンシティブ データの検出 （2212 ページ）
- カスタム 機密データ タイプ （2213 ページ）

機密データ検出の基本

社会保障番号、クレジット カード番号、運転免許証番号などのセンシティブ データは、インターネットに意図的に、または誤って漏洩される可能性があります。システムには、ASCII テキストのセンシティブ データに関するイベントを検出し、生成できるセンシティブ データ プロセッサが用意されています。このプロセッサは、特に誤って漏洩されたデータの検出に役立ちます。

グローバル センシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジット カード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト
- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータ タイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データ タイプをモニターする宛先ポート
- 各データ タイプをモニターするアプリケーション プロトコル

指定するデータ パターンを検出するためのカスタム データ タイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータ タイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータ タイプを作成したりすることが考えられます。

システムはトラフィックに対して個別のデータ タイプを照合することによって、TCPセッションごとにセンシティブ データを検出します。侵入ポリシーの、各データ タイプのデフォルト設定およびすべてのデータ タイプに適用されるグローバル オプションのデフォルト設定は変更できます。Firepower システムには、一般的に使用されているデータ タイプがすでに定義されています。カスタム データ タイプを作成することも可能です。

センシティブデータのプリプロセッサルールは、各データタイプに関連付けられます。各データ タイプのセンシティブ データ検出とイベント生成を有効にするには、そのデータ タイプに対応するプリプロセッサ ルールを有効にします。設定ページのリンクを使用すると、センシティブ データ ルールにフィルタリングされたビューが [ルール（Rules）] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入ポリシーに保存する際に提示されるオプションによって、データタイプに関連付けられたルールが有効になっていてセンシティブデータ検出が無効になっている場合には、自動的にセンシティブ データ プリプロセッサを有効にすることができます。

ヒント 機密データ プリプロセッサでは、FTP またはHTTP を使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内の機密データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

このシステムは、暗号化または難読化された機密データ、あるいは圧縮または符号化された形式の機密データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)123-4567 を検出しますが、(5 5 5) 1 2 3 - 4 5 6 7 のようにスペースで難読化されたバージョン、あるいは (555)-123--4567 のようにHTML コードが介在するバージョンは検出しません。ただし、(555)-123-4567 のように、HTMLにコーディングされた番号のパターンの途中にコードが入っていなければ検出されます。

グローバル センシティブ データ検出オプション

グローバル センシティブ データ オプションはポリシーに固有であり、すべてのデータ タイプに適用されます。

マスク

ルールをトリガーしたパケットで、クレジット カード番号および社会保障番号の下位4桁を除くすべての桁を「X」に置換します。Web インターフェイスの侵入イベント パケット ビューおよびダウンロードされたパケットでは、マスクされた番号が表示されます。

ネットワーク

センシティブ データをモニターする1つ以上の宛先ホストを指定します。単一のIPアドレス、アドレスブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、`any` として解釈されます。これは、任意の宛先 IP アドレスを意味します。

グローバルしきい値（Global Threshold）

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データ タイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ～ 65535 の値を指定できます。

シスコでは、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出して イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大1件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

個別のセンシティブ データ タイプのオプション

最低でも、カスタム データ タイプごとにイベントしきい値を指定し、モニタする少なくとも1 つのポートまたはアプリケーション プロトコルを指定する必要があります。

各システム定義済みデータ タイプでは、デフォルト値が変更されない限り、アクセス不能な sd_pattern キーワードを使用して、トラフィックで検出する組み込みデータ パターンを定義します。カスタム データ タイプを作成して、そのデータ タイプに対し、単純な正規表現を使用して独自のデータ パターンを指定することもできます。

センシティブ データ タイプは、センシティブ データ検出が有効になっているすべての侵入ポリシーに表示されます。システム提供のデータ タイプは読み取り専用として表示されます。カスタム データ タイプの場合、名前とパターン フィールドは読み取り専用として表示されますが、他のオプションはポリシー固有の値に設定できます。

表 *172 :* 個別のデータ タイプのオプション

オプション	説明
データ タイプ	データ タイプの一意の名前を指定します。
しきい値（Threshold）	イベント生成の基準とする、データ タイプのオカレンス数を指定します。1 ～ 255 の値を指定できます。 プリプロセッサが検出したデータ タイプに対して生成するイベント数は、セッションごとに 1 つであることに注意してください。グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立していることにも注意してください。つまり、データ タイプ イベントしきい値に達すると、グローバルイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も同様です。
宛先ポート（Destination Ports）	データ タイプでモニターする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する any を指定できます。
アプリケーション プロトコル（Application Protocols）	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。モニタするアプリケーション プロトコルを識別するには、アプリケーション ディテクタをアクティブにする必要があります。 従来のデバイスの場合、この機能には制御ライセンスが必要であることに注意してください。
パターン	検出するパターンを指定します。このフィールドは、カスタム データ タイプの場合にのみ存在します。

関連トピック

ディテクタのアクティブおよび非アクティブの設定 （2653 ページ）

システム提供のセンシティブ データのタイプ

それぞれの侵入ポリシーには、よく使用されるデータ パターンを検出するためのシステム提供のデータ タイプが含まれています。これらのデータ パターンには、クレジット カード番号、

電子メールアドレス、米国の電話番号、および米国の社会保障番号などがあります（番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります）。

それぞれのシステム提供のデータ タイプは、ジェネレータ ID（GID）が 138 に設定された単一のセンシティブ データのプリプロセッサ ルールに関連付けられます。侵入ポリシーで関連する機密データ ルールを有効にして、ポリシーで使用する各データ タイプに対して イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

次の表に、各データ タイプの説明と対応するプリプロセッサ ルールの一覧を示します。

表 *173*：システム提供のセンシティブ データのタイプ

データ タイプ	説明	プリプロセッサ ルール GID
クレジットカード番号	Visa®、MasterCard®、Discover®、および American Express® の 15 桁または 16 桁のクレジット カード番号（通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン）に一致します。また、Luhn アルゴリズムを使用してクレジット カード番号の検査数字を確認します。	138:2
電子メール アドレス	電子メール アドレスに一致します。	138:5
米国の電話番号	米国の電話番号（`(\d{3}) ?\d{3}-\d{4}` のパターンに準拠）に一致します。	138:6
米国の 社会保障番号（ハイフンなし）	米国の 9 桁の社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用していない番号）に一致します。	138:4
米国の 社会保障番号（ハイフンあり）	米国の 9 桁の社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用している番号）に一致します。	138:3

社会保障番号以外の 9 桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の 4 桁のシリアル番号の前にある 3 桁のエリア番号と 2 桁のグループ番号を検証するアルゴリズムを使用します。プリプロセッサは 2009 年 11 月末までの社会保障グループ番号を検証します。

機密データの検出のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護、または手順に示されているとおり。

機密データの検出の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

センシティブ データ検出の設定

機密データ検出は、システムのパフォーマンスに非常に大きな影響を与える可能性があるため、シスコでは以下のガイドラインに従うことを推奨しています。

- 基本侵入ポリシーとして [アクティブなルールなし（No Rules Active）] デフォルト ポリシーを選択します。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - **アプリケーション層プリプロセッサ**での **FTP と Telnet の設定**
  - [トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] の下の [IP 最適化（IP Defragmentation）] および [TCP ストリームの構成（TCP Stream Configuration）]

始める前に

クラシックデバイスの場合、この手順には 保護 または Control ライセンスが必要です。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（ ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブデータの検出（Sensitive Data Detection）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 6 次の選択肢があります。

- グローバルセンシティブデータ検出オプション（2205ページ）の説明に従って、グローバル設定を変更します。
- [ターゲット（Targets）] セクションでデータ タイプを選択し、個別のセンシティブ データ タイプのオプション（2205ページ）の説明に従って、データ タイプ構成を変更します。
- カスタムセンシティブデータを検査するには、カスタム機密データ タイプ（2213ページ）を参照してください。

ステップ 7 データ タイプでモニターするアプリケーション プロトコルを追加または削除します。監視対象のアプリケーション プロトコルおよび機密データ（2210 ページ）を参照してください。

（注）
FTP トラフィック内の機密データを検出するには、次の点を確認します。

- ファイルポリシーがアクセス コントロール ポリシーに対して有効になっていることを確認します。
- `Ftp data` アプリケーションプロトコルを追加する必要があります。

ステップ 8 オプションで、センシティブ データ プリプロセッサ ルールを表示するには、[センシティブ データ検出のルールの設定（Configure Rules for Sensitive Data Detection）] をクリックします。

リストされているルールを有効または無効にすることができます。[ルール（Rules）]ページで使用可能なその他の操作（ルールの抑制、レートベース攻撃防止など）のセンシティブデータルールも設定できます。詳細については、侵入ルールのタイプ（2014ページ）を参照してください。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

ポリシーでセンシティブ データ プリプロセッサ ルールを有効にして、センシティブ データ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブデータ検出を有効にするよう求めるプロンプトが出されます。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、センシティブ データ検出ルール（138:2、138:3、138:4、138:5、138:6、138:>999999、または 139:1）を有効にします。詳細については、侵入ルールの状態（2031ページ）、グローバルセンシティブデータ検出オプション（2205ページ）、システム提供のセンシティブデータのタイプ（2206ページ）、およびカスタム機密データタイプ（2213 ページ）を参照してください。
- 設定変更を展開します設定変更の展開（172 ページ）を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出（2212 ページ）

監視対象のアプリケーション プロトコルおよび機密データ

各データ タイプでモニタするアプリケーション プロトコルを最大 8 つ指定できます。選択するアプリケーションプロトコルごとに、少なくとも1つのディテクタを有効にする必要があります。デフォルトでは、すべてのディテクタがアクティブになっています。有効になっているディテクタがないアプリケーションプロトコルについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

各データ タイプをモニタするアプリケーション プロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブデータを検出する場合を除き、シスコでは最も包括的なカバレッジにするために、アプリケーションプロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定するとしたら、既知の HTTP ポート 80 を設定することお勧めします。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーション プロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブ データを検出する場合は、`FTP data` アプリケーション プロトコルを指定する必要があります。この場合、ポート番号を指定する利点はありません。

関連トピック

ディテクタのアクティブおよび非アクティブの設定（2653 ページ）
特別なケース：FTP トラフィックでのセンシティブ データの検出（2212 ページ）

モニター対象のアプリケーション プロトコルの選択

モニター対象のアプリケーション プロトコルは、システムが提供するセンシティブ データ タイプとカスタムのセンシティブデータ タイプの両方で指定できます。選択するアプリケーション プロトコルはポリシー固有になります。

始める前に

クラシックデバイスの場合、この手順には Control ライセンスが必要です。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブデータの検出（Sensitive Data Detection）] の横にある[編集（Edit）]（）をクリックします。

ステップ 6 [データ タイプ（Data Types）] の下でデータ タイプの名前をクリックします。

ステップ 7 [アプリケーションプロトコル（Application Protocols）] フィールドの横にある [編集（Edit）]（） をクリックします。

ステップ 8 次の選択肢があります。

- モニターするアプリケーションプロトコルを追加するには、[使用可能（Available）] リストからアプリケーションプロトコルを 1 つ以上選択して、右矢印（[>]）をクリックします。モニタするアプリケーション プロトコルは、8 つまで追加できます。
- モニター対象からアプリケーションプロトコルを削除するには、[有効（Enabled）] リストから削除するプロトコルを選択して、左矢印（[<]）をクリックします。

ステップ 9 [OK] をクリックします。

ステップ 10 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、ナビゲーション ウィンドウで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出 （2212 ページ）

特別なケース：FTP トラフィックでのセンシティブ データの検出

一般に、センシティブデータをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、アプリケーション プロトコルを指定します。

ただし、FTP トラフィックでセンシティブ データを検出するには、ポートまたはアプリケーション プロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブ データは、FTPアプリケーションプロトコルのトラフィックで検出されますが、FTPアプリケーション プロトコルは断続的に発生し、一時的なポート番号を使用するため、センシティブ データを検出するのが困難です。FTP トラフィックでセンシティブデータを検出するには、以下の設定を含めることが**必須**となります。

- `FTP data` アプリケーション プロトコルを指定すると、FTP トラフィックでのセンシティブ データの検出が可能になります。

  FTP トラフィックでセンシティブ データを検出するという特殊な場合では、`FTP data` アプリケーションプロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブ データを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。

- FTP データ ディテクタが有効であることを確認します（デフォルトで有効にされています）。
- 設定に、センシティブデータをモニターするポートが少なくとも 1 つ含まれていることを確認します。
- ファイルポリシーがアクセス コントロール ポリシーに対して有効になっていることを確認します。

FTP トラフィックでセンシティブデータを検出することだけが目的の場合を除き（そのような場合はほとんどありません）、FTP ポートを指定する必要はありません。通常のセンシティブデータ設定には、HTTP ポートや電子メール ポートなどの他のポートが含まれることになります。モニター対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、シスコでは FTP コマンド ポート `23` を指定することを推奨しています。

関連トピック

FTP/Telnet デコーダ （2787 ページ）
ディテクタのアクティブおよび非アクティブの設定 （2653 ページ）
センシティブ データ検出の設定 （2208 ページ）

カスタム 機密データ タイプ

作成するカスタム データ タイプごとに、単一の機密データ プリプロセッサ ルールも作成します。このルールのジェネレータ ID（GID）は 138 で、[Snort ID]（SID）は 1000000 以上（これは、ローカル ルールの SID）です。

ポリシーで使用する各カスタム データ タイプに対し、関連付けられた機密データ ルールを有効にして検出を有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

機密データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべてのシステム定義済み機密データ ルールおよびカスタム機密データ ルールを表示するフィルタリングされたビューの侵入ポリシーの [ルール（Rules）] ページが表示されます。また、侵入ポリシーの [ルール（Rules）] ページでローカル フィルタリング カテゴリを選択することで、カスタム機密データ ルールをカスタム ローカル ルールとともに表示できます。カスタム機密データ ルールは、侵入ルール エディタ ページ（**[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]**）には表示されないことに注意してください。

カスタムデータタイプを作成すると、システム内の任意の侵入ポリシーで有効にすることができます。カスタム データ タイプを有効にするには、そのカスタム データ タイプの検出に使用するポリシーで、関連する機密データ ルールを有効にする必要があります。

カスタム機密データ タイプのデータ パターン

カスタム データ タイプのデータ パターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字は正規表現内で特別な意味を持つリテラル文字です。

表 *174 :* 機密データ パターンのメタ文字

メタ文字	説明	例
?	先行する文字またはエスケープ シーケンスのゼロまたは 1 つのオカレンスに一致します。つまり、先行する文字またはエスケープ シーケンスはオプションです。	`colou?r` は、`color` または `colour` に一致します。
{n}	先行する文字またはエスケープ シーケンスの n 回の繰り返しに一致します。	たとえば、`\d{2}` は `55`、`12` などに `\l{3}` は `AbC`、`www` など、`\w{3}` は `a1B`、25C など、`x{5}` は`xxxxx` に一致します

メタ文字	説明	例
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\? は疑問符、\\ はバックスラッシュ、\d は数字に一致します。

特定の文字をリテラル文字として機密データ プリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 *175*：機密データ パターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

カスタム機密データ パターンを定義するときは、文字クラスを使用できます。

表 *176*：機密データ パターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ～ 9 に一致します。	0 ～ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ～ 9 以外
\l（小文字の「エル」）	任意の ASCII 文字に一致します。	a ～ zA ～ Z
\L	ASCII 文字ではないバイトに一致します。	a ～ z および A ～ Z 以外
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア（_）は含まれないことに注意してください。	a ～ z、A ～ Z、および 0 ～ 9
\W	ASCII 英数字でないバイトに一致します。	a ～ z、A ～ Z、および 0 ～ 9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データ パターン 1234 は 1234 に一致します。

以下に、システム定義済み機密データ ルール 138:4 で使用するデータ パターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオ

プション指定子のメタ文字、リテラル ハイフン（-）文字、および左右の括弧 () 文字を使用して、米国の電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタム データ パターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータ パターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})? ?\d{3}-?\d{4}
```

上記の2番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- `(555)123-4567`
- `555123-4567`
- `5551234567`

ただし、2 番目の例のパターンでは、以下の潜在的に無効な無効なパターンも検出されて、結果的に誤検出となります。

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の `a` を検出するデータ パターンを作成するとします。このようなデータ パターンは、わずか数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

カスタム センシティブ データ タイプの設定

データ タイプのセンシティブ データ ルールがいずれかの侵入ポリシーで有効にされている場合、そのデータ タイプを削除することはできません。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（ ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブデータの検出（Sensitive Data Detection）] の横にある[編集（Edit）]（）をクリックします。

ステップ 6 [データタイプ（Data Types）] の横にある[追加（Add）] ()をクリックします。

ステップ 7 データ タイプの名前を入力します。

ステップ 8 このデータ タイプで検出するパターンを入力します。カスタム機密データ タイプのデータ パターン （2213 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 必要に応じて、データ タイプ名をクリックし、個別のセンシティブ データ タイプのオプション （2205 ページ）で説明されているオプションを変更します。

ステップ 11 必要に応じて、[削除（Delete）]（）をクリックしてカスタムデータタイプを削除し、[OK] をクリックして確認します。

（注）
いずれかの侵入ポリシーでデータ タイプのセンシティブ データ ルールが有効になっている場合は、そのデータ タイプを削除できないことが警告されます。再度削除を試みる前に、影響を受けるポリシーでセンシティブ データ ルールを無効にする必要があります。侵入ルール状態の設定 （2032 ページ）を参照してください。

ステップ 12 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- データ型を使用する各ポリシーで、関連付けられたカスタム センシティブ データの前処理ルールを有効にします。侵入ルール状態の設定 （2032 ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

カスタムセンシティブ データ タイプの編集 （2216 ページ）

カスタムセンシティブ データ タイプの編集

カスタム センシティブ データ タイプのすべてのフィールドを編集できます。ただし、名前またはパターン フィールドを変更すると、システム内のすべての侵入ポリシーのこれらの設定が変更されることに注意してください。その他のオプションは、ポリシー固有の値に設定できます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある [編集（Edit）] をクリックします。

ステップ 6 [ターゲット（Targets）] セクションで、カスタム データ タイプの名前をクリックします。

ステップ 7 [データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] をクリックします。

ステップ 8 データ タイプの名前およびパターンを変更します。カスタム機密データ タイプのデータ パターン （2213 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

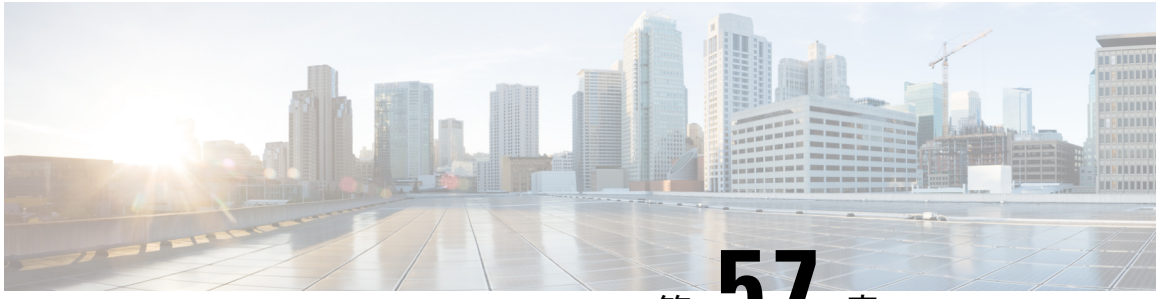
ステップ 10 残りのオプションをポリシー固有の値に設定します。個別のセンシティブ データ タイプのオプション （2205 ページ）を参照してください。

ステップ 11 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。



第 57 章

侵入イベントロギングのグローバル制限

次のトピックでは、侵入イベントロギングをグローバルに制限する方法について説明します。

- グローバル ルールのしきい値の基本 （2219 ページ）
- グローバル ルールしきい値オプション （2220 ページ）
- グローバルなしきい値のライセンス要件 （2222 ページ）
- グローバルしきい値の要件と前提条件 （2222 ページ）
- グローバルなしきい値の設定 （2223 ページ）
- グローバルしきい値の無効化 （2224 ページ）

グローバル ルールのしきい値の基本

グローバル ルールのしきい値は、侵入ポリシーによってイベント ロギングの限界を設定します。すべてのトラフィックに対するグローバル ルールのしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントがポリシーで記録および表示される頻度を制限できます。ポリシー内で共有オブジェクトのルール、標準テキストルール、またはプリプロセッサルールごとにしきい値を設定できます。グローバルしきい値を設定すると、上書きする特定のしきい値を指定していないポリシー内の各ルールでそのしきい値が適用されます。しきい値により、多数のイベントでいっぱいになることを回避できます。

すべての侵入ポリシーにはデフォルトのグローバル ルールしきい値が含まれていて、デフォルトですべての侵入ルールとプリプロセッサ ルールに適用されます。このデフォルトのしきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。

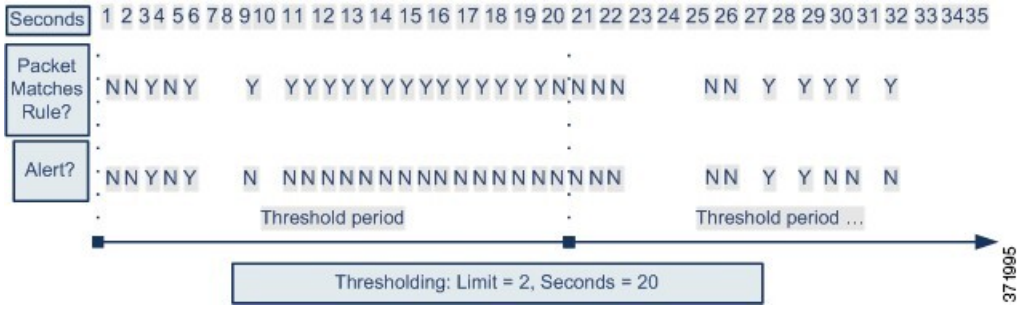
次の操作を実行できます。

- グローバルしきい値の変更。
- グローバルしきい値の無効化。
- 特定のルールに個別のしきい値を設定して、グローバルしきい値の上書き。

  たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。

ヒント　複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

次の図で、グローバルルールのしきい値がどのように機能するかを示します。この例では、特定のルールに対して攻撃が進行中です。グローバル制限しきい値は、各ルールのイベント生成が 20 秒あたり 2 つのイベントに制限されるように設定されています。期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の2つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



グローバル ルールしきい値オプション

デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。グローバル ルールしきい値オプションのデフォルト値は次のとおりです。

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

これらのデフォルト値は次のように変更することができます。

表 *177:* しきい値のタイプ

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。 たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。

オプション	説明
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。 たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは 1 つのイベントを生成すると、[Seconds] と [Count] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
Both	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに1回イベントを記録して表示します。 たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーされると、しきい値が満たされ、以後のイベントは無視されるため）。

[追跡対象（Track By）] オプションにより、イベント インスタンスの数が送信元 IP アドレスと宛先 IP アドレスのどちらに基づいて計算されるかが決まります。

また、しきい値を定義するインスタンスの数と期間を次のように指定できます。

表 *178*：インスタンス/時間のしきい値設定オプション

オプション	説明
カウント	[制限（Limit）] しきい値の場合は、しきい値を満たすために必要な、追跡する IP アドレスまたはアドレス範囲単位で指定された期間単位のイベント インスタンスの数。 [しきい値（Threshold）] しきい値の場合は、しきい値として使用するルールの一致回数。

オプション	説明
秒（Seconds）	[制限（Limit）] しきい値の場合は、攻撃を追跡する期間の秒数。 [しきい値（Threshold）] しきい値の場合は、カウントをリセットするまでの経過時間（秒数）。しきい値タイプを [Limit] に、トラッキングを [Source] に、[Count] を 10 に、[Seconds] を 10 に設定した場合、特定のソース ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

関連トピック

グローバルなしきい値の設定 （2223 ページ）
侵入イベントしきい値 （2033 ページ）

グローバルなしきい値のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

グローバルしきい値の要件と前提条件

モデルのサポート

いずれか（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

グローバルなしきい値の設定

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [侵入ルールしきい値（Intrusion Rule Thresholds）] で [グローバル ルールしきい値（Global Rule Thresholding）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [グローバルルールしきい値（Global Rule Thresholding）] の横にある [編集（Edit）]（） をクリックします。

ステップ 6 [タイプ（Type）] を使用して、[秒（Seconds）] フィールドで指定された時間内に適用するしきい値のタイプを指定します。

ステップ 7 [追跡対象（Track By）] を使用して、追跡方法を指定します。

ステップ 8 [カウント（Count）] フィールドに値を入力します。

ステップ 9 [秒（Seconds）] フィールドに値を入力します。

ステップ 10 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

グローバル ルールしきい値オプション （2220 ページ）
レイヤでの侵入ルールの設定 （2191 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

グローバルしきい値の無効化

デフォルトですべてのルールにしきい値を適用するのではなく、特定のルールに関するイベントにしきい値を適用する場合は、最高位のポリシー階層でグローバルしきい値を無効にできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（ ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [侵入ルールしきい値（Intrusion Rule Thresholds）] で、[グローバル ルールしきい値（Global Rule Thresholding）] の隣にある [無効（Disabled）] をクリックします。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

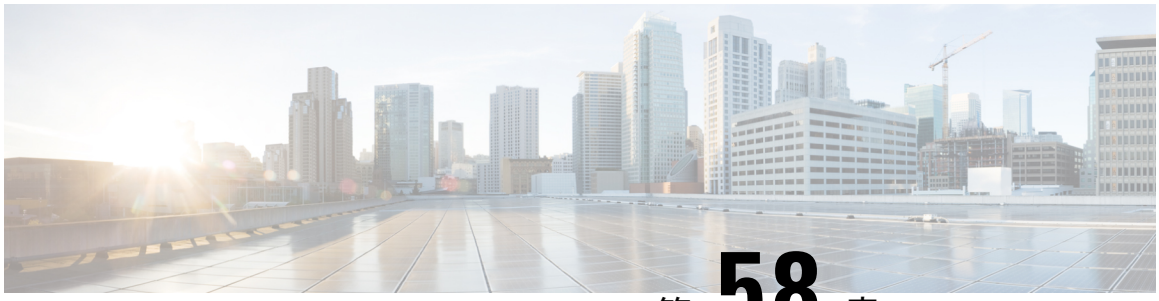
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）
レイヤでの侵入ルールの設定 （2191 ページ）



第 58 章

侵入防御のパフォーマンスの調整

以下のトピックでは、侵入防御のパフォーマンスを調整する方法について説明します。

- 侵入防御のパフォーマンス チューニングについて （2225 ページ）
- 侵入防御パフォーマンスの調整のライセンス要件 （2226 ページ）
- 侵入防御パフォーマンスの調整の要件と前提条件 （2226 ページ）
- 侵入に関するパターン一致の制限 （2227 ページ）
- 正規表現による侵入ルールのオーバーライドの制限 （2228 ページ）
- 侵入ルールの正規表現制限のオーバーライド （2229 ページ）
- パケットごとの侵入イベント生成の制限 （2230 ページ）
- パケットごとに生成される侵入イベントの制限 （2231 ページ）
- パケットおよび侵入ルールの遅延しきい値構成 （2231 ページ）
- 侵入パフォーマンス統計情報のロギング設定 （2239 ページ）
- 侵入パフォーマンス統計情報のロギングの設定 （2240 ページ）

侵入防御のパフォーマンス チューニングについて

Cisco では、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能を提供しています。次の操作を実行できます。

- イベントキューで許可するパケット数を指定できます。ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。
- パケットペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。
- 複数のイベントが生成された場合にパケットまたはパケットストリームごとに複数のイベントをルールエンジンがログに記録するようにして、レポートされるイベント以外の情報も収集できます。
- デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを保つことができます。

- デバイスがそのパフォーマンスをモニタおよび報告する動作に関する基本的なパラメータを設定できます。システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

これらのパフォーマンス設定は、各アクセス コントロール ポリシーごとに設定し、その設定はその親のアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

侵入防御パフォーマンスの調整のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入防御パフォーマンスの調整の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

侵入に関するパターン一致の制限

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）]（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[編集（Edit）]** > **[その他（More）]** > **[詳細設定（Advanced Settings）]**）をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある[編集（Edit）]（✎）をクリックします。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップウィンドウ内の [パターン一致の制限（Pattern Matching Limits）] をクリックします。

ステップ 4 [パケットごとに分析するパターン状態の最大値（Maximum Pattern States to Analyze Per Packet）] フィールドに、キューに含めるイベントの最大数の値を入力します。

ステップ 5 Snort 2 で、ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[今後の再構成の対象となるトラフィックでコンテンツチェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] チェックボックスをオンにします。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。

重要
Snort 3 では、[今後の再構成の対象となるトラフィックでコンテンツチェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] チェックボックスの設定は次のとおりです。

- オン：再構成前に TCP ペイロードを検出することを示します。これには、ストリームの再構成の前後のパケットのインスペクションが含まれます。このプロセスでは、より多くの処理オーバーヘッドが必要になり、パフォーマンスが低下する可能性があります。
- オフ：再構成後に TCP ペイロードを検出することを示します。

ステップ 6 [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

正規表現による侵入ルールのオーバーライドの制限

デフォルトの正規表現の制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

注意 非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザ以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

表 *179* : 正規表現の制約オプション

オプション	説明
検索結果の制限状態（Match Limit State）	[制限に合わせる（Match Limit）] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[制限に合わせる（Match Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の試行を許可する • [カスタム（Custom）] を選択して、[制限に合わせる（Match Limit）] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
制限に合わせる（Match Limit）	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。

オプション	説明
検索結果の再起制限状態（Match Recursion Limit State）	[再起制限に合わせる（Match Recursion Limit）] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の再帰を許可する • [カスタム（Custom）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [再起制限に合わせる（Match Recursion Limit）] が意味を持つためには、[制限に合わせる（Match Limit）] よりも小さい必要があることに注意してください。
再起制限に合わせる（Match Recursion Limit）	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

関連トピック

概要：pcre キーワード （2098 ページ）

侵入ルールの正規表現制限のオーバーライド

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある[編集（Edit）]（✎）をクリックします。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップウィンドウ内の [正規表現の制限（Regular Expression Limits）] をクリックします。

ステップ 4 正規表現による侵入ルールのオーバーライドの制限（2228ページ）で説明するオプションを変更できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

パケットごとの侵入イベント生成の制限

侵入ルールエンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザ インターフェイスに報告します。侵入イベント ロギングの制限を設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

表 *180 :* 侵入イベント ロギング制限のオプション

オプション	説明
パケットごとに保存されるイベントの最大数（Maximum Events Stored Per Packet）	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
パケットごとにログに記録されるイベントの最大数（Maximum Events Logged Per Packet）	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[パケットごとに保存されるイベントの最大数（Maximum Events Stored Per Packet）] 値を超えてはいけません。
イベント ロギングの順位決定の基準（Prioritize Event Logging By）	イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。 • `priority`。イベントの優先順位によってキュー内のイベントを並べ替えます。 • `content_length`。最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコーダ イベントおよびプリプロセッサ イベントよりも優先されます。

パケットごとに生成される侵入イベントの制限

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある[編集（Edit）]（✎）をクリックします。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップウィンドウ内の [侵入イベントのログ制限（Intrusion Event Logging Limits）] をクリックします。

ステップ 4 パケットごとの侵入イベント生成の制限（2230ページ）に示したオプションを変更できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

パケットおよび侵入ルールの遅延しきい値構成

各アクセス コントロール ポリシーには、しきい値を使用してパケットとルールの処理パフォーマンスを管理する、遅延ベースの設定があります。

パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

ルール遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間が遅延しきい値ルールをある回数（設定可能）連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

遅延ベースのパフォーマンス設定

デフォルトでシステムが使用するパフォーマンス設定は、システムに導入された最新の侵入ルールの更新の遅延ベースのパフォーマンス設定です。

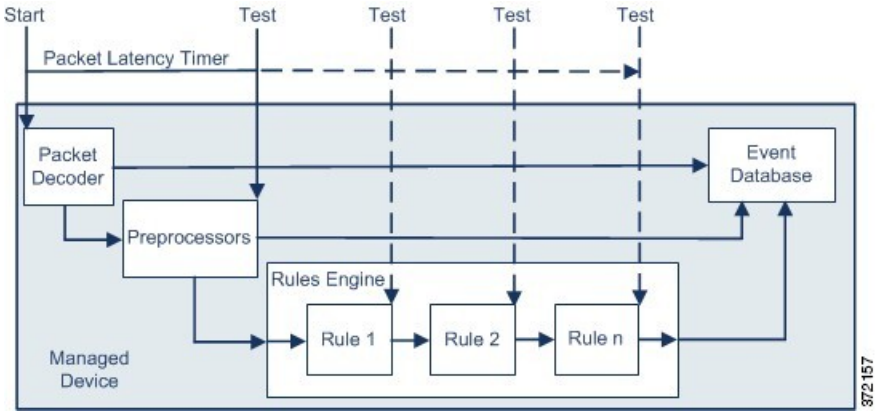
実際に適用される遅延の設定は、アクセス コントロール ポリシーと関連付けられているネットワーク分析ポリシー（NAP）のセキュリティ レベルによって異なります。通常、デフォルトの NAP ポリシーが関連付けられます。ただし、カスタム ネットワーク分析ルールが設定されている場合、ルールの中にデフォルトの NAP ポリシーより強力な NAP ポリシーを指定しているものがあれば、カスタム ルールの中で最もセキュアな NAP ポリシーが、遅延の設定のベースとなります。デフォルトの NAP ポリシーまたはカスタム ルールによってカスタム NAP ポリシーが呼び出された場合、評価で使用されるセキュリティ レベルは、それぞれのカスタム NAP ポリシーがベースとするシステム提供のベース ポリシーになります。

以上の説明は、有効なしきい値やネットワーク分析の設定が継承されるか、ポリシーに直接構成されるかにかかわらず当てはまります。

パケット遅延しきい値構成

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミング テスト ポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間が任意のテスト ポイントでしきい値を超えると、パケットの検査は停止します。

ヒント　パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケット処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

（注）　パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

パケット遅延のしきい値は、パッシブおよびインライン展開の両方でシステムのパフォーマンスを向上させ、インライン展開では過度の処理時間を必要とするパケットの検査を停止することにより遅延を低減できます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

パケット遅延しきい値構成の注意事項

デフォルトでは、パケット処理に関する遅延ベースのパフォーマンス設定は無効になっています。この設定を有効にすることもできます。ただし、シスコはしきい値設定のデフォルト値を変更しないことを推奨します。

下の情報は、カスタム値の指定を選択した場合にのみ適用されます。

表 *181* : パケット遅延しきい値構成オプション

オプション	説明
しきい値（マイクロ秒）（Threshold (microseconds)）	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。

パケット遅延しきい値の有効化

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある[編集（Edit）]（✎）をクリックします。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。

ステップ 3 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップウィンドウで [パケット処理（Packet Handling）] をクリックします。

ステップ 4 [有効（Enabled）] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

パケット遅延しきい値の設定

デフォルトでは、パケット処理に関する遅延ベースのパフォーマンス設定は無効になっています。この設定を有効にすることもできます。ただし、シスコはしきい値設定のデフォルト値を変更しないことを推奨します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある[編集（Edit）]（✎）をクリックします。

[システム（System）]（⚙） > **[モニタリング（Monitoring）]** > **[統計（Statistics）]**

ステップ 3 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 4 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップウィンドウで [パケット処理（Packet Handling）] をクリックします。

デフォルトで、[インストール済みのルールの更新（Installed Rule Update）] が選択されます。このデフォルトを使用することを推奨します。

表示された値には、自動設定が反映されません。

ステップ 5 カスタム値を指定する場合は、次の点に注意してください。

- [有効（Enabled）] チェックボックスをオンにして、パケット遅延しきい値構成の注意事項（2233 ページ）を参照して推奨される最小の [しきい値（Threshold）] 設定を確認します。
- パケット処理タブとルール処理タブの両方でカスタム値を指定する必要があります。

ステップ 6 [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ルール遅延しきい値構成

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

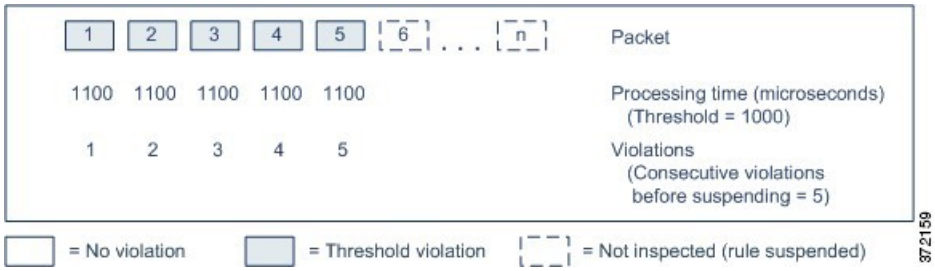
- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。

上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。

（注） パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一

時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザーが非常に大きなファイルをダウンロードするときなど、ネットワークパフォーマンスの低下がパケットインスペクションを遅らせる場合

ルール遅延しきい値構成の注記

デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことを推奨します。

このトピック内の情報は、カスタム値を指定するように選択した場合にのみ適用されます。

ルールによるパケット処理時間が、[ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）] で指定された回数連続して [しきい値（Threshold）] を超えると、ルール遅延しきい値構成は [停止時間（Suspension Time）] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。侵入ルールの状態オプション （2031 ページ）を参照してください。

表 *182:* ルール遅延しきい値構成のオプション

オプション	説明
しきい値	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。
ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）	ルールが一時停止される前に、ルールによるパケットの検査時間が [しきい値（Threshold）] で設定された時間を超えることができる、連続した回数を指定します。
停止時間（Suspension Time）	ルールのグループを一時停止する秒数を指定します。

ルール遅延しきい値の設定

デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことを推奨します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある[編集（Edit）]（）をクリックします。

代わりに[表示（View）]（）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップウィンドウで [ルール処理（Rule Handling）] をクリックします。

デフォルトで、[インストール済みのルールの更新（Installed Rule Update）] が選択されます。このデフォルトを使用することを推奨します。

表示された値には、自動設定が反映されません。

ステップ 4 カスタム値を指定する場合は、次の点に注意してください。

- ルール遅延しきい値構成の注記 （2237 ページ）の任意のオプションを設定できます。
- パケット処理タブとルール処理タブの両方でカスタム値を指定する必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- イベントを生成するには、遅延ルール（134:1 と 134:2）を有効にします。詳細については、「侵入ルールの状態オプション （2031 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

侵入パフォーマンス統計情報のロギング設定

[サンプル時間（秒）（Sample time (seconds)）] と [パケットの最小数（Minimum number of packets）]

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

注意 サンプル時間に非常に低い値（1 秒など）を設定すると、デバイスに大きな影響を与える可能性があります。デバイスに記録されたパフォーマンス統計情報がディスク容量の問題を引き起こし、デバイスの動作に影響を与える可能性があります。したがって、非常に低い値を設定しないことをお勧めします。

トラブルシューティング オプション：[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）]

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

注意 サポートによって指示された場合を除き、[ログセッション/プロトコル分布（Log Session/Protocol Distribution）] を有効にしないでください。

トラブルシューティング オプション：[概要（Summary）]

トラブルシューティングの電話中に、Snortプロセスのシャットダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）] トラブルシューティング オプションも有効にする必要があります。

注意 サポートから指示された場合を除き、[概要（Summary）] を有効にしないでください。

侵入パフォーマンス統計情報のロギングの設定

手順

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] をクリックし、[パフォーマンス設定（Performance Settings）] の横にある[編集（Edit）]（✎）をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 表示されるポップアップウィンドウの [パフォーマンス統計情報（Performance Statistics）] をクリックします。

ステップ 3 侵入パフォーマンス統計情報のロギング設定 （2239 ページ） での説明通り、[サンプル時間（Sample time）] または [パケットの最小数（Minimum number of packets）] を変更します。

注意
[サンプル時間（Sample time）] に非常に低い値（1 秒など）を設定すると、デバイスに大きな影響を与える可能性があります。デバイスに記録されたパフォーマンス統計情報がディスク容量の問題を引き起こし、デバイスの動作に影響を与える可能性があります。したがって、非常に低い値を設定しないことをお勧めします。

ステップ 4 任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション（Troubleshoot Options）] セクションを展開し、そのオプションを変更します。

ステップ 5 **[OK]** をクリックします。

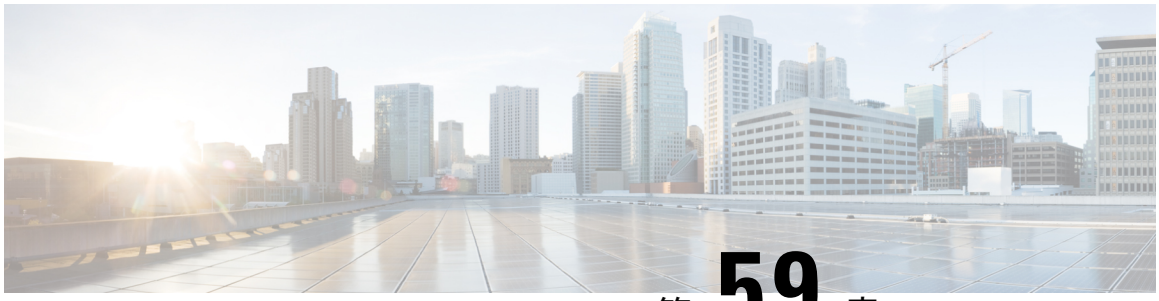
次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

第 IX 部

ネットワークマルウェア防御とファイルポリシー

- ネットワークマルウェア防御とファイルポリシー （2243 ページ）



第 59 章

ネットワークマルウェア防御とファイルポリシー

次のトピックでは、ファイル制御、ファイルポリシー、ファイルルール、Advanced Malware Protection（AMP）、クラウド接続、および動的分析接続の概要を示します。

- ネットワークにおけるマルウェア防御とファイルポリシーについて （2243 ページ）
- ファイルポリシーの要件と前提条件 （2245 ページ）
- ファイルおよびマルウェア ポリシーのライセンス要件 （2245 ページ）
- ファイルポリシーとマルウェア検出のベストプラクティス （2246 ページ）
- マルウェア防御の設定方法 （2249 ページ）
- マルウェア防御のためのクラウド接続 （2255 ページ）
- ファイル ポリシーとファイル ルール （2266 ページ）
- レトロスペクティブな性質の変更 （2286 ページ）
- ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション （2286 ページ）
- ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整 （2289 ページ）
- （オプション）Secure Endpoint を使用したマルウェア防御 （2290 ページ）
- ネットワークマルウェア防御とファイルポリシーの履歴 （2295 ページ）

ネットワークにおけるマルウェア防御とファイルポリシーについて

マルウェアを検出してブロックするには、ファイル ポリシーを使用します。また、ファイル ポリシーを使用して、ファイルタイプごとにトラフィックを検出および制御することもできます。

Firepower の高度なマルウェア防御（AMP）は、ネットワーク トラフィックでのマルウェアの伝送を検出、キャプチャ、追跡、分析、ロギング、および必要に応じてブロックできます。Secure Firewall Management Center Web インターフェイスでは、この機能は マルウェア防御 と

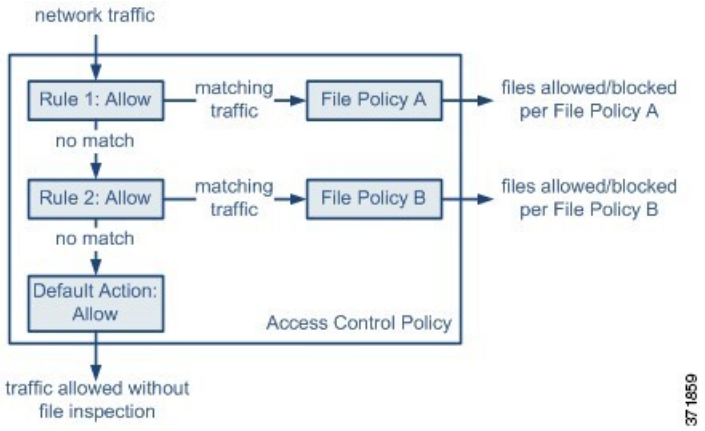
呼ばれ、以前は *AMP for Firepower* とも呼ばれていました。高度なマルウェア防御は、シスコクラウドからインラインおよび脅威データを展開した管理対象デバイスを使用してマルウェアを特定します。

すべてのアクセス コントロール設定に含まれるネットワーク トラフィックを処理するアクセス コントロール ルールとファイル ポリシーを関連付けます。

システムがネットワーク上のマルウェアを検出すると、ファイルおよびマルウェアイベントを生成します。ファイルイベントおよびマルウェアイベントのデータを分析するには、Cisco Secure Firewall Management Center アドミニストレーション ガイド の「ファイルイベント/マルウェアイベントとネットワーク ファイル トラジェクトリ」の章を参照してください。

ファイル ポリシー

ファイル ポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス コントロール設定の一部としてこれを使用して、マルウェア防御とファイル制御を実行できます。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。次の図のような、インライン展開での単純なアクセス コントロール ポリシーがあるとします。



このポリシーには 2 つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルト アクションもまた「トラフィックの許可」ですが、ファイル ポリシー インスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- `Rule 1` に一致するトラフィックは`File Policy A` で検査されます。
- `Rule 1` に一致しないトラフィックは`Rule 2` に照らして評価されます。`Rule 2` に一致するトラフィックは`File Policy B` で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルト アクションにファイル ポリシーを関連付けることはできません。

異なるファイルポリシーを個々のアクセスコントロールルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。

ファイルポリシーの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者

ファイルおよびマルウェア ポリシーのライセンス要件

操作内容	必要なライセンス	ファイルルールのアクション
特定のタイプのすべてのファイルをブロックまたは許可します（すべての .exe ファイルをブロックなど）	IPS （Firewall Threat Defense デバイスの場合） 保護（従来のデバイスの場合）	許可（Allow）、ブロック（Block）、リセットしてブロック（Block with reset）
マルウェアが含まれているか、または含まれている可能性があると判断した場合に、ファイルを選択的に許可またはブロックします	IPS （Firewall Threat Defense デバイスの場合） 保護（従来のデバイスの場合） マルウェア防御	マルウェア クラウド ルックアップ（Malware Cloud Lookup）、マルウェア ブロック（Block Malware）
ファイルの保存（Store files）	IPS （Firewall Threat Defense デバイスの場合） 保護（従来のデバイスの場合） マルウェア防御	[ファイルの保存（Store Files）] で選択されたファイル ルール アクション

マルウェア防御ライセンスの詳細については、次を参照してください。

- Cisco Secure Firewall Management Center アドミニストレーション ガイド のマルウェア防御ライセンス

ファイルポリシーとマルウェア検出のベストプラクティス

以下で説明する項目に加えて、マルウェア防御の設定方法（2249ページ）および参照されているトピックの手順に従ってください。

ファイルルールのベストプラクティス

ファイルルールを設定する場合、次の注意事項と制約事項に注意してください。

- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- ポリシーには複数のルールを含めることができます。ルールを作成する場合、このルールが以前のルールよりも「優先されている」ことを確認します。
- 動的分析でサポートされているファイルタイプは、他のタイプの分析でサポートされているファイル タイプのサブセットです。各分析タイプでサポートされているファイル タイプを表示するには、ファイル ルール設定ページに移動し、[マルウェア ブロック（Block Malware）] アクションを選択して、対象のチェックボックスをオンにします。

  システムがすべてのファイルタイプを検査するには、動的分析と他の分析タイプで個別のルール（同じポリシー内）を作成します。
- [マルウェア クラウドルックアップ（Malware Cloud Lookup）] アクションまたは [マルウェア ブロック（Block Malware）] アクションを使ってファイル ルールが設定されている場合、Firewall Management Center が AMP クラウドとの接続を確立できないと、接続が復元されるまで、システムは設定済みルール アクション オプションを実行できません。
- シスコでは、[ファイルブロック（Block Files）] アクションと [マルウェアブロック（Block Malware）] アクションで [接続のリセット（Reset Connection）] を有効にすることを推奨しています。これにより、ブロックされたアプリケーションセッションがTCP接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP接続が自身をリセットするまで、クライアント セッションが開いたままになります。
- 大量のトラフィックをモニターしている場合、キャプチャしたすべてのファイルを保存したり、動的分析用に送信したり**しないでください**。そのようにすると、システムパフォーマンスに悪影響が及ぶことがあります。
- システムで検出されるすべてのファイルタイプに対してマルウェア分析を実行できるわけではありません。[アプリケーション プロトコル（Application Protocol）]、[転送の方向

（Direction of Transfer）]、および[アクション（Action）]ドロップダウン リストで値を選択すると、システムはファイル タイプのリストを限定します。

ファイル検出のベストプラクティス

ファイル検出については、次の注意事項と制限事項を考慮してください。

- アダプティブ プロファイリングが有効でなければ、アクセス コントロール ルールは、AMP を含め、ファイルの制御を実行できません。
- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーションプロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはインライン タップ モードの展開では、FTP データ セッションとその制御セッションからのトラフィックは同じ内部リソースに負荷分散されない場合があります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキストベースのファイルを送信すると、一部のメール クライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジ リターン（CR）文字を使用し、UNIX/Linux ベースのホストはライン フィード（LF）文字を使用するので、メール クライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメール クライアントは、認識できないファイル タイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。
- ISO ファイルを検出するには、ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション（2286 ページ） の説明のように、[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] オプションを 36870 を超える値に設定します。
- rar5 を含む一部の .rar アーカイブ内の .Exe ファイルは検出できません。
- ファイルの性質が Neutral の場合、そのファイルの性質は不明です。

ファイルブロッキングのベストプラクティス

ファイルブロッキングについては、次の注意事項と制限事項を考慮してください。

- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルは**マルウェア ブロック** ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。

- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- [ファイル ブロック（Block Files）] アクションおよび [マルウェア ブロック（Block Malware）] アクションを持つファイル ルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアントアプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイル ダウンロードの自動再開をブロックします。
- まれに、HTTP アップロードセッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイルイベントの生成を行いません。
- **ファイル ブロック** ルールでブロックされる NetBios-ssn 経由ファイル転送（SMB ファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- （SMB ファイル転送などの）NetBIOS-ssn 経由で転送されたファイルを検出またはブロックするファイル ルールを作成した場合、進行中のファイル転送はシステムにより検査されません。ただし、ファイル ポリシーを呼び出すアクセス コントロール ポリシーを展開した後に、転送された新しいファイルがシステムにより検査されます。
- SMB には、同じ IP アドレスと異なるポートを持つ複数のパラレル セッションを作成する、マルチチャネルと呼ばれる機能があります。マルチチャネルを使用するトランザクションでは、ファイルのダウンロードはこれらのセッションにわたって多重化され、システムにより単一のファイルとして検査されません。
- 1 つの TCP または SMB セッションで同時に転送されたファイルは検査されません。
- クラスタ環境では、クラスタ ロールの変更またはデバイス障害が原因で既存の SMB セッションが新しいデバイスに移動されると、進行中のファイル転送のファイルが検査されないことがあります。
- Microsoft Windows システム間での一部の SMB ファイル転送では、迅速なファイル転送のため、非常に大きな TCP ウィンドウ サイズを使用します。このようなファイル転送を検出またはブロックするには、**[ネットワーク分析ポリシー（Network Analysis Policy）]** > **[TCPストリームの設定（TCP Stream Configuration）]** > **[トラブルシューティングオプション（Troubleshooting Options）]** にある [最大キューイングバイト（Maximum Queued Bytes）] と [最大キューイングセグメント（Maximum Queued Segments）] の値を大きくすることを推奨します。
- Firepower Threat Defense の高可用性を設定したときに、元のアクティブなデバイスがファイルを識別している間にフェールオーバーが発生した場合、ファイルタイプは同期されません。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。

ファイルポリシーのベストプラクティス

ファイルポリシーを設定する場合、次の一般的な注意事項と制約事項に注意してください。

- 1 つのファイル ポリシーを、[許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを含むアクセス コントロール ルールに関連付けることができます。
- ただし、アクセス コントロールのデフォルト アクションによって処理されるトラフィックを検査するためにファイル ポリシーを使用**できない**ことに注意してください。
- 新しいポリシーの場合、ポリシーが使用中でないことが Web インターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数が Web インターフェイスに示されます。どちらの場合も、テキストをクリックすると [アクセス コントロール ポリシー（Access Control Policies）] ページに移動できます。
- ファイルブロッキングが機能するには、アクセス コントロール ポリシーに適用する NAP ポリシーが保護モードで動作している必要があります（インラインモードとも呼ばれます）。
- 設定に応じて、システムがファイルを初めて検出したときに、そのファイルを検査してクラウド ルックアップの結果を待機するか、または、クラウド ルックアップの結果を待機せずにファイルを通過させることができます。
- デフォルトでは、暗号化されたペイロードのファイル検査は無効になっています。これにより、ファイル検査が設定されたアクセス制御ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

注目 次のジェネレータ ID（GID）を持つファイル検査プリプロセッサは、ファイル/マルウェアポリシーに対してデフォルトで有効になっています：GID: 146 および GID: 147。

- [マルウェア（Malware）] アクションまたは [ファイルの保存（Store Files）] オプションのいずれかを使用するファイル ポリシーでアクセス コントロール ポリシーをイネーブルにすると、デバイスのコンピューティング能力とシステムパフォーマンスが低下します。

マルウェア防御の設定方法

ここでは、悪意のあるソフトウェアからネットワークを保護するために、システムのセットアップで実行する必要がある手順について説明します。

手順

ステップ 1 マルウェア防御の計画と準備 （2250 ページ）

ステップ 2 ファイル ポリシーの設定 （2252 ページ）

ステップ 3 アクセス コントロール設定へのファイル ポリシーの追加 （2252 ページ）

ステップ 4 ネットワーク検出ポリシーを設定して、ファイルとマルウェアイベントをネットワーク上のホストと関連付けます。

（ネットワーク検出をオンにするだけでなく、ネットワーク上のホストを検出して組織のネットワーク マップを構築するように設定する必要があります。）

ネットワーク検出ポリシー （2657 ページ）およびサブトピックを参照してください。

ステップ 5 管理対象デバイスにポリシーを展開します。

設定変更の展開 （172 ページ）を参照してください。

ステップ 6 予想したとおりに悪意のあるファイルを処理していることを確認するためにシステムをテストします。

ステップ 7 マルウェア防御のメンテナンスとモニタリングの設定 （2255 ページ）

次のタスク

- （オプション）ネットワーク内のマルウェアの検出をさらに強化するには、シスコの Secure Endpoint 製品を導入して統合します。（オプション）Secure Endpoint を使用したマルウェア防御 （2290 ページ）およびサブトピックを参照してください。
- ファイルおよびマルウェア イベントを調査する方法を理解します。

  Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*File/Malware Events and Network File Trajectory*」を参照してください。

マルウェア防御の計画と準備

この手順は、マルウェアを防御するようにシステムを設定するための完全なプロセスの最初の手順です。

手順

ステップ 1 ライセンスを購入してインストールします。

ファイルおよびマルウェア ポリシーのライセンス要件 （2245 ページ） および『Cisco Secure Firewall Management Center アドミニストレーション ガイド』のライセンスを参照してください。

ステップ 2 ファイル ポリシーおよびマルウェア防御がアクセス コントロール プランにどのように適合するかを理解します。

アクセス制御の概要 （1717 ページ）の章を参照してください。

ステップ 3 ファイル分析およびマルウェア防御ツールについて理解します。

ファイル ルール アクション （2275 ページ）およびサブトピックを参照してください。

また、高度およびアーカイブ ファイル インスペクション オプション （2267 ページ）も考慮してください。

ステップ 4 マルウェア防御（ファイル分析と動的分析）にパブリック クラウドまたはプライベート（オンプレミス）クラウドを使用するかどうかを決定します。

マルウェア防御のためのクラウド接続（2255 ページ）およびサブトピックを参照してください。

ステップ 5 マルウェア防御にプライベート（オンプレミス）クラウドを使用する場合は、これらの製品を購入、展開、テストします。

詳細については、シスコのセールス担当者または認定リセラーにお問い合わせください。

ステップ 6 選択したクラウドとの通信を許可するようにファイアウォールを設定します。

Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Security, Internet Access, and Communication Ports*」を参照してください。

ステップ 7 Firepower とマルウェア防御クラウド（パブリックまたはプライベート）の間の接続を設定します（該当する場合）。

- AMP クラウドについては、AMP オプションの変更 （2261 ページ）を参照してください。
- オンプレミスの Secure Malware Analytics アプライアンスを展開した場合は、オンプレミスの動的分析アプライアンスへの接続 （2263 ページ）を参照してください。（パブリック Secure Malware Analytics クラウドへのアクセスを設定する必要はありません。）

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

「マルウェア防御の設定方法 （2249 ページ）」を参照してください。

ファイル ポリシーの設定

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

マルウェア防御の設定方法 （2249 ページ）を参照してください。

手順

ステップ 1 ファイル ポリシーおよびファイル ルールの制限事項を確認します。

ファイルポリシーとマルウェア検出のベストプラクティス （2246ページ）およびサブトピックを参照してください。

ステップ 2 ファイル ポリシーを作成します。

ファイルポリシーの作成または編集 （2266 ページ）を参照してください。

ステップ 3 ファイル ポリシー内にルールを作成します。

ファイル ルール （2273 ページ）およびサブトピックを参照してください。

ステップ 4 詳細オプションを設定します。

高度およびアーカイブ ファイル インスペクション オプション （2267ページ）を参照してください。

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

「マルウェア防御の設定方法 （2249 ページ）」を参照してください。

アクセス コントロール設定へのファイル ポリシーの追加

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

マルウェア防御の設定方法 （2249 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシーでファイル ポリシーのガイドラインを確認します。（これらは以前に確認したファイル ルールおよびファイル ポリシーのガイドラインとは異なります。）

ファイル インスペクションおよび侵入インスペクションの順序（1726 ページ）を確認してください。

ステップ 2 アクセス コントロール ポリシーとファイル ポリシーを関連付けます。

マルウェア保護のためのアクセス コントロール ルールの設定（2253 ページ）を参照してください

ステップ 3 管理対象デバイスにアクセス コントロール ポリシーを割り当てます。

アクセス コントロール ポリシーのターゲット デバイスの設定（1757 ページ）を参照してください。

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

「マルウェア防御の設定方法（2249 ページ）」を参照してください。

マルウェア保護のためのアクセス コントロール ルールの設定

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化/無効化した場合、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェアブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero分析またはMSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカルマルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除した場合には、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。

（注） ファイルポリシーがアクセスコントロールルールに含まれている場合、インライン正規化は自動的に有効になります。詳細については、インライン正規化プリプロセッサ （2872ページ） を参照してください。

始める前に

- AMP を含むファイル制御をアクセス コントロール ルールで実行するためには、適応型プロファイルの設定 （2937ページ） で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする**必要があります**。
- このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者ユーザーである必要があります。

手順

ステップ 1 （[ポリシー（Policy）] > [アクセス制御（Access Control）] から）アクセス コントロール ルール エディタで、[許可（Allow）]、[インタラクティブブロック（Interactive Block）]、または [リセットしてインタラクティブブロック（Interactive Block with reset）] の [アクション（Action）] を選択します。

ステップ 2 （レガシー UI のみ。）[検査（Inspection）] をクリックします。

ステップ 3 アクセスコントロールルールに一致するトラフィックを検査する場合は [ファイルポリシー（File Policy）] を選択し、または一致するトラフィックに対するファイルインスペクションを無効にする場合は [なし（None）] を選択します。

ステップ 4 （オプション）[ロギング（Logging）] をクリックし、[ログファイル（Log Files）] チェックボックスをオフにして、一致する接続のファイルまたはマルウェアイベントのロギングを無効にします。

（注）
Cisco では、ファイルイベントおよびマルウェアイベントのロギングを有効のままにすることを推奨しています。

ステップ 5 ルールを保存します。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

ファイルポリシーの作成または編集 （2266 ページ）

Snort 再起動のシナリオ （162 ページ）

マルウェア防御のメンテナンスとモニタリングの設定

ネットワークの保護には継続的なメンテナンスが必要不可欠です。

始める前に

マルウェアからネットワークを保護するようにシステムを設定します。

マルウェア防御の設定方法 （2249 ページ）および参照手順を確認してください。

手順

ステップ 1 システムが常に最新かつ効果的に保護されていることを確認します。

システムの保守：動的分析の対象となるファイル タイプの更新 （2266 ページ）を参照してください。

ステップ 2 マルウェア関連のイベントおよびヘルス モニタリングのアラートを設定します。

「*Configuring* マルウェア防御 *Alerting*」の詳細および以下のモジュールの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

- ローカル マルウェア分析（Local Malware Analysis）
- セキュリティインテリジェンス
- デバイスでの脅威データの更新
- 侵入およびファイル イベント レート
- AMP for Firepower のステータス
- Secure Endpointのステータス

次のタスク

マルウェア防御ワークフローの「次の項目について」を確認してください。

「マルウェア防御の設定方法 （2249 ページ）」を参照してください。

マルウェア防御のためのクラウド接続

マルウェアからネットワークを保護するためには、パブリック クラウドまたはプライベート クラウドに接続する必要があります。

AMP クラウド

高度なマルウェア防御（AMP）クラウドは、ビッグ データ分析や連続分析によりネットワーク上のマルウェアを検出およびブロックするシスコ ホステッド サーバーです。

AMP クラウドは、管理対象デバイスがネットワーク トラフィックから検出した潜在的なマルウェアの性質と、ローカルマルウェア分析とファイルの事前分類のデータ更新を提供します。

組織で Secure Endpoint を展開し、データをインポートするように Firepower を設定している場合、システムは、スキャン レコード、マルウェア検出、隔離、侵害の兆候（IOC）など、AMP クラウドからこのデータをインポートします。

シスコでは、既知のマルウェアの脅威についてシスコ クラウドからデータを取得するために次のオプションを提供しています。

- **AMP パブリック クラウド**

  Secure Firewall Management Center がパブリック シスコ クラウドと直接通信します。米国、欧州、アジアに 3 つのパブリック AMP クラウドがあります。

- **AMP プライベート クラウド**

  ネットワーク上に展開された AMP プライベート クラウドは、圧縮型、オンプレミス AMP クラウドおよびパブリック AMP クラウドに接続するための匿名プロキシとして機能します。詳細は、Cisco AMP プライベート クラウド （2258 ページ）を参照してください。

  Secure Endpoint と統合する場合、AMP プライベート クラウドにはいくつかの制限があります。Secure Endpoint と AMP プライベート クラウド （2292 ページ）を参照してください。

動的分析クラウド

- **Secure Malware Analytics クラウド**

  動的分析の送信に適したファイルを処理し、脅威スコアと動的分析レポートを提供するパブリック クラウド。Firepower は、Secure Malware Analytics 分析で 200 サンプル/日をサポートします。

- **オンプレミス Secure Malware Analytics アプライアンス**

  組織のセキュリティ ポリシーがシステムによるネットワーク外部へのファイルの送信を許可しない場合は、オンプレミスアプライアンスを設定できます。このアプライアンスはパブリック Secure Malware Analytics クラウドには接続しません。

  詳細については、オンプレミスアプライアンスの動的分析（Cisco Secure Malware Analytics）（2263 ページ）を参照してください。

AMP および Secure Malware Analytics クラウドへの接続の設定

- AMP クラウド接続の設定 （2257 ページ）
- 動的分析接続 （2262 ページ）

AMP クラウド接続の設定

次のトピックでは、さまざまなシナリオでの AMP クラウド接続の設定について説明します。

- AMP クラウドの選択 （2257 ページ）
- AMP プライベート クラウドへの接続 （2259 ページ）
- Firepower と Secure Endpoint の統合 （2293 ページ）

次のトピックも関連しています。

- Cisco AMP プライベート クラウド （2258 ページ）
- AMP クラウド接続の要件とベストプラクティス （2257 ページ）
- AMP クラウドへの接続の管理（パブリックまたはプライベート） （2260 ページ）

AMP クラウド接続の要件とベストプラクティス

AMP クラウド接続要件

AMP クラウドを設定するには、管理者ユーザーである必要があります。

Firewall Management Center が AMP クラウドと通信できるようにするには、Cisco Secure Firewall Management Center アドミニストレーション ガイド のセキュリティ、インターネット アクセス、および通信ポートを参照してください。

AMP とハイ アベイラビリティ

高可用性ペアの Firewall Management Center はファイル ポリシーおよび関連する設定を共有しますが、AMP クラウド接続、キャプチャされたファイル、ファイル イベント、マルウェア イベントを共有することはありません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firewall Management Center で同じであるようにするためには、アクティブとスタンバイ両方の Firewall Management Center がクラウドにアクセスできる必要があります。

これらの要件は、パブリック、プライベート両方の AMP クラウドに適用されます。

AMP クラウド接続とマルチテナンシー

マルチドメイン展開では、マルウェア防御 接続はグローバル レベルで設定します。各 Firewall Management Center には、マルウェア防御 接続を 1 つだけ設定できます。

AMP クラウドの選択

システムでは、デフォルトで米国（US）AMP パブリッククラウドへの接続が設定され、有効になっています。（この接続は web インターフェイスに マルウェア防御 と表示されますが、AMP for Firepower と表示される場合もあります。）マルウェア防御 クラウド接続の削除または無効化はできませんが、地理的に異なる AMP クラウドの切り替え、または AMP プライベート クラウドの接続が設定が可能です。

始める前に

- AMP プライベート クラウドを使用する場合は、このトピックの代わりにAMP プライベート クラウドへの接続 （2259 ページ）を参照してください。
- Firepower が Secure Endpoint と統合されていない場合は、AMP クラウド接続を 1 つだけ設定できます。この接続には、**AMP for Networks** または **AMP for Firepower** というラベルが付けられています。
- Secure Endpoint を展開済みで、このアプリケーションを Firepower と統合するために 1 つ以上の AMP クラウドを追加する場合は、Firepower と Secure Endpoint の統合 （2293 ページ） を参照してください。
- AMP クラウド接続の要件とベストプラクティス （2257 ページ）を参照してください。

手順

ステップ 1 **[統合（Integration）] > [AMP] > [AMP管理（AMP Management）]**を選択します。

ステップ 2 鉛筆をクリックし、既存のクラウド接続を編集します。

ステップ 3 [クラウド名（Cloud Name）] ドロップダウン リストから、Secure Firewall Management Center から最も近い地域にあるクラウドを選択します。

APJC はアジア/太平洋/日本/中国です。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 展開がハイ アベイラビリティ構成の場合は、AMP クラウド接続の要件とベストプラクティス （2257 ページ）を参照してください。
- （任意）AMP オプションの変更 （2261 ページ）。

Cisco AMP プライベート クラウド

Firewall Management Center は AMP クラウドに接続し、ネットワーク トラフィックで検出されたファイルの判定結果をクエリしたり、レトロスペクティブ マルウェア イベントを受信したりします。このクラウドはパブリックまたはプライベートに指定することができます。

部門のプライバシーやセキュリティ保護の観点から、モニター対象ネットワークと AMP クラウドとの間で頻繁にあるいは直接接続することが困難、または不可能な場合があります。このような場合、AMP クラウドの圧縮型、オンプレミス バージョンとして機能するシスコ独自の製品、ユーザーのネットワークと AMP クラウドの安全なメディエータである、Cisco AMP プライベート クラウドを設定できます。Firewall Management Center を AMP プライベート クラウドに接続すると、パブリック AMP クラウドとの既存の直接接続は無効化されます。

AMP プライベート クラウドを介した AMP クラウド ファネルとのすべての接続は、監視対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。これには、ネットワーク トラフィックで検出されたファイルの判定結果のクエリ、レトロスペクティブ マルウェア イベントの受信などが含まれます。AMP プライベート クラウドは、エンドポイント データを外部接続では一切共有しません。

（注） AMP プライベート クラウドは動的分析を実行**しません**。また、Cisco Collective Security Intelligence（CSI）に依存するその他の機能（URL フィルタリングやセキュリティ インテリジェンス フィルタリングなど）のための脅威インテリジェンスの匿名での取得もサポートしていません。

AMP プライベート クラウド（「AMPv」とも呼ばれる）の詳細については、https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html を参照してください。

AMP プライベート クラウドへの接続

始める前に

- AMP のマニュアルの指示に従って、Cisco AMP プライベート クラウドまたはクラウドを設定します。設定時に、プライベート クラウドのホスト名をメモしてください。このホスト名は、Firewall Management Center で接続を設定するときに必要になります。
- Firewall Management Center が AMP プライベート クラウドと通信できることを確認し、プライベート クラウドがインターネットにアクセスし、パブリック AMP クラウドと通信できることを確認します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Security, Internet Access, and Communication Ports*」にあるトピックを参照してください。
- 展開で Secure Endpoint と統合されていない場合は、Firewall Management Center ごとに AMP クラウド接続を 1 つだけ設定できます。この接続には、**AMP for Networks** または **AMP for Firepower** というラベルが付けられています。

  Secure Endpoint と統合する場合には、複数の Secure Endpoint クラウド接続を設定できます。

手順

ステップ 1 **[統合（Integration）] > [AMP] > [AMP管理（AMP Management）]**を選択します。

ステップ 2 [AMPクラウド接続の追加（Add AMP Cloud Connection）] をクリックします。

ステップ 3 [クラウド名（Cloud Name] ドロップダウン リストから [プライベート クラウド（Private Cloud）] を選択します。

ステップ 4 名前を入力します。

この情報は、AMP プライベート クラウドによって生成または送信されるマルウェア イベントに表示されます。

ステップ 5 [ホスト（Host）] フィールドに、プライベート クラウドの設定時に設定したプライベート クラウドのホスト名を入力します。

ステップ 6 [証明書アップロードパス（Certificate Upload Path）] フィールドの横にある [参照（Browse）] をクリックして、プライベート クラウドの有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMP プライベート クラウドのマニュアルを参照してください。

ステップ 7 このプライベートクラウドを マルウェア防御 と Secure Endpoint の両方に使用する場合は、**[AMP for Firepowerに使用（Use for AMP for Firepower）]** チェックボックスをオンにします。

マルウェア防御 通信を処理する別のプライベート クラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMP プライベート クラウド接続の場合は、オフにできません。

マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firewall Management Center には、マルウェア防御 接続を 1 つだけ設定できます。

ステップ 8 プロキシを使用して AMP プライベート クラウドと通信するには、[接続にプロキシを使用（Use Proxy for Connection）] チェックボックスをオンにします。

ステップ 9 [登録（Register）] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMP プライベート クラウド管理コンソールを続行して登録を完了することを確認します。

ステップ 10 管理コンソールにログインして登録プロセスを完了します。詳細については、AMP プライベート クラウドのマニュアルを参照してください。

次のタスク

高可用性展開では、両方の Management Center で AMP クラウド接続を設定します。これらの設定は同期されません。

AMP クラウドへの接続の管理（パブリックまたはプライベート）

Firewall Management Center を使用して、マルウェア防御 や Secure Endpoint またはその両方に使用されるパブリックおよびプライベート AMP クラウドへの接続を管理します。

クラウドからマルウェア関連の情報を受信する必要がなくなった場合は、パブリックまたはプライベート AMP クラウドとの接続を削除します。Secure Endpoint または AMP プライベート クラウド管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、Secure Firewall Management Center の Web インターフェイスに障害発生状態で表されます。

また、接続は一時的に無効にすることもできます。クラウド接続を再度有効化すると、クラウドは、無効化されていた期間にキューに保持していたデータを含めて、システムへのデータ送信を再開します。

注意 無効化された接続の場合、プライベート AMP クラウドは、接続を再有効化するまでマルウェア イベントや侵害の兆候などを保存できます。まれに、イベント レートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべての情報をクラウドで保存できないことがあります。

マルチドメイン展開では、現在のドメインで作成された接続が表示されます。これは、管理が可能な接続です。また、先祖ドメインで作成した接続も表示されますが、この接続は管理できません。下位ドメインの接続を管理するには、そのドメインに切り替えます。各 Firewall Management Center は、グローバル ドメインに属する マルウェア防御 接続を 1 つのみ保持できます。

手順

ステップ 1 **[統合（Integration）]** > **[AMP]** > **[AMP管理（AMP Management）]** を選択します。

ステップ 2 AMP クラウド接続を管理します。

- 削除：[削除（Delete）]（ ）をクリックして、選択内容を確認します。
- 有効化または無効化：スライダをクリックして、選択内容を確認します。

次のタスク

高可用性展開では、両方の Management Center で AMP クラウド接続を設定します。これらの設定は同期されません。

AMP オプションの変更

手順

ステップ 1 **[統合（Integration）]** > **[その他の統合（Other Integrations）]**を選択します。

ステップ 2 **クラウド サービス** をクリックします。

ステップ 3 次のオプションを選択します。

表 *183 : AMP for Networks* のオプション

オプション	説明
ローカル マルウェア検出の自動更新を有効にする（Enable Automatic Local Malware Detection Updates）	ローカルマルウェア検出エンジンは、Cisco が提供する署名を使用して統計的にファイルを分析し、事前に分類します。このオプションを有効にすると、Firewall Management Center が 30 分ごとに署名の更新を確認します。
マルウェア イベントの URL を Cisco と共有する（Share URI from Malware Events with Cisco）	ネットワーク トラフィックで検出されたファイルに関する情報を AMP クラウドに送信することができます。この情報には、検出されたファイルに関連する URI 情報と SHA-256 ハッシュ値が含まれます。共有はオプトインですが、この情報を Cisco に送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。

ステップ 4 [保存（Save）] をクリックします。

動的分析接続

動的分析の要件

動的分析を使用するには、管理者、アクセス管理者、またはネットワーク管理者のユーザーであり、グローバルドメインにいる必要があります。

適切なライセンスを使用して、システムが自動的に Secure Malware Analytics クラウドにアクセスします。

動的分析では、管理対象デバイスがポート 443 から Secure Malware Analytics Cloud またはオンプレミス Secure Malware Analytics Appliance に、直接あるいはプロキシを介してアクセスできる必要があります。

動的分析の対象となるファイル （2281 ページ）も参照してください。

オンプレミス Secure Malware Analytics Appliance に接続する場合は、オンプレミスの動的分析アプライアンスへの接続 （2263 ページ）の前提条件も参照してください。

デフォルト動的分析接続の表示

デフォルトで、Secure Firewall Management Center は、ファイルの送信やレポートの取得のために、パブリック Secure Malware Analytics Cloud に接続できます。この接続は、設定したり、削除したりすることはできません。

手順

ステップ 1 **[統合（Integration）]** > **[AMP]** > **[AMPダイナミック分析接続（Dynamic Analysis Connections）]** を選択します。

ステップ 2 [編集（Edit）]（） をクリックします。

（注）
[統合（Integration）] > **[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]** ページの **[関連付け（Association）]**（） の詳細については、パブリック クラウドでの動的分析の結果へのアクセスの有効化 （2265 ページ）を参照してください。

オンプレミスアプライアンスの動的分析（Cisco Secure Malware Analytics）

組織にパブリックの Secure Malware Analytics クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの Secure Malware Analytics アプライアンスを展開することができます。このオンプレミスアプライアンスは、パブリッククラウドと同様に適格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートをシステムに返します。ただし、このオンプレミスアプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

オンプレミス Secure Malware Analytics アプライアンスの詳細については、https://www.cisco.com/c/en/us/products/security/threat-grid/index.htmlを参照してください。

オンプレミスの動的分析アプライアンスへの接続

ネットワークでオンプレミスの Secure Malware Analytics アプライアンスをインストールする場合は、動的分析接続を設定してファイルを送信し、アプライアンスからレポートを取得できます。オンプレミスのアプライアンスの動的分析接続を設定するには、オンプレミスのアプライアンスに Secure Firewall Management Center を登録します。

始める前に

- オンプレミス Secure Malware Analytics アプライアンスを設定します。

  このアプライアンスのドキュメントは、https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html から入手できます。

  バージョンの要件については、『*Cisco Firepower Compatibility Guide*』を参照してください。

- Secure Malware Analytics アプライアンスが自己署名公開キー証明書を使用している場合は、Secure Malware Analytics アプライアンスから証明書をダウンロードします。詳細については、Secure Malware Analytics アプライアンスの管理者ガイド参照してください。

認証局（CA）によって署名された証明書を使用する場合、証明書は次の要件を満たしている必要があります。

- サーバーキーと署名付き証明書を Secure Malware Analytics アプライアンスにインストールする必要があります。Secure Malware Analytics アプライアンスの管理者ガイドのアップロード手順に従います。
- CA のマルチレベル署名チェーンがある場合、Firewall Management Center にアップロードされる単一のファイルに必要なすべての中間証明書とルート証明書が含まれている必要があります。
- すべての証明書は PEM でエンコードされている必要があります。
- ファイルの改行は、DOS ではなく UNIX でなければなりません。

- プロキシを使用してオンプレミスのアプライアンスに接続する場合は、プロキシを設定します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Modify Firewall Management Center Management Interfaces*」を参照してください。
- 管理対象デバイスは、ポート 443 で直接またはプロキシを介して Secure Malware Analytics アプライアンスにアクセスできる必要があります。

手順

ステップ 1 **[統合（Integration）]** > **[AMP]** > **[AMPダイナミック分析接続（Dynamic Analysis Connections）]** を選択します。

ステップ 2 [新しい接続を追加（Add New Connection）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [ホスト（Host）] に入力します。

ステップ 5 [証明書のアップロード（Certificate Upload）] の横にある [参照（Browse）] をクリックして、オンプレミスのアプライアンスの証明書をアップロードします。

Secure Malware Analytics アプライアンスから自己署名証明書が提示される場合は、そのアプライアンスからダウンロードした証明書をアップロードします。

Secure Malware Analytics アプライアンスから CA 署名付き証明書が提示される場合は、証明書署名チェーンを含むファイルをアップロードします。

ステップ 6 設定済みのプロキシを使用して接続を確立する場合は、[使用可能な場合はプロキシを使用する（Use Proxy When Available）] チェックボックスをオンにします。

ステップ 7 [登録（Register）] をクリックします。

ステップ 8 [はい（Yes）] をクリックして、オンプレミスの Secure Malware Analytics アプライアンスのログインページを表示します。

ステップ 9 オンプレミスの Secure Malware Analytics アプライアンスにユーザー名とパスワードを入力します。

ステップ 10 [サインイン（Sign in）] をクリックします。

ステップ 11 次の選択肢があります。

- 以前にオンプレミスのアプライアンスに Secure Firewall Management Center を登録した場合は、[戻る（Return）] をクリックします。
- Secure Firewall Management Center を登録していない場合は、[アクティブ化（Activate）] をクリックします。

パブリック クラウドでの動的分析の結果へのアクセスの有効化

Secure Malware Analytics では、分析されたファイルに関して、Firewall Management Center で使用できるレポートよりもさらに詳細なレポートが提供されます。組織に Secure Malware Analytics Cloud アカウントがある場合、Secure Malware Analytics ポータルに直接アクセスして、管理対象デバイスから分析のために送信されたファイルに関する追加の詳細を表示できます。ただし、プライバシー上の理由から、ファイル分析の詳細は、そのファイルを提出した組織だけが使用できます。そのため、この情報を表示するためには、Firewall Management Center を、管理対象デバイスによって提出されたファイルと関連付ける必要があります。

始める前に

Secure Malware Analytics クラウドのアカウントがあり、アカウントのログイン情報を持っている必要があります。

手順

ステップ 1 **[統合（Integration）]** > **[AMP]** > **[AMPダイナミック分析接続（Dynamic Analysis Connections）]** を選択します。

ステップ 2 Secure Malware Analytics クラウドに対応するテーブル行で、**[関連付け（Association）]**（）をクリックします。

Secure Malware Analytics ポータル ウィンドウが開きます。

ステップ 3 Secure Malware Analytics クラウドにサインインします。

ステップ 4 [クエリの送信（Submit Query）] をクリックします。

（注）
[デバイス（Devices）] フィールドのデフォルト値を変更しなでください。

このプロセスで問題が発生した場合は、Secure Malware Analytics 担当者にお問い合わせください。

この変更が有効になるまでに最大で 24 時間かかることがあります。

次のタスク

関連付けが有効化された後、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Viewing Dynamic Analysis Results in the Cisco Cloud」 を参照してください。

システムの保守：動的分析の対象となるファイル タイプの更新

動的分析の対象となるファイル タイプのリストは、定期的に更新される（多くても 1 日 1 回）脆弱性データベース（VDB）によって決定されます。管理者ユーザーは、動的分析の対象となるファイルタイプを更新できます。

システムに現在のリストがあることを次のように確認します。

手順

ステップ 1 次のいずれかを実行します。

- （推奨）Cisco Secure Firewall Management Center アドミニストレーション ガイドで説明されている脆弱性データベース更新の自動化を参照してください。
- 新しい VDB の更新を定期的に確認し、必要に応じて、Cisco Secure Firewall Management Center アドミニストレーション ガイドで説明されているように *VDB* を手動で更新します。

  このオプションを選択した場合は、定期的な通知をスケジュールすることをお勧めします。

ステップ 2 ファイル ポリシーで [動的分析可能（Dynamic Analysis Capable）] ファイル タイプ カテゴリではなく個々のファイル タイプを指定する場合は、ファイル ポリシーを更新して新しくサポートされるファイル タイプを使用します。

ステップ 3 対応するファイルタイプのリストが変更されている場合は、管理対象デバイスに展開します。

ファイル ポリシーとファイル ルール

ファイルポリシーの作成または編集

始める前に

マルウェア保護のポリシーを設定する場合は、ファイルポリシーの設定（2252 ページ）の必要なすべての手順を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [マルウェアとファイル（Malware & File）]** を選択します。

ステップ 2 新しいポリシーを作成するか、既存のポリシーを編集します。

既存のポリシーを編集する場合：代わりに [表示（View）]（ ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント

既存のファイルポリシーのコピーを作成するには、[コピー（Copy）]（ ）をクリックして、表示されるダイアログボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

ステップ 3 ファイル ルールの作成 （2284 ページ）の説明に従って、ファイル ポリシーに 1 つ以上のルールを追加します。

ステップ 4 必要に応じて、[詳細（Advanced）] を選択し、高度およびアーカイブ ファイル インスペクション オプション （2267 ページ）の説明に従って詳細オプションを設定します。

ステップ 5 ファイル ポリシーを保存します。

次のタスク

- マルウェア保護のポリシーを設定する場合は、ファイル ポリシーの設定 （2252 ページ）の必要なその他の手順を参照してください。
- 該当しない場合は、次のようになります。
  - アクセス コントロール設定へのファイル ポリシーの追加 （2252 ページ）の説明に従って、アクセス コントロール ルールにファイル ポリシーを追加します。
  - 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

高度およびアーカイブ ファイル インスペクション オプション

ファイルポリシーエディタの [詳細設定（Advanced Settings）] には、次の一般オプションがあります。

- [初回ファイル分析（First Time File Analysis）]：最初に検出されたファイルを分析すると同時に AMP クラウドの判定結果を保留にする場合にこのオプションを選択します。ファイルは、マルウェア クラウド ルックアップと Spero 分析、ローカル マルウェア分析、またはダイナミック分析を実行するように設定されているルールに一致する必要があります。このオプションの選択を解除すると、初めて検出されたファイルの判定結果が [不明（Unknown）] になります

- [カスタム検出リストを有効にする（Enable Custom Detection List）]：カスタム検出リストにあるファイルをブロックします。
- [クリーンリストを有効にする（Enable Clean List）]：有効にすると、このポリシーはクリーン リストにあるファイルを許可します。
- **[AMPクラウドの判定結果が不明な場合は、脅威スコアに基づいて判定結果をオーバーライドします（If AMP Cloud disposition is Unknown, override disposition based upon threat score）]**：オプションを選択します。
  - [無効（Disabled）]を選択すると、システムはAMPクラウドによって提供された判定結果をオーバーライドしません。
  - 脅威スコアのしきい値を設定すると、動的分析スコアがしきい値以下である場合、AMPクラウドの判定が[不明（Unknown）]のファイルはマルウェアと見なされます。
  - しきい値に低い値を選択すると、マルウェアとして扱われるファイルの数が増えます。ファイルポリシーで選択したアクションによっては、その結果、ブロックされるファイルの数が増える可能性があります。
  - 数値の脅威スコアの範囲については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Threat Scores and Dynamic Analysis Summary Reports」を参照してください。

ファイルポリシーエディタの [詳細設定（Advanced Settings）] には、次のアーカイブファイル検査オプションがあります。

- [アーカイブを検査する（Inspect Archives）]：アクセス コントロールの詳細設定の[保存する最大ファイルサイズ（Maximum file size to store）]と同じ大きさのアーカイブ ファイルまで、アーカイブ ファイルのコンテンツのインスペクションをできるようにします。
- [暗号化されたアーカイブのブロック（Block Encrypted Archives）]：パスワードで保護されたアーカイブをブロックします。
- [検査不可能なアーカイブをブロックする（Block Uninspectable Archives）]：暗号化以外の理由でシステムが検査できないコンテンツを含むアーカイブ ファイルをブロックします。これは通常、破損したファイル、または指定した最大アーカイブ深度を超えるファイルに適用されます。
- **[最大アーカイブ深度（Max Archive Depth）]**：指定した深度を超えるネストされたアーカイブ ファイルをブロックします。トップレベルのアーカイブ ファイルはこの数で考慮されません。深さは最初にネストされたファイルで 1 から始まります。

アーカイブ ファイル

アーカイブ ファイルとは、`.zip` や `.rar` ファイルなどの他のファイルを含むファイルです。

ブロック アクションを含むファイル ルールにアーカイブ内のいずれかの個別ファイルが一致する場合は、その個別ファイルだけでなくアーカイブ全体がブロックされます。

アーカイブファイルのインスペクションのオプションについては、高度およびアーカイブファイル インスペクション オプション （2267 ページ）を参照してください。

検査可能なアーカイブ ファイル

- **ファイル タイプ**

  検査可能なアーカイブファイルタイプの完全なリストがFMC Webインターフェイスのファイルルール設定ページに表示されます。このページを表示するには、ファイル ルールの作成 （2284 ページ）を参照してください。

  検査可能な格納ファイルが同じページに表示されます。

- **ファイルサイズ（File size）**

  アクセス コントロールの詳細設定の [保存する最大ファイルサイズ（Maximum file size to store）] ファイル ポリシーと同じ大きさのアーカイブ ファイルまで検査できます。

- **ネストされたアーカイブ**

  アーカイブファイルには他のアーカイブ ファイルを含められます。その結果、複数のアーカイブ ファイルが含めることができます。ファイルがネストされるレベルは、そのアーカイブ ファイルの深さです。トップレベルのアーカイブ ファイルは深さの数に含まれないことに注意してください。深さは最初にネストされたファイルで 1 から始まります。

  システムは、最も外側のアーカイブ ファイル（レベル 0）の下にネストされた最大 3 つのレベルのファイルを検査できます。その深さ（または指定したそれより低い最大深さ）を超えるアーカイブ ファイルをブロックするようファイル ポリシーを設定できます。

  最大アーカイブ ファイルの深さ 3 を超えるファイルをブロックしないよう選択した場合、抽出可能な内容と深さ 3 以上でネストされた内容を含むアーカイブ ファイルがモニター対象のトラフィックに現れると、システムは検査可能だったファイルについてのみデータを検査して報告します。

  圧縮解除されたファイルに適用できるすべての機能（動的分析やファイル ストレージなど）は、アーカイブ ファイル内のネストされたファイルに使用可能です。

- **暗号化ファイル**

  コンテンツが暗号化されているか検査できないアーカイブをブロックするように設定できます。

- **検査されないアーカイブ**

  アーカイブファイルを含むトラフィックがセキュリティ インテリジェンスのブロックリストまたはブロックしないリストに登録された場合、またはトップレベルのアーカイブファイルの SHA-256 値がカスタム検出リストにある場合、システムはアーカイブファイルの内容を検査しません。

  ネストされたファイルがブロックされた場合、アーカイブ全体がブロックされます。しかし、ネストされたファイルが許可された場合、アーカイブは自動的に渡されません（他のネストされたファイルおよび特性による）。

rar5 を含む一部の .rar アーカイブ内の .Exe ファイルは検出できません。

アーカイブ ファイルの性質

アーカイブ ファイルの性質は、アーカイブ内部のファイルに割り当てられた性質に基づきます。識別されたマルウェア ファイルを含んでいる**すべて**のアーカイブは、マルウェア（Malware）の性質になります。識別されたマルウェア ファイルを含んでいないアーカイブの場合、不明なファイルが 1 つでも含まれていれば 不明（Unknown）の性質、クリーン ファイルのみが含まれていれば クリーン（Clean）の性質になります。

表 *184 :* 内容に基づくアーカイブ ファイルの性質

アーカイブ ファイルの性質	不明なファイルの数	クリーン ファイルの数	マルウェア ファイルの数
Unknown	1 つ以上	任意	0
Clean	[0]	1 つ以上	[0]
Malware	すべて	すべて	1 つ以上

他のファイルと同様に、アーカイブ ファイルにも、該当する性質に関する条件が適用される場合はカスタム検出（Custom Detection）または利用不可（Unavailable）の性質が割り当てられます。

アーカイブの内容と詳細の表示

アーカイブ ファイルの内容を検査するようにファイル ポリシーが設定されている場合は、[分析（Analysis）] > [ファイル（Files）] メニューのページにあるコンテキスト メニューおよびネットワーク ファイル トラジェクトリ ビューアを使用して、アーカイブ ファイルがファイル イベント、マルウェアイベントに現れた場合、またはキャプチャされたファイルとして現れた場合に、アーカイブ内のファイルに関する情報を表示できます。

アーカイブのすべてのファイル コンテンツは表形式でリストされます。そのリストには、名前、SHA-256ハッシュ値、タイプ、カテゴリ、およびアーカイブの深さといった関連情報の概略が含まれています。ネットワーク ファイル トラジェクトリ アイコンはファイルごとに表示されます。そのアイコンをクリックすることで、特定のファイルに関する詳細な情報を表示することができます。

カスタム リストを使用したファイル性質のオーバーライド

AMP クラウドにあるファイルの性質が不正確だとわかっている場合、クラウドから性質を上書きするファイルの SHA-256 値をファイル リストに追加できます。

- AMP クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- AMP クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これ以降に検出された場合、デバイスでは、ファイルの性質を再評価せずに許可またはブロックできます。ファイル ポリシーに応じてクリーン リストまたはカスタム検出リストを使用できます。

（注） ファイルの SHA-256 値を計算するには、マルウェア クラウド ルックアップを実行するか、一致ファイルでマルウェアをブロックするルールをファイル ポリシーで設定する必要があります。

Firepower でのファイル リストの使用の詳細については、ファイル リスト （1338 ページ）を参照してください。

または、該当する場合はSecure Endpoint からの一元的なファイル リスト （2271 ページ）を参照します。

Secure Endpoint からの一元的なファイル リスト

組織で Secure Endpoint を展開している場合、Firepower は AMP クラウドにファイルの性質を照会するときに、Secure Endpoint で作成されたブロック リストおよび許可リストを使用できます。

要件：

- 組織で AMP パブリック クラウドを使用している必要がある。
- 組織で Secure Endpoint を導入している。
- Firepower と Secure Endpoint の統合 （2293 ページ） の手順を使用して、システムを Secure Endpoint に登録している。

これらのリストを作成して展開するには、Secure Endpoint のマニュアルまたはオンライン ヘルプを参照してください。

（注） Firepower で作成されたファイル リストは、Secure Endpoint で作成されたファイル リストをオーバーライドします。

ファイル ポリシーの管理

[ファイル ポリシー（File Policies）] ページには、既存のファイル ポリシーが最終更新日とともに表示されます。このページは、ファイル ポリシーの管理に使用できます。

（注） 動的分析の対象となるファイルタイプのリストが更新されたかどうか検査するために、システムは更新をチェックします（多くても1日に1回）。対象になるファイルタイプのリストが変更された場合、これはファイル ポリシーの変更を意味します。このファイル ポリシーを使用するアクセス コントロール ポリシーがいずれかのデバイスに展開されている場合、そのアクセス コントロール ポリシーには失効マークが付けられます。更新したファイル ポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。システムの保守：動的分析の対象となるファイル タイプの更新 （2266 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[マルウェアとファイル（Malware & File）]** を選択します。

ステップ 2 ファイル ポリシーを管理します。

- [比較（Compare）]：**[ポリシーの比較（Compare Policies）]** をクリックします（「ポリシーの比較」を参照）。
- 作成：ファイル ポリシーを作成するには、[新規ファイル ポリシー（New File Policy）] をクリックし、ファイルポリシーの作成または編集 （2266ページ）で説明する手順を実行します。
- コピー：ファイルポリシーをコピーするには、[コピー（Copy）]（ ）をクリックします。

  代わりに [表示（View）]（ ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：ファイルポリシーを削除するには、[削除（Delete）]（ ）をクリックし、プロンプトが表示されたら [はい（Yes）] と [OK] をクリックします。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- [展開（Deploy）]：**[展開（Deploy）]** > **[展開（Deployment）]** をクリックします（設定変更の展開 （172 ページ） を参照）。
- 編集：既存のファイルポリシーを変更するには、[編集（Edit）]（ ）をクリックします。
- レポート：[レポート（Report）]（ ） をクリックします（現在のポリシーレポートの生成 （192 ページ）を参照）。

ファイル ルール

ファイルのポリシーには、その親であるアクセス コントロール ポリシーと同様に、各ルールの条件に一致したファイルをシステムがどのように処理するかを決定するルールが含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

たとえば、あるファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- 性質に基づいてファイルをブロックする（悪意があることを示す評価の有無に関係なく）
- デバイスにファイルを保存する（詳細については、キャプチャされたファイルとファイル ストレージ （2282 ページ）を参照してください）
- ローカル マルウェア分析、Spero 分析、または動的分析のために、保存（キャプチャ）したファイルを送信する

さらに、ファイル ポリシーによって以下を実行できます。

- クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う
- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブ ファイル（`.zip` や `.rar` など）の内容を検査する
- アーカイブ ファイルの内容が暗号化されている場合、アーカイブのネスト レベルが最大レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブ ファイルをブロックする

ファイル ルールのコンポーネント

表 *185 :* ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn（SMB）を介して伝送されるファイルを検出し、検査できます。デフォルトの [任意（Any）] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn（SMB）トラフィック内のファイルを検出します。パフォーマンスを向上させるには、ファイル ルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。

ファイル ルールのコンポーネント	説明
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn（SMB）の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn（SMB）の発信トラフィックを検査できます。 **ヒント** [任意（Any）] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。個々のファイル タイプを検出したり、ファイル タイプ カテゴリ全体を検出したりするよう、ファイル ルールを設定できます。 たとえば、すべてのマルチメディア ファイルをブロックしたり、ShockWave Flash（swf）ファイルのみをブロックしたりできます。または、ユーザが BitTorrent（torrent）ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。 実行可能ファイルには、マクロとスクリプトを実行できるファイルタイプが含まれていることに注意してください。マルウェアが含まれている可能性があるためです。 システムで検査可能なファイル タイプのリストについては、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェアとファイル（Malware & File）] を選択して、一時的な新しいファイル ポリシーを作成してから、[ルールの追加（Add Rule）] をクリックします。ファイル タイプ カテゴリを選択すると、システムが検査できるファイル タイプが [ファイルタイプ（File Types）] リストに表示されます。 **（注）** 頻繁にトリガーされるファイル ルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとすると（たとえば YouTube は多量の Flash コンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。

ファイル ルールのコンポーネント	説明
ファイル ルール アクション	ファイル ルールのアクションによって、ルールの条件に一致したトラフィックをシステムが処理する方法が決定されます。 選択したアクションに応じて、システムでファイルを保存するか、ファイルに対してSpero分析、ローカルマルウェア分析、または動的分析を実行するかを設定できます。[ブロック（Block）] アクションを選択すると、システムでブロックされた接続をリセットするかどうかも設定できます。 これらのアクションおよびオプションの説明については、ファイル ルール アクション （2275 ページ）を参照してください。 ファイル ルールは数値上の順番ではなく、ルール アクションの順番で評価されます。詳細については、「ファイル ルール アクション：評価順序 （2284 ページ）」を参照してください。

ファイル ルール アクション

ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。各ファイル ルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する1つのアクションが関連付けられます。効果を発揮するには、ファイルポリシーに1つ以上のルールが含まれている必要があります。1 つのファイル ポリシー内に、ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを使用できます。

ファイル ルール アクション

- [ファイル検出（Detect Files）] ルールを使用すると、ファイルの伝送を許可しながら、特定のファイル タイプの検出をデータベースに記録できます。
- ファイルブロック ルールを使用すると、特定のファイルタイプをブロックできます。ファイル転送がブロックされたときに接続をリセットするオプション、およびキャプチャされたファイルを管理対象デバイスに保存するオプションを設定できます。
- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ルールを使用すると、ネットワークを通過するファイルの性質を取得して記録したうえでその伝送を許可できます。
- [マルウェア ブロック（Block Malware）] ルールを使用すると、特定のファイル タイプの SHA-256 ハッシュ値を計算した後、AMP クラウドを照会して、ネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示すファイルをブロックできます。

ファイル ルール アクションのオプション

選択したアクションに応じて、さまざまなオプションがあります。

ファイル ルール アクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェア クラウド ルックアップが可能か
MSEXE 用の Spero 分析*（Spero Analysis* for MSEXE）	No	はい：実行可能ファイルを送信できます	No	はい：実行可能ファイルを送信できます
動的分析*（Dynamic Analysis*）	No	はい：不明なファイルの性質の実行可能ファイルを送信できます	No	はい：不明なファイルの性質の実行可能ファイルを送信できます
容量処理（Capacity Handling）	×	○	×	○
ローカル マルウェア分析（Local Malware Analysis）	×	○	×	○
接続のリセット（Reset Connection）	はい（推奨）	はい（推奨）	×	×
ファイルの保存（Store files）	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイルタイプを保存できます	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイルタイプを保存できます

* これらのオプションの詳細については、マルウェア防御オプション（ファイル ルール アクション） （2277 ページ）およびそのサブトピックを参照してください。

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化または無効化、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除すると、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

マルウェア防御オプション（ファイル ルール アクション）

システムでは、ファイルにマルウェアが含まれるかどうかを判断するために、ファイル インスペクションと分析のいくつかの方法が適用されます。

ファイル ルールでオプションを有効にするオプションに応じて、システムは次のツールと順序でファイルを検査します。

1. Spero 分析 （2280 ページ）およびAMP クラウドのルックアップ （2280 ページ）
2. ローカル マルウェア分析（Local Malware Analysis） （2280 ページ）
3. 動的分析（Dynamic Analysis） （2281 ページ）

これらのツールの比較については、マルウェア防御のオプションの比較 （2277ページ）を参照してください。

（該当する場合は、そのファイル タイプに基づいてすべてのファイルをブロックすることもできます。詳細については、ファイル タイプによるすべてのファイルのブロック （2284ページ）を参照してください）。

（オプション）Secure Endpoint を使用したマルウェア防御 （2290 ページ） およびサブトピックからシスコの Secure Endpoint 製品に関する情報も参照してください。

マルウェア防御のオプションの比較

次の表では、各タイプのファイル分析の利点と欠点、および各マルウェア防御方法によってファイルの性質が決定される方法について説明します。

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析	実行可能ファイルの構造分析。Spero シグネチャを分析のために AMP クラウドに送信します。	ローカルマルウェア分析または動的分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
ローカルマルウェア分析（Local Malware Analysis）	動的分析より消費するリソースが少なく、特に検出されたマルウェアが一般的な場合は結果がより迅速に返されます。	動的分析よりも結果の詳細度が低くなります。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
動的分析*（Dynamic Analysis*）	を使用した不明なファイルの詳細な分析 Secure Malware Analytics	対象ファイルはパブリッククラウドまたはオンプレミスアプライアンスにアップロードされます。分析の完了には少し時間がかかります	脅威スコアによってファイルの悪意の度合いが決定されます。性質はファイルポリシーに設定されている脅威スコアしきい値に基づいている場合があります。
Spero 分析とローカル マルウェア分析	AMP クラウドのリソースを使用してマルウェアを特定しながら、ローカルマルウェア分析と動的分析を設定するよりも少ないリソースを消費します。	動的分析、Spero 分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
Spero 分析と動的分析	ファイルおよび Spero シグネチャの送信時に AMP クラウドの全機能を使用します	ローカルマルウェア分析を使用する場合よりも結果の取得に時間がかかります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイル ポリシーで設定されている脅威スコアしきい値に基づいて、および Spero 分析でマルウェアが特定された場合は、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。

分析タイプ	利点	制限事項	マルウェアの特定
ローカルマルウェア分析と動的分析	両方のタイプのファイル分析を使用することで詳細な結果が得られます	どちらか一方の場合よりも消費するリソースが多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
Spero 分析、ローカルマルウェア分析、および動的分析	詳細結果	3 つすべてのタイプのファイル分析を実行するため消費するリソースが最も多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。Spero 分析またはローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
（指定されたファイルタイプのすべてのファイルの送信をブロック）	マルウェア防御のライセンスは必要ありません （このオプションは技術的なマルウェア防御オプションではありません。）	正規ファイルもブロックされます	（分析は実行されません。）

（注） 事前分類はファイルの性質を決定するものではありません。ファイルが動的分析の対象であるかどうかを判断する要因の 1 つにすぎません。

Spero 分析

Spero分析では、実行可能なファイルのファイル構造の特性（メタデータやヘッダー情報など）を調べます。この情報に基づいてSperoシグネチャを生成した後、ファイルが対象の実行可能なファイルである場合、デバイスはそれをAMPクラウド内のSperoヒューリスティックエンジンに送信します。Sperooシグネチャに基づいて、そのファイルがマルウェアかどうかをSperoエンジンが決定します。また、ファイルをAMPクラウドに送信することなく、Spero分析用に送信するようにルールを設定することもできます。

Spero 分析用にファイルを手動で送信することはできません。

AMP クラウドのルックアップ

高度なマルウェア防御を使用した評価の対象となるファイルの場合、Firewall Management Centerはマルウェア クラウド ルックアップを実行し、そのSHA-256ハッシュ値に基づいてファイルの性質をAMPクラウドに照会します。

パフォーマンスを改善するために、システムはクラウドから返される性質をキャッシュ化し、AMPクラウドでクエリを実行する代わりに、既知のファイルのキャッシュ済みの性質を使用します。このキャッシュの詳細ついては、キャッシュ済み性質の有効期間（2280ページ）を参照してください。

ローカル マルウェア分析（*Local Malware Analysis*）

ローカルマルウェア分析では、管理対象デバイスでTalosインテリジェンスグループから提供される検出ルールを使用して、実行可能ファイル、PDF、Office文書、およびその他のタイプのファイルで最も一般的なタイプのマルウェアの有無をローカルで検査することができます。ローカル分析ではAMPクラウドにクエリを実行せず、ファイルも実行しないため、ローカルマルウェア分析では時間とシステム リソースが節約できます。

システムはローカルマルウェアによってマルウェアを識別すると、その既存のファイルの性質を[不明（Unknown）]から[マルウェア（Malware）]に更新します。その上で、システムは新しいマルウェア イベントを生成します。システムはマルウェアを識別しなかったとしても、ファイルの性質を[不明（Unknown）]から[正常（Clean）]に更新することはしません。ローカル マルウェア分析を実行した後、システムはファイル情報（SHA-256ハッシュ値、タイムスタンプ、ファイルの性質など）をキャッシュに入れて、特定の期間内にそのファイルを再度検出した場合に再び分析を行わなくてもマルウェアを識別できるようにします。このキャッシュの詳細ついては、キャッシュ済み性質の有効期間（2280 ページ）を参照してください。

ローカルマルウェア分析では、Secure Malware Analyticsクラウドとの通信を確立する必要はありません。ただし、ファイルをダイナミック分析用にクラウドに送信するため、また、アップデートをローカルマルウェア分析ルールセットにダウンロードするために、クラウドとの通信を設定する必要があります。

キャッシュ済み性質の有効期間

AMPクラウドのクエリから返された、脅威スコアに関連付けられた性質、およびローカル マルウェア分析によって割り当てられた性質には、存続可能時間（TTL）が設定されます。性質が更新されないまま、TTL値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質および関連する脅威スコアには次のTTL値が割り当てられます。

- クリーン：4 時間
- 不明：1 時間
- マルウェア：1 時間

このキャッシュに対するクエリで、キャッシュされた性質がタイムアウトになったことが識別された場合、システムはローカル マルウェア分析データベースおよび AMP クラウドに新しい性質を再びクエリします。

動的分析（*Dynamic Analysis*）

Secure Malware Analytics（以前の Threat Grid）、シスコのファイル分析、および脅威インテリジェンスプラットフォームを使用して動的分析用ファイルを自動的に送信するようにファイルポリシーを設定できます。

デバイスは、デバイスがファイルを保存するかどうかに関係なく、適格なファイルを Secure Malware Analytics（指定したいずれかのパブリック クラウドまたはオンプレミス アプライアンス）に送信します。

Secure Malware Analytics 悪意のあるファイルかどうかを判断するためにサンドボックス環境でファイルを実行してファイルの動作を分析し、ファイルにマルウェアが含まれる可能性を示す脅威スコアを返します。脅威スコアから、脅威スコアを割り当てた理由が含まれる動的分析のサマリー レポートを表示できます。また、Secure Malware Analytics では、組織が送信したファイルの詳細レポートを表示したり、組織が送信しなかったファイルのデータが限定されたスクラビング処理レポートを表示したりすることもできます。

Cisco Secure Malware Analytics の詳細については、https://www.cisco.com/c/en/us/products/security/threat-grid/index.htmlを参照してください。

動的分析を実行するようにシステムを設定するには、動的分析接続（2262 ページ）のトピックを参照してください。

動的分析の対象となるファイル

動的分析用ファイルの対象は、次の条件によって異なります。

- ファイル タイプ
- ファイル サイズ
- ファイル ルールのアクション

さらに、次のパターンがあります。

- システムは設定したファイル ルールに一致するファイルのみを送信します。
- 分析用の送信時にファイルのマルウェア クラウド ルックアップの性質が不明または使用不可になっている必要があります。
- システムは潜在的なマルウェアとしてファイルを事前分類する必要があります。

動的分析とキャパシティ処理

キャパシティ処理を使用すると、デバイスがクラウドと通信できない場合、または送信の最大数に達した場合に、システムがクラウドにファイルを一時的に送信できないと、動的分析の対象となるファイルを一時的に保存することができます。システムは、妨害状態が経過すると保存したファイルを送信します。

一部のデバイスはデバイスのハードドライブまたはマルウェアストレージパックにファイルを保存できます。マルウェア ストレージ パック （2283 ページ） も参照してください。

キャプチャされたファイルとファイル ストレージ

ファイルストレージ機能を使用すると、選択したファイル（トラフィックで検出された）をキャプチャして、ファイルのコピーをデバイスのハードドライブかマルウェアストレージパック（インストールされている場合）に自動的に保存できます。

デバイスがファイルをキャプチャした後に、以下の選択肢があります。

- 後で分析するために、キャプチャしたファイルをデバイスのハードドライブに保存する。
- さらに手動で分析したりアーカイブしたりするために、保存したファイルをローカル コンピュータにダウンロードする。
- AMP クラウド ルックアップまたは動的分析の対象となるキャプチャ ファイルを手動で送信します。

注意すべき点として、デバイスがファイルを保存した後は、以後それを検出しても、デバイスが引き続きそれを保存していれば、そのファイルを再度キャプチャすることはありません。

（注） ファイルがネットワーク上で初めて検出された際には、ファイルの検出を表すファイルイベントを生成できます。ただし、ファイル ルールがマルウェア クラウド ルックアップを行う場合は、システムが AMP クラウドにクエリを行い、判定結果が返るまで、より多く時間を要します。この遅延により、システムはネットワークでこのファイルが2回目に検出され、ファイルの判定結果を即座に判断できるまでは、このファイルを保存できません。

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- [分析（Analysis）] > [ファイル（Files）] > [キャプチャされたファイル（Captured Files）] からのキャプチャされたファイルに関する情報（動的分析のためにファイルが保存されたのか送信されたかどうか、ファイルの性質、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。
- ファイルのトラジェクトリを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。
- ファイルをクリーン リストまたはカスタム検出リストに追加することで、以後の検出時には常に、クリーンまたはマルウェアの判定結果を持つファイルとして扱う。

ファイル ポリシーでファイル ルールを設定して、特定のタイプまたは特定のファイル判定結果（使用できる場合）のファイルをキャプチャして保存します。ファイルポリシーをアクセス コントロール ポリシーと関連付けて、それをデバイスに展開した後、トラフィック内の一致

ファイルが検出され、保存されます。また、保存するファイルサイズの最小値と最大値を設定できます。

システム バックアップに保存ファイルは含まれません。

キャプチャしたファイル情報は、[分析（Analysis）] > [ファイル（Files）] > [キャプチャしたファイル（Captured Files）] で表示し、コピーをオフライン分析用にダウンロードすることができます。

マルウェア ストレージ パック

ファイル ポリシー構成によっては、デバイスがハード ドライブにかなりの量のファイル データを保存することがあります。デバイスにマルウェア ストレージ パックを設置できます。システムがファイルをマルウェア ストレージ パックに保存することにより、イベントおよび設定ファイルを保存するために、プライマリ ハード ドライブにより多くスペースを確保できます。システムは定期的に古いファイルを削除します。デバイスのプライマリ ハード ドライブに使用可能な領域が十分でなく、マルウェア ストレージパックも設置されていない場合、ファイルを保存することはできません。

⚠

注意 シスコから供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。

マルウェア ストレージ パックが設置されていない場合、ファイルを保存するデバイスを設定すると、プライマリ ハード ドライブのスペースの特定の部分がキャプチャ ファイル ストレージに割り当てられます。ダイナミック分析用に一時的にファイルに保存するよう容量処理を設定すると、システムはファイルをクラウドに再送信できるようになるまで、同じハード ドライブ割り当てを使用してそれらのファイルを保存します。

デバイスにマルウェア ストレージ パックを設置してファイル ストレージまたは容量処理を設定すると、デバイスはマルウェア ストレージ パック全体をこれらのファイルの保存用として割り当てます。デバイスは、マルウェア ストレージ パックに他の情報を保存することはできません。

キャプチャ ファイル ストレージに割り当てられたスペースがいっぱいになると、システムは割り当てられたスペースがシステム定義しきい値に達するまで、保管されている古いファイルを削除します。保存されていたファイルの数によっては、システムがファイルを削除した後、ディスク使用率がかなり減る場合があります。

マルウェア ストレージ パックを設置する時点で、デバイスがすでにファイルを保存している場合、次にデバイスを再起動したときに、プライマリ ハード ドライブに保存されていたキャプチャ ファイルまたは容量処理ファイルはすべて、マルウェア ストレージ パックに移動します。それ以降デバイスが保存するファイルはすべて、マルウェア ストレージ パックに保存されます。

FirepowerデバイスでMSPを使用する詳細については、「Firepower ハードウェア設置ガイド」を参照してください。

ファイル タイプによるすべてのファイルのブロック

マルウェア ファイル伝送のブロックに加えて、マルウェアを含むかどうかにかかわらず、特定のタイプのすべてのファイルをブロックする必要がある場合は、それを実行できます。

システムでマルウェアを検出できるすべてのファイル タイプだけでなく、さらに多数のファイル タイプに対するファイル制御がサポートされています。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。

タイプに基づいてすべてのファイルをブロックする方法は、技術的にはマルウェア防御機能ではないため、マルウェア防御 ライセンスは不要で、AMP クラウドにクエリは実行されません。

ファイル ルール アクション：評価順序

ファイル ポリシーには、状況に応じて異なるアクションを持つ複数のルールが含まれる可能性があります。複数のルールを特定の状況に適用できる場合、このトピックで説明する評価順序が適用されます。通常、（優先度の高い順に）単純なブロッキング、次にマルウェア インスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。

ファイル ルール アクションの優先度は次のとおりです。

- ファイル ブロック（*Block Files*）
- マルウェア ブロック（*Block Malware*）
- マルウェア クラウド ルックアップ（*Malware Cloud Lookup*）
- ファイル検出（*Detect Files*）

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、「Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）」を参照してください。

ファイル ルールの作成

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化または無効化、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除すると、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

始める前に

マルウェア保護のルールを設定する場合は、ファイルポリシーの設定（2252ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェアとファイル（Malware & File）] を選択します。

ステップ 2 編集アイコンをクリックして、既存のファイルポリシーを変更します。

ステップ 3 ファイルポリシーエディタで、[ルールの追加（Add Rule）] をクリックします。

ステップ 4 ファイルルールのコンポーネント（2273ページ）の説明に従って、[アプリケーションプロトコル（Application Protocol）] および [転送の宛先（Direction of Transfer）] を選択します。

ステップ 5 [ファイル タイプ（File Types）] を 1 つ以上選択します。

表示されるファイル タイプは、選択したアプリケーション プロトコル、転送の方向、およびアクションによって異なります。

ファイル タイプのリストを、次のようにフィルタ処理できます。

- 1 つ以上の [ファイル タイプ カテゴリ（File Type Categories）] を選択し、[選択したカテゴリのすべてのタイプ（All types in selected Categories）] をクリックします。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[Search name and description] フィールドに **`Windows`** と入力します。

ヒント
ファイル タイプの上にポインタを移動すると、説明が表示されます。

ステップ 6 ファイルルールアクション：評価順序（2284ページ）を確認し、ファイルルールアクション（2275 ページ）の説明に従ってファイル ルール [アクション（Action）] を選択します。

利用可能なアクションは、インストールしたライセンスによって異なります。ファイルおよびマルウェア ポリシーのライセンス要件（2245 ページ）を参照してください。

ステップ 7 選択したアクションに応じて、以下のオプションを設定します。

- ファイルのブロック後に接続をリセットする
- ルールに一致するファイルを保存する
- Spero 分析を有効にする*
- ローカル マルウェア分析を有効にする*
- 動的分析およびキャパシティ処理を有効にする

* これらのオプションの詳細については、ファイル ルール アクション （2275 ページ）とマルウェア防御オプション（ファイルルールアクション） （2277 ページ）およびそのサブトピックを参照してください。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- マルウェア保護のポリシーを設定する場合は、ファイルポリシーの設定 （2252 ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

マルウェア防御のためのアクセス制御ルールのロギング

システムはファイルポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを Secure Firewall Management Center データベースに自動的にロギングします。ログファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。

また、システムは、呼び出し元のアクセス コントロール ルールのロギング設定にかかわらず、関連付けられた接続の終了を Secure Firewall Management Center データベースにロギングします。

レトロスペクティブな性質の変更

ファイルの性質は変更される可能性があります。たとえば、新しい情報が見つかると、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。過去 1 週間にクエリを行ったファイルの性質が変更された場合、AMP クラウドはシステムに通知して、システムが次回そのファイルの送信を検出した際に自動的にアクションをとれるようにします。変更された性質は、レトロスペクティブな性質と呼ばれます。

ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション

ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があります。

表 *186 :* アクセス コントロール ファイルおよび マルウェア防御 の詳細オプション

フィールド	説明	ガイドラインと制限
ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）	ファイルタイプを検出するときに検査するバイト数を指定します。	0 ～ 4294967295（4 GB） 0 にすると制限が解除されます。 デフォルト値は、TCP パケットの最大セグメントサイズ（1460バイト）です。ほとんどの場合、システムは最初のパケットによって、一般的なファイルタイプを特定できます。 ISO ファイルを検出するには、36870 よりも大きい値を入力します。
ファイルを許可するのにかかるマルウェア ブロックのクラウドルックアップの制限時間（秒）（Allow file if cloud lookup for Block Malware takes longer than (seconds)）	マルウェア クラウド ルックアップの実行中に、システムが [マルウェア ブロック（Block Malware）] ルールに一致し、性質がキャッシュに入っていないファイルの最後のバイトを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	0 ～ 30 秒 サポートに連絡することなく、このオプションを 0 に設定しないでください。 シスコは、接続の障害によってトラフィックのブロックを防ぐために、デフォルト値を使用することをお勧めします。
SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA--256 hash values for files larger than (in bytes)）	システムが特定のサイズを超えるファイルを保管すること、ファイルでマルウェア クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	0 ～ 4294967295（4 GB） 0 にすると制限が解除されます。 この値は、[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [動的分析テストの最大ファイルサイズ(バイト)（Maximum file size for dynamic analysis testing (bytes)）] の値以上に設定する必要があります。

フィールド	説明	ガイドラインと制限
[高度なファイル インスペクションと保存のための最小ファイル サイズ（バイト）（Minimum file size for advanced file inspection and storage (bytes)）]	これらの設定は以下を指定します。 • 次のディテクタを使用してシステムが検査できるファイルサイズ： • Spero 分析 • サンドボクシングと事前分類 • ローカル マルウェア分析/ClamAV • アーカイブインスペクション • システムがファイルルールを使用して保存できるファイルサイズ。	0 ～ 10485760（10MB） 0にするとファイル ストレージが無効になります。 [保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。
[高度なファイル インスペクションと保存のための最大ファイル サイズ（Minimum file size for advanced file inspection and storage (bytes)）]		0 ～ 10485760（10MB） 0にするとファイル ストレージが無効になります。 [保存する最小ファイルサイズ（バイト）（Minimum file size to store (bytes)）] の値以上、および [SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。
ダイナミック分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）	システムが AMP クラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	0 ~ 10485760（10 MB） [動的分析テストの最大ファイルサイズ（バイト）（Maximum file size for dynamic analysis testing (bytes)）] および [SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 システムは AMP クラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。

フィールド	説明	ガイドラインと制限
ダイナミック分析の最大ファイルサイズ(バイト)（Maximum file size for dynamic analysis testing (bytes)）	システムが AMP クラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	0 ~ 10485760（10 MB） [動的分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）] の値以上、[SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 システムは AMP クラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者ユーザーである必要があります。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced Settings）] をクリックします。

ステップ 2 [ファイルおよびマルウェアの設定（Files and Malware Settings）] の横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション（2286 ページ）で説明されている任意のオプションを設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

（オプション）Secure Endpoint を使用したマルウェア防御

シスコの Secure Endpoint は、システムから提供され、Firepower 展開と統合し、マルウェア防御を補完できる個別のマルウェア防御製品です。

Secure Endpoint はシスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。個別ユーザーのエンドポイント（コンピュータやモバイルデバイス）で軽量コネクタとして実行し、高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。

Secure Endpoint の利点を次に示します。

- 部門全体のためにカスタム マルウェア検出ポリシーとプロファイルを設定し、すべてのユーザーのファイルに対してフラッシュ スキャンおよび完全スキャンを実行する
- マルウェア分析の実行：ヒートマップ、詳細なファイル情報、ネットワーク ファイル トラジェクトリ、脅威の根本原因の表示など
- アウトブレイク コントロールのさまざまな要素を設定する：自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーション ブロッキング、除外リストなど
- カスタム保護の作成、グループポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタムの許可されたアプリケーションリストの作成
- Secure Endpoint 管理コンソールを使用してマルウェアの影響を軽減する。管理コンソールの堅牢かつ柔軟な Web インターフェイスを使用すると、エンドポイント向け Secure Endpoint 展開のあらゆる側面を制御し、アウトブレイクのすべての段階を管理できます。

Secure Endpoint の詳細については、次を参照してください。

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html。
- Secure Endpoint 管理コンソールのオンライン ヘルプ。
- Secure Endpoint のドキュメントは http://docs.amp.cisco.comで入手できます。

マルウェア防御の比較：Firepower と Secure Endpoint

表 *187*：製品の検出による高度なマルウェア保護の違い

機能	Firepower Malware Protection（マルウェア防御）	Secure Endpoint
ファイル タイプの検出とブロッキングの方法（ファイル制御）	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	未サポート
マルウェアの検出とブロッキングの方法	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	個々のエンドポイント（エンドユーザー コンピュータとモバイルデバイス）でAMPクラウドとの通信を行うコネクタを使用
ネットワーク トラフィックを検査	管理対象デバイスを通過するトラフィック	なし（エンドポイントにインストールされたコネクタがファイルを直接検査する）
マルウェア インテリジェンスのデータ ソース	AMPクラウド（パブリックまたはプライベート）	AMPクラウド（パブリックまたはプライベート）
マルウェア検出の堅牢性	限定されたファイル タイプ	すべてのファイル タイプ
マルウェア分析の選択肢	Firewall Management Center ベース、および AMP クラウドでの分析	Firewall Management Center ベース、および Secure Endpoint 管理コンソールの追加オプション
マルウェアの影響軽減	ネットワーク トラフィックでのマルウェア ブロッキング、Firewall Management Center が開始する修復	Secure Endpoint ベースの検疫およびアウトブレイク コントロール オプション、Firewall Management Center が開始する修復
生成されるイベント	ファイル イベント、キャプチャされたファイル、マルウェア イベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェア イベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェア イベント情報（接続データなし）
ネットワーク ファイル トラジェクトリ	Firewall Management Center ベース	Firewall Management Center と Secure Endpoint の管理コンソールには、それぞれネットワーク ファイル トラジェクトリがあります。いずれも使用可能です。
必要なライセンスまたはサブスクリプション	とファイル制御の実行に必要なライセンス マルウェア防御	Secure Endpoint サブスクリプションFirewall Management Center への Secure Endpoint データの取り込みに必要なライセンスはありません。

Firepower と Secure Endpoint の統合について

組織で Secure Endpoint が導入されている場合、必要に応じてその製品を Firepower 展開と統合できます。

Secure Endpoint との統合に専用の Firepower ライセンスは必要ありません。

Firepower と Secure Endpoint の統合の利点

Secure Endpoint 展開をシステムに統合すると、次のような利点があります。

- Secure Endpoint で設定する中央集中型のブロックされたアプリケーションおよび許可されたアプリケーションによって、Firepower から AMP クラウドに送信されるファイル SHA の判定が決まります。

  「Secure Endpoint からの一元的なファイル リスト （2271 ページ）」を参照してください。

- システムは Secure Endpoint によって検出されたマルウェア イベントを Secure Firewall Management Center にインポートできるため、システムによって生成されたマルウェア イベントとともにこれらのイベントを管理できます。これらのイベントでインポートされたデータには、スキャン、マルウェア検出、隔離、ブロックされた実行、クラウドの呼び出し、およびモニターするホストに対して Firewall Management Center が表示する侵害の兆候（IOC）が含まれます。

  詳細については、*Secure Endpoint*を使用したマルウェア イベント分析（Cisco Secure Firewall Management Center アドミニストレーション ガイド）を参照してください。

- Secure Endpoint コンソールでは、ファイルの軌跡およびその他の詳細を表示できます。

  詳細については、*Secure Endpoint* コンソールでのイベント データの使用（Cisco Secure Firewall Management Center アドミニストレーション ガイド）を参照してください。

重要 Cisco AMP プライベート クラウドを使用する場合は、Secure Endpoint と AMP プライベート クラウド （2292 ページ）の制限事項を参照してください。

Secure Endpoint と AMP プライベート クラウド

ネットワーク上の Secure Endpoint データを収集するように Cisco AMP プライベート クラウドを設定した場合、すべての Secure Endpoint コネクタはプライベート クラウドにデータを送信します。そのデータは Secure Firewall Management Center に転送されます。プライベート クラウドは、エンドポイント データを外部接続では一切共有しません。

組織で AMP プライベート クラウドを展開している場合、プライベート クラウドを介した AMP クラウド ファネルとのすべての接続は、監視対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。これには Secure Endpoint データのインポートが含まれます。プライベート クラウドは、エンドポイント データを外部接続では一切共有しません。

AMP プライベートクラウドを使用する場合、次の統合機能は使用できません。

- Secure Endpoint で設定された、ブロックされたアプリケーションと許可されたアプリケーションのリストの使用。（これらのリストは、ファイルをブロックまたは許可するために使用されます。）
- Firepower から生成されたマルウェアイベントの Secure Endpoint での可視性。

必要なキャパシティをサポートするように複数のプライベート クラウドを設定できます。

Firepower と Secure Endpoint の統合

組織がシスコの Secure Endpoint 製品を展開している場合は、そのアプリケーションを Firepower と統合し、Firepower と Secure Endpoint の統合の利点 （2292 ページ）で説明されている利点を実現できます。

Secure Endpoint と統合する場合、マルウェア防御（AMP for Firepower）接続がすでに設定されていても、Secure Endpoint 接続を設定する必要があります。複数の Secure Endpoint クラウド接続を設定できます。

（注） Secure Endpoint 接続が正しく登録されていなくても、マルウェア防御 は影響を受けません。

始める前に

- このタスクを実行するには、管理者ユーザーである必要があります。
- 展開で Cisco AMP プライベートクラウドを使用している場合Secure Endpoint と AMP プライベート クラウド （2292 ページ）は、の制限事項を参照してください。
- ネットワークで Secure Endpointが設定されていて、正しく機能している必要があります。
- Firewall Management Center はインターネットにアクセスできる必要があります。
- Firewall Management Center と Secure Endpoint が相互に通信できることを確認します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Security, Internet Access, and Communication Ports」にあるトピックを参照してください。
- Firewall Management Center を工場出荷時の初期状態に復元した後、または以前のバージョンに戻した後に AMP クラウドに接続している場合は、Secure Endpoint 管理コンソールを使用して以前の接続を削除します。
- この手順中に Secure Endpoint コンソールにログインするには、Secure Endpoint クレデンシャルが必要です。

手順

ステップ 1 **[統合（Integration）]** > **[AMP]** > **[AMP管理（AMP Management）]**を選択します。

ステップ 2 [AMPクラウド接続の追加（Add AMP Cloud Connection）] をクリックします。

ステップ 3 **[クラウド名（Cloud Name）]** ドロップダウン リストから、使用するクラウドを選択します。

- Firewall Management Center の地理的な場所に最も近い AMP クラウド。

  APJC はアジア/太平洋/日本/中国です。

- AMP プライベート クラウド（AMPv）の場合、[プライベートクラウド（Private Cloud）] を選択し、Cisco AMP プライベート クラウド （2258 ページ）の手順に進みます。

ステップ 4 このクラウドをマルウェア防御 と Secure Endpoint の両方に使用する場合は、[AMP for Firepower に使用（Use for AMP for Firepower）] チェックボックスをオンにします。

マルウェア防御（AMP for Firepower）通信を処理する別のクラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMP 接続の場合は、オフにできません。

ステップ 5 [登録（Register）] をクリックします。

[回転状態（Spinning state）]（） アイコンは、たとえば、Firewall Management Center で接続を設定した後、Secure Endpoint 管理コンソールの使用を許可する前に、接続が保留中であることを示します。[拒否（Denied）]（） アイコンは、クラウドが接続を拒否したこと、または他の理由で接続が失敗したことを示します。

ステップ 6 Secure Endpoint 管理コンソールを続行することを確認し、管理コンソールにログインします。

ステップ 7 管理コンソールを使用して、Secure Endpoint データを Firewall Management Center に送信することを AMP クラウドに許可します。

ステップ 8 Firewall Management Center が受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。

デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、Secure Endpoint 管理コンソールで **[管理（Management）]** > **[グループ（Groups）]** を選択します。詳細については、管理コンソールのオンライン ヘルプを参照してください。

ステップ 9 [許可（Allow）] をクリックして接続を有効にして、データの転送を開始します。

[拒否（Deny）] をクリックすると Firewall Management Center に戻りますが、接続には拒否マークが付きます。接続を拒否/許可しないまま Secure Endpoint 管理コンソールの [アプリケーション（Applications）] ページから別のページに移動した場合、Firewall Management Center の Web インターフェイスでは接続に保留中のマークが付きます。これらのいずれの状況でも、ヘルスモニターは失敗した接続のアラートを生成**しません**。後で AMP クラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成します。

Secure Endpoint 接続の登録が未完了であっても、マルウェア防御 接続は無効になりません。

ステップ 10 接続が正しく設定されていることを確認するには、次の手順を実行します。

a) **[統合（Integration）]** > **[AMP]** > **[AMP管理（AMP Management）]** ページで、**[Cisco AMP ソリューション タイプ（Cisco AMP Solution Type）]** 列に Secure Endpoint が含まれている [クラウド名（Cloud Name）] をクリックします。

b) 表示される Secure Endpoint コンソール ウィンドウで、**[アカウント（Accounts）] > [アプリケーション（Applications）]** を選択します。
c) Firewall Management Center が一覧に含まれていることを確認します。
d) Secure Endpoint コンソール ウィンドウで、**[管理（Manage）]>[コンピュータ（Computers）]** を選択します。
e) Firewall Management Center が一覧に含まれていることを確認します。

次のタスク

- Secure Endpoint コンソール ウィンドウで、必要に応じて設定を行います。たとえば、管理センターのグループ メンバーシップの定義や、ポリシーの割り当てを行います。詳細については、Secure Endpoint のオンライン ヘルプまたはその他のドキュメントを参照してください。
- 高可用性展開では、両方の Management Center で AMP クラウド接続を設定します。これらの設定は同期されません。
- デフォルトのヘルス ポリシーは、Firewall Management Center から Secure Endpoint ポータルへの最初の接続が成功した後で接続できなくなった場合、または AMP ポータルを使って接続が登録解除された場合に警告を出します。

  [システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] の **Secure Endpoint ステータス** モニターが有効になっていることを確認します。

ネットワークマルウェア防御とファイルポリシーの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
AMP クラウドとの通信	7.0	任意（Any）	レガシーポート 32137 は、AMP パブリッククラウドまたはプライベートクラウドとの通信でサポートされなくなりました。 新規/変更された画面：**[システム（System）]** > **[統合（Integration）]** > **[クラウドサービス（Cloud Services）]** ページの **[ネットワーク用 AMP にレガシーポート32137を使用（Use Legacy Port 32137 for AMP for Networks）]** オプションは使用できなくなりました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
章の再構成	変更は 6.4 で行われましたが、再発行されたすべてのバージョンに適用されます	任意（Any）	混乱を避けるため、この章の内容が再構成されました。 一部のコンテンツは、Cisco Secure Firewall Management Center アドミニストレーション ガイド の「*File/Malware Events and Network File Trajectory*」の章との間で交換されました。
URL フィルタリング情報を新しい URL フィルタリングの章に移動しました。	6.3	任意（Any）	URL フィルタリングのクラウド通信の設定に関する情報を新しい URL フィルタリングの章に移動しました。章内の Cisco CSI のトピックの構成に関連する変更を加えました。

第 X 部

暗号化トラフィックの処理

- トラフィックの復号の概要 （2299 ページ）
- 復号ポリシー （2327 ページ）
- 復号ルール （2349 ページ）
- 復号ルールとポリシーの例 （2403 ページ）

第 60 章

トラフィックの復号の概要

以下のトピックでは TLS/SSL（Transport Layer Security/Secure Sockets Layer）インスペクションの概要を示し、TLS/SSL インスペクション設定の前提条件と詳細な導入シナリオについて説明します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

SSL プロトコルと TLS プロトコルの詳細については、「SSL vs. TLS - What's the Difference?」[英語] などのリソースを参照してください。

- トラフィック復号の説明 （2299 ページ）
- TLS/SSL ハンドシェイク処理 （2301 ページ）
- 復号 ルールとポリシーの基本 （2307 ページ）
- TLS 暗号化アクセラレーション （2316 ページ）
- 復号ポリシー とルールの設定方法 （2319 ページ）
- 復号ポリシー の履歴 （2322 ページ）

トラフィック復号の説明

インターネット上の大半のトラフィックは暗号化されており、ほとんどの場合、復号する必要はありません。復号しなくても、それに関する一部の情報を収集し、必要に応じてネットワークからブロックすることができます。

選択できるタイプは、次のとおりです。

- トラフィックを復号し、完全な一連の詳細検査の対象とします。
  - [高度なマルウェア防御（Advanced Malware Protection）]
  - セキュリティ インテリジェンス

- Threat Intelligence Director
- アプリケーション ディテクタ
- URL およびカテゴリのフィルタリング

- トラフィックを暗号化したままにしてアクセス制御をセットアップし、復号ポリシーに検索させ、ブロックできるようにします。
  - 古いプロトコルバージョン（セキュアソケットレイヤなど）
  - セキュアでない暗号スイート
  - リスクが高く、ビジネスとの関連性が低いアプリケーション
  - 信頼できない発行元識別名

アクセス コントロール ポリシー

アクセス コントロール ポリシーは、復号ポリシー を含む、サブポリシーとその他の設定を呼び出すメイン設定です。アクセスコントロールと 復号ポリシー を関連付けると、システムでは、この 復号ポリシー を使用して暗号化セッションを処理し、その後でそれらのセッションをアクセスコントロールルールで評価します。TLS/SSL インスペクションを設定していない場合、またはデバイスで SSL インスペクションをサポートしていない場合は、アクセス コントロール ルールですべての暗号化トラフィックが処理されます。

TLS/SSL インスペクションの設定で暗号化トラフィックの通過が許可されている場合、アクセスコントロールルールによっても暗号化トラフィックが処理されます。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイル インスペクションを無効にしています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

注意

復号ルールには、パフォーマンスに影響を及ぼす可能性があるオーバーヘッドの処理が必要です。トラフィックの復号を決定する前に、トラフィックを復号する場合としない場合（2308ページ）を参照してください。

管理対象デバイスで Snort 3 が有効になっていれば、システムは TLS 1.3 トラフィックの復号をサポートします。復号ポリシーの詳細オプションで TLS 1.3 の復号を有効にすることができます。詳細については、復号ポリシーの詳細オプション（2345 ページ）を参照してください。

Firepower システムは相互認証をサポートしていません。つまり、クライアント証明書を Secure Firewall Management Center にアップロードして、[復号-再署名（Decrypt - Resign）] アクションまたは [復号-既知のキー（Decrypt - Known Key）] 復号ルール アクションに使用することはできません。詳細については、復号と再署名（発信トラフィック）（2310ページ）および既知のキーでの復号（着信トラフィック）（2311 ページ）を参照してください。

FlexConfig を使用して TCP 最大セグメントサイズ（MSS）の値を設定すると、観測される MSS が設定よりも小さくなる可能性があります。詳細については、「TCP MSS について （744 ページ）」を参照してください。

関連トピック

TLS/SSL ハンドシェイク処理 （2301 ページ）
復号 ルールとポリシーの基本 （2307 ページ）

TLS/SSL ハンドシェイク処理

このマニュアルでは、*TLS/SSL* ハンドシェイクという用語は SSL プロトコルとその後継プロトコルである TLS の両方の暗号化セッションを開始する、2 ウェイ ハンドシェイクを表します。

インライン展開では、Firepower システムは TLS/SSL ハンドシェイクを処理し、ClientHello メッセージを修正する可能性があり、セッションの TCP プロキシ サーバーとして機能します。

以下の図はインライン展開を示しています。

（正常に TCP 3 ウェイハンドシェイクが完了した後）クライアントがサーバーとの TCP 接続を確立すると、管理対象デバイスは TCP セッションでの暗号化されたセッションの開始の試行をモニターします。TLS/SSL ハンドシェイクは、クライアントとサーバー間の特殊なパケットの交換を利用して、暗号化セッションを確立します。SSL と TLS プロトコルでは、これらの特殊なパケットはハンドシェイク メッセージと呼ばれます。ハンドシェイク メッセージは、クライアントとサーバの両方がサポートする暗号化属性を伝えます。

- ClientHello：クライアントは各暗号化属性に複数のサポートされる値を指定します。
- ServerHello：サーバーは各暗号化属性に 1 つのサポートされる値を指定し、ServerHello 応答がシステムがセキュリティで保護されたセッション中に使用する暗号化方式を決定します。

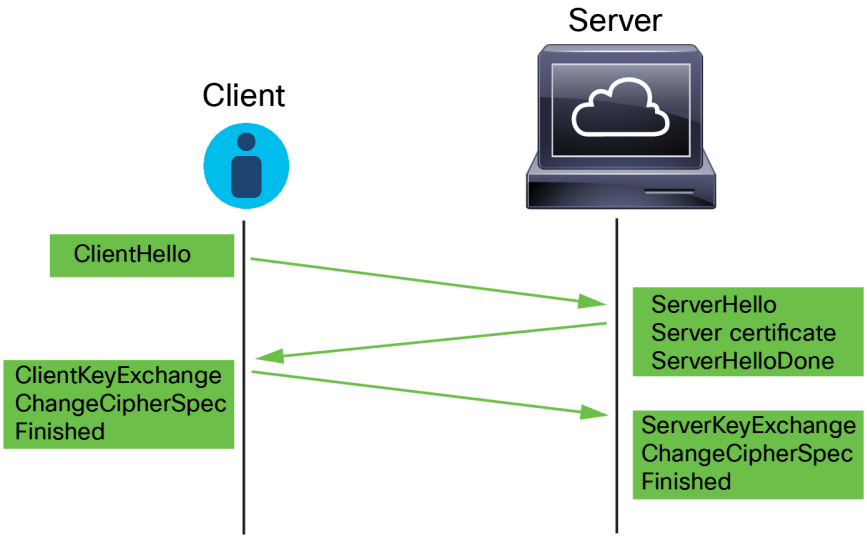
TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッション データをキャッシュに保存し、それによりフル ハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバー証明書データをキャッシュに保存し、それにより同じ証明書を使用する後続のセッションでのより速いハンドシェイクの処理が可能になります。

ClientHello メッセージ処理

セキュアな接続が確立できる場合、クライアントはパケットの宛先として機能するサーバに ClientHello メッセージを送信します。クライアントは TLS/SSL ハンドシェイクを開始するメッセージを送信するか、または宛先サーバーからの ServerHello メッセージへの応答に含めます。

概要

次の図は例を示しています。RFC 8446, sec. 4 も参照してください。cloudflare.com で「What Happens in a TLS Handshake?」 などのリソースを参照することもできます。



このプロセスは次のように要約できます。

1. ClientHello がプロセスを開始します。

   ClientHello メッセージには、サーバーの完全修飾ドメイン名を持つ Server Name Indication（SNI）が含まれています。

2. 管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式で認証に証明書が使用される場合、サーバー証明書メッセージのすぐ後に ServerHello メッセージが送信されます。

   サーバー証明書には、完全修飾ドメイン名と IP アドレスを持つサブジェクトの代替名（SAN）が含まれています。SAN の詳細については、識別名 （1332 ページ）を参照してください。

3. 管理対象デバイスはこれらのメッセージを受信すると、システムに設定されている復号ルールとの照合を試みます。これらのメッセージには、ClientHello メッセージまたはセッション データ キャッシュにはなかった情報が含まれます。具体的には、復号ルールの識別名、証明書ステータス、暗号スイート、およびバージョン条件で、これらのメッセージと照合される可能性があります。

プロセス全体が暗号化されます。

データ交換

TLS/SSL復号を設定した場合、管理対象デバイスがClientHelloメッセージを受信すると、システムはそのメッセージを**[復号-再署名（Decrypt - Resign）]**、または**[復号-既知のキー（Decrypt - Known Key）]**アクションを含む 復号ルール と照合しようとします。照合はClientHelloメッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。考えられるデータには次のものがあります。

表 *188*：復号ルール 条件のデータの可用性

復号ルール 条件	データの存在場所
ゾーン	ClientHello
Networks	ClientHello
VLAN タグ	ClientHello
ポート	ClientHello
ユーザ	ClientHello
アプリケーション	ClientHello（サーバ名インジケータの拡張機能）
カテゴリ	ClientHello（サーバ名インジケータの拡張機能）
Certificate	サーバー証明書（キャッシュされている可能性あり）
識別名	サーバー証明書（キャッシュされている可能性あり）
証明書のステータス（Certificate Status）	サーバー証明書（キャッシュされている可能性あり）
暗号スイート	ServerHello
Versions	ServerHello

重要 [暗号スイート（Cipher Suite）]と[バージョン（Version）]のルール条件は、[ブロック（Block）]または[リセットしてブロック（Block with reset）]のルールアクションが使用されているルールでのみ使用します。[暗号スイート（Cipher Suite）]または[バージョン（Version）]を[復号 - 再署名（Decrypt - Resign）]または[復号 - 既知のキー（Decrypt - Known Key）]ルールアクションとともに使用しないでください。ルールのこれらの条件を他のルールアクションとともに使用すると、システムのClientHello処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

ClientHello の変更

ClientHello メッセージが **[復号-再署名（Decrypt - Resign）]**、または **[復号-既知のキー（Decrypt - Known Key）]** ルールに一致したら、システムは ClientHello メッセージを次のように変更します。

- （TLS 1.2 のみ。TLS 1.3 は圧縮をサポートしていません。）圧縮方法：クライアントがサポートする圧縮方法を指定する、`compression_methods` 要素を削除します。システムは圧縮されたセッションを復号できません。
- 暗号スイート：システムがサポートしない場合、`cipher_suites` 要素から暗号スイートを削除します。システムが指定した暗号スイートのいずれもサポートしない場合、システムは、元の変更されていない要素を送信します。この変更により、復号できないトラフィックの、サポートされない暗号スイートと不明な暗号スイートが削減されます。
- セッション識別子：キャッシュされたセッションデータと一致しないセッションチケット拡張（(RFC 5077、セクション 3.2）と `Session Identifier` 要素から値を削除します。ClientHello 値がキャッシュされたデータと一致した場合、一時停止したセッションは、クライアントとサーバーが完全な TLS/SSL ハンドシェイクを実行せずに、中断したセッションを再開できます。この変更は、セッション再開の可能性を高め、復号できないトラフィックの、セッションが未キャッシュのタイプを削減します。
- 楕円曲線：システムがサポートしない場合、サポートされる楕円曲線拡張機能から楕円曲線を削除します。システムが指定した楕円曲線のいずれもサポートしない場合、管理対象デバイスは拡張機能を削除し、`cipher_suites` 要素から関連する暗号スイートを削除します。
- ALPN 拡張機能：システムでサポートされていないアプリケーション層プロトコルネゴシエーション（ALPN）拡張機能から値を削除します（たとえば、HTTP/2 プロトコル）。
- 他の拡張機能：Next Protocol Negotiation（NPN）および TLS チャネル ID 拡張機能を削除します。

  [復号 - 再署名（Decrypt - Resign）]、または **[復号 - 既知のキー（Decrypt - Known Key）]** アクションにより 復号ルール は、ClientHello ネゴシエーション時に Extended Master Secret（EMS）拡張機能をネイティブにサポートするので、よりセキュアな通信が可能になりました。EMS 拡張機能は、 RFC 7627 によって定義されています。

システムが ClientHello メッセージを変更した後、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）を合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

ClientHello メッセージが [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] ルールに一致しない場合、システムはメッセージを変更しません。次に、メッセージがアクセス コントロール評価（ディープ インスペクションを含めることができる）で合格するかどうかを決定します。メッセージが検査に合格すれば、システムはそれを宛先サーバーに送信します。

トラフィックが [モニター（Monitor）] ルール条件に一致する場合、ClientHello は変更されません。

Man-In-The-Middle; 中間者

メッセージを変更した後はクライアントおよびサーバで計算されたメッセージ認証コード（MAC）が一致しなくなるため、TLS/SSL ハンドシェイク時のクライアントとサーバの間の直接通信はできなくなります。すべての後続のハンドシェイクメッセージ（および一度設定された暗号化セッション）に対し、管理対象デバイスは、中間者として機能します。ここでは 2 つの TLS/SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバーの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。

（注） システムが復号できる暗号スイートは頻繁に更新されるので、復号ルールの条件で使用可能な暗号スイートと直接対応しません。復号できる暗号スイートの現在のリストについては、Cisco TAC に連絡してください。

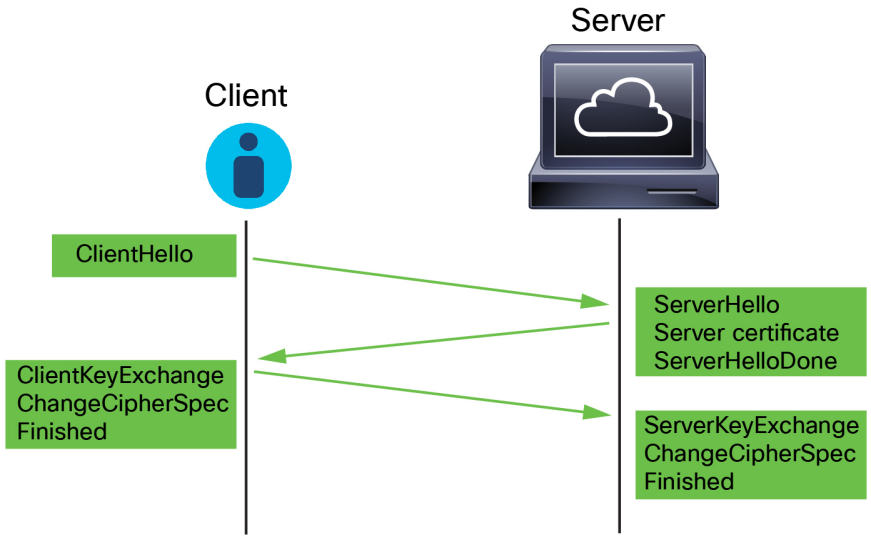
関連トピック

復号できないトラフィックのデフォルト処理オプション （2342 ページ）
ServerHello とサーバー証明書メッセージの処理 （2305 ページ）

ServerHello とサーバー証明書メッセージの処理

概要

次の図は例を示しています。RFC 8446, sec. 4 も参照してください。cloudflare.com で「What Happens in a TLS Handshake?」 などのリソースを参照することもできます。



このプロセスは次のように要約できます。

1. ClientHello がプロセスを開始します。

ClientHello メッセージには、サーバーの完全修飾ドメイン名を持つ Server Name Indication（SNI）が含まれています。

2. 管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式で認証に証明書が使用される場合、サーバー証明書メッセージのすぐ後に ServerHello メッセージが送信されます。

   サーバー証明書には、完全修飾ドメイン名と IP アドレスを持つサブジェクトの代替名（SAN）が含まれています。SAN の詳細については、識別名 （1332 ページ）を参照してください。

3. 管理対象デバイスはこれらのメッセージを受信すると、システムに設定されている復号ルールとの照合を試みます。これらのメッセージには、ClientHello メッセージまたはセッション データ キャッシュにはなかった情報が含まれます。具体的には、復号ルールの識別名、証明書ステータス、暗号スイート、およびバージョン条件で、これらのメッセージと照合される可能性があります。

プロセス全体が暗号化されます。

復号ルール アクション

メッセージが 復号ルール と一致しない場合、管理対象デバイスは、復号ポリシー のデフォルトアクション （2341 ページ）を実行します。

メッセージが、アクセス コントロール ポリシーに関連付けられた 復号ポリシー に属するルールに一致する場合、管理対象デバイスは必要に応じて続行します。

アクション：モニター（Monitor）
TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはトラフィックを追跡してログに記録しますが、暗号化トラフィックを復号しません。

アクション：ブロック（Block）、またはリセットしてブロック（Block with Reset）
管理対象デバイスは TLS/SSL セッションをブロックし、設定されている場合は TCP 接続をリセットします。

アクション：復号しない（Do Not Decrypt）
TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスは、TLS/SSL セッションの間で交換されるアプリケーション データを復号しません。

アクション：復号 - 既知のキー（Decrypt - Known Key）
管理対象デバイスは、以前に Secure Firewall Management Center にインポートした内部証明書オブジェクトをサーバー証明書データに一致させようとします。内部証明書オブジェクトは作成できないため、また、秘密キーを所有する必要があるため、既知のキー復号を使用しているサーバーを所有していることを想定しています。

証明書が既知の証明書と一致した場合、TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、TLS/SSL セッション中に交換されたアプリケーション データを復号および再暗号化します。

クライアントとの初回接続と後続の接続の間でサーバーが証明書を変更した場合、将来の接続を復号するには、Secure Firewall Management Center に新しいサーバー証明書をインポートする必要があります。

アクション：復号 - 再署名（Decrypt - Resign）

管理対象デバイスはサーバー証明書メッセージを処理し、サーバー証明書に以前にインポートまたは生成した認証局（CA）で再署名します。TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、TLS/SSL セッション中に交換されたアプリケーションデータを復号および再暗号化します。

（注） Firepower システムは相互認証をサポートしていません。つまり、クライアント証明書を Secure Firewall Management Center にアップロードして、[復号-再署名（Decrypt - Resign）] アクションまたは [復号-既知のキー（Decrypt - Known Key）] 復号ルール アクションに使用することはできません。詳細については、復号と再署名（発信トラフィック）（2310ページ）および既知のキーでの復号（着信トラフィック）（2311 ページ）を参照してください。

関連トピック

ClientHello メッセージ処理 （2301 ページ）

復号 ルールとポリシーの基本

ここでは、復号ポリシー とルールの作成時に注意する必要がある情報について説明します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

SSL プロトコルと TLS プロトコルの詳細については、「SSL vs. TLS - What's the Difference?」[英語] などのリソースを参照してください。

関連トピック

復号のケース （2308 ページ）
トラフィックを復号する場合としない場合 （2308 ページ）
その他の 復号ルール アクション （2311 ページ）
復号ルール のコンポーネント （2311 ページ）
復号ルールの評価の順序 （2313 ページ）

TLS 1.3 復号のベストプラクティス （2347 ページ）

復号のケース

システムを通過するときに暗号化されたトラフィックは許可またはブロックできるだけで、ディープインスペクションやすべての範囲のポリシー適用（侵入防御など）は対象にできません。

すべての暗号化された接続：

- 復号またはブロックする必要があるか判断するために、復号ポリシーを介して送信されます。

  また、 復号ルールを設定し、非セキュアな SSL プロトコルを使用するトラフィックや、期限切れまたは無効な証明書を使用するトラフィックなど、ネットワークに必要ないとわかっているタイプの暗号化トラフィックをブロックできます。

- ブロックされていないトラフィックは、復号の有無に関係なく、アクセス コントロール ポリシーを経由して、最終的に許可またはブロックの判断が行われます。

以下のような、システムの Threat Defense およびポリシーの適用機能を利用できるのは、復号されたトラフィックのみです。

- [高度なマルウェア防御（Advanced Malware Protection）]
- セキュリティ インテリジェンス
- Threat Intelligence Director
- アプリケーション ディテクタ
- URL およびカテゴリのフィルタリング

トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

次に要約を示します。

- 暗号化されたトラフィックはポリシーで許可またはブロックすることができます。暗号化されたトラフィックは検査できません
- 復号されたトラフィックは脅威に対する防御とポリシーの適用に従います。復号されたトラフィックはポリシーで許可またはブロックできます。

関連トピック

ファイルポリシーと侵入ポリシーを使用したディープインスペクション （1723 ページ）

トラフィックを復号する場合としない場合

ここでは、トラフィックを復号する場合と暗号化されたファイアウォールの通過を許可する場合のガイドラインを示します。

トラフィックを復号しない場合

次によって禁止されている場合は、トラフィックを復号してはいけません。

- 法律：たとえば、一部の法域では、財務情報の復号が禁止されています
- 会社のポリシー：たとえば、会社によって特権的な通信の復号が禁止されている場合があります
- プライバシー規制
- 証明書のピン留め（*TLS/SSL* ピニングとも呼ばれる）を使用するトラフィックは、接続の切断を防ぐため、暗号化されたままにする必要があります

（Snort 3）復号ポリシー は、トラフィックがプレフィルタされている場合を除き、[信頼（Trust）]、[ブロック（Block）]、または [リセットしてブロック（Block With Reset）] のアクションを持つアクセスコントロールルールに一致する接続に関してバイパスされません。暗号化トラフィックは最初に 復号ポリシー によって評価され、次にアクセス コントロール ポリシーに進みます。ここで最終的な許可またはブロックの決定が行われます。

暗号化されたトラフィックは、次のものを含むがこれらに限定されない任意の 復号ルール 条件で許可またはブロックできます。

- 証明書のステータス（期限切れまたは無効な証明書など）
- プロトコル（セキュアでない SSL プロトコルなど）
- ネットワーク（セキュリティ ゾーン、IP アドレス、VLAN タグなど）
- 正確な URL または URL カテゴリ
- ポート
- ユーザー グループ

復号ルールは、このトラフィックに対して [復号しない（Do not Decrypt）] アクションを提供します。詳細については、復号ルール [復号しない（Do Not Decrypt）] アクション （2386 ページ）を参照してください。

（注） このトピックの最後にある関連情報リンクでは、ルール評価のいくつかの側面について説明します。URL やアプリケーション フィルタリングなどの条件には、暗号化されたトラフィックに関する制限があります。これらの制限事項を必ず確認してください。

[復号しない（Do Not Decrypt）] ルールでの URL フィルタリング使用の詳細については、復号ルール [復号しない（Do Not Decrypt）] アクション （2386 ページ）を参照してください。

トラフィックを復号する場合

システムの脅威に対する防御とポリシーの適用機能を利用できるのは、暗号化されたすべてのトラフィックです。管理対象デバイスでトラフィックの復号を許可する場合（メモリと処理能

力に基づいて）、法律または規制によって禁止されていないトラフィックを復号する必要があります。復号するトラフィックを決定する必要がある場合は、ネットワーク上のトラフィックを許可するリスクに基づいて決定します。システムは、URLの評価、暗号スイート、プロトコル、その他多くの要因を含む、ルール条件を使用してトラフィックを分類するための柔軟なフレームワークを提供します。

関連トピック

復号と再署名（発信トラフィック） （2310 ページ）
既知のキーでの復号（着信トラフィック） （2311 ページ）
復号ルール の注意事項と制限事項 （2350 ページ）
SSL ルールの順序
URL 条件（URL フィルタリング）
アプリケーション ルールの順序 （1741 ページ）
TLS 1.3 復号のベストプラクティス （2347 ページ）

復号と再署名（発信トラフィック）

この情報は、レガシー復号のポリシーとルールにのみ適用されます。

[復号と再署名（Decrypt - Resign）] 復号ルールアクションでは、システムは中間者となり、傍受、復号、および検査（トラフィックの通過が許可されている場合）し、再暗号化することができます。[復号と再署名（Decrypt - Resign）] ルール アクションは発信トラフィックで使用されます。つまり、宛先サーバーは保護ネットワーク外にあります。

Firewall Threat Defense デバイスは、ルールで指定された内部認証局（CA）オブジェクトを使用してクライアントとネゴシエートし、クライアントと Firewall Threat Defense デバイス間に TLS/SSL トンネルを構築します。同時に、デバイスは宛先 Web サイトに接続し、サーバーと Firewall Threat Defense デバイス間に SSL トンネルを作成します。

このため、クライアントには、宛先サーバーからの証明書ではなく、復号ルールで設定された CA 証明書が表示されます。クライアントは、接続を完了するためにファイアウォールの証明書を信頼する必要があります。Firewall Threat Defense デバイスは、クライアントと宛先サーバー間のトラフィックで両方向に復号/再暗号化を実行します。

前提条件

[復号と再署名（Decrypt - Resign）] ルール アクションを使用するには、CA ファイルとペアの秘密キー ファイルを使用して、内部 CA オブジェクトを作成する必要があります。CA と秘密キーをまだ使用していない場合は、システムで生成できます。

（注） Firepower システムは相互認証をサポートしていません。つまり、クライアント証明書を Secure Firewall Management Center にアップロードして、[復号-再署名（Decrypt - Resign）] アクションまたは [復号-既知のキー（Decrypt - Known Key）] 復号ルール アクションに使用することはできません。詳細については、復号と再署名（発信トラフィック） （2310ページ）および既知のキーでの復号（着信トラフィック） （2311 ページ）を参照してください。

関連トピック

復号ルールの復号アクション （2388 ページ）
外部証明書オブジェクト （1361 ページ）

既知のキーでの復号（着信トラフィック）

この情報は、レガシー復号のポリシーとルールにのみ適用されます。

[復号 - 既知のキー（Decrypt - Known Key）] 復号ルール アクションは、サーバーの秘密鍵を使用してトラフィックを復号します。[復号と既知のキー（Decrypt - Known Key）] ルール アクションは着信トラフィックで使用されます。つまり、宛先サーバは保護ネットワーク内にあります。

既知のキーを使用して復号する主な目的は、社内サーバーを外部の攻撃から保護することです。

前提条件

[復号 - 既知のキー（Decrypt - Known Key）] ルール アクションを使用するには、サーバーの証明書ファイルとペアの秘密キーファイルを使用して、内部証明書オブジェクトを作成する必要があります。

（注） Firepower システムは相互認証をサポートしていません。つまり、クライアント証明書を Secure Firewall Management Center にアップロードして、[復号-再署名（Decrypt - Resign）] アクションまたは [復号-既知のキー（Decrypt - Known Key）] 復号ルール アクションに使用することはできません。詳細については、復号と再署名（発信トラフィック） （2310ページ）および既知のキーでの復号（着信トラフィック） （2311 ページ）を参照してください。

関連トピック

既知のキーでの復号（着信トラフィック） （2311 ページ）
復号ルールの復号アクション （2388 ページ）
内部証明書オブジェクト （1362 ページ）

その他の 復号ルール アクション

この情報は、レガシー復号のポリシーとルールにのみ適用されます。

以下では、その他の 復号ルール アクションについて説明します。

関連トピック

復号ルールのブロックアクション （2388 ページ）
復号ルール モニターアクション （2386 ページ）

復号ルール のコンポーネント

この情報は、レガシー復号のポリシーとルールにのみ適用されます。

復号ルールにはそれぞれ次のコンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

復号ポリシーのルールには1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールが処理する特定のトラフィックを指定します。こうした条件では、セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを照合できます。使用する条件は、ターゲット デバイスのライセンスによって異なります。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。暗号化された一致したトラフィックは、モニタ、許可、ブロック、または復号できます。復号および許可された暗号化トラフィックは、さらなる検査の影響下に置かれます。システムは、ブロックされた暗号化トラフィックに対してはインスペクションを実行しないことに注意してください。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1 つのルールに一致するトラフィックのレコードを 1 つ保持できます。復号ポリシーでの設定に従って、システムが暗号化セッションをブロックするか、復号なしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。接続のログは、Secure Firewall Management Center のデータベースの他に、システム ログ（Syslog）または SNMP トラップ サーバーに記録できます。

ロギングの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Best Practices for Connection Logging」を参照してください。

ヒント　復号ルールを適切に作成し順序付けするのは複雑なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。想定どおりにトラフィックを処理できるように、復号ポリシーインターフェイスには、ルールに関する強力な警告およびエラーのフィードバックシステムが用意されています。

カテゴリ

復号ルール カテゴリ（アプリケーション、カテゴリ、証明書ステータスなど）の使用方法については、復号ルール 条件 （2365 ページ）を参照してください。

復号ルールの評価の順序

この情報は、レガシー復号のポリシーとルールにのみ適用されます。

復号ポリシーで復号ルールを作成する場合、ルールエディタの [挿入（Insert）] リストを使用してその位置を指定します。復号ポリシー内の復号ルールには、1 から始まる番号が付けられています。復号ルールは、ルール番号の昇順で上から順にトラフィックと照合されます。

ほとんどの場合、ネットワークトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の復号ルールに従って実行されます。モニタールール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。こうした条件には、単純なものと複雑なものがあります。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求されたURL、ユーザー、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号トラフィックに対してモニター、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号できないトラフィックはアクセス コントロールの対象です。ただし、アクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなります。

特定の条件（ネットワークや IP アドレスなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、ルールの後ろのほうに順序付けする必要があります。OSIモデルの詳細については、こちらのWikipediaの記事を参照してください。

ヒント 適切な復号ルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

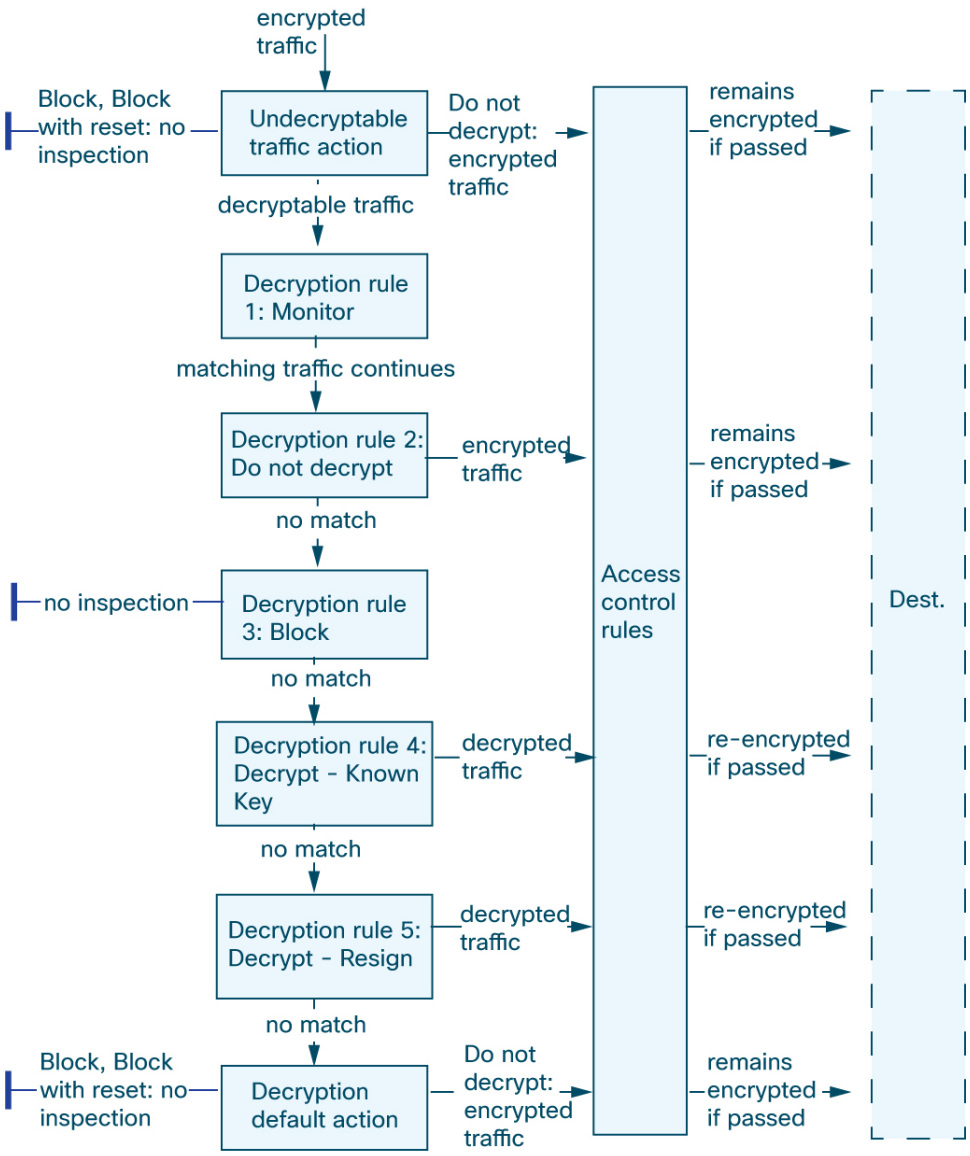
番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、3つのカテゴリ（管理者、標準、ルート）があります。カスタムカテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

関連トピック

アクセス制御ルールのベストプラクティス （1736 ページ）
復号できないトラフィックのデフォルト処理オプション （2342 ページ）
SSL ルールの順序

複数ルールの例

次のシナリオは、インライン展開での 復号ルール によるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号できないトラフィックについてシステムは、それ以上のインスペクションなしでブロックするか、あるいはアクセスコントロールによるインスペクション用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **復号ルール1：モニター（Monitor）**は、暗号化トラフィックを次に評価します。モニタールールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。

- **復号ルール 2**：**復号しない（Do Not Decrypt）**は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセスコントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。
- **復号ルール 3**：**ブロック（Block）**は、暗号化トラフィックを 4 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **復号ルール 4**：**復号 - 既知のキー（Decrypt - Known Key）**は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザーのアップロードする秘密キーを使用して復号されます。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。復号ルールに一致しないトラフィックは、引き続き次のルールと照合されます。
- **復号ルール 5**：**復号 - 再署名（Decrypt - Resign）**は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバー証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **復号ポリシーデフォルトアクション**は、いずれの 復号ルール にも一致しないすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

TLS 暗号化アクセラレーション

TLS 暗号化アクセラレーション 次のことを促進します。

- TLS/SSL 暗号化および復号
- VPN（TLS/SSL および IPsec を含む）

サポート対象ハードウェア

以下のハードウェア モデルは TLS 暗号化アクセラレーションをサポートしています。

- Cisco Secure Firewall 3100
- Firepower 2100

- Firepower 4100/9300

  Firepower 4100/9300 Firewall Threat Defense コンテナ インスタンスでの TLS 暗号化アクセラレーションのサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

仮想アプライアンス上および上記以外のハードウェアでの TLS 暗号化アクセラレーション はサポートされていません。

（注） TLS 暗号化アクセラレーションおよび 4100/9300 の詳細については、『*FXOS Configuration Guide*』を参照してください。

サポートしていない機能 TLS 暗号化アクセラレーション

TLS 暗号化アクセラレーション でサポートしていない機能は次のとおりです。

- Firewall Threat Defense コンテナ インスタンス が有効になっている管理対象デバイス。
- インスペクション エンジンが接続を維持するように設定されていて、インスペクション エンジンが予期せず失敗した場合は、エンジンが再起動されるまでTLS/SSL トラフィックはドロップされます。

  この動作はによって制御されます、**configure snort preserve-connection {enable | disable}**コマンド。

TLS 暗号化アクセラレーション の注意事項と制限事項

管理対象デバイスで TLS 暗号化アクセラレーションが有効になっている場合は、次の点に留意してください。

HTTP のみのパフォーマンス

トラフィックを復号しない管理対象デバイスでTLS暗号化アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。

Federal Information Processing Standards（FIPS）

TLS暗号化アクセラレーションと連邦情報処理標準（FIPS）が両方とも有効になっている場合は、次のオプションの接続が失敗します。

- サイズが 2048 バイト未満の RSA キー
- Rivest 暗号 4（RC4）
- 単一データ暗号化標準規格（単一 DES）
- Merkle–Damgard 5（MD5）
- SSL v3

セキュリティ認定準拠モードで動作するようにFirewall Management Centerと管理対象デバイスを設定すると、FIPS が有効になります。このモードで動作しているときに接続を許可するには、よりセキュアなオプションを採用するように Web ブラウザを設定します。

詳細については、次を参照してください。

- FIPS でサポートされている暗号方式：SSL 設定について （863 ページ）。
- セキュリティ認定準拠のモード。
- コモン クライテリア。

TLS ハートビート

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスは、TLS ハートビート エクステンションを使用するパケットを処理する場合、復号ポリシーの [復号不可のアクション（Undecryptable Actions）] の [復号エラー（Decryption Errors）] の設定で指定されているアクションを実行します。

- Block
- Block with reset

詳細については、復号できないトラフィックのデフォルト処理オプション （2342 ページ）を参照してください。

アプリケーションが TLS ハートビートを使用しているかどうかを判断するには、TLS ハートビートのトラブルシューティング （2394 ページ）を参照してください。

ネットワーク分析ポリシー（NAP）で [最大ハートビート長（Max Heartbeat Length）] を設定して TLS ハートビートの処理方法を決定できます。詳細については、SSL プリプロセッサ （2845 ページ）を参照してください。

TLS/SSL オーバーサブスクリプション

TLS/SSL オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS 暗号化アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、復号ポリシーの [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイク エラー（Handshake Errors）] の設定に従います。

- デフォルト アクションを継承（Inherit default action）

- Do not decrypt
- Block
- Block with reset

復号ポリシー の [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定が [復号しない（Do Not decrypt）] で、関連付けられたアクセスコントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

大量のオーバーサブスクリプションが発生している場合は、次のオプションがあります。

- 管理対象デバイスをアップグレードして、TLS/SSL の処理能力を向上させます。
- 復号ポリシー を変更して、復号の優先順位が高くないトラフィック用に [Do Not Decrypt] ルールを追加します。

TLS 暗号アクセラレーションのステータスの表示

このトピックでは、TLS暗号化アクセラレーションが有効になっているかどうかを確認する方法について説明します。

Firewall Management Center で次の作業を実行します。

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** をクリックします。

ステップ 3 [編集（Edit）]（✎） をクリックして、管理対象デバイスを編集します。

ステップ 4 [デバイス（Device）]ページをクリックします。TLS暗号化アクセラレーション ステータスが [全般（General）] セクションに表示されます。

復号ポリシー とルールの設定方法

このトピックでは、ネットワーク上のTLS/SSLトラフィックをブロック、モニター、または許可するために、これらのポリシーで 復号ポリシー および復号ルール を設定するために必要なタスクの概要を説明します。

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者である必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	[復号-既知のキー復号ルール（Decrypt - Known Key）]（内部サーバーへの着信トラフィックを復号するための） の場合、内部証明書オブジェクトを作成します。	内部証明書オブジェクトは、サーバーの証明書と秘密キーを使用します。内部証明書オブジェクト （1362 ページ）を参照してください。
ステップ 2	[復号-再署名復号ルール（Decrypt - Resign）]（ネットワーク外部のサーバーに発信トラフィックを復号するための） の場合、内部認証局（CA）オブジェクトを作成します。	内部 CA オブジェクトは、CA と秘密キーを使用します。内部認証局オブジェクト （1354 ページ）を参照してください。
ステップ 3	復号ポリシーを作成し、オプションでルールを作成します。	同時に複数のルールを備えた復号ポリシーを作成できます。ルールなしで復号ポリシーを作成することもできます。たとえば、後でルールを追加したり、[復号しない（Do not Decrypt）] ルールアクションを使用するポリシーを作成したりします。詳細については、を参照してください。
ステップ 4	復号ポリシーのデフォルトアクションを設定します。	デフォルトアクションは、トラフィックが復号ポリシーによって定義されたルールに一致しない場合に実行されます。復号ポリシー のデフォルトアクション （2341 ページ）を参照してください。
ステップ 5	復号できないトラフィックの処理方法を指定します。	トラフィックは、セキュアでないプロトコル、不明な暗号スイートの使用、またはハンドシェイクや復号でエラーが発生した場合など、さまざまな理由で復号できなくなる可能性があります。復号できないトラフィックのデフォルト処理オプション （2342 ページ）を参照してください。
ステップ 6	復号ポリシーの詳細設定を構成します。	詳細設定には、HTTP/3 アドバタイズメントの無効化、TLS 1.3 復号の有効化、TLS サーバーアイデンティティ プローブの有効化が含まれます。詳細については、復号ポリシーの詳細オプション （2345 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 7	復号ポリシーをアクセス コントロール ポリシーに関連付けます。	復号ポリシーをアクセス コントロール ポリシーに関連付けていない限り、SSL ポリシーの影響はありません。関連付けた後、アクセス コントロール ルールに一致するトラフィックを許可またはブロックし、その他のアクションを実行することができます。アクセス制御への他のポリシーの関連付け（1765ページ）を参照してください。
ステップ 8	復号されたトラフィックを許可またはブロックするようにアクセス コントロール ルールを設定します。	アクセス コントロール ポリシーのコンポーネント（1745 ページ）を参照してください。
ステップ 9	アクセス制御ポリシーで TLS サーバー アイデンティティ検出を有効にするかどうかを選択します。	詳細については、「アクセス コントロール ポリシーの詳細設定（1759ページ）」を参照してください。
ステップ 10	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。「設定変更の展開（172ページ）」を参照してください。

復号ポリシー の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
復号ポリシー。	7.3.0	7.3.0	機能をより適切に反映するために、機能の名前が復号ポリシーに変更されました。1 つ以上の [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] ルールを同時に使用して復号ポリシーを構成できるようになりました。 新規/変更された画面： • 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御のヘディング（Access Control heading）]** > **[復号（Decryption）]**（復号ポリシーの新規作成） • [復号ポリシーの作成（Create Decryption Policy）] ダイアログボックスには、[アウトバウンド接続（Outbound Connections）] と [インバウンド接続（Inbound Connections）] の 2 つのタブページが追加されました。 [アウトバウンド接続（Outbound Connections）] タブページを使用して、1 つ以上の復号ルールを [復号-再署名（Decrypt - Resign）] ルールアクションで構成します。(You can either upload or generate certificate authorities at the same time）. CA とネットワークおよびポートの組み合わせごとに、1 つの復号ルールが作成されます。 [インバウンド接続（Inbound Connections）] タブページを使用して、1 つ以上の復号ルールを [復号-既知のキー（Decrypt - Known Key）]ルールアクションで構成します。（同時にサーバーの証明書をアップロードできます。）サーバー証明書とネットワークおよびポートの組み合わせごとに、1 つの復号ルールが作成されます。 • **[ポリシー（Policies）]** > **[アクセス制御のヘディング（Access Control heading）]** > **[復号（Decryption）]**（複合ルールの編集）**[詳細設定（Advanced Settings）]** には、TLS 1.3 復号のベストプラクティス（2347 ページ） で説明されている新しいオプションがあります。 • **[ポリシー（Policies）]** > **[アクセス制御のヘディング（Access Control Heading）]** > **[アクセス制御（Access Control）]**（アクセス制御ポリシーの編集）、**[復号（Decryption）]** という単語をクリックして、復号ポリシーをアクセス制御ポリシーに関連付けます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
TLS 1.3 復号。	7.2.0	7.2.0	SSL ポリシーの詳細なアクションで TLS 1.3 復号を有効にできるようになりました。TLS 1.3 復号では、管理対象デバイスで Snort 3 を実行する必要があります。 他のオプションも利用できます。詳細については、TLS 1.3 復号のベストプラクティス （2347 ページ）を参照してください。 新規/変更画面：**[SSLポリシー（SSL Policy）]** > **[詳細設定（Advanced Settings）]**
SSL ポリシーの詳細設定。	7.2.0	7.1.0	SSL ポリシーの詳細設定 新規/変更画面：**[SSLポリシー（SSL Policy）]** > **[詳細設定（Advanced Settings）]**
レピュテーションが不明な URL の処理を指定する機能。	6.7.0	6.7.0	詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについて （1816 ページ）を参照してください。
[復号-既知（Decrypt - Known）] キールールのための ClientHello の変更。	6.7.0	6.7.0	詳細については、ClientHello メッセージ処理 （2301 ページ）を参照してください。
TLS 1.3 トラフィックで証明書を抽出して、アクセス制御ルールの URL およびアプリケーションの条件とのトラフィックの照合を有効にする機能。	6.7.0	6.7.0	新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **（アクセス コントロール ポリシーの編集）** > **[詳細（Advanced）]** リンク。 詳細は、復号ポリシーの詳細オプション （2345 ページ）を参照してください。
カテゴリとレピュテーションに基づく URL フィルタリングの変更。	6.7.0	6.5.0	詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについて （1816 ページ）を参照してください。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
TLS 暗号化アクセラレーションを無効にすることはできません。	6.4.0	6.4.0	TLS暗号化アクセラレーションすべてのサポート対象デバイスで有効にします。 ネイティブインターフェイスを持つ管理対象デバイスでは、TLS暗号化アクセラレーションを無効にできません。 Firewall Threat Defense コンテナ インスタンス の TLS 暗号化アクセラレーションは、この表の次の行で示すように限定されています。 削除されたコマンド： • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**
Firepower 4100/9300 モジュール/セキュリティエンジンのいずれかの Firewall Threat Defense コンテナインスタンスでの TLS暗号化アクセラレーションのサポート。	6.4.0	6.4.0	モジュール/セキュリティ エンジンのいずれかの Firewall Threat Defense コンテナ インスタンスで TLS 暗号化アクセラレーションを有効にできるようになりました。他のコンテナ インスタンスの TLS 暗号化アクセラレーションは無効ですが、ネイティブインスタンスでは有効になっています。 新規/変更されたコマンド： • **config hwCrypto enable** • **show crypto accelerator status** replaces **system support ssl-hw-status**)
TLS/SSL ハードウェアアクセラレーションは *TLS* 暗号化アクセラレーションと呼ばれるようになりました。	6.4.0	6.4.0	名前の変更は、TLS/SSL暗号化と復号アクセラレーションがより多くのデバイスでサポートされていることを反映しています。デバイスによっては、アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [デバイス（Device）] > [全般（General）] > [TLS暗号化アクセラレーション（TLS Crypto Acceleration）]**
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）。	6.3.0.1	6.3.0.1	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。
Extended Master Secret 拡張機能はサポートされていません。	6.3.0	6.3.0	拡張機能は [復号 - 再署名（Decrypt - Resign）] ルールの ClientHello 変更時に削除されます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
TLS/SSL ハードウェア アクセラレーションはデフォルトでは、有効です。	6.3.0	6.3.0	TLS/SSL ハードウェア アクセラレーション デフォルトですべてのサポート対象デバイスで有効になっていますが、必要に応じて無効にすることができます。
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）。	6.2.3.9	6.2.3.9	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。
アグレッシブ TLS 1.3 ダウングレード。	6.2.3.7	6.2.3.7	**system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** CLI コマンドを使用して、TLS 1.2 への TLS 1.3 トラフィックのダウングレードの動作を決定できます。詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。
TLS/SSL ハードウェア アクセラレーションが導入されました。	6.2.3	6.2.3	特定の管理対象デバイス モデルでは、パフォーマンスが向上する、ハードウェアでの TLS/SSL 暗号化および復号が実行されます。デフォルトでは、この機能は有効です。 影響を受ける画面：TLS/SSL ハードウェア アクセラレーションのステータスを表示するには、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）]**、[全般（General）] ページ。
カテゴリとレピュテーションの条件がサポートされています。	6.2.2	6.2.2	カテゴリ/レピュテーションの条件を使用したアクセス コントロール ルールまたは SSL ルール。
セーフサーチをサポート	6.1.0	6.1.0	SSL ポリシーにより復号され、その後アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによりブロック（またはインタラクティブにブロック）された接続については、HTTP 応答ページが表示されます。このような場合、システムは応答ページを暗号化して、再暗号化された SSL ストリームの最後にそれを送信します。 SafeSearch により好ましくないコンテンツがフィルタリングされ、成人向けサイトの検索が停止されます。
TLS/SSL ポリシー	6.0.0	6.0.0	導入された機能。

第 61 章

復号ポリシー

ここでは、復号ポリシーの作成、設定、管理、およびロギングの概要を示します。

- 復号ポリシーについて （2327 ページ）
- 復号ポリシー の要件と前提条件 （2328 ページ）
- 復号ポリシーの作成 （2328 ページ）
- 復号ポリシー のデフォルトアクション （2341 ページ）
- 復号できないトラフィックのデフォルト処理オプション （2342 ページ）
- 復号ポリシーの詳細オプション （2345 ページ）

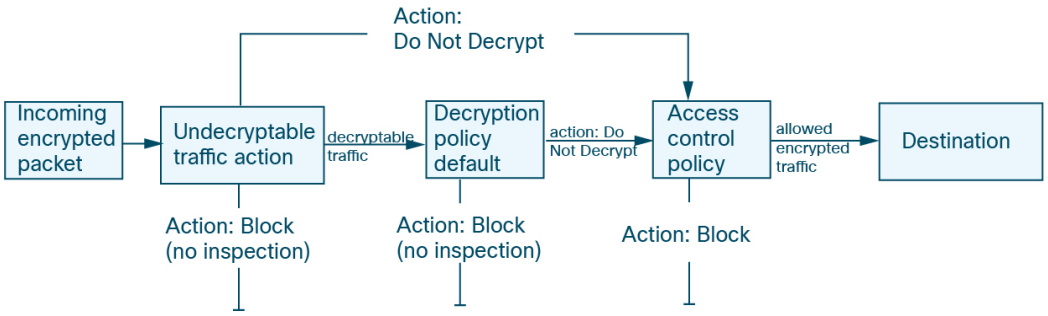
復号ポリシーについて

復号ポリシーにより、ネットワーク上の暗号化トラフィックの処理方法が決まります。1 つ以上の復号ポリシーを設定し、復号ポリシーをアクセス コントロール ポリシーに関連付けてから、そのアクセス コントロール ポリシーを管理対象デバイスに展開できます。デバイスで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックを処理して検査します。次に TCP 接続上で TLS/SSL 暗号化セッションが識別された場合は、復号ポリシーが引き継いで暗号化トラフィックの処理および復号が実行されます。

着信トラフィックを復号するルール（[復号 - 既知のキー（Decrypt - Known Key）] ルールアクション）および発信トラフィック（[復号 - 再署名（Decrypt - Resign）] ルールアクション）など、複数のルールを同時に作成できます。[復号しない（Do Not Decrypt）] または他のルールアクション（[ブロック（Block）] や [モニター（Monitor）] など）を使用してルールを作成する場合は、空の復号ポリシーを作成してからルールを追加します。

[復号しない（Do Not Decrypt）] ポリシーの例

以下は、[復号しない（Do Not Decrypt）] ルールアクションを使用した復号ポリシーの例です。



最も単純な復号ポリシーでは、次の図に示されているように、展開先のデバイスは単一のデフォルトアクションで暗号化トラフィックを処理するように指示されます。デフォルト アクションの設定では、それ以上のインスペクションなしで復号可能トラフィックをブロックするか、復号されていない復号可能トラフィックをアクセスコントロールで検査するように指定できます。システムは、暗号化されたトラフィックを許可するか、またはブロックできます。デバイスは復号できないトラフィックを検出すると、トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないままにして、アクセスコントロールによる検査を行います。

復号ポリシー の要件と前提条件

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

復号ポリシーの作成

次のいずれかのタイプの復号ポリシーを作成できます。

- アウトバウンド保護ポリシーは、アウトバウンド接続を保護するルールを使用します。つまり、宛先サーバーは保護されたネットワークの外部にあります。このタイプのルールには、[復号 - 再署名（Decrypt - Resign）] ルールアクションがあります。

  アウトバウンド接続保護を使用した復号ポリシーの作成（2329ページ）を参照してください

- インバウンド保護ポリシーは、インバウンド接続を保護するルールを使用します。つまり、宛先サーバーは保護されたネットワークの内部にあります。このタイプのルールには、[復号 - 既知のキー（Decrypt - Known Key）] ルールアクションがあります。

  インバウンド接続保護を使用した復号ポリシーの作成（2330ページ）を参照してください

- その他のアクション（[復号しない（Do Not Decrypt）]、[ブロック（Block）]、および[リセットしてブロック（Block with Reset）] を含む）。

  「他のルールアクションを使用した復号ポリシーの作成（2340ページ）」を参照してください。

アウトバウンド接続保護を使用した復号ポリシーの作成

このタスクでは、アウトバウンド接続を保護するルールを使用して復号ポリシーを作成する方法について説明します。つまり、宛先サーバーは保護されたネットワークの外部にあります。このタイプのルールには、[復号 - 再署名（Decrypt - Resign）] ルールアクションがあります。

復号ポリシーを作成するときは、複数の [復号 - 既知のキー（Decrypt - Known Key）] ルールや複数の [復号 - 再署名（Decrypt - Resign）] ルールなど、複数のルールを同時に作成できます。

始める前に

アウトバウンド接続を保護する復号ポリシーを作成する前に、管理対象デバイスの内部 CA 証明書をアップロードする必要があります。これは、次のいずれかの方法で実行できます。

- **オブジェクト** > **オブジェクト管理** > **PKI** > **内部 CA** に移動して PKI（1352 ページ）を参照し、内部 CA 証明書オブジェクトを作成します。
- この復号ポリシーの作成時点で実行。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[復号（Decryption）]** をクリックします。

ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

次の文字は、復号ポリシー名には使用できません。

- 先頭のピリオド
- #、;、{、}、=、$、<、>

ステップ 5 [内部証明書（Internal Certificates）] リストから、ルールの証明書をアップロードまたは選択します。

内部証明書の詳細については、「アウトバウンド保護のための内部CAの生成（2337ページ）」と「アウトバウンド保護のための内部CAのアップロード（2339ページ）」を参照してください。

ステップ 6 （任意）ネットワークとポートを選択します。

詳細については、次を参照してください。

- ネットワークルール条件（816 ページ）
- ポートルールの条件（819 ページ）

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- ルール条件の追加：復号ルール 条件（2365 ページ）
- デフォルトのポリシーアクションの追加： 復号ポリシー のデフォルトアクション（2341 ページ）
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「Logging Connections with a Policy Default Action」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシーの詳細オプション（2345 ページ）
- アクセス制御への他のポリシーの関連付け（1765ページ）の説明に従って、復号ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開（172 ページ）を参照してください。

インバウンド接続保護を使用した復号ポリシーの作成

このタスクでは、インバウンド接続を保護するルールを使用して復号ポリシーを作成する方法について説明します。つまり、宛先サーバーは保護されたネットワーク内にあります。このタイプのルールには、[復号 - 既知のキー（Decrypt - Known Key）] ルールアクションがあります。

復号ポリシーを作成するときは、複数の [復号 - 既知のキー（Decrypt - Known Key）] ルールや複数の [復号 - 再署名（Decrypt - Resign）] ルールなど、複数のルールを同時に作成できます。

始める前に

インバウンド接続を保護する復号ポリシーを作成する前に、内部サーバーの内部証明書をアップロードする必要があります。これは、次のいずれかの方法で実行できます。

- **オブジェクト**>**オブジェクト管理**>**PKI**>**内部証明書**に移動し PKI （1352 ページ） を参照して、内部証明書オブジェクトを作成します。
- この復号ポリシーの作成時点で実行。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]**>**[アクセス制御（Access Control）]** 見出し > **[復号（Decryption）]** をクリックします。

ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

次の文字は、復号ポリシー名には使用できません。

- 先頭のピリオド
- #、;、{、}、=、$、<、>

ステップ 5 [内部CA（Internal CA）] リストから、ルールの証明書をアップロードまたは選択します。

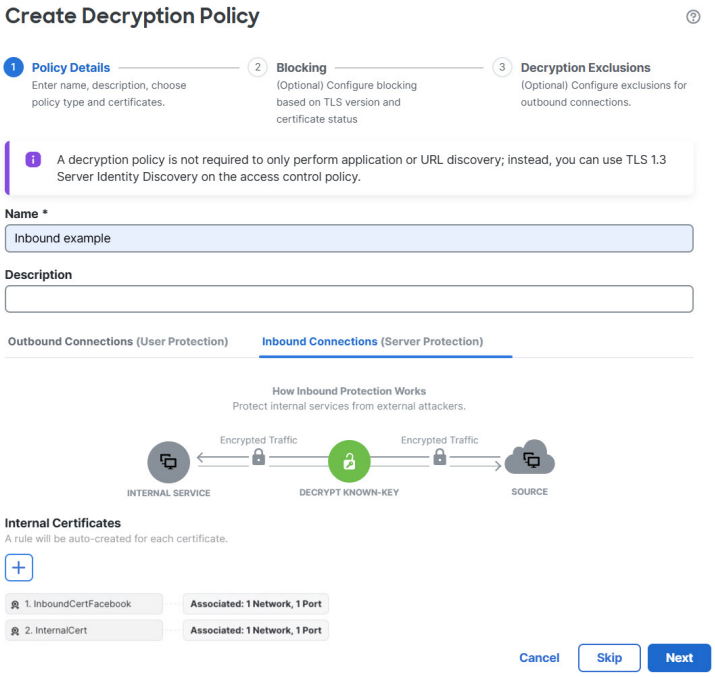
内部 CA 証明書の詳細については、「内部認証局オブジェクト （1354 ページ）」を参照してください。

ステップ 6 （任意）ネットワークとポートを選択します。

詳細については、次を参照してください。

- ネットワークルール条件 （816 ページ）
- ポートルールの条件 （819 ページ）

ステップ 7 [インバウンド接続（Inbound Connections）] タブをクリックします。



ステップ 8 [Next] をクリックします。

ステップ 9 復号ポリシーの除外 （2333 ページ）に進みます。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

- ルール条件の追加：復号ルール 条件 （2365 ページ）
- デフォルトのポリシーアクションの追加： 復号ポリシー のデフォルトアクション （2341 ページ）
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「*Logging Connections with a Policy Default Action*」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシーの詳細オプション （2345 ページ）
- アクセス制御への他のポリシーの関連付け （1765 ページ）の説明に従って、復号ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

復号ポリシーの除外

このタスクでは、特定のタイプのトラフィックを復号から除外する方法について説明します。該当するトラフィックについて、復号ポリシーで[復号しない（Do not decrypt）]ルールを作成します。このルールは、当初アウトバウンド復号ポリシー（つまり、[復号 - 再署名（Decrypt - Resign）]ポリシーアクションを使用するポリシー）に対してのみ有効になっています。

始める前に

アウトバウンド接続を保護する復号ポリシーを作成する前に、管理対象デバイスの内部CA証明書をアップロードする必要があります。これは、次のいずれかの方法で実行できます。

- **オブジェクト**>**オブジェクト管理**>**PKI**>**内部CA**に移動してPKI （1352 ページ） を参照し、内部CA証明書オブジェクトを作成します。
- この復号ポリシーの作成時点で実行。

手順

ステップ1 次で説明されているタスクを完了します。

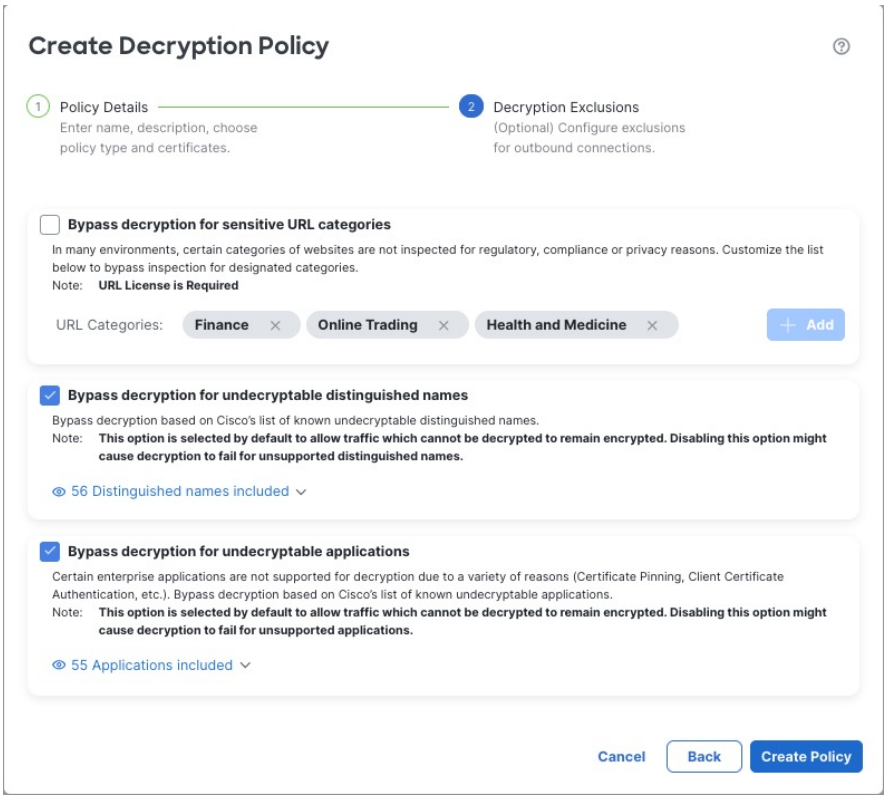
- アウトバウンド接続保護を使用した復号ポリシーの作成 （2329 ページ）
- 詳細については、インバウンド接続保護を使用した復号ポリシーの作成 （2330ページ）を参照してください。

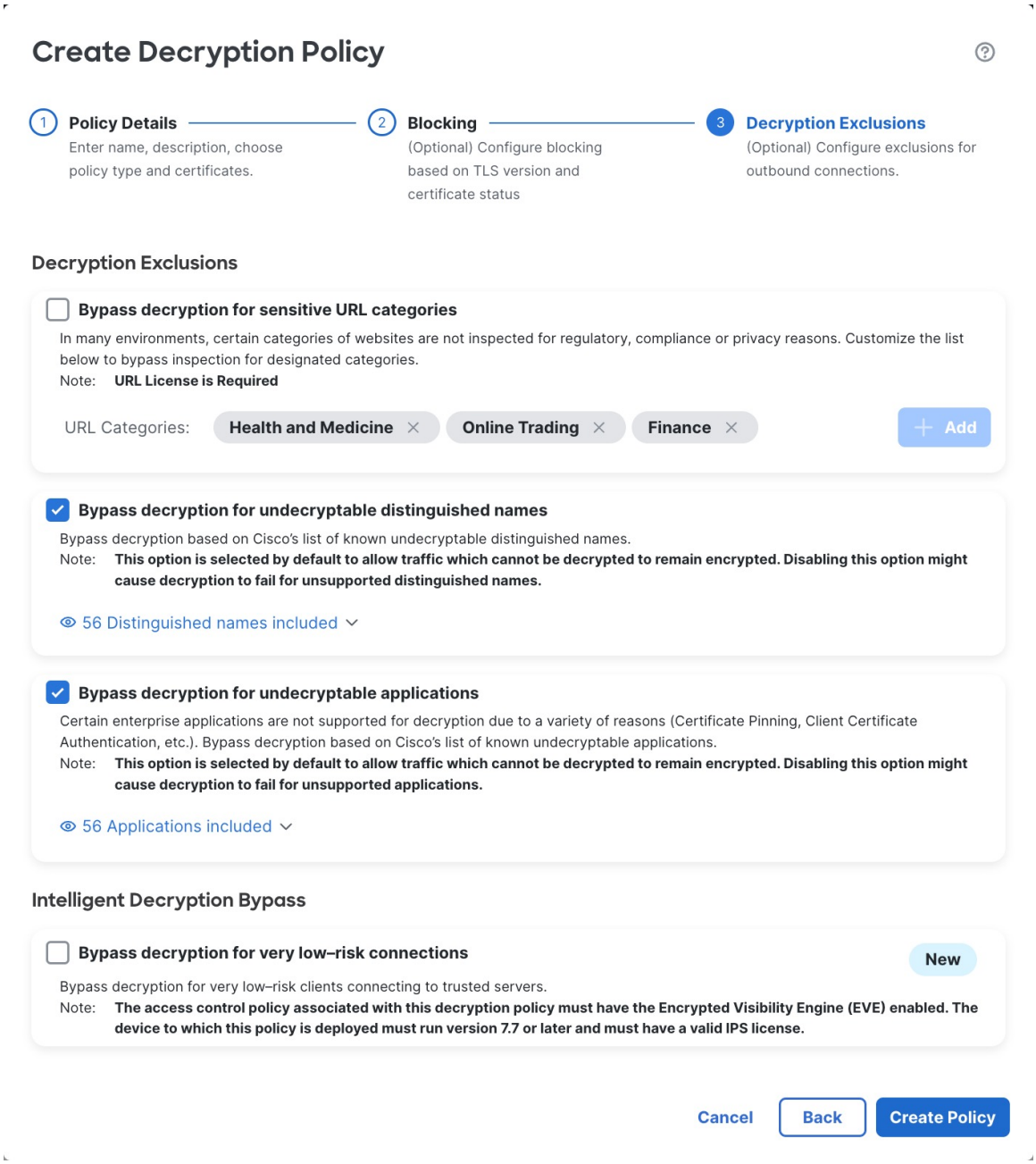
ステップ2 除外ページには次のオプションがあります。すべてのオプションは、アウトバウンド保護ポリシー（[復号 - 再署名（Decrypt - Resign）]ルールアクション）に対して有効になり、他のすべての復号ポリシーアクションに対しては無効になります。

項目	説明
機密URLカテゴリの復号のバイパス（Bypass decryption for sensitive URL categories）	指定されたカテゴリからのトラフィックを復号しない場合は、このチェックボックスをオンにします。お住まいの地域の法律によっては、特定のトラフィック（金融や健康関連など）の復号が禁止されている場合があります。詳細については、お住まいの地域の当局にお問い合わせください。 カテゴリを追加するには、[追加（Add）]をクリックします。 カテゴリを削除するには、[削除（Delete）]（×）をクリックします。

項目	説明
復号不能な識別名の復号のバイパス（Bypass decryption for undecryptable distinguished names）	証明書の再署名によって接続が失敗する可能性があるためトラフィックを復号しない場合は、このボックスをオンにします。通常、この動作は 証明書のピン留めに関連付けられています。この操作については で説明されています。TLS/SSL 証明書のピン留めのガイドライン （2358 ページ） 復号できない識別名のリストは、シスコが管理しています。
復号不能なアプリケーションの復号のバイパス（Bypass decryption for undecryptable applications）	証明書の再署名によって接続が失敗する可能性があるためトラフィックを復号しない場合は、このボックスをオンにします。 通常、この動作は 証明書のピン留めに関連付けられています。この操作については で説明されています。TLS/SSL 証明書のピン留めのガイドライン （2358 ページ） 復号できないアプリケーションは、脆弱性データベース（VDB）で自動的に更新されます。すべてのアプリケーションのリストは、Cisco Secure Firewall アプリケーションディテクタのページで確認できます。シスコが復号できないと判断したアプリケーションは、**undecryptable** タグで識別されています。 復号できないアプリケーションのリストは、シスコによって管理されています。

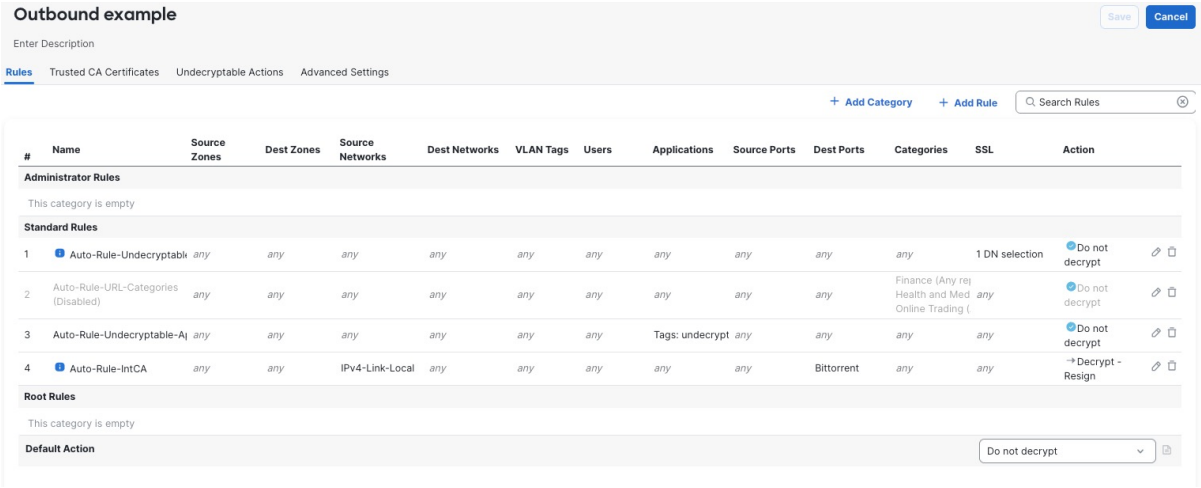
次の図は、デフォルトのオプションを示しています。


Create Decryption Policy
1 Policy Details
Enter name, description, choose policy type and certificates.
2 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.
Bypass decryption for sensitive URL categories
In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.
Note: URL License is Required
URL Categories:
Finance
Online Trading
Health and Medicine
Add
Bypass decryption for undecryptable distinguished names
Bypass decryption based on Cisco's list of known undecryptable distinguished names.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.
56 Distinguished names included
Bypass decryption for undecryptable applications
Certain enterprise applications are not supported for decryption due to a variety of reasons (Certificate Pinning, Client Certificate Authentication, etc.). Bypass decryption based on Cisco's list of known undecryptable applications.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.
55 Applications included
Cancel
Back
Create Policy



ステップ 3 [ポリシーの作成（Create Policy）] をクリックします。

次の図は、アウトバウンド保護ポリシーの例を示しています。



前の例では、ルールの除外の選択に対応する [復号しない（Do Not Decrypt）] ルールが、[復号 - 再署名（Decrypt - Resign）] ルールの前に自動的に追加されます。機密 URL カテゴリのルールは、デフォルトでは除外が無効になっているため、無効になっています。[機密URLカテゴリの復号のバイパス（Bypass decryption for sensitive URL categories）] チェックボックスをオンにした場合、このルールは有効になっています。

ステップ 4 [ポリシーの作成（Create Policy）] をクリックします。

次のタスク

- ルール条件の追加：復号ルール 条件 （2365 ページ）
- デフォルトのポリシーアクションの追加：復号ポリシー のデフォルトアクション （2341 ページ）
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「Logging Connections with a Policy Default Action」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシーの詳細オプション （2345 ページ）
- アクセス制御への他のポリシーの関連付け （1765 ページ）の説明に従って、復号ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アウトバウンド保護のための内部 CA の生成

このタスクでは、アウトバウンド接続を保護する復号ルールを作成するときに、オプションで内部認証局を生成する方法について説明します。CSR への応答として発行された署名付き証明書のアップロード （1357 ページ）の説明に従って、**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]** を使用してこれらのタスクを実行することもできます。

始める前に

内部認証局オブジェクト（1354ページ）に記載されている内部認証局オブジェクトを生成するための要件をよく理解してください。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[復号（Decryption）]** をクリックします。

ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）] フィールドにポリシーの名前を入力し、[説明（Description）] フィールドに任意の説明を入力します。

ステップ 5 [アウトバウンド接続（Outbound Connections）] タブをクリックします。

ステップ 6 [内部CA（Internal CA）] リストから、**[新規作成（Create New）]** > **[CAの生成（Generate CA）]** をクリックします。

ステップ 7 内部 CA に [名前（Name）] を付け、2 文字の [国名（Country Name）]を指定します。

ステップ 8 [自己署名（Self-Signed）]または [CSR] をクリックします。

これらのオプションの詳細については、内部認証局オブジェクト（1354ページ）を参照してください。

ステップ 9 表示されたフィールドに必要な情報を入力します。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 [CSR] を選択した場合は、署名要求が完了したら、次のように [証明書のインストール（Install Certificate）] をクリックします。

a) この手順の前のステップを繰り返します。

b) [内部CA（Internal CA）] リストの CA を次のように編集します。

c) [Install Certificate] をクリックします。

d) 画面に表示される指示に従ってタスクを完了します。

ステップ 12 「インバウンド接続保護を使用した復号ポリシーの作成（2330ページ）」の説明に従って、ポリシーの作成を続行します。

アウトバウンド保護のための内部 CA のアップロード

このタスクでは、アウトバウンド接続を保護する復号ルールを作成するときに、オプションで内部認証局をアップロードする方法について説明します。CSR への応答として発行された署名付き証明書のアップロード（1357 ページ）の説明に従って、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を使用してこれらのタスクを実行することもできます。

始める前に

内部認証局オブジェクト（1354 ページ）に記載されている内部認証局オブジェクトを生成するための要件をよく理解してください。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[復号（Decryption）]** をクリックします。

ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）] フィールドにポリシーの名前を入力し、[説明（Description）] フィールドに任意の説明を入力します。

ステップ 5 [アウトバウンド接続（Outbound Connections）] タブをクリックします。

ステップ 6 [内部CA（Internal CA）] リストから、**[新規作成（Create New）]** > **[CAのアップロード（Upload CA）]**をクリックします。

ステップ 7 内部 CA に名前を付けます。

ステップ 8 表示されたフィールドに、証明書とその秘密鍵を貼り付けるか、参照して見つけます。

ステップ 9 CA にパスワードが設定されている場合は、[暗号化（Encrypted）] チェックボックスをオンにして、隣のフィールドにパスワードを入力します。

ステップ 10 「アウトバウンド接続保護を使用した復号ポリシーの作成（2329 ページ）」の説明に従って、ポリシーの作成を続行します。

アウトバウンド保護のための内部証明書のアップロード

このタスクでは、アウトバウンド接続を保護する復号ルールを作成するときに、内部認証局をアップロードする方法について説明します。CA 証明書および秘密キーのインポート（1355 ページ）で説明されているように、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を使用して内部 CA をアップロードすることもできます。

始める前に

内部認証局オブジェクト（1354 ページ）で説明されているいずれかの形式の内部認証局があることを確認してください。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[復号（Decryption）]** をクリックします。

ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）] フィールドにポリシーの名前を入力し、[説明（Description）] フィールドに任意の説明を入力します。

ステップ 5 [インバウンド接続（Inbound Connections）] タブをクリックします。

ステップ 6 [内部証明書（Internal Certificates）] リストから、[追加（Add）] (＋) をクリックします。

ステップ 7 [アップロード（Upload）] をクリックします。

ステップ 8 内部 CA に名前を付けます。

ステップ 9 表示されたフィールドに、証明書とその秘密鍵を貼り付けるか、参照して見つけます。

ステップ 10 証明書にパスワードが設定されている場合は、[暗号化（Encrypted）]チェックボックスをオンにして、隣のフィールドにパスワードを入力します。

ステップ 11 「インバウンド接続保護を使用した復号ポリシーの作成（2330ページ）」の説明に従って、復号ポリシーの作成を続行します。

他のルールアクションを使用した復号ポリシーの作成

[復号しない（Do Not Decrypt）]、[ブロック（Block）]、[リセットしてブロック（Block With Reset）]、または[モニター（Monitor）]ルールアクションを使用して復号ルールを作成するには、復号ポリシーを作成および編集して、ルールを追加します。

復号ポリシーを作成するときは、複数の [復号 - 既知のキー（Decrypt - Known Key）] ルールや複数の [復号 - 再署名（Decrypt - Resign）] ルールなど、複数のルールを同時に作成できます。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[復号（Decryption）]** をクリックします。

ステップ 3 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

次の文字は、復号ポリシー名には使用できません。

- 先頭のピリオド

- #、;、{、}、=、$、<、>

ステップ 4 ポリシーが作成されるまで待機します。

ステップ 5 復号ポリシー名の横にある [編集（Edit）]（✎）をクリックします。

ステップ 6 [ルールの追加（Add Rule）] をクリックします。

ステップ 7 ルールに [名前（Name）] を付けます。

ステップ 8 詳細については、[アクション（Action）] リストからルールアクションをクリックし、次のいずれかのセクションを参照してください。

- 復号ルール [復号しない（Do Not Decrypt）] アクション （2386 ページ）
- 復号ルールのブロックアクション （2388 ページ）
- 復号ルール モニターアクション （2386 ページ）

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- ルール条件の追加：復号ルール 条件 （2365 ページ）
- デフォルトのポリシーアクションの追加： 復号ポリシー のデフォルトアクション （2341 ページ）
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「Logging Connections with a Policy Default Action」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシーの詳細オプション （2345 ページ）
- アクセス制御への他のポリシーの関連付け （1765ページ）の説明に従って、復号ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

復号ポリシー のデフォルトアクション

復号ポリシーのデフォルトアクションは、ポリシーのモニター以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。復号ルールがまったく含まれない復号ポリシーを展開する場合、ネットワーク上のすべての復号可能トラフィックの処理方法が、デフォルトアクションで決定されます。デフォルトアクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

復号ポリシーのデフォルトアクションを設定する方法：

1. まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
2. **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[復号（Decryption）]** をクリックします。
3. 復号ポリシーの名前の横にある [編集（Edit）]（） をクリックします。
4. [デフォルトアクション（Default Action）] 行で、リストから次のいずれかのアクションをクリックします。

表 *189 :* 復号ポリシー のデフォルトアクション

デフォルト アクション	暗号化トラフィックに対して行う処理
ブロック（Block）	それ以上のインスペクションは行わずに TLS/SSL セッションをブロックします。
Block with reset	それ以上のインスペクションは行わずに TLS/SSL セッションをブロックし、TCP 接続をリセットします。トラフィックに UDP のようなコネクションレス型プロトコルが使用される場合は、このオプションを選択します。この場合、コネクションレス型プロトコルにより、リセットされるまで接続の再確立が試みられます。 また、このアクションでは、ブラウザの接続リセット エラーも表示されるため、接続がブロックされたことがユーザーに通知されます。
復号しない（Do not decrypt）	アクセス コントロールを使用して暗号化トラフィックを検査します。

復号できないトラフィックのデフォルト処理オプション

表 *190 :* 復号化できないトラフィック タイプ

タイプ	説明	デフォルト アクション	使用可能なアクション
圧縮されたセッション（Compressed Session）	TLS/SSL セッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）

タイプ	説明	デフォルト アクション	使用可能なアクション
SSLv2 セッション	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、ClientHello メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 であることに注意してください。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Unknown Cipher Suite	システムが認識できない暗号スイートです。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Unsupported Cipher Suite	検出された暗号スイートに基づく復号化を、システムはサポートしていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
セッションが未キャッシュ（Session not cached）	TLS/SSL セッションでセッションの再利用が有効化されており、クライアントとサーバがセッション識別子を使ってセッションを再確立しているのに、システムでセッション識別子がキャッシュされていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
ハンドシェイク エラー（Handshake Errors）	TLS/SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Decryption Errors	トラフィックの復号化中にエラーが発生しました。	Block	Block Block with Reset

復号ポリシーを最初に作成する場合、デフォルトアクションによって処理される接続のログは、デフォルトでは無効化されています。復号化できないトラフィックの処理ではデフォルトアクションのログ設定も適用されるため、復号化できないトラフィック用のアクションで処理される接続のログは、デフォルトでは無効化されています。

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できないことに注意してください。詳細については、復号ルール の注意事項と制限事項 （2350 ページ）を参照してください。

関連トピック

復号できないトラフィックのデフォルト処理を設定する （2344 ページ）

復号できないトラフィックのデフォルト処理を設定する

システムによる復号や検査ができない特定タイプの暗号化トラフィックを処理するために、復号できないトラフィックのアクションを復号ポリシーレベルで設定できます。復号ルールを含まない復号ポリシーを展開する場合、ネットワーク上のすべての復号できない暗号化トラフィックの処理方法は、復号できないトラフィックのアクションによって決まります。

復号できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロック。
- 接続をブロックした後でリセットする。接続がブロックされるまで接続を試行し続ける UDP などのコネクションレス型プロトコルの場合、このオプションをお勧めします。
- アクセス コントロールを使用して暗号化トラフィックを検査します。
- 復号ポリシーからデフォルトのアクションを継承します。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]** をクリックします。

ステップ 3 復号ポリシーの名前の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 復号ポリシーエディタで、[復号できないアクション（Undecryptable Actions）] をクリックします。

ステップ 5 各フィールドで、復号ポリシーのデフォルトアクションを選択するか、復号できないタイプのトラフィックに対して実行する別のアクションを選択します。詳細については、復号できないトラフィックのデフォルト処理オプション （2342 ページ）と 復号ポリシー のデフォルトアクション （2341 ページ）を参照してください。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 復号できないトラフィックのアクションで処理される接続に関するデフォルトロギングを設定します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Logging Connections with a Policy Default Action*」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

復号ポリシーの詳細オプション

復号ポリシー の [詳細設定（Advanced Settings）] ページには、ポリシーが適用される Snort 3 用に設定されたすべての管理対象デバイスに適用されるグローバル設定があります。

復号ポリシー 詳細設定は、以下を実行する管理対象デバイスではすべて無視されます。

- 7.1 より前のバージョン
- Snort 2

[ESNIを要求するフローをブロックする（Block flows requesting ESNI）]

Encrypted Server Name Indication（ESNI（提案の草案へのリンク））は、クライアントが要求している内容を TLS 1.3 サーバーに伝える方法です。https://tools.ietf.org/html/draft-ietf-tls-esniSNI は暗号化されており、システムではサーバーを判別できないため、SNI 接続は必要に応じてブロックできます。

HTTP/3 アドバタイズメントを無効にする

このオプションを選択すると、TCP 接続の ClientHello から HTTP/3（RFC 9114）が削除されます。HTTP/3 は QUIC トランスポートプロトコルの一部であり、TCP トランスポートプロトコルではありません。クライアントによる HTTP/3 のアドバタイジングをブロックすると、QUIC 接続に埋め込まれている可能性のある攻撃や回避の試行に対する保護が提供されます。

信頼できないサーバー証明書をクライアントに伝播する

これは、[復号-再署名（Decrypt - Resign）] ルールアクションに一致するトラフィックにのみ適用されます。

このオプションを有効にすると、サーバー証明書が信頼されていない場合に、管理対象デバイスの認証局（CA）がサーバーの証明書の代わりに使用されます。信頼されていないサーバー証明書とは、Secure Firewall Management Center で信頼できる CA としてリストされていない証明書です。（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**）。

[TLS 1.3復号の有効化（Enable TLS 1.3 Decryption）]

TLS 1.3 接続に復号ルールを適用するかどうか。このオプションを有効にしない場合、復号ルールは TLS 1.2 以下のトラフィックにのみ適用されます。「TLS 1.3 復号のベストプラクティス（2347 ページ）」を参照してください。

[適応型TLSサーバーアイデンティティプローブの有効化（Enable adaptive TLS server identity probe）]

TLS 1.3 復号が有効な場合、自動的に有効になります。 プローブは、サーバーとの部分的な TLS接続であり、その目的はサーバー証明書を取得してキャッシュすることです。（証明書がすでにキャッシュされている場合、プローブは確立されません。）

復号ポリシーが関連付けられているアクセス コントロール ポリシーで TLS 1.3 サーバーアイデンティティ検出が無効になっている場合、サーバー名指定（SNI）の使用が試行されますが、これは信頼性が高くありません。

適応型 TLS サーバー アイデンティティ プローブは、以前のリリースのようにすべての接続では発生せず、次のいずれかの条件で発生します。

- 証明書の発行者：復号ルールの DN ルール条件で発行者 DN の値が一致する場合に一致します。

  詳細については、識別名（DN）のルール条件 （2373 ページ）を参照してください。

- 証明書ステータス：復号ルールでいずれかの証明書ステータス条件が一致する場合に一致します。

  詳細については、証明書ステータスの 復号ルール条件 （2379 ページ）を参照してください。

- 内部/外部証明書：内部証明書は、[復号-既知のキー（Decrypt - Known Key）] ルールアクションで使用される証明書と照合できます。外部証明書は、証明書ルール条件で照合できます。

  詳細については、既知のキーでの復号（着信トラフィック） （2311 ページ）および証明書の 復号ルール条件 （2372 ページ）を参照してください。

- アプリケーション ID：アクセス コントロール ポリシーまたは復号ポリシーのアプリケーションルール条件と照合できます。

  詳細については、アプリケーションルール条件 （817 ページ）を参照してください。

- URL カテゴリ：アクセス コントロール ポリシーの URL ルール条件と照合できます。

  詳細については、URL ルール条件 （821 ページ）を参照してください。

（注） [適応型TLSサーバーでの検出モードの有効化（Enable adaptive TLS server discovery mode）] は、AWS に展開されたどの Secure Firewall Threat Defense Virtual でもサポートされていません。Secure Firewall Management Center で管理されているそのような管理対象デバイスがある場合、接続イベント **PROBE_FLOW_DROP_BYPASS_PROXY** は、デバイスがサーバー証明書の抽出を試みるたびに増加します。

TLS 1.3 復号のベストプラクティス

推奨事項：詳細オプションを有効にする場合

復号ポリシーとアクセス コントロール ポリシーの両方に、トラフィックが復号されているかどうかに関係なく、トラフィックの処理方法に影響する詳細オプションがあります。

詳細オプションは次のとおりです。

- 復号ポリシー：
  - TLS 1.3 復号
  - TLS 適応型サーバーのアイデンティティプローブ
- アクセス コントロール ポリシー：TLS 1.3 サーバーアイデンティティ検出

  アクセス コントロール ポリシー設定は、復号ポリシー設定よりも優先されます。

次の表を使用して、有効にするオプションを決定します。

TLS 適応型サーバーのアイデンティティプローブ設定（復号ポリシー）	TLS 1.3 サーバーアイデンティティ検出設定（アクセス コントロール ポリシー）	結果	推奨される状況
有効	無効	復号ポリシーに復号ポリシーの詳細オプション（2345ページ）で指定されたいずれかのルール条件が含まれ、かつサーバー証明書がキャッシュされていない場合に適応プローブが送信されます。	• アクセスコントロールルールでアプリケーション条件または URL 条件を使用していない • トラフィックを復号している
有効	有効	サーバー証明書がキャッシュされていない場合、プローブは常に送信されます。	アクセスコントロールルールに URL 条件またはアプリケーション条件がある場合にのみ使用する
無効	有効	サーバー証明書がキャッシュされていない場合、プローブは常に送信されます。	非推奨

TLS 適応型サーバーのアイデンティティプローブ設定（復号ポリシー）	TLS 1.3 サーバーアイデンティティ検出設定（アクセス コントロール ポリシー）	結果	推奨される状況
無効	無効	プローブは送信されません。	実用性は非常に限定される。トラフィックを復号せず、アクセスコントロールルールでアプリケーション条件またはURL 条件を使用しない場合にのみ使用する

（注） キャッシュされた TLS サーバーの証明書は、特定の Firewall Threat Defense のすべての Snort インスタンスで利用できます。キャッシュはCLI コマンドでクリアでき、デバイスの再起動時に自動的にクリアされます。

参照

詳細については、secure.cisco.com で TLS サーバーアイデンティティ検出の説明を参照してください。

第 62 章

復号ルール

ここでは、復号ルールの作成、設定、管理、トラブルシューティングの概要を示します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

SSL プロトコルと TLS プロトコルの詳細については、「SSL vs. TLS - What's the Difference?」[英語] などのリソースを参照してください。

- 復号ルールの概要 （2349 ページ）
- 復号ルール の要件と前提条件 （2350 ページ）
- 復号ルール の注意事項と制限事項 （2350 ページ）
- 復号ルールトラフィック処理 （2360 ページ）
- 復号ルール 条件 （2365 ページ）
- 復号ルール アクション （2386 ページ）
- TLS/SSL ハードウェア アクセラレーションのモニター （2389 ページ）
- 復号ルール のトラブルシューティング （2391 ページ）

復号ルールの概要

復号ルールを設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号せずにアクセス コントロールで検査する、あるいはアクセス コントロールの分析用にトラフィックを復号するなど、複数の管理対象デバイスをカバーしたきめ細かな暗号化トラフィックの処理メソッドを構築できます。

復号ルール の要件と前提条件

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

復号ルール の注意事項と制限事項

復号ルール を設定するときは、次の点に注意してください。復号ルール を適切に設定するのは複雑なタスクですが、暗号化トラフィックを処理する効果的な導入環境の構築には不可欠なタスクです。ルールをどのように設定するかには、制御できない特定のアプリケーションの動作を含む、多くの要素が影響します。

さらに、ルールが互いをプリエンプトしたり、追加ライセンスが必要になったりすることがあります。また、ルールに無効な設定が含まれる可能性もあります。慎重に設定されたSSLルールは、ネットワークトラフィックの処理に必要なリソースの軽減にも寄与します。過度に複雑なルールを作成し、ルールを誤って順序付けすると、パフォーマンスに悪影響を与える可能性があります。

詳細については、アクセス制御ルールのベストプラクティス（1736ページ）を参照してください。

TLS暗号化アクセラレーションに特に関連するガイドラインについては、TLS暗号化アクセラレーション （2316 ページ）を参照してください。

関連トピック

ルールとその他のポリシーの警告
アクセス制御ルールのベストプラクティス （1736 ページ）
TLS/SSL 復号の使用上のガイドライン （2351 ページ）
復号ルール サポートされていない機能 （2352 ページ）
TLS/SSL 復号禁止のガイドライン （2352 ページ）
TLS/SSL 復号：再署名のガイドライン （2354 ページ）
TLS/SSL 復号：既知のキーのガイドライン （2357 ページ）
TLS/SSL ブロックのガイドライン （2358 ページ）
TLS/SSL 証明書のピン留めのガイドライン （2358 ページ）
TLS/SSL ハートビートのガイドライン （2358 ページ）

TLS/SSL 匿名の暗号スイートの制限事項 （2359 ページ）
TLS/SSL 正規化のガイドライン （2359 ページ）
その他の 復号ルール ガイドライン （2359 ページ）
SSL ルールの順序

TLS/SSL 復号の使用上のガイドライン

一般的なガイドライン

復号ルールには、パフォーマンスに影響を及ぼす可能性があるオーバーヘッドの処理が必要です。ポリシーまたはルールを設定する前に、復号してディープインスペクションの対象とする必要があるトラフィックを決定します。

パッシブまたはインライン タップ モード インターフェイスを使用するデバイスでトラフィックを復号することはできません。

復号できないトラフィックのガイドライン

Web サイト自体が復号できない、または Web サイトで TLS/SSL ピン留めが使用されている場合、特定のトラフィックを復号できないと判断できます。SSL ピン留めでは、ブラウザにエラーが表示されることなく、復号されたサイトへのユーザーアクセスが効果的に阻止されます。

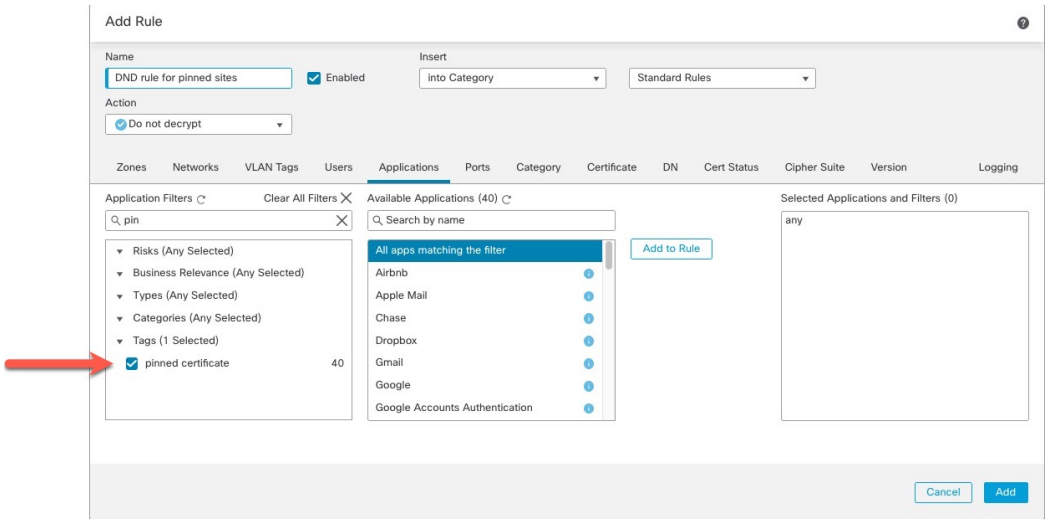
証明書のピン留めの詳細については、TLS/SSL のピニングについて （2395 ページ）を参照してください。

そのようなサイトのリストは次のように管理されています。

- **Cisco-Undecryptable-Sites** という名前の識別名（DN）グループ
- **ピン留めされた証明書**または**復号不可**のアプリケーションフィルタ

トラフィックを復号しており、ユーザーが復号されたサイトにアクセスしたときにブラウザにエラーが表示されないようにする場合は、復号ルールの下部に [復号しない（Do Not Decrypt）] ルールを設定することを推奨します。

ピン留めされた証明書のアプリケーションフィルタの設定例を次に示します。



復号ルール サポートされていない機能

RC4 暗号はサポートされていない

Rivest Cipher 4（*RC4* または *ARC4* ともいう）暗号は脆弱性があることで知られており、安全でないと見なされています。

復号ポリシー は RC4 暗号スイートをサポート対象外としています。組織の要件と一致するように復号ポリシー ポリシーの **[復号不可のアクション（Undecryptable Actions）]** ページで、**[サポート対象外の暗号スイート（Unsupported Cipher Suite）]** アクションを設定する必要があります。詳細については、復号できないトラフィックのデフォルト処理オプション （2342 ページ）を参照してください。

パッシブ、インラインタップモード、およびSPANインターフェイスはサポートされていません。

TLS/SSL トラフィックは、パッシブ、インラインタップモード、または SPAN インターフェイスでは復号できません。

TLS/SSL 復号禁止のガイドライン

次によって禁止されている場合は、トラフィックを復号してはいけません。

- 法律：たとえば、一部の法域では、財務情報の復号が禁止されています
- 会社のポリシー：たとえば、会社によって特権的な通信の復号が禁止されている場合があります
- プライバシー規制
- 証明書のピン留め（*TLS/SSL* ピニングとも呼ばれる）を使用するトラフィックは、接続の切断を防ぐため、暗号化されたままにする必要があります

暗号化されたトラフィックは、次のものを含むがこれらに限定されない任意の 復号ルール 条件で許可またはブロックできます。

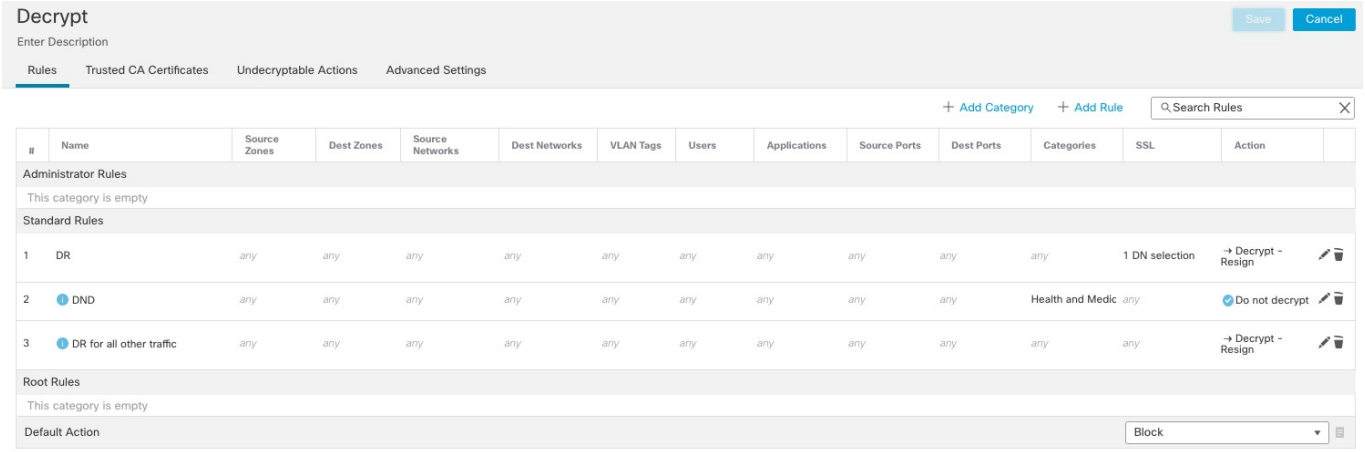
- 証明書のステータス（期限切れまたは無効な証明書など）
- プロトコル（セキュアでない SSL プロトコルなど）
- ネットワーク（セキュリティ ゾーン、IP アドレス、VLAN タグなど）
- 正確な URL または URL カテゴリ
- ポート
- ユーザー グループ

[復号しない（Do Not Decrypt）] ルールのカテゴリの制限

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。シスコでは、URL フィルタリングカテゴリの継続的な更新と改善に努めていますが、厳密に科学的なものではありません。一部の Web サイトはまったく分類されておらず、一部の Web サイトは不適切に分類されている可能性があります。

理由のないトラフィックの復号を避けるために、[復号しない（Do Not Decrypt）] ルールのカテゴリを過度に使用しないでください。たとえば、[健康と薬（Health and Medicine）] カテゴリには、患者のプライバシーを脅かさない WebMD の Web サイトが含まれています。

以下は、[健康と薬（Health and Medicine）] カテゴリの Web サイトの復号を防ぐ一方で、WebMD およびその他すべての復号を許可することができるサンプル復号ポリシーです。復号ルールに関する一般的な情報については、TLS/SSL 復号の使用上のガイドライン（2351 ページ）を参照してください。



（注） URL フィルタリングとアプリケーション検出を混同しないでください。アプリケーション検出は、Web サイトからのパケットの一部を読み取り、それが何であるか（Facebook メッセージや Salesforce など）をより具体的に判断することに依存します。詳細については、アプリケーション制御の設定のベストプラクティス （1732 ページ）を参照してください。

TLS/SSL 復号：再署名のガイドライン

[Decrypt - Resign] アクションには、1 つの内部認証局（CA）証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、システムは CA 証明書を使用してサーバー証明書を再署名してから、中間者（man-in-the-middle）として機能します。ここでは 2 つの TLS/SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。各セッションにはさまざまな暗号セッションの詳細が含まれており、システムはこれを使用することでトラフィックの復号と再暗号化が行えます。

ベスト プラクティス

次の点を推奨します。

- [Decrypt - Known Key] ルールアクションを推奨する着信トラフィックとは対照的に、発信トラフィックの復号に対しては [Decrypt - Resign] ルールアクションを使用します。

  [復号 - 既知のキー（Decrypt - Known Key）] の詳細については、TLS/SSL 復号：既知のキーのガイドライン （2357 ページ）を参照してください。

- [復号-再署名（Decrypt - Resign）] ルールアクションを設定する場合は、必ず [キーのみを置換（Replace Key Only）] チェックボックスをオンにします。

  ユーザーが自己署名証明書を使用する web サイトを参照すると、web ブラウザにセキュリティ警告が表示され、セキュリティで保護されていないサイトと通信していることに気付きます。

  ユーザーが信頼できる証明書を使用する web サイトを参照すると、セキュリティ警告は表示されません。

詳細

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部 CA 証明書の署名アルゴリズム タイプに基づいて実施されます。各 [復号 - 再署名（Decrypt - Resign）] アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、異なる署名アルゴリズムで暗号化された複数のタイプの発信トラフィックを復号する 復号ルール ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが [復号 - 再署名（Decrypt - Resign）] ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成する場合は、EC ベースの外部証明書と暗号スイートをルールに追加する必要があります。

同様に、RSA ベースの CA 証明書を参照する [復号 - 再署名（Decrypt - Resign）] ルールは、RSA アルゴリズムで暗号化された発信トラフィックとのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

注意事項と制約事項

また次の点に注意してください。

匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 の付録 F.1.1.1 を参照してください。（TLS 1.3 では、代わりに RFC 8446 付録 C.5 を参照してください。）

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

バージョンまたは暗号スイートのルール条件を使用しない

重要 **[復号 - 再署名（Decrypt - Resign）]**、**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、または **[復号 - 既知のキー（Decrypt - Known Key）]** ルールアクションを含むルールでは、**[暗号スイート（Cipher Suite）]** または **[バージョン（Version）]** ルール条件を決して使用しないでください。これらの条件をルールで他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

[復号 - 再署名（Decrypt - Resign）] ルールアクションと証明書署名要求

[復号-再署名（Decrypt - Resign）] ルールアクションを使用するには、証明書署名要求（CSR）を作成し、信頼された証明機関によって署名する必要があります。（FMC を使用して CSR を作成できます：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[PKI]** > **[内部CA（Internal CAs）]**。）

[復号-再署名（Decrypt - Resign）] ルールで使用するには、認証局（CA）に次の拡張機能の少なくとも 1 つが必要です。

- **CA: TRUE**

  詳細については、RFC3280、セクション 4.2.1.10 にある、基本制約に関する説明を参照してください。

- **KeyUsage=CertSign**

  詳細については、RFC 5280、セクション 4.2.1.3 を参照してください。

CSR または CA に前述の拡張機能の少なくとも 1 つがあることを確認するには、openssl のドキュメントなどの参考資料で説明されている、**openssl** コマンドを使用できます。

これが必要なのは、[復号 - 再署名（Decrypt - Resign）] インスペクションが機能するために、復号ポリシーで使用された証明書がオンザフライで証明書を生成し、中間者として機能し、すべての TLS/SSL 接続をプロキシするようにそれらに署名するためです。

証明書のピン留め

ブラウザが証明書ピニングを使用してサーバー証明書を確認する場合は、サーバー証明書に再署名しても、このトラフィックを復号できません。このトラフィックを許可するには、サーバー証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して 復号ルール を設定します。

一致しない暗号スイート

証明書と一致しない暗号スイートで復号ルールを保存しようとすると、次のエラーが表示されます。この問題を解決するには、TLS/SSL 暗号スイートの確認（2400 ページ）を参照してください。

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

信頼できない認証局

サーバー証明書の再署名に使用する認証局（CA）をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザーに出されます。これを防止するには、クライアントの信用できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。

HTTP プロキシの制限

クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバーが CONNECT HTTP メソッドを使用してトンネル TLS/SSL 接続を確立する場合、システムはトラフィックを復号できません。システムによるこのトラフィックの処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号できないアクションが決定します。

署名済み CA のアップロード

内部 CA オブジェクトを作成して証明書署名要求（CSR）の生成を選択した場合は、オブジェクトに署名付き証明書をアップロードするまで、この CA を [復号 - 再署名（Decrypt - Resign）] アクションに使用できません。

署名アルゴリズムの不一致

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定し、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズムタイプの不一致が生じた場合、ポリシーエディタでルールの横に**情報**（ ）が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズムタイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン[警告（warning）]（ ）が表示され、復号ポリシーに関連付けたアクセス コントロール ポリシーは適用できなくなります。

TLS/SSL 復号：既知のキーのガイドライン

[復号 - 既知のキー（Decrypt - Known Key）] アクションを設定した場合は、1 つまたは複数のサーバー証明書と秘密キー ペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、システムは適切な秘密キーを使用してセッションの暗号化と復号化キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号する場合です。

また次の点に注意してください。

匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 の付録 F.1.1.1 を参照してください。（TLS 1.3 では、代わりに RFC 8446 付録 C.5 を参照してください。）

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

識別名または証明書が一致しない

[復号 - 既知のキー（Decrypt - Known Key）] アクションを指定して 復号ルール を作成した場合は、[識別名（Distinguished Name）] や [証明書（Certificate）] 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。

バージョンまたは暗号スイートのルール条件を使用しない

重要 **[復号 - 再署名（Decrypt - Resign）]**、**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、または **[復号 - 既知のキー（Decrypt - Known Key）]** ルール アクションを含むルールでは、**[暗号スイート（Cipher Suite）]** または **[バージョン（Version）]** ルール条件を決して使用しないでください。これらの条件をルールで他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

楕円曲線デジタル署名アルゴリズム（*ECDSA*）証明書によってトラフィックがブロックされる

（TLS 1.3 復号が有効の場合のみ）[復号 - 既知のキー（Decrypt - Known Key）] アクションで ECDSA 証明書を使用すると、一致するトラフィックがブロックされます。これを回避するには、証明書を別のタイプの証明書とともに使用します。

TLS/SSL ブロックのガイドライン

[インタラクティブブロック（Interactive Block）] または [リセット付きインタラクティブブロック（Interactive Block with reset）] アクション付きのアクセス コントロール ポリシーと 復号ルール が関連付けられている場合、システムはカスタマイズ可能な応答ページを表示します。

ルールでロギングを有効にすると、（**[分析（Analysis）] > [イベント（Events）] > [接続（Connections）]** で）2 つの接続イベントが表示されます。インタラクティブ ブロックのイベントと、ユーザーがサイトの継続を選択したかどうかを示す別のイベントです。

関連トピック

HTTP 応答ページの設定 （1836 ページ）

TLS/SSL 証明書のピン留めのガイドライン

一部のアプリケーションでは、アプリケーション自体に元のサーバー証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで 復号ルール を設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL のピン留めは中間者攻撃を避けるために使用されるため、防止または回避する方法はありません。ピニングトラフィックが復号対象から除外されるように、[復号 - 再署名（Decrypt - Resign）] ルールの前に [復号しない（Do Not Decrypt）] ルールを追加することを推奨します。

- そのアプリケーション用に、[復号-再署名（Decrypt - Resign）] ルールよりも順序が前の、[復号しない（Do Not Decrypt）] ルールを作成します。
- Web ブラウザを使用してアプリケーションにアクセスするようユーザに指示します。

ルールの順序の詳細については、SSL ルールの順序を参照してください。

アプリケーションが TLS/SSL のピン留めを使用しているかどうかを判断するには、TLS/SSL ピニングのトラブルシューティング （2396 ページ）を参照してください。

TLS/SSL ハートビートのガイドライン

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

ネットワーク分析ポリシー（NAP）で [最大ハートビート長（Max Heartbeat Length）] を設定して TLS ハートビートの処理方法を決定できます。詳細については、SSL プリプロセッサ （2845 ページ）を参照してください。

詳細については、「TLS ハートビートについて （2394 ページ）」を参照してください。

TLS/SSL 匿名の暗号スイートの制限事項

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 の付録 F.1.1.1 を参照してください。（TLS 1.3 では、代わりに RFC 8446 付録 C.5 を参照してください。）

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

復号ルール の [暗号スイート（Cipher Suite）] 条件に匿名の暗号スイートを追加することはできますが、システムは、ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために 復号ルール を設定する必要があります。詳細については、SSL ルールの順序を参照してください。

TLS/SSL 正規化のガイドライン

インライン正規化プリプロセッサで [余剰ペイロードの正規化（Normalize Excess Payload）] オプションを有効にすると、プリプロセッサによる復号トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これで TLS/SSL セッションは終了しません。トラフィックが許可された場合、トリミングされたパケットは TLS/SSL セッションの一部として暗号化されます。

その他の 復号ルール ガイドライン

ユーザーとグループ

ルールにグループまたはユーザを追加した後、そのグループまたはユーザを除外するようにレルムの設定を変更すると、ルールは適用されなくなります。（レルムを無効にする場合も同様です。）レルムの詳細については、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）を参照してください。

復号ルール のカテゴリ

復号ポリシーに [復号-再署名（Decrypt - Resign）] アクションがあっても Web サイトが復号されない場合は、そのポリシーに関連付けられているルールの [カテゴリ（Category）] ページを確認します。

場合によっては、認証などの目的で Web サイトが別のサイトにリダイレクトされ、リダイレクト先のサイトの URL カテゴリが復号を試みているサイトとは異なることがあります。たとえば、`gmail.com`（[Webベース電子メール（Web based email）] カテゴリ）は認証のために `accounts.gmail.com`（[インターネットポータル（Internet Portals）] カテゴリ）にリダイレクトされます。関連するすべてのカテゴリを必ず SSL ルールに含めます。

（注） URL カテゴリに基づいてトラフィックを完全に処理するには、URL フィルタリングも設定する必要があります。URL フィルタリング （1815 ページ）の章を参照してください。

ローカル データベースにない URL のクエリ

[復号-再署名（Decrypt - Resign）] ルールを作成し、ローカル データベースにカテゴリとレピュテーションがない Web サイトをユーザが参照すると、データが復号されないことがあります。一部の Web サイトはローカル データベースで分類されません。分類されない場合、その Web サイトのデータはデフォルトでは復号されません。

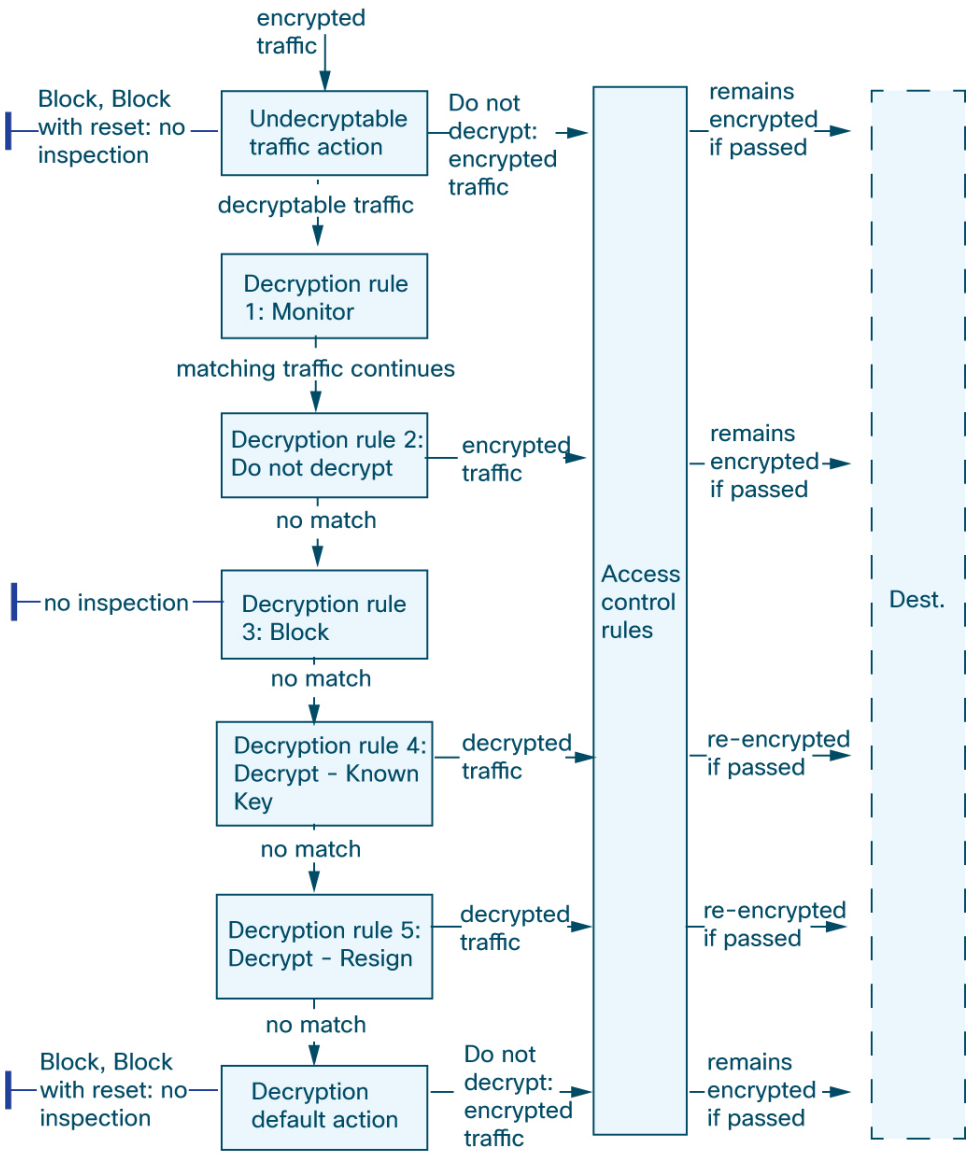
[システム（System）]>[統合（Integration）]> **クラウド サービス** を設定して、[不明なURLをCisco Cloudに問い合わせる（Query Cisco cloud for unknown URLs）] チェック ボックスをオンにすることで、この動作を制御できます。

復号ルールトラフィック処理

トラフィックはユーザーが指定した順序で 復号ルール と照合されます。ほとんどの場合、暗号化トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の復号ルールに従って実行されます。こうした条件には、単純なものと複雑なものがあります。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求されたURL、ユーザー、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号トラフィックに対してモニター、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化後および復号できないトラフィックは、アクセス コントロールを使用して検査します。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、暗号化ペイロードの侵入およびファイル検査を、システムは無効化します。

次のシナリオは、インライン展開での 復号ルール によるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィック アクション**（**Undecryptable Traffic Action**）は、暗号化されたトラフィックを最初に評価します。復号できないトラフィックについてシステムは、それ以上のインスペクションなしでブロックするか、あるいはアクセスコントロールによるインスペクション用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **復号ルール1：モニター**（**Monitor**）は、暗号化トラフィックを次に評価します。モニタールールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。

- **復号ルール 2**：**復号しない（Do Not Decrypt）**は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。
- **復号ルール 3**：**ブロック（Block）**は、暗号化トラフィックを 4 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **復号ルール 4**：**復号 - 既知のキー（Decrypt - Known Key）**は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザーのアップロードする秘密キーを使用して復号されます。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。復号ルールに一致しないトラフィックは、引き続き次のルールと照合されます。
- **復号ルール 5**：**復号 - 再署名（Decrypt - Resign）**は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバー証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **復号ポリシーデフォルトアクション**は、いずれの 復号ルール にも一致しないすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

暗号化トラフィック インスペクションの設定

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号には、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の復号ポリシーへのアップロード時、復号ルールの作成時、およびプロセスでの関連オブジェクトの作成時に臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

証明書とキー ペアによる暗号化トラフィックの復号

セッション暗号化に使用するサーバー証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておくと、システムは着信する暗号化トラフィックを復号できます。[復号-既知のキー（Decrypt - Known Key）] アクションが設定された復号ポリシールールでそのオブ

ジェクトを参照している場合に、当該ルールにトラフィックが一致すると、アップロードされた秘密キーを使用してセッションが復号されます。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、システムは発信トラフィックの復号もできます。[復号 - 再署名（Decrypt - Resign）] アクションが設定された復号ルールでそのオブジェクトを参照している場合に、当該ルールにトラフィックが一致すると、クライアントブラウザに渡されたサーバー証明書が再署名され、システムが中間者（man-in-the-middle）として機能してセッションが復号されます。 オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

暗号化セッションの特性に基づいたトラフィック制御

システムによる暗号化トラフィックの制御は、セッション ネゴシエートに使用されたサーバー証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、復号ルール条件でオブジェクトを参照してトラフィックを照合できます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使用される暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する
組織が信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバー証明書を信頼する • CA が証明書を直接発行した • サーバー証明書を発行した中間 CA に CA が証明書を発行した
サーバー証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバー証明書が、アップロードされたサーバー証明書と一致する
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名と一致する

関連トピック

暗号スイート リスト （1327 ページ）
識別名 （1332 ページ）
PKI （1352 ページ）

復号ルールの評価の順序

この情報は、レガシー復号のポリシーとルールにのみ適用されます。

復号ポリシーで復号ルールを作成する場合、ルールエディタの [挿入（Insert）] リストを使用してその位置を指定します。復号ポリシー内の復号ルールには、1 から始まる番号が付けられています。復号ルールは、ルール番号の昇順で上から順にトラフィックと照合されます。

ほとんどの場合、ネットワークトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の復号ルールに従って実行されます。モニタールール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。こうした条件には、単純なものと複雑なものがあります。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求されたURL、ユーザー、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号トラフィックに対してモニター、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号できないトラフィックはアクセス コントロールの対象です。ただし、アクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなります。

特定の条件（ネットワークや IP アドレスなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

ヒント 適切な復号ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、3 つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

関連トピック

アクセス制御ルールのベストプラクティス （1736 ページ）
復号できないトラフィックのデフォルト処理オプション （2342 ページ）
SSL ルールの順序

復号ルール 条件

復号ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、証明書の条件が設定され、バージョンの条件が設定されていないルールは、セッションSSLまたはTLSのバージョンにかかわりなく、セッションのネゴシエーションに使用されるサーバー証明書に基づいてトラフィックを評価します。

すべての復号ルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理：最も重要なこととして、ルール アクションはルールの条件に一致する暗号化トラフィックに対して、モニター、信頼、ブロック、または復号を行うかどうかを判定します。
- ロギング：ルールアクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

TLS/SSLインスペクション設定では、次のように復号されたトラフィックの処理、検査、ログ記録を行います。

- 復号ポリシーの復号できないアクションは、システムが復号できないトラフィックを処理します。
- ポリシーのデフォルトアクションは、モニター以外のどの復号ルールの条件にも一致しないトラフィックを処理します。

システムが暗号化セッションを信頼またはブロックしたときに、接続イベントをログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- 復号しない（Do not decrypt）接続の場合、システムはセッション終了時にイベントを生成します

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

注意 TLS/SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに 復号ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれることに注意してください。

関連トピック

セキュリティゾーンルール条件 （1877 ページ）
ネットワークルール条件 （816 ページ）
VLAN タグルール条件 （1792 ページ）
ユーザールール条件 （817 ページ）
アプリケーションルール条件 （817 ページ）
ポートルールの条件 （819 ページ）
カテゴリルール条件 （2371 ページ）
サーバー証明書ベースの 復号ルール条件 （2371 ページ）

セキュリティゾーンルール条件

セキュリティゾーンはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することで、トラフィックフローを管理、分類、および復号しやすくします。

セキュリティゾーンは、トラフィックをその送信元と宛先のセキュリティゾーンで制御または復号します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ヒント　ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

ネットワークルール条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネル ルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注）　アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

VLAN タグルール条件

（注）　アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense

- インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
- ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

ユーザールール条件

接続を開始したユーザー、またはユーザーが属するグループに基づいてトラフィックが照合されます。たとえば、財務グループの全員がネットワークリソースにアクセスすることを禁止するブロックルールを設定できます。

Microsoft Active Directory レルムのユーザーに対してのみユーザー ルール条件を設定できます。

設定されたレルムのユーザーとグループの設定に加えて、次の特殊なアイデンティティユーザーのポリシーを設定できます。

- [失敗した認証（Failed Authentication）]：キャプティブポータルでの認証に失敗したユーザー。
- [ゲスト（Guest）]：キャプティブポータルでゲストユーザーとして設定されたユーザー。
- [認証不要（No Authentication Required）]：アイデンティティの [認証不要（No Authentication Required）] ルールアクションに一致するユーザー。
- [不明（Unknown）]：識別できないユーザー。たとえば、設定されたレルムによってダウンロードされていないユーザー。

アクセス制御ルールのみの場合、ID ポリシーをアクセス コントロール ポリシーに最初に関連付ける必要があります（アクセス制御への他のポリシーの関連付け （1765 ページ）を参照）。

アプリケーションルール条件

システムはIP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリ

ケーションの任意の組み合わせをもとに、ユーザー定義の再利用可能フィルタを作成できます。

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザー定義ディテクタが有効になります。アプリケーション ディテクタの詳細については、アプリケーション ディテクタの基本 （2633 ページ）を参照してください。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

アプリケーション フィルタの利点

アプリケーション フィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザーがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーション フィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーション トラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーション トラフィックは常に最新のディテクタによってモニターされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *191* : アプリケーションの特性

特性	説明	例
タイプ	アプリケーション プロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。

特性	説明	例
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲームアプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも1つのカテゴリに属します。	Facebookはソーシャルネットワーキングのカテゴリに含まれます。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオストリーミングWebアプリケーションには、ほとんどの場合、`high bandwidth`と`displays ads`というタグが付けられます。

関連トピック

アプリケーション制御の設定のベストプラクティス （1732 ページ）

ポートルールの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTD など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

カテゴリルール条件

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。

詳細については、URL フィルタリングの概要 （1815 ページ）を参照してください。

[復号しない（Do Not Decrypt）] ルールアクションを含むルールの復号ポリシーでカテゴリルール条件を使用している場合は、復号ルール [復号しない（Do Not Decrypt）] アクション （2386 ページ）を参照してください。

サーバー証明書ベースの 復号ルール条件

復号ルールでは、サーバー証明書の特性に基づいて暗号化トラフックを処理および復号できます。復号ルールは、以下のサーバー証明書属性に基づいて設定することができます。

- 識別名条件を設定すると、証明書所有者またはサーバー証明書の発行元 CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバー証明書を発行した CA に基づいてトラフィックを処理できます。
- 復号ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。
- 復号ルールの証明書ステータス条件では、トラフィックの暗号化に使用されたサーバー証明書のステータスに基づいて暗号化されたトラフィックを処理して、証明書が有効か、失効しているか、期限切れか、まだ有効でないか、自己署名済みか、信頼できる CA によって署名済みか、証明書失効リスト（CRL）が有効かどうか、証明書のサーバー名指定（SNI）が要求内のサーバーと一致するかどうかなどの検査を行うことができます。
- 復号ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。
- 復号ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出したりする場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに追加できます。サーバー証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

関連トピック

証明書の 復号ルール条件 （2372 ページ）
証明書ステータスの 復号ルール条件 （2379 ページ）
外部認証局の信頼 （2378 ページ）
証明書ステータスでのトラフィックの照合
暗号スイートの 復号ルール 条件 （2382 ページ）
暗号化プロトコルバージョンの復号ルール条件 （2385 ページ）

証明書の 復号ルール条件

証明書ベースの復号ルール条件を作成するときにサーバー証明書をアップロードしたり、再利用可能な外部証明書オブジェクトとして証明書を保存して、サーバー証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [使用可能な証明書（Available Certificates）] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名に関する以下の特性に基づいて検索できます。

- サブジェクトまたは発行元の共通名（CN）、あるいは URL が証明書のサブジェクト代替名（SAN）に含まれている

  ユーザーがブラウザに入力する URL が共通名（CN）と一致する

- 件名または発行元の組織（O）
- 件名または発行元の部門（OU）

1 つの証明書のルール条件で複数の証明書を照合することもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[選択した証明書（Selected Certificates）] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- [復号 - 既知のキー（Decrypt - Known Key）] アクションも選択すると、証明書条件を設定できなくなります。このアクションでは、トラフィック復号用のサーバー証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われていることになります。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける内部 CA オブジェクトのいずれかが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [Decrypt - Resign] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズムタイプの不一致が検出されると、ポリシーエディタでルールの横に警告が表示されます。

- システムが新しいサーバーへの暗号化セッションを最初に検出したときは、証明書データを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。最初のセッションの後に、管理対象デバイスは、サーバーの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号の可能性を最大化できます。

識別名（DN）のルール条件

このトピックでは、復号ルールで識別名条件を使用する方法について説明します。よくわからない場合は、Web ブラウザを使用して証明書のサブジェクト代替名（SAN）と共通名を見つけ、それらの値を識別名条件として 復号ルール ルールに追加できます。

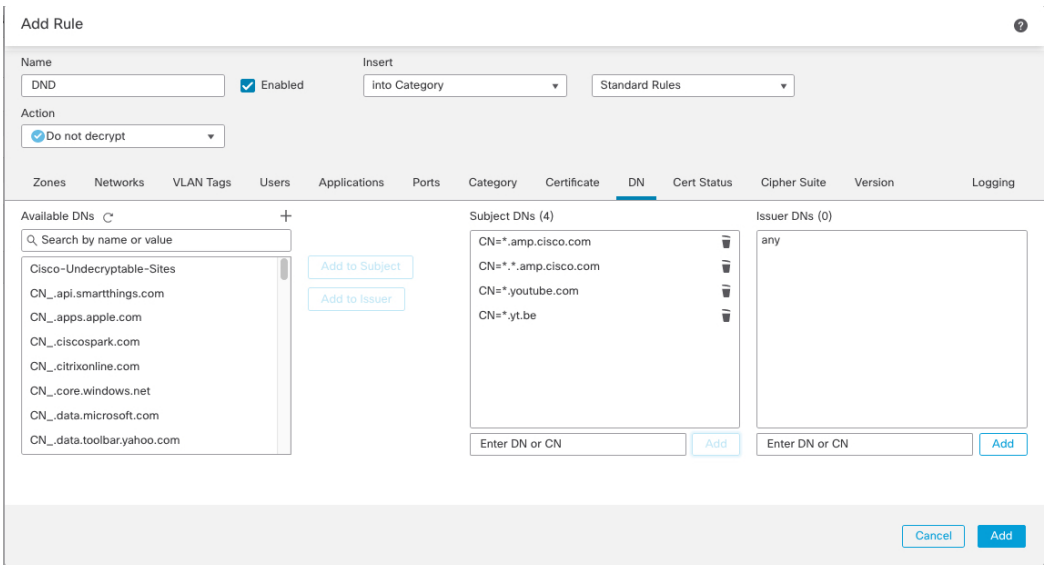
SAN の詳細については、RFC 528、セクション 4.2.1.6 を参照してください。

ここでは、次の点について説明します。

- DN ルールマッチングの例
- システムでの SNI と SAN の使用方法
- 証明書の共通名とサブジェクト代替名を見つける方法
- DN ルール条件を追加する方法

DN ルールマッチングの例

以下は、[復号しない（Do Not Decrypt）] ルールの DN ルール条件の例です。`amp.cisco.com` または YouTube に向かうトラフィックを復号しないようにしたいとします。次のように DN 条件を設定できます。



前述の DN ルール条件は次の URL に一致するため、トラフィックは復号されません。以前のルールによって復号は防止されました。

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

前述の DN ルール条件は、次の URL のいずれにも一致しないため、トラフィックは [復号しない（Do Not Decrypt）] ルールには一致しませんが、同じ 復号ポリシー内の他の 復号ルールには一致する可能性があります。

- amp.cisco.com
- youtube.com
- yt.be

上記のホスト名のいずれかと一致するには、ルールに CN を追加します（たとえば、`CN=yt.be` を追加すると、その URL に一致します）。

システムでの SNI と SAN の使用方法

クライアント要求の URL のホスト名部分は、サーバー名指定（SNI）です。クライアントは、TLS ハンドシェイクの SNI 拡張を使用して、接続するホスト名（たとえば、`auth.amp.cisco.com`）を指定します。次に、サーバーは、単一の IP アドレスですべての証明書をホストしながら、接続を確立するために必要な、対応する秘密キーと証明書チェーンを選択します。

SNI と証明書の CN または SAN が一致する場合、ルールにリストされている DN と比較するときに SNI を使用します。SNI がない場合、または証明書と一致しない場合は、ルールにリストされている DN と比較するときに、証明書の CN を使用します。

証明書の共通名とサブジェクト代替名を見つける方法

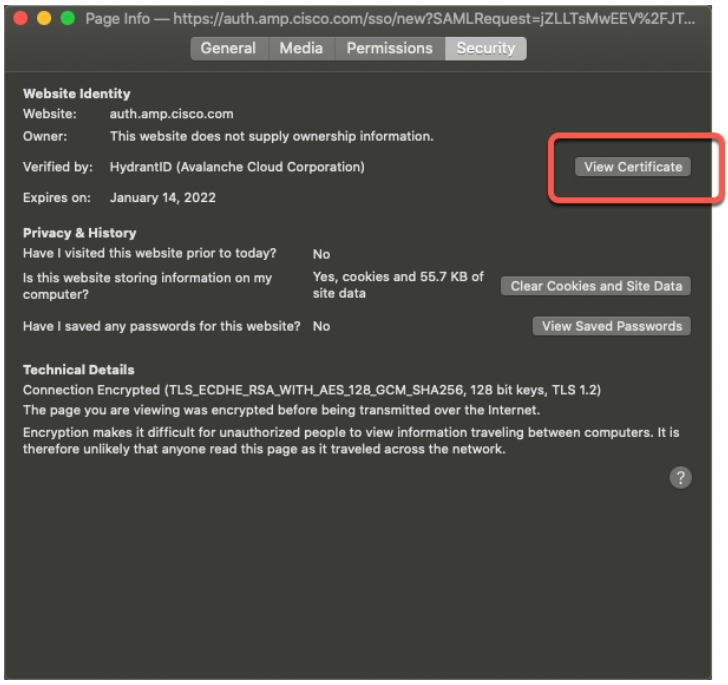
証明書の共通名を見つけるには、次の手順を使用します。これらの手順を使用して、自己署名証明書の共通名と SAN を見つけることもできます。

これらの手順は Firefox 用ですが、他のブラウザも同様です。次の手順では、例として `amp.cisco.com` を使用します。

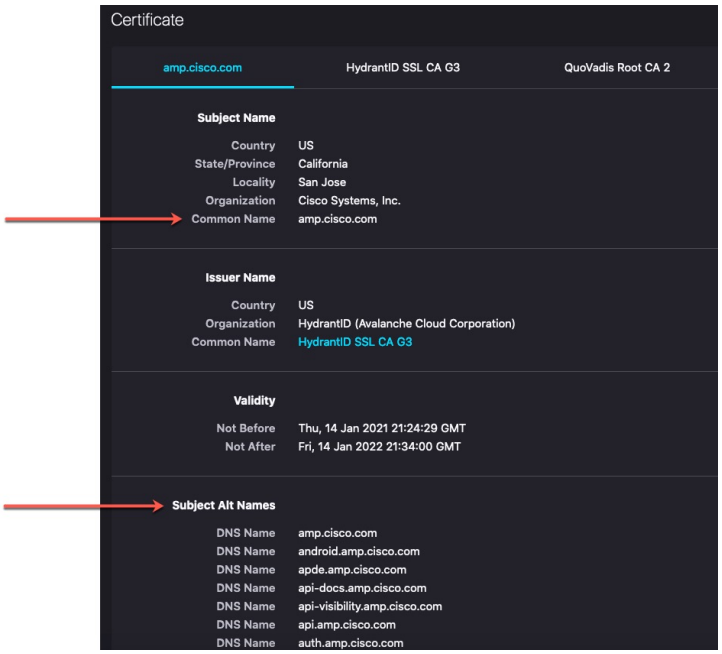
1. Firefox で `amp.cisco.com` にアクセスします。
2. ブラウザのロケーションバーで、URL の左側にある をクリックします。
3. **[この接続は保護されています（Connection secure）] > [詳細情報（More Information）]** をクリックします

（セキュリティで保護されていない場合、または自己署名証明書の場合は、**[この接続は保護されていません（Connection not secure）]** > **[詳細情報（More Information）]** をクリックします）。

4. [ページ情報（Page Info）] ダイアログボックスで、[証明書の表示（View Certificate）] をクリックします。



5. 次のページには、証明書の詳細が表示されます。



次の点に注意してください。

- CN=auth.amp.cisco.com をDNルール条件として使用すると、そのホスト名（つまり、SNI）のみに一致します。SNI amp.cisco.com は一致しません。
- できるだけ多くのドメイン名フィールドに一致させるには、ワイルドカードを使用します。

  たとえば、auth.us.amp.cisco.com と一致させるには、CN=*.*.amp.cisco.com を使用します。auth.us.amp.cisco.com と一致させるには、CN=*.*.amp.cisco.com を使用します。

  CN=*.example.com のようなDNは www.example.com に一致しますが、example.com には一致しません。両方のSNIに一致させるには、ルール条件で2つのDNを使用します。
- ただし、ワイルドカードは使いすぎないでください。たとえば、CN=*.google.com のようなDNオブジェクトは、非常に多数のSANに一致します。CN=*.google.com の代わりに、CN=*.youtube.com などのDNオブジェクトをDNオブジェクトとして使用して、www.youtube.com などの名前と一致させるようにします。

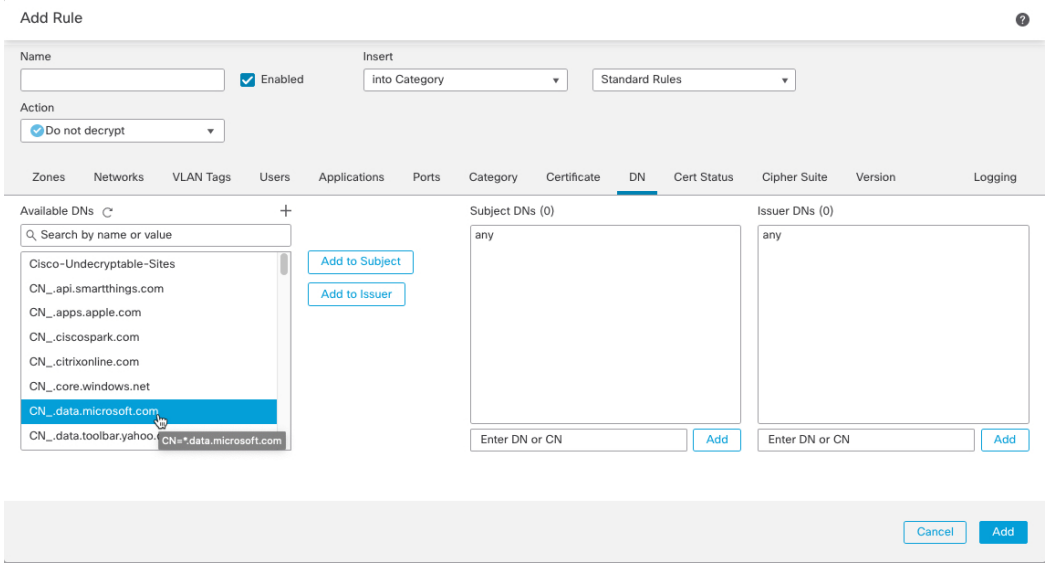
  CN=*.youtube.com、CN=youtu.be、CN=*.yt.be などのSANに一致するSNIのバリエーションを使用することもできます。
- 自己署名証明書も同じように機能するはずです。発行元DNがサブジェクトDNと同じであるという事実によって、自己署名証明書であることを確認できます。

DN ルール条件を追加する方法

一致させるCNがわかったら、次のいずれかの方法で 復号ルール を編集します。

- 既存のDNを使用します。

  DNの名前をクリックし、[サブジェクトに追加（Add to Subject）] または [発行元に追加（Add to Issuer）] をクリックします（[サブジェクトに追加（Add to Subject）] の方がはるかに一般的です）。DNオブジェクトの値を表示するには、マウスポインタをその上に移動します。

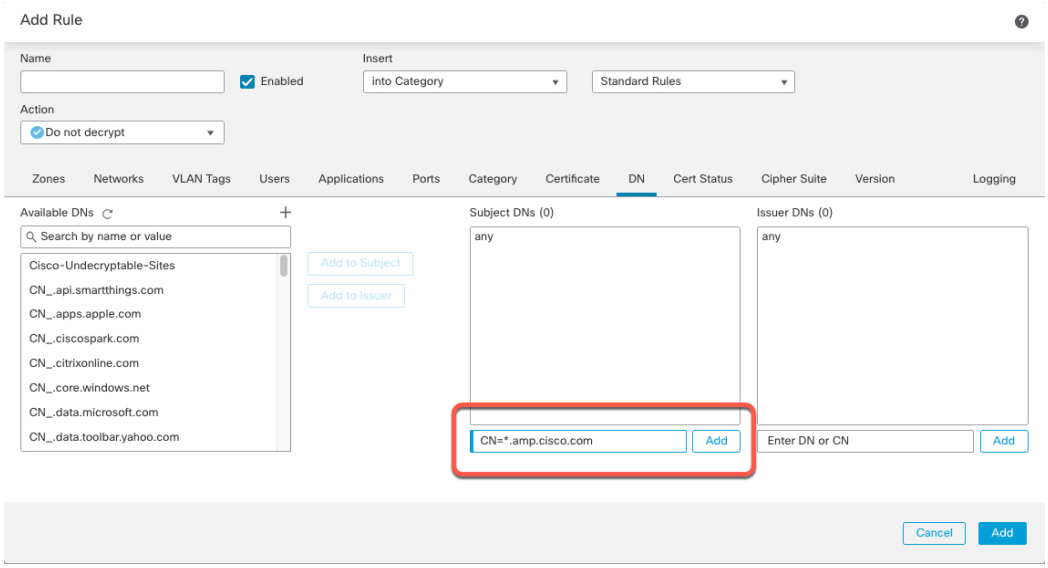


- 新しい DN オブジェクトを作成します。

  [利用可能なDN（Available DNs）] の右側にある [追加（Add）] (＋) をクリックします。DN オブジェクトは、名前と値で構成されている必要があります。

- DN を直接追加します。

  [サブジェクトDN（Subject DNs）] フィールドまたは [発行元DN（Issuer DNs）] フィールドの下部にあるフィールドに DN を入力します（[サブジェクトDN（Subject DNs）] のほうが一般的です）。DN を入力したら、[追加（Add）] をクリックします。



関連トピック

識別名 （1332 ページ）

外部認証局の信頼

復号ポリシーにルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバー証明書の検証に、これらの信頼できる CA を使用できるようになります。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により、暗号化証明書が失効されているかどうかも確認できます。

ヒント　信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。また、ルート発行者 CA に基づいてトラフィックを信頼するように証明書ステータス条件を設定する場合、信頼できる CA の信頼チェーン内のすべてのトラフィックは、復号する必要はなく、復号せずに許可することができます。

詳細については、信頼できる CA オブジェクト （1359 ページ）を参照してください。

（注）　復号ポリシーを作成すると、ポリシーの [信頼できるCA証明書（Trusted CA Certificate）] タブページに、いくつかの信頼できる CA 証明書が入力されます。これらには、[信頼できるCAの選択（Select Trusted CAs）] リストに追加される **Cisco-Trusted-Authorities** グループが含まれます。

手順

ステップ 1　まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2　**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[復号（Decryption）]** をクリックします。

ステップ 3　編集する 復号ポリシー の横にある [編集（Edit）]（） をクリックします。

ステップ 4　[ルールの追加（Add Rule）] をクリックして新しい復号ルールを追加するか、[編集（Edit）]（） をクリックして既存のルールを編集します。

ステップ 5　[証明書（Certificates）] タブをクリックします。

ステップ 6　次のように、[使用可能な証明書（Available Certificates）] で、追加する信頼できる CA を見つけます。

- ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[使用可能な証明書（Available Certificates）] リストの上にある [追加（Add）] () をクリックします。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[使用可能な証明書（Available Certificates）] リストの上にある [名前または値で検索（Search by name or value）]

プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

ステップ 7 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 8 [Add to Rule] をクリックします。

ヒント
選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 9 ルールを追加するか、編集を続けます。

次のタスク

- SSL ルールに証明書ステータスの復号ルール ルール条件を追加します。詳細については、証明書ステータスでのトラフィックの照合を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

証明書ステータスの 復号ルール条件

設定する証明書ステータスの復号ルールごとに、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

複数の証明書ステータスの有無を単一の証明書ステータス ルール条件で照合するように選択できます（いずれか 1 つの基準に一致するだけで、その証明書はルールに一致します）。

このパラメータを設定するときは、復号ルールを設定するのか、ブロック ルールを設定するのかを検討する必要があります。通常、ブロック ルールでは [はい（Yes）]、復号ルールでは [いいえ（No）] をクリックします。次に例を示します。

- [復号 - 再署名（Decrypt - Resign）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書でのトラフィックを復号します。その動作を変更するには、[期限切れ（Expired）] で [いいえ（No）] をクリックし、期限切れの証明書を持つトラフィックが復号され、再署名されないようにします。
- [ブロック（Block）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書を持つトラフィックを許可します。その動作を変更するには、[期限切れ（Expired）] で [はい（Yes）] をクリックし、期限切れの証明書を持つトラフィックをブロックします。

次の表は、暗号化用のサーバー証明書のステータスを基準に、システムが暗号化トラフィックを評価する方法を示しています。

表 *192 :* 証明書ステータスのルール条件の基準

ステータス チェック	Yes を設定	No を設定
Revoked	ポリシーは、サーバー証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバー証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行し頼しており、ポリシーにアップロー証明書にはこのサーバ証明書を失効が含まれていません。
Self-signed	検出されたサーバー証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるトと発行元の識別名を含んでいます
Valid	以下のすべてを満たしています。 • ポリシーが証明書を発行した CA を信用できる。 • 署名は有効である。 • 発行元は有効である。 • ポリシーの信頼できる CA のいずれも証明書を失効させていません。 • 現在の日付が証明書の有効期間の開始日と終了日の範囲内にある。	以下の 1 つ以上を満たしています。 • 証明書を発行した CA をポリシていない。 • 署名が無効である。 • 発行元が無効である。 • ポリシーの信用できる CA の 1証明書が失効している。 • 現在の日付が証明書の有効期間り前です。 • 現在の日付が証明書の有効期限り後です。
Invalid signature	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名証されます。
Invalid issuer	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーのCA 証明書のリストに登録されてい
Expired	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終かそれより前です。
Not yet valid	現在の日付が証明書の有効期限の開始日より前です。	現在の日付が証明書の有効期限の開かそれより後です。

ステータス チェック	Yes を設定	No を設定
無効な証明書	証明書が有効ではありません。以下の 1 つ以上を満たしています。 • 証明書の拡張子が無効であるか一貫していません。つまり、証明書の拡張子に無効な値（たとえば間違ったエンコーディング）が含まれているか、他の拡張子と矛盾する値がいくつか含まれています。 • 指定された目的に証明書を使用できません。 • 基本的制約のパス長パラメータを超過しています。 詳細については、RFC 5280、セクション 4.2.1.9 を参照してください。 • 証明書の発行日付または有効期限の値が無効です。これらの日付は、UTCTime または GeneralizedTime としてエンコードできます。 詳細については、RFC 5280、セクション 4.1.2.5 を参照してください。 • 名前制約の形式が認識されていません。たとえば、電子メールアドレス形式のフォームは RFC 5280、セクション 4.2.1.10 で言及されていません。これは、不適切な拡張子や、一部の新機能が現時点でサポートされていないことが原因で発生する場合があります。 サポートされていない名前制約タイプが見つかりました。OpenSSL では、ディレクトリ名、DNS 名、電子メール、および URI タイプのみがサポートされています。 • 指定された目的に関してルート認証局を信頼できません。 • ルート認証局が指定された目的を拒否しています。	証明書は有効です。以下のすべます。 • 有効な証明書の拡張子。 • 指定した目的に証明書を使 • 有効な基本的制約のパス長 • 有効な発行日付または有効 • 有効な名前制約。 • 指定された目的に関してル頼できる。 • ルート証明書が指定した目いる。

ステータス チェック	Yes を設定	No を設定
無効な CRL	証明書失効リスト（CRL）のデジタル署名が有効ではありません。以下の 1 つ以上を満たしています。 • CRL の [次回の更新（Next Update）] または [最後の更新（Last Update）] フィールドの値が無効である。 • CRL がまだ有効ではない。 • CRL の期限が切れている。 • CRL パスを確認する際にエラーが発生した。拡張CRLの確認が有効になっている場合にのみ、このエラーが発生する。 • CRL が検出できない。 • 検出できた唯一のCRLが証明書の範囲と一致しなかった。	CRLが無効です。以下のすべてを満す。 • [次回の更新（Next Update）] と新（Last Update）] フィールドのある。 • CRL の日付が有効である。 • パスが有効である。 • CRL が検出された。 • CRL が証明書の範囲と一致する
サーバーの不一致	サーバー名がサーバーのサーバー名指定（SNI）名と一致しません。これは、サーバー名を偽装しようとする試みを示している可能性があります。	サーバー名は、クライアントがアクしているサーバーの SNI 名と一致し

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間CA証明書とそのCRLをオブジェクトとしてアップロードする必要があります。その後、信頼できるCA証明書の復号ポリシーのリストに、信頼できる CA のオブジェクトを追加します。

暗号スイートの 復号ルール 条件

ブロックまたはリセット付きブロックのルールアクションのために暗号スイートのルール条件に追加できる、システム定義の暗号スイートが提供されています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。

重要 暗号スイートルール条件は、トラフィックをブロックするためだけに使用する必要があります。トラフィックを復号するためには使用しないでください。

（注） 新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[選択した暗号スイート（Selected Cipher Suites）] リストに最大 50 の暗号スイートおよび暗号スイートリストを追加できます。暗号スイート条件に追加できる暗号スイートとして、次のものがサポートされています。

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加すると、設定を展開できません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号がサポートされません。それら

の暗号スイートを使用してルールを作成すると、アクセス コントロール ポリシーを展開できなくなります。

- ルールを使用するには、復号ポリシー で [暗号スイート（Cipher Suite）] 条件に匿名の暗号スイートを追加できます。また、ClientHello が処理されない順序で設定する必要があります。詳細については、「SSL ルールの順序」を参照してください。
- 暗号スイーをルール条件として指定する際、ルールを ClientHello メッセージで指定された暗号スイートの完全なリストではなく、ServerHello メッセージのネゴシエートされた暗号スイートと照合することを検討してください。ClientHello の処理中に、管理対象デバイスは ClientHello メッセージからサポートされていない暗号スイートを削除します。ただし、これにより指定されたすべての暗号スイートが削除されることになる場合、システムでは元のリストを保持します。システムがサポートされていない暗号スイートを保持する場合、後続の評価は復号化されないセッションになります。

暗号化プロトコルバージョンの復号ルール条件

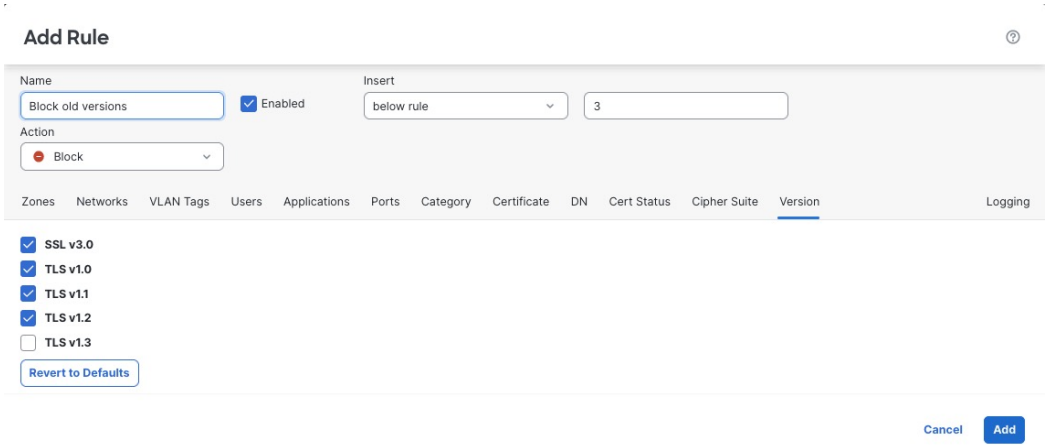
SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

SSL 3.0 は、[復号しない（Do Not Decrypt）]、[ブロック（Block）]、または [リセット付きブロック（Block with Reset）] ルールアクションで使用できます。

バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、SSL バージョン 2.0 で暗号化されたトラフィックの復号がサポートされていないためです。復号できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。詳細については、復号できないトラフィックのデフォルト処理を設定する （2344 ページ）を参照してください。

重要 プロトコルバージョンルール条件は、トラフィックをブロックするためだけに使用する必要があります。トラフィックを復号するためには使用しないでください。

たとえば、すべての SSL v3.0、TLS v1.0、TLS v1.1、TLS v1.2 トラフィックをブロックするには、次のようにオプションを設定します。



復号ルール アクション

ここでは、復号ルールで利用可能なアクションについて説明します。

復号ルール モニターアクション

[Monitor] アクションは、トラフィックを許可または拒否するように設計されていません。むしろ、その主な目的は、一致するトラフィックが最終的にどのように処理されるかに関係なく、接続ロギングを強制することです。トラフィックが [モニター（Monitor）] ルール条件に一致する場合、ClientHello メッセージは変更されません。

その後、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号するかが決定されます。モニタールール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニター ルールの主要な目的はネットワーク トラフィックを追跡することであるため、ルールのロギング設定や、あとで接続を処理するデフォルトのアクションにかかわらず、システムはモニター対象トラフィックの接続終了イベントを自動的に Secure Firewall Management Center データベースに記録します。

復号ルール [復号しない（Do Not Decrypt）] アクション

[復号しない（Do Not Decrypt）] アクションは、アクセス コントロール ポリシーのルールおよびデフォルト アクションに従って暗号化トラフィックを評価するため転送します。一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。暗号化トラフィックに対しては、侵入やファイル インスペクションなどのディープ インスペクションを行うことはできません。

[復号しない（Do Not Decrypt）] ルール アクションの一般的な理由は、以下のとおりです。

- TLS/SSL トラフィックの復号が法律によって禁止されている。
- 信頼できると判明しているサイトである。
- トラフィックを調べることによって中断できるサイト（Windows Update など）である。
- TLS/SSL フィールドの値を表示するには、接続イベントを使用します。（接続イベント フィールドを表示するためにトラフィックを復号する必要はありません。）詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Requirements for Populating Connection Event Fields」を参照してください。

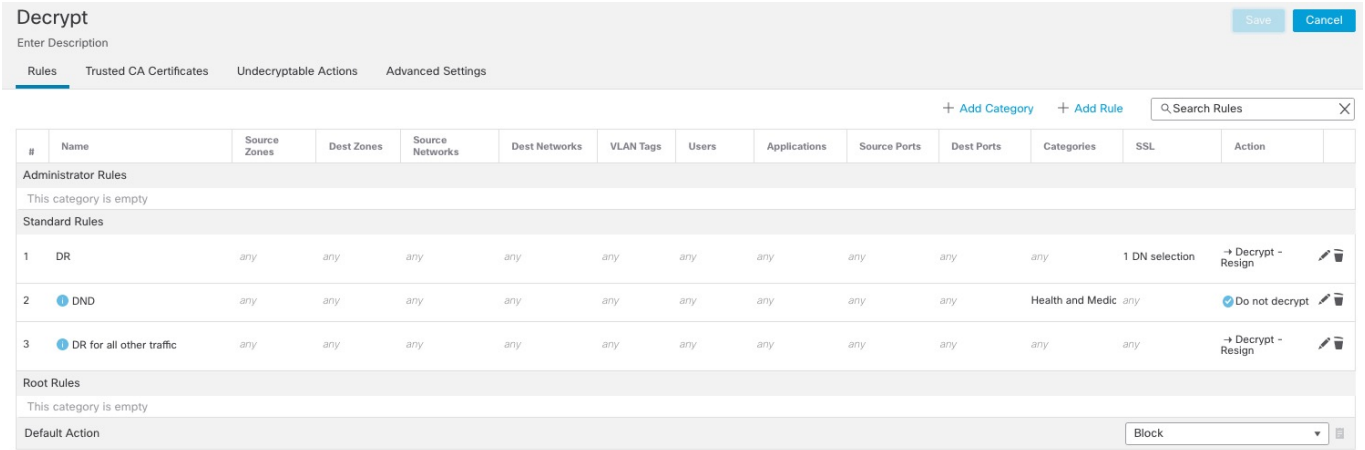
詳細については、「復号できないトラフィックのデフォルト処理オプション （2342 ページ）」を参照してください。

[復号しない（Do Not Decrypt）] ルールのカテゴリの制限

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。シスコでは、URL フィルタリングカテゴリの継続的な更新と改善に努めていますが、厳密に科学的なものではありません。一部の Web サイトはまったく分類されておらず、一部の Web サイトは不適切に分類されている可能性があります。

理由のないトラフィックの復号を避けるために、[復号しない（Do Not Decrypt）] ルールのカテゴリを過度に使用しないでください。たとえば、[健康と薬（Health and Medicine）] カテゴリには、患者のプライバシーを脅かさない WebMD の Web サイトが含まれています。

以下は、[健康と薬（Health and Medicine）] カテゴリの Web サイトの復号を防ぐ一方で、WebMD およびその他すべての復号を許可することができるサンプル復号ポリシーです。復号ルールに関する一般的な情報については、TLS/SSL 復号の使用上のガイドライン （2351 ページ）を参照してください。



（注） URL フィルタリングとアプリケーション検出を混同しないでください。アプリケーション検出は、Web サイトからのパケットの一部を読み取り、それが何であるか（Facebook メッセージや Salesforce など）をより具体的に判断することに依存します。詳細については、アプリケーション制御の設定のベストプラクティス （1732 ページ）を参照してください。

復号ルールのブロックアクション

システムを通過させないトラフィックに対して次の復号ルールアクションが用意されています。

- [ブロック（Block）] では、接続が終了するため、クライアント ブラウザにエラーが表示されます。

  エラーメッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

- [リセットしてブロック（Block with reset）] では、接続がリセットされるため、クライアント ブラウザにエラーが表示されます。

  このエラーでは、接続がリセットされたことはわかりますが、その理由はわかりません。

ヒント パッシブまたはインライン（タップモード）展開では、デバイスがトラフィックを直接検査しないため、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用できないことに注意してください。パッシブまたはインライン（タップモード）インターフェイスを含むセキュリティゾーン条件内で、[ブロック（Block）] または [リセットしてブロック（Block with reset）] アクションを使用したルールを作成すると、ポリシーエディタでルールの横に警告（⚠）が表示されます。

復号ルールの復号アクション

[復号 - 証明書の置き換え（Decrypt - Replace Cert）]、**[復号 - 既知のキー（Decrypt - Known Key）]**、および **[復号 - 再署名（Decrypt - Resign）]** アクションは、暗号化トラフィックを復号します。復号されたトラフィックは、アクセス制御を使用して検査されます。アクセスコントロールルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここではデータの確認に加えて、侵入、禁止ファイル、マルウェアを検出およびブロックできます。システムは、許可されたトラフィックを再暗号化してから宛先に渡します。

信頼できる認証局（CA） からの証明書を使用してトラフィックを復号することをお勧めします。これにより、**Invalid Issuer** が接続イベント内の SSL 証明書ステータス列に表示されないようにします。

信頼できるオブジェクトを追加する方法の詳細については、信頼できる認証局オブジェクト（1358 ページ）を参照してください。

関連項目：TLS 1.3 復号のベストプラクティス （2347 ページ）

関連トピック

TLS 1.3 復号のベストプラクティス （2347 ページ）

TLS/SSL ハードウェア アクセラレーションのモニター

次のトピックでは、TLS/SSL のステータスのモニター方法について説明します。

情報カウンタ

If a system under load is working well, you should see large counts for the following counters. Because there are 2 sides to the tracker process per connection, you can see these counters increase by 2 per connection. The PRIV_KEY_RECV and SECU_PARAM_RECV counters are the most important, and are highlighted. The CONTEXT_CREATED and CONTEXT_DESTROYED counters relate to the allocation of cryptographic chip memory.

```
> show counters
Protocol      Counter                          Value   Context
SSLENC        CONTEXT_CREATED                 258225   Summary
SSLENC        CONTEXT_DESTROYED               258225   Summary
TLS_TRK       OPEN_SERVER_SESSION             258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION             258225   Summary
TLS_TRK       UPSTREAM_CLOSE                  516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE                516450   Summary
TLS_TRK       FREE_SESSION                    516450   Summary
TLS_TRK       CACHE_FREE                      516450   Summary
TLS_TRK       PRIV_KEY_RECV                   258225   Summary
TLS_TRK       NO_KEY_ENABLE                   258225   Summary
TLS_TRK       SECU_PARAM_RECV                 516446   Summary
TLS_TRK       DECRYPTED_ALERT                 258222   Summary
TLS_TRK       DECRYPTED_APPLICATION         33568976   Summary
TLS_TRK       ALERT_RX_CNT                    258222   Summary
TLS_TRK       ALERT_RX_WARNING_ALERT          258222   Summary
TLS_TRK       ALERT_RX_CLOSE_NOTIFY           258222   Summary
TCP_PRX       OPEN_SESSION                    516450   Summary
TCP_PRX       FREE_SESSION                    516450   Summary
TCP_PRX       UPSTREAM_CLOSE                  516450   Summary
TCP_PRX       DOWNSTREAM_CLOSE                516450   Summary
TCP_PRX       FREE_CONN                       258222   Summary
TCP_PRX       SERVER_CLEAN_UP                 258222   Summary
TCP_PRX       CLIENT_CLEAN_UP                 258222   Summary
```

アラート カウンタ

We implemented the following counters according to the TLS 1.2 specification. FATAL or BAD alerts could indicate issues; however, ALERT_RX_CLOSE_NOTIFY is normal.

For details, see RFC 5246 section 7.2.

```
TLS_TRK      ALERT_RX_CNT                              311   Summary
TLS_TRK      ALERT_TX_CNT                                2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT                   2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT                   2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT                    308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                        3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                        2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY                     308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC                     2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC                     2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE                    1   Summary
```

エラー カウンタ

These counters indicate system errors. These counts should be low on a healthy system. The BY_PASS counters indicate packets that have been passed directly to or from the inspection engine (Snort) process (which runs in software) without decryption. The following example lists some of the bad counters.

Counters with a value of 0 are not displayed. To view a complete list of counters, use the command **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                          Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM             2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET           2   Summary
TLS_TRK      ENC_FAIL                            82   Summary
TLS_TRK      DEC_FAIL                           211   Summary
TLS_TRK      DEC_CKE_FAIL                     43194   Summary
TLS_TRK      ENC_CB_FAIL                       4335   Summary
TLS_TRK      DEC_CB_FAIL                        909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                    818   Summary
TLS_TRK      RECORD_PARSE_ERR                   123   Summary
TLS_TRK      IN_ERROR                         44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD            43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE               123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR           123   Summary
TLS_TRK      DECRYPT_FAIL                     43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                   127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                 127   Summary
```

重大カウンタ

The fatal counters indicate serious errors. These counters should be at or near 0 on a healthy system. The following example lists the fatal counters.

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

The RING_FULL counter is not a fatal counter, but indicates how often the system overloaded the cryptographic chip. The ACCELERATOR_RESET counter is the number of times the TLS 暗号化アクセラレーション process failed unexpectedly, which also causes the failure of pending operations, which

are the numbers you see in ACCELERATOR_CORE_TIMEOUT and RSA_PRIVATE_DECRYPT_FAILED.

If you have persistent problems, disable TLS 暗号化アクセラレーション (or **config hwCrypto disable**) and work with Cisco TAC to resolve the issues.

（注） You can do additional troubleshooting using the **show snort tls-offload** and **debug snort tls-offload** commands. Use the **clear snort tls-offload** command to reset the counters displayed in the **show snort tls-offload** command to zero.

復号ルール のトラブルシューティング

次のトピックでは、復号ルール のトラブルシューティングの方法について説明します。

TLS/SSL オーバーサブスクリプションについて

TLS/SSL オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS暗号化アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS暗号化アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、復号ポリシーの [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定に従います。

- デフォルト アクションを継承（Inherit default action）
- Do not decrypt
- Block
- Block with reset

復号ポリシー の [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定が [復号しない（Do Not decrypt）] で、関連付けられたアクセス コントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

TLS/SSL オーバーサブスクリプションのトラブルシューティング

管理対象デバイスで TLS 暗号化アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスに SSL オーバーサブスクリプションが発生しているかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] イベントを追加する必要があります。

始める前に

- [復号不可のアクション（Undecryptable Actions）] ページの [ハンドシェイクエラー（Handshake Error）] の設定を使用して、復号ポリシー を設定します。

  詳細については、復号できないトラフィックのデフォルト処理を設定する（2344 ページ）を参照してください。

- Secure Firewall Management Center と脅威防御管理ネットワーク管理ガイドの 復号ルール ルールでの復号可能な接続のロギングに関するセクションの説明に従い、SSL ルールのロギングを有効にします。

手順

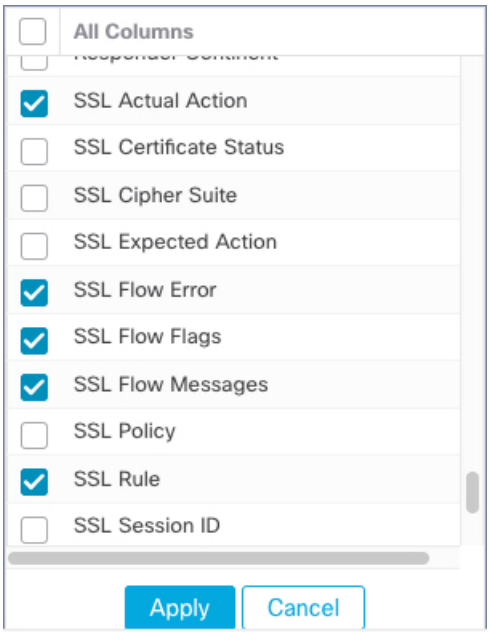
ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** の順にクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。

次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。（ダイアログボックスの [無効になったカラム（Disabled Columns）] セクションで確認。）



カラムは、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Connection and Security Intelligence Event Fields*」 で説明されている順序で追加されます。

ステップ 5 [適用（Apply）] をクリックします。
TLS/SSL オーバーサブスクライブは、[SSL Flow Flags] 列の `ERROR_EVENT_TRIGGERED` および `OVER_SUBSCRIBED` の値で示されます。

ステップ 6 TLS/SSL オーバーサブスクライブが発生している場合は、管理対象デバイスにログインして、次のコマンドのいずれかを入力します。

コマンド（Command）	結果
show counters	**TCP_PRX BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。
show snort tls-offload	**BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。

TLS ハートビートについて

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスは、TLS ハートビート エクステンションを使用するパケットを処理する場合、復号ポリシーの [復号不可のアクション（Undecryptable Actions）] の [復号エラー（Decryption Errors）] の設定で指定されているアクションを実行します。

- Block
- Block with reset

関連トピック

TLS ハートビートのトラブルシューティング （2394 ページ）

TLS ハートビートのトラブルシューティング

管理対象デバイスで TLS 暗号化アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスが TLS ハートビート エクステンションを使用してトラフィックを監視しているかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローメッセージ（SSL Flow Messages）] イベントを追加する必要があります。

始める前に

SSL ハートビートは、接続イベント テーブル ビューの [SSLフローメッセージ（SSL Flow Messages）] 列の `HEARTBEAT` の値で示されます。ネットワーク内のアプリケーションが SSL ハートビートを使用しているかどうかを確認するには、最初に次のタスクを実行します。

- [復号できないアクション（Undecryptable Actions）] ページの [復号エラー（Decryption Error）] の設定で、復号ポリシー を設定します。

  詳細については、復号できないトラフィックのデフォルト処理を設定する （2344 ページ）を参照してください。

- Secure Firewall Management Center と脅威防御管理ネットワーク管理の説明に従って、SSL ルールのログを有効にします。

手順

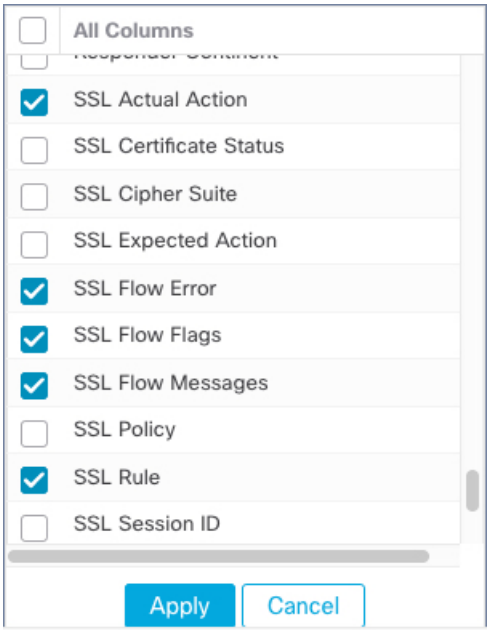
ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。

次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。



カラムは、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Connection and Security Intelligence Event Fields*」 で説明されている順序で追加されます。

ステップ 5 [適用（Apply）] をクリックします。
TLS ハートビートは、[SSLフローメッセージ（SSL Flow Messages）] 列の `HEARTBEAT` の値で示されます。

ステップ 6 ネットワーク上のアプリケーションで SSL ハートビートを使用する場合は、復号ルール の注意事項と制限事項 （2350 ページ）を参照してください。

TLS/SSL のピニングについて

一部のアプリケーションでは、アプリケーション自体に元のサーバー証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで 復号ルール を設定した場合は、アプ

リケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL ピニングが行われていることを確認するには、Facebook などのモバイル アプリケーションへのログインを試みます。ネットワーク接続エラーが表示された場合は、Web ブラウザを使用してログインします。（たとえば、Facebook のモバイル アプリケーションにログインすることはできませんが、Safari または Chrome を使用して Facebook にログインすることはできます）。Firepower Management Center の接続イベントは、TLS/SSL ピニングのさらなる証明として使用できます

（注） TLS/SSL ピニングはモバイル アプリケーションに限定されません。

ネットワーク上のアプリケーションでSSL ピン留めを使用する場合は、TLS/SSL 証明書のピン留めのガイドライン （2358 ページ）を参照してください。

関連トピック

TLS/SSL ピニングのトラブルシューティング （2396 ページ）

TLS/SSL ピニングのトラブルシューティング

デバイスで SSL ピニングが発生しているかどうかを確認するには、接続イベントを表示します。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を追加する必要があります。

始める前に

- Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの 復号ルールの復号可能な接続のログに関するセクションの説明に従い、復号ルールのログを有効にします。
- Facebook のようなモバイル アプリケーションにログインします。ネットワーク接続エラーが表示されたら、Chrome または Safari を使用して Facebook にログインします。Web ブラウザを使用してログインできても、ネイティブ アプリケーションではできない場合は、SSL ピニングが発生している可能性があります。

手順

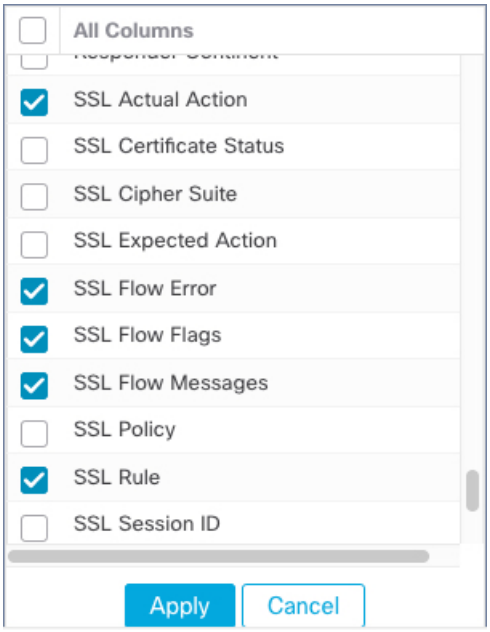
ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** の順にクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。

次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および[SSLルール（SSL Rule）]列を追加します。



列は、Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの「Connection and Security Intelligence Event Fields」 セクションで説明されている順序で追加されます。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 次に SSL ピニングの動作を特定する方法について説明します。

ステップ 7 ネットワーク内のアプリケーションでSSL ピニングが使用されていることを確認する場合は、復号ルール の注意事項と制限事項 （2350 ページ）を参照してください。

次のタスク

TLS/SSL 接続イベントを使用して、次のいずれかが表示されれば、TLS/SSL ピニングの発生を確認できます。

- クライアントがサーバーから SERVER_HELLO、SERVER_CERTIFICATE、SERVER_HELLO_DONE メッセージを受信した後に TCP Reset を受信すると、SSL ALERT メッセージを送信するアプリケーションの場合、次のように表示されます。（パケットキャプチャを使用すると、アラート `Unknown CA (48)` が表示される場合があります）。

- [SSLフローフラグ（SSL Flow Flags）] 列に ALERT_SEEN は表示されますが、APP_DATA_C2S や APP_DATA_S2C は表示されません。
- 管理対象デバイスでSSLハードウェア アクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_ALERT、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE が表示されます。
- 管理対象デバイスで SSL ハードウェア アクセラレーションがサポートされていないか、ハードウェアアクセラレーション機能が無効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE が表示されます。
- [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

- SSL ハンドシェイク終了後にアラートではなく TCP Reset を送信するアプリケーションの場合は、次のように表示されます。
  - [SSLフローフラグ（SSL Flow Flags）] 列に ALERT_SEEN、APP_DATA_C2S、APP_DATA_S2C は表示されません。
  - 管理対象デバイスでSSLハードウェア アクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED が表示されます。
  - 管理対象デバイスで SSL ハードウェア アクセラレーションがサポートされていないか、ハードウェアアクセラレーション機能が無効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED が表示されます。
  - [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

関連トピック

不明または不正な証明書または認証局のトラブルシュート （2398 ページ）

不明または不正な証明書または認証局のトラブルシュート

接続イベントを表示して、デバイスに不明な認証局、不正な証明書、または不明な証明書があるかどうかを判断できます。この手順は、TLS/SSL 証明書がピン留めされている場合にも使用できます。接続イベントテーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を追加する必要があります。

始める前に

- 復号ルールを設定します。
- Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの 復号ルールの復号可能な接続のログに関するセクションの説明に従い、復号ルールのログを有効にします。

手順

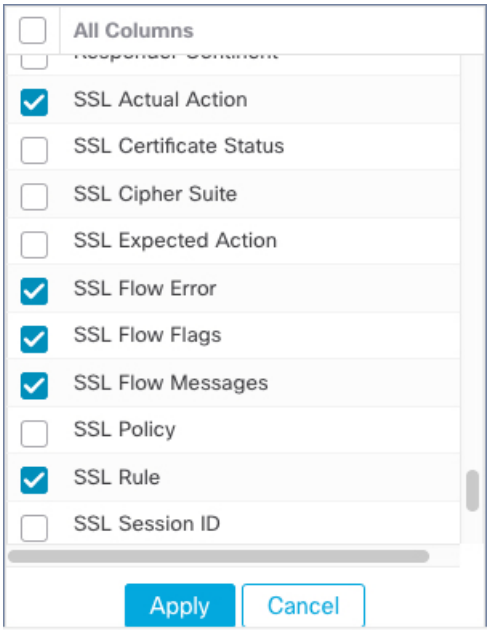
ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** の順にクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。

次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および[SSLルール（SSL Rule）] 列を追加します。



列は、Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの「Connection and Security Intelligence Event Fields」 セクションで説明されている順序で追加されます。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 次の表は、証明書または認証局が不正か、または欠落しているかを判断する方法を説明しています。

SSL フローフラグ	意味
CLIENT_ALERT_SEEN_UNKNOWN_CA	有効な証明書チェーンまたは部分的なチェーンが SSL クライアントアプリケーションによって受信されましたが、CA 証明書が見つからなかったか、既知の信頼できる CA と一致しなかったため、証明書が受け入れられなかったことを示しています。このメッセージは、常に回復不能なエラーを示しています。
CLIENT_ALERT_SEEN_BAD_CERTIFICATE	証明書が破損しているか、正しく検証されていない署名が含まれているか、またはその他の問題がありました。
CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN	証明書の処理中に他の（詳細不明の）問題が発生し、受け入れられなくなりました。

TLS/SSL 暗号スイートの確認

始める前に

このトピックでは、暗号スイートの条件を持つ復号ルールを保存する際に次のエラーが表示された場合に実行する必要があるアクションについて説明します。

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature
algorithm that matches the resigning CA's signature algorithm
```

このエラーは、復号ルールの条件として選択した 1 つ以上の暗号スイートが復号ルールに使用されている証明書と互換性がないことを示しています。この問題を解決するには、使用している証明書へのアクセス権が必要です。

（注） このトピックでのタスクには、TLS/SSL 暗号化がどのように機能するかの知識が必要です。

手順

ステップ 1 指定した暗号スイートで**[復号 - 再署名（Decrypt - Resign）]**、**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、または **[復号 - 既知のキー（Known Key）]** のいずれかを持つ 復号ルール ルールを保存しようとすると、次のエラーが表示されます。

例：

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

ステップ 2 トラフィックの復号に使用している証明書を見つけ、必要に応じて、openssl コマンドを実行できるシステムにその総名所をコピーします。

ステップ 3 次のコマンドを実行し、証明書で使用されている署名アルゴリズムを表示します。

openssl x509 -in *CertificateName* **-text -noout**

出力の最初に次のような数行が表示されます。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

ステップ 4 **Signature algorithm** によって次が通知されます。

- 使用されている暗号化関数（前の例では、**ECDSA** は楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）を意味します）。
- 暗号化されたメッセージのダイジェストの作成に使用されたハッシュ関数（前の例では **SHA256**）。

ステップ 5 それらの値に一致する暗号スイーツのリソース（*OpenSSL at University of Utah* など）を検索します。暗号スイートは RFC 形式である必要があります。
また、その他のさまざまなサイト（Mozilla wiki の Server Side TLS や RFC 5246 の Appendix C など）も検索できます。マイクロソフトのドキュメントの Cipher Suites in TLS/SSL（Schannel SSP）[英語] には、暗号スイーツの詳細な説明があります。

ステップ 6 必要に応じて、OpenSSL 名を Firepower Management システムが使用している RFC 名に変換します。
`https://testssl.sh` サイトの『RFC mapping list』を参照してください。

ステップ 7 前の例の **ecdsa-with-SHA256** では、Mozilla wiki で『Modern Compatibility List』を参照できます。

a) 名前に **ECDSA** または **SHA-256** を持つ暗号スイートのみを選択します。これらの暗号スイートは次のように動作します。

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) 対応する RFC 暗号スイートを RFC マッピング リストで検索します。これらの暗号スイートは次のように動作します。

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

ステップ 8 前述の暗号スイートを復号ルールに追加します。

第 63 章

復号ルールとポリシーの例

この章は、このガイドで説明されている概念に基づいて作成されており、ベストプラクティスおよび推奨事項に従う 復号ルール を使用した SSL ポリシーの特定の例を提供します。この例を実際の状況に当てはめ、組織のニーズに合わせて調整してください。

要約すると、次のようになります。

- 信頼できるトラフィック（圧縮された大規模なサーバーバックアップの転送など）の場合は、事前フィルタ処理とフローオフロードを使用して、検査を完全にバイパスします。
- 特定の IP アドレスに適用されるものなど、迅速に評価できる復号ルールを、「最初」に配置します。
- 処理（[復号-再署名（Decrypt - Resign）]）を必要とする 復号ルール と、安全ではないプロトコルバージョンおよび暗号スイートをブロックするルールを「最後」に配置します。

- 復号ルール ベスト プラクティス （2403 ページ）
- 推奨ポリシーとルールの設定 （2407 ページ）
- 復号ポリシーのウォークスルー （2412 ページ）

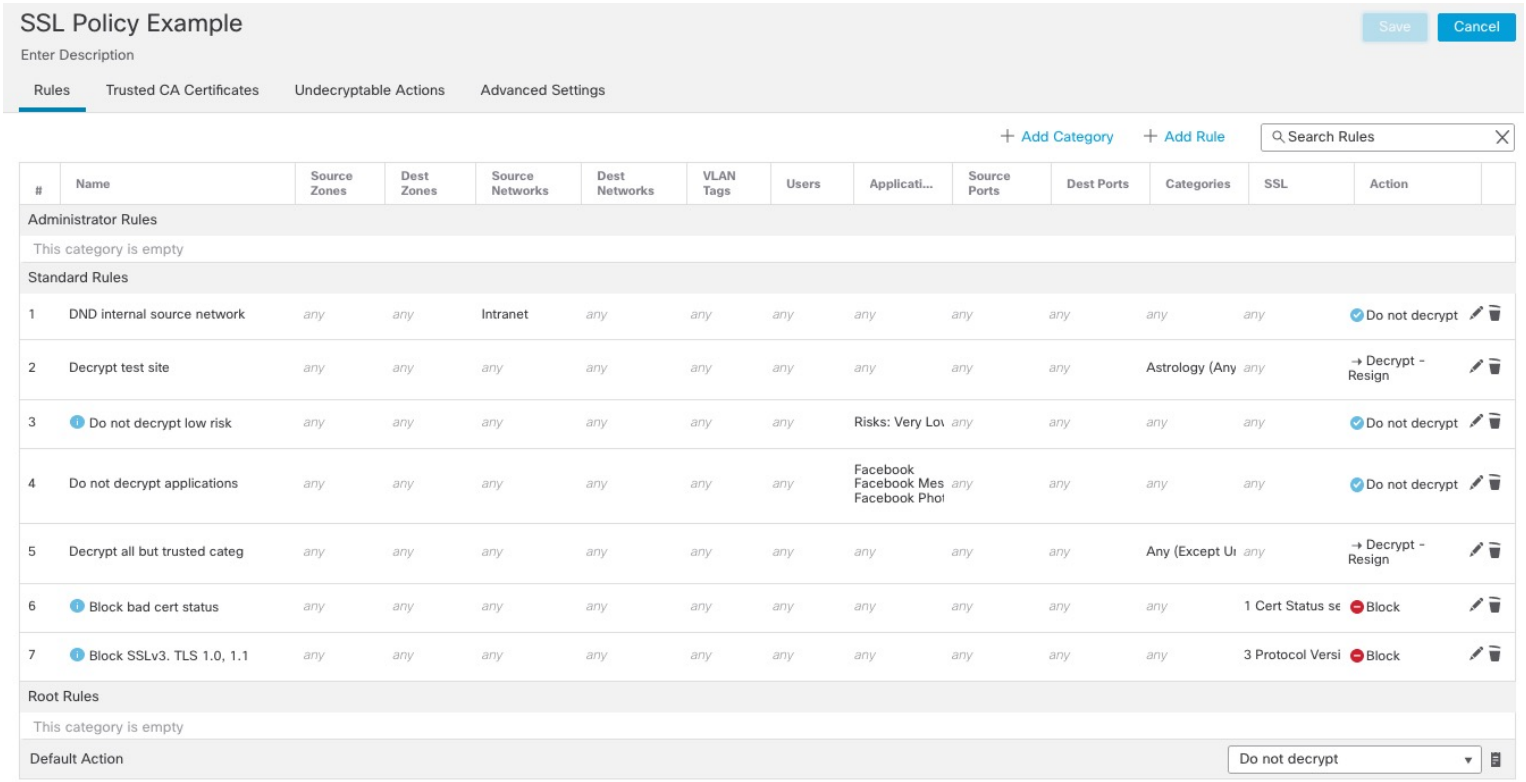
復号ルール ベスト プラクティス

この章では、復号ルール を持つ 復号ポリシー の例を示し、シスコのベストプラクティスと推奨事項について説明します。まず、復号ポリシー とアクセス コントロール ポリシーの設定について説明し、次にすべてのルール、および特定の方法でルールを順序付けすることを推奨する理由について説明します。

一般的なガイドライン

- トラフィックの復号には、処理とメモリが必要です。トラフィックを過剰に復号すると、パフォーマンスに影響を与える可能性があります。復号ポリシーとルールを設定する前に、トラフィックを復号する場合としない場合 （2308 ページ）。
- 復号から除外する必要があるトラフィックの中には、性質上復号不可能なトラフィックがあります。通常、復号不可能なトラフィックはTLS/SSL証明書ピンニングを使用しています。。

以下は、この章で説明する 復号ルールです。



プレフィルタとフローオフロードによる検査のバイパス

プレフィルタはアクセス制御の最初のフェーズで、システムがより大きいリソース消費の評価を実行する前に行われます。プレフィルタリングはシンプルかつ高速で、初期に実行されます。プレフィルタリングでは、限定された外部ヘッダーを基準にしてトラフィックを迅速に処理します。内部ヘッダーを使用し、より堅牢なインスペクション機能を備えた後続の評価とこのプレフィルタリングを比較します。

次の目的でプレフィルタリングを設定します。

- パフォーマンスの向上：インスペクションを必要としないトラフィックの除外は、早ければ早いほど適切です。特定のタイプのプレーン テキストをファストパスまたはブロックし、カプセル化された接続を検査することなく外側のカプセル化ヘッダーに基づいてトンネルをパススルーします。早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。
- カプセル化トラフィックに合わせたディープインスペクションの調整：同じ検査基準を使用してカプセル化接続を後で処理できるように、特定のタイプのトンネルを再区分できます。アクセス制御はプレフィルタ後に内側のヘッダーを使用するため、再区分は必須です。

Firepower 4100/9300 または Secure Firewall 3100 が使用可能な場合は、大規模なフローオフロードを使用できます。フローオフロードは、信頼できるトラフィックに検査エンジンをバイパスさせてパフォーマンスを向上させる手法です。たとえば、データセンターでサーバーのバックアップを転送するために使用できます。

関連トピック

大規模フローのオフロード （1914 ページ）
プレフィルタリングとアクセス コントロール （1894 ページ）
Fastpath プレフィルタリングのベストプラクティス （1897 ページ）

[復号しない（Do Not Decrypt）] のベストプラクティス

評価期間中のトラフィックのロギング

通常、[復号しない（Do Not Decrypt）] ルールではロギングを無効化にする必要がありますが、ルールに一致するトラフィックが不明な場合は、ロギングを一時的に有効にすることができます。正しいトラフィックが一致していることを確認したら、それらのルールのロギングを無効にします。

復号できないトラフィックのガイドライン

Web サイト自体が復号できない、または Web サイトで TLS/SSL ピン留めが使用されている場合、特定のトラフィックを復号できないと判断できます。SSL ピン留めでは、ブラウザにエラーが表示されることなく、復号されたサイトへのユーザーアクセスが効果的に阻止されます。

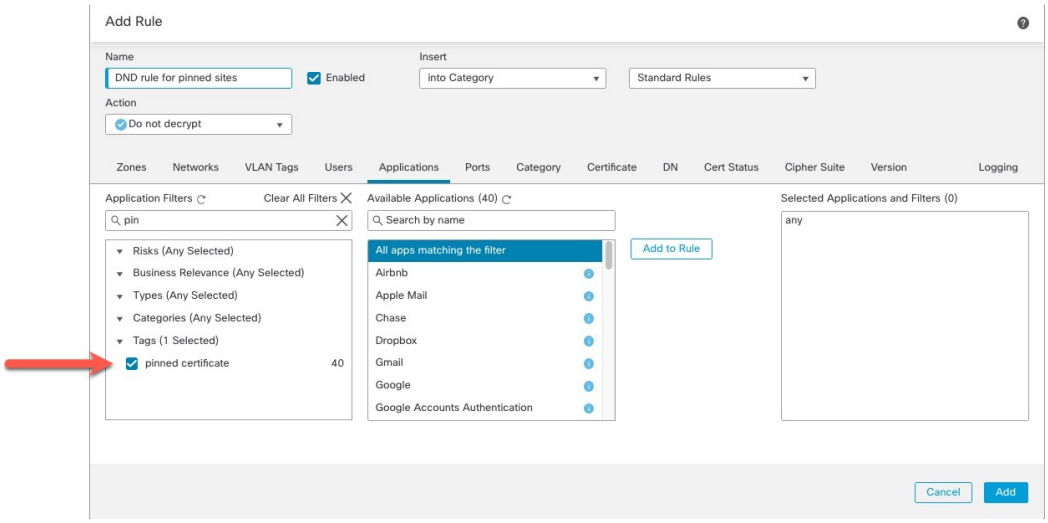
証明書のピン留めの詳細については、TLS/SSL のピニングについて （2395 ページ）を参照してください。

そのようなサイトのリストは次のように管理されています。

- **Cisco-Undecryptable-Sites** という名前の識別名（DN）グループ
- **ピン留めされた証明書**または**復号不可**のアプリケーションフィルタ

トラフィックを復号しており、ユーザーが復号されたサイトにアクセスしたときにブラウザにエラーが表示されないようにする場合は、復号ルールの下部に [復号しない（Do Not Decrypt）] ルールを設定することを推奨します。

ピン留めされた証明書のアプリケーションフィルタの設定例を次に示します。



[復号-再署名（Decrypt - Resign）] と [復号-既知のキー（Decrypt - Known Key）] のベストプラクティス

このトピックでは、[復号-再署名（Decrypt - Resign）] と [復号-既知のキー（Decrypt - Known Key）] のベストプラクティスについて説明します。復号ルール

バージョンまたは暗号スイートのルール条件を使用しない

重要 **[復号 - 再署名（Decrypt - Resign）]**、**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、または **[復号 - 既知のキー（Decrypt - Known Key）]** ルール アクションを含むルールでは、**[暗号スイート（Cipher Suite）]** または **[バージョン（Version）]** ルール条件を決して使用しないでください。これらの条件をルールで他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

[復号 - 再署名（Decrypt - Resign）] の証明書のピン留めによるベストプラクティス

一部のアプリケーションでは、アプリケーション自体に元のサーバー証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで 復号ルール を設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL のピン留めは中間者攻撃を避けるために使用されるため、防止または回避する方法はありません。ピニングトラフィックが復号対象から除外されるように、[復号 - 再署名（Decrypt - Resign）] ルールの前に [復号しない（Do Not Decrypt）] ルールを追加することを推奨します。

証明書のピン留めの詳細については、『*Cisco Secure Firewall Management Center* デバイス設定ガイド』の TLS/SSL のピニングについて （2395 ページ）

[復号 - 既知のキー（Decrypt - Known Key）] のベストプラクティス

[復号 - 既知のキー（Decrypt - Known Key）] ルールアクションは、内部サーバーに向かうトラフィックに使用するアクションであるため、常に 復号 ルール（[ネットワーク（Networks）] ルール条件）に宛先ネットワークを追加するか、アクセスコントロールルール（[ゾーン（Zones）] タブページ）にセキュリティゾーンを追加する必要があります。その結果、サーバーが配置されているネットワークまたはインターフェイスにトラフィックが直接送信され、ネットワーク上のトラフィックが減少します。

最初に配置する 復号ルール

パケットの最初の部分に一致するルールを最初に配置します。例として、IPアドレスを参照するルール（[ネットワーク（Networks）] ルール条件）があります。

最後に配置する 復号ルール

次のルール条件を持つルールは最後に配置する必要があります。そのようなルールの場合、システムでトラフィックを長時間検査する必要があるためです。

- アプリケーション
- カテゴリ
- 証明書
- 識別名（DN）
- 証明書ステータス
- 暗号スイート
- バージョン

推奨ポリシーとルールの設定

推奨のポリシー設定は次のとおりです。

- 復号ポリシー：
  - デフォルトアクションは [復号しない（Do Not Decrypt）] です。
  - ロギングをイネーブルにします。
  - [SSL v2セッション（SSL v2 Session）] と [圧縮されたセッション（Compressed Session）] の両方で、[復号不可のアクション（Undecryptable Actions）] を [ブロック（Block）] に設定します。
  - ポリシーの詳細設定で TLS 1.3 復号とを有効にします。

- 復号ルール：[復号しない（Do Not Decrypt）] ルールアクションが使用されるルールを除く、すべてのルールのロギングを有効にします。（これは任意です。復号されていないトラフィックに関する情報を表示する場合は、そのルールのロギングも有効にします。）
- アクセス コントロール ポリシー：
  - 復号ポリシー をアクセス コントロール ポリシーに関連付けます（関連付けをしないと、復号ポリシーとルールは機能しません）。
  - デフォルトのポリシーアクションを [侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] に設定します。
  - ロギングをイネーブルにします。

関連トピック

復号ポリシー の設定 （2409 ページ）
復号ルール の設定 （2427 ページ）
アクセス コントロール ポリシーの設定 （2411 ページ）

推奨ポリシーとルールの設定

推奨のポリシー設定は次のとおりです。

- 復号ポリシー：
  - デフォルトアクションは [復号しない（Do Not Decrypt）] です。
  - ロギングをイネーブルにします。
  - [SSL v2セッション（SSL v2 Session）] と [圧縮されたセッション（Compressed Session）] の両方で、[復号不可のアクション（Undecryptable Actions）] を [ブロック（Block）] に設定します。
  - ポリシーの詳細設定で TLS 1.3 復号とを有効にします。
- 復号ルール：[復号しない（Do Not Decrypt）] ルールアクションが使用されるルールを除く、すべてのルールのロギングを有効にします。（これは任意です。復号されていないトラフィックに関する情報を表示する場合は、そのルールのロギングも有効にします。）
- アクセス コントロール ポリシー：
  - 復号ポリシー をアクセス コントロール ポリシーに関連付けます（関連付けをしないと、復号ポリシーとルールは機能しません）。
  - デフォルトのポリシーアクションを [侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] に設定します。
  - ロギングをイネーブルにします。

関連トピック

復号ポリシー の設定 （2409 ページ）
復号ルール の設定 （2427 ページ）
アクセス コントロール ポリシーの設定 （2411 ページ）

復号ポリシー の設定

復号ポリシー に推奨される次のベストプラクティス設定の設定方法。

- デフォルトアクションは [復号しない（Do Not Decrypt）] です。
- ロギングをイネーブルにします。
- [SSL v2セッション（SSL v2 Session）] と [圧縮されたセッション（Compressed Session）] の両方で、[復号不可のアクション（Undecryptable Actions）] を [ブロック（Block）] に設定します。
- ポリシーの詳細設定で TLS 1.3 復号とを有効にします。

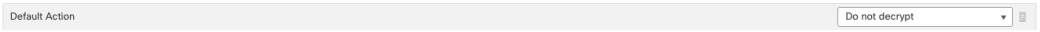
手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]** をクリックします。

ステップ 3 復号ポリシー の横にある [編集（Edit）]（ ） をクリックします。

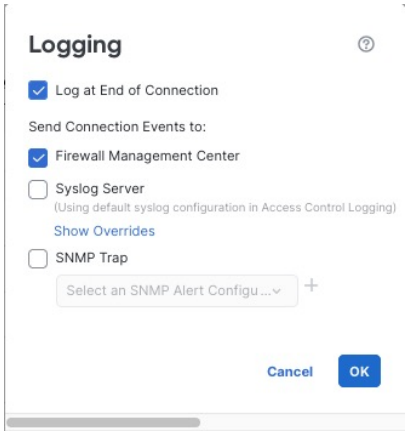
ステップ 4 ページの下部にある [デフォルトのアクション（Default Action）] リストから、[復号しない（Do Not Decrypt）] をクリックします。
次の図は例を示しています。



ステップ 5 行の最後で、[ロギング（Logging）]（ ） をクリックします。

ステップ 6 [接続の終了時にロギングする（Log at End of Connection）] チェックボックスをオンにします。

次の図は例を示しています。



ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

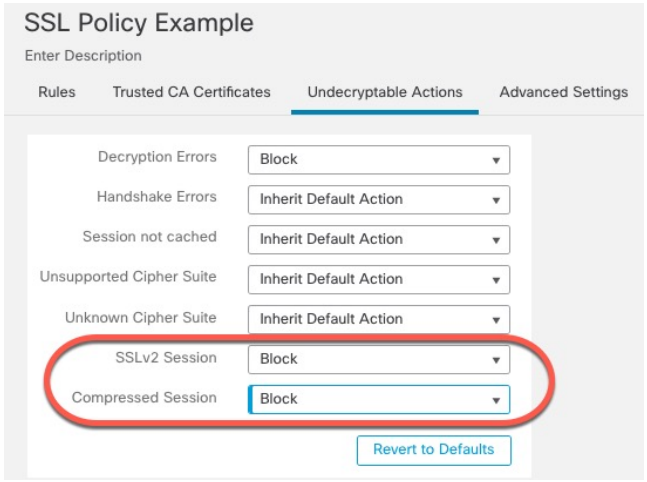
ステップ 9 [復号不可のアクション（Undecryptable Actions）] タブをクリックします。

ステップ 10 [SSLv2セッション（SSLv2 Session）] と [圧縮セッション（Compressed Session）] のアクションは [ブロック（Block）] に設定することを推奨します。

ネットワークで SSLv2 を許可しないでください。圧縮された TLS/SSL トラフィックはサポートされていないためブロックする必要があります。

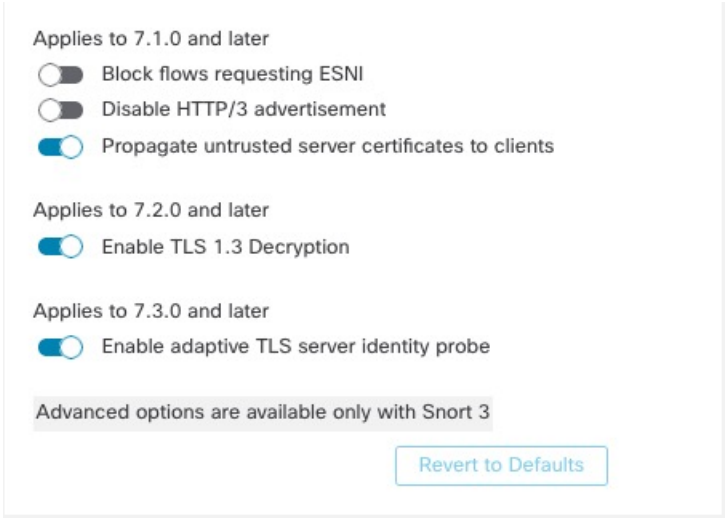
各オプションの設定について詳しくは、復号できないトラフィックのデフォルト処理オプション （2342 ページ）」を参照してください。

次の図は例を示しています。



ステップ 11 [詳細設定（Advanced Settings）] タブページをクリックします。

ステップ 12 [TLS 1.3復号の有効化（Enable TLS 1.3 Decryption）] チェックボックスをオンにします。他のオプションの詳細については、復号ポリシーの詳細オプション （2345 ページ）



ステップ 13 ページの上部にある [保存（Save）] をクリックします。

次のタスク

復号ルールの設定 （2427ページ） の説明に従い、復号ルールを設定し、各ルールを設定します。

アクセス コントロール ポリシーの設定

アクセス コントロール ポリシーに推奨される次のベストプラクティス設定の設定方法：

- 復号ポリシー をアクセス コントロール ポリシーに関連付けます（関連付けをしないと、復号ポリシーとルールは機能しません）。
- デフォルトのポリシーアクションを [侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] に設定します。
- ロギングをイネーブルにします。

手順

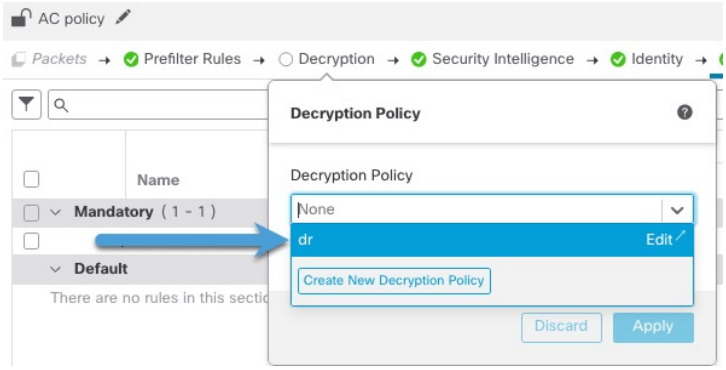
ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** をクリックします。

ステップ 3 アクセス コントロール ポリシーの横にある [編集（Edit）]（✎） をクリックします

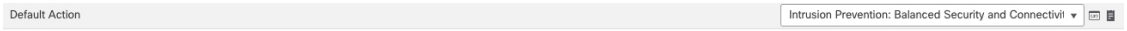
ステップ 4 （復号ポリシーがまだ設定されていない場合は、後で設定できます）。

a) 次の図に示すように、ページの上部にある [復号（Decryption）] リンクをクリックします。



b) リストから、有効にする復号ポリシーの名前をクリックします
c) [Apply] をクリックします。
d) ページの上部にある [保存（Save）] をクリックします。

ステップ 5 ページの下部にある [Default Action（デフォルトアクション）] リストで、[侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] をクリックします。
次の図は例を示しています。



ステップ 6 **ロギング**（ ） をクリックします。

ステップ 7 [接続の終了時にロギングする（Log at End of Connection）] チェックボックスをオンにして、[OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

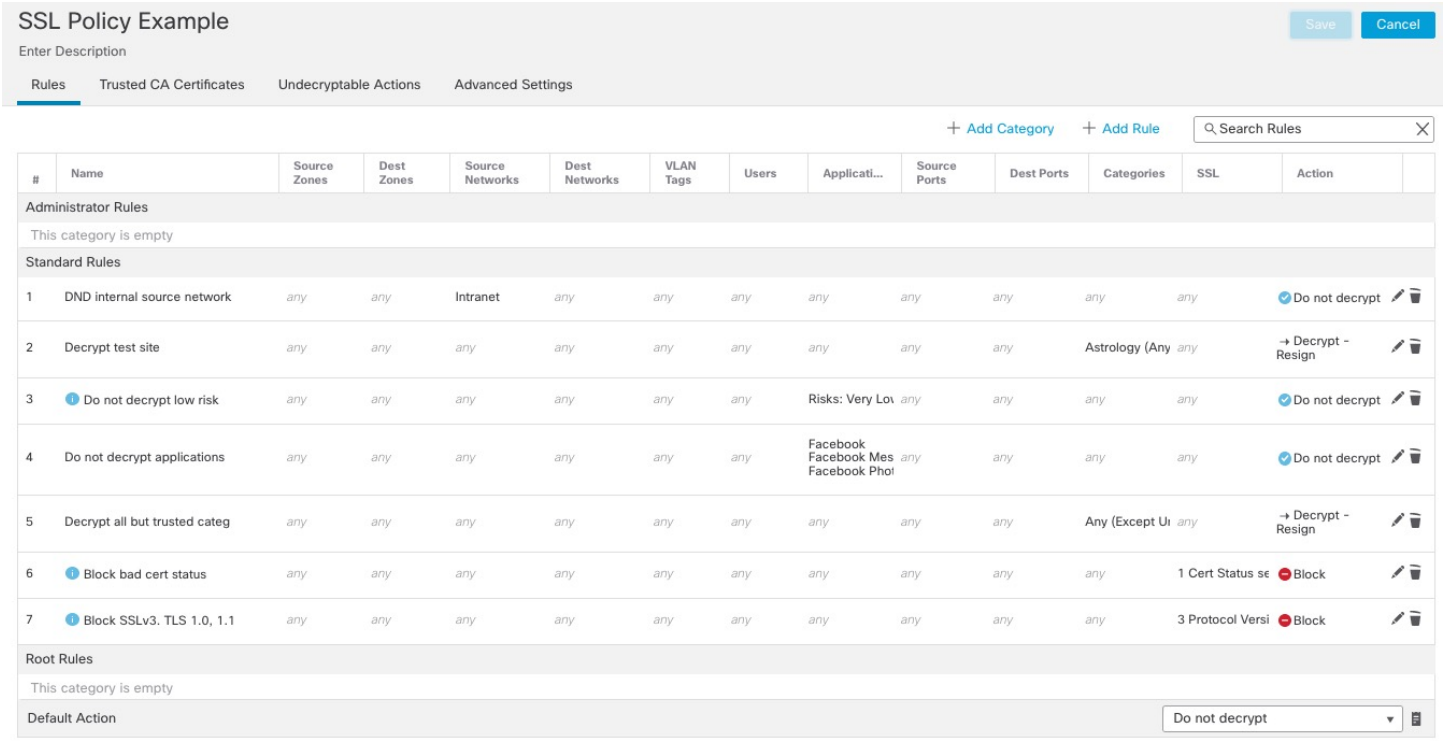
次のタスク

「復号ルール 例 （2417 ページ）」を参照してください。

復号ポリシーのウォークスルー

この章では、ベストプラクティスを採用するルールを使用する復号ポリシーを作成する方法について、段階的な説明とウォークスルーを示します。復号ポリシーのプレビューに続いてベストプラクティスの概要を示し、最後にポリシーのルールについて説明します。

以下は、この章で説明する復号ポリシーです。



詳細については、次の項を参照してください。

関連トピック

推奨ポリシーとルールの設定 （2407 ページ）
プレフィルタするトラフィック （2418 ページ）
（2418 ページ）
：特定のトラフィックを復号する （2418 ページ）
カテゴリの [復号-再署名（Decrypt - Resign）] ルールの作成 （2420 ページ）
低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない（2419ページ）
復号ルール：証明書とプロトコルバージョンをブロックまたは監視する （2421 ページ）

推奨ポリシーとルールの設定

推奨のポリシー設定は次のとおりです。

- 復号ポリシー：
  - デフォルトアクションは [復号しない（Do Not Decrypt）] です。
  - ロギングをイネーブルにします。
  - [SSL v2セッション（SSL v2 Session）] と [圧縮されたセッション（Compressed Session）] の両方で、[復号不可のアクション（Undecryptable Actions）] を [ブロック（Block）] に設定します。

- ポリシーの詳細設定で TLS 1.3 復号とを有効にします。

- 復号ルール：[復号しない（Do Not Decrypt）] ルールアクションが使用されるルールを除く、すべてのルールのロギングを有効にします。（これは任意です。復号されていないトラフィックに関する情報を表示する場合は、そのルールのロギングも有効にします。）
- アクセス コントロール ポリシー：
  - 復号ポリシー をアクセス コントロール ポリシーに関連付けます（関連付けをしないと、復号ポリシーとルールは機能しません）。
  - デフォルトのポリシーアクションを [侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] に設定します。
  - ロギングをイネーブルにします。

関連トピック

復号ポリシー の設定 （2409 ページ）
復号ルール の設定 （2427 ページ）
アクセス コントロール ポリシーの設定 （2411 ページ）

復号ポリシー の設定

復号ポリシー に推奨される次のベストプラクティス設定の設定方法。

- デフォルトアクションは [復号しない（Do Not Decrypt）] です。
- ロギングをイネーブルにします。
- [SSL v2セッション（SSL v2 Session）] と [圧縮されたセッション（Compressed Session）] の両方で、[復号不可のアクション（Undecryptable Actions）] を [ブロック（Block）] に設定します。
- ポリシーの詳細設定で TLS 1.3 復号とを有効にします。

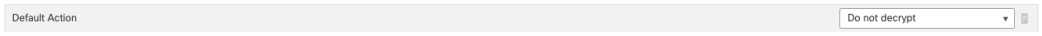
手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]** をクリックします。

ステップ 3 復号ポリシー の横にある [編集（Edit）]（✎） をクリックします。

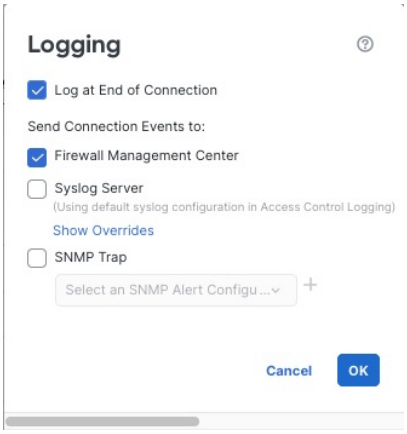
ステップ 4 ページの下部にある [デフォルトのアクション（Default Action）] リストから、[復号しない（Do Not Decrypt）] をクリックします。
次の図は例を示しています。



ステップ 5 行の最後で、[ロギング（Logging）]（ ）をクリックします。

ステップ 6 [接続の終了時にロギングする（Log at End of Connection）]チェックボックスをオンにします。

次の図は例を示しています。



ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

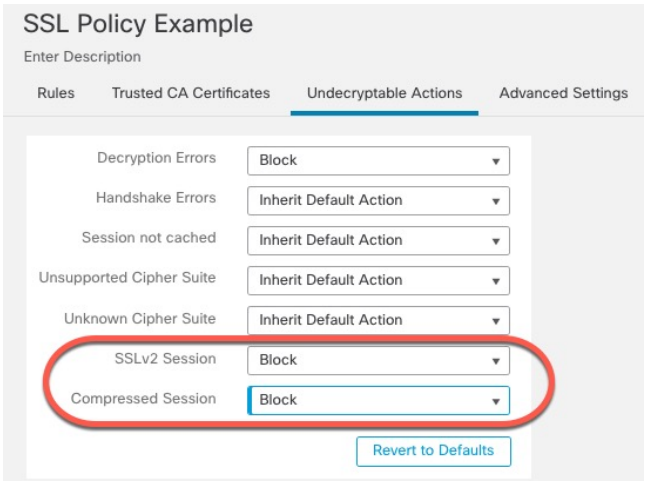
ステップ 9 [復号不可のアクション（Undecryptable Actions）] タブをクリックします。

ステップ 10 [SSLv2セッション（SSLv2 Session）] と [圧縮セッション（Compressed Session）] のアクションは [ブロック（Block）] に設定することを推奨します。

ネットワークで SSLv2 を許可しないでください。圧縮された TLS/SSL トラフィックはサポートされていないためブロックする必要があります。

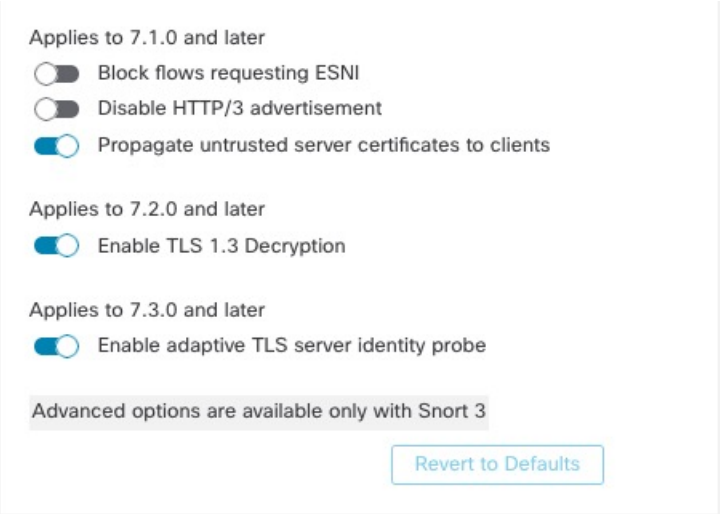
各オプションの設定について詳しくは、復号できないトラフィックのデフォルト処理オプション （2342 ページ）」を参照してください。

次の図は例を示しています。



ステップ 11 [詳細設定（Advanced Settings）] タブページをクリックします。

ステップ 12 [TLS 1.3復号の有効化（Enable TLS 1.3 Decryption）] チェックボックスをオンにします。他のオプションの詳細については、復号ポリシーの詳細オプション （2345 ページ）



ステップ 13 ページの上部にある [保存（Save）] をクリックします。

次のタスク

復号ルールの設定 （2427ページ） の説明に従い、復号ルールを設定し、各ルールを設定します。

アクセス コントロール ポリシーの設定

アクセス コントロール ポリシーに推奨される次のベストプラクティス設定の設定方法：

- 復号ポリシー をアクセス コントロール ポリシーに関連付けます（関連付けをしないと、復号ポリシーとルールは機能しません）。
- デフォルトのポリシーアクションを [侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] に設定します。
- ロギングをイネーブルにします。

手順

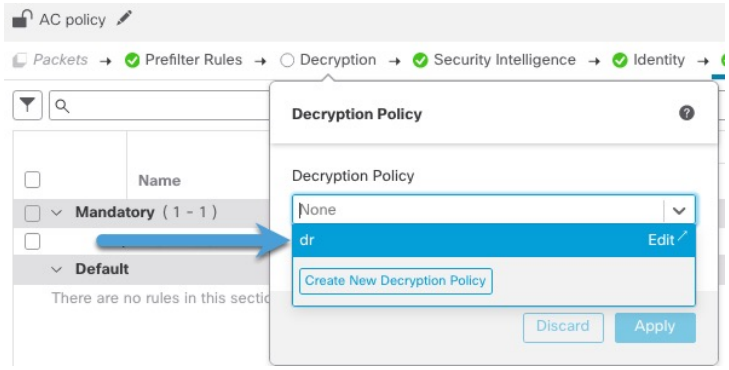
ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** をクリックします。

ステップ 3 アクセス コントロール ポリシーの横にある [編集（Edit）]（✎） をクリックします

ステップ 4 （復号ポリシーがまだ設定されていない場合は、後で設定できます）。

a) 次の図に示すように、ページの上部にある [復号（Decryption）] リンクをクリックします。

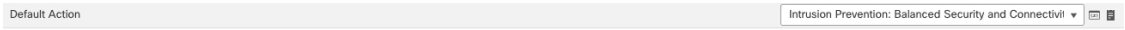


b) リストから、有効にする復号ポリシーの名前をクリックします

c) [Apply] をクリックします。

d) ページの上部にある [保存（Save）] をクリックします。

ステップ 5 ページの下部にある [Default Action（デフォルトアクション）] リストで、[侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] をクリックします。
次の図は例を示しています。



ステップ 6 **ロギング**（ ） をクリックします。

ステップ 7 [接続の終了時にロギングする（Log at End of Connection）] チェックボックスをオンにして、[OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

「復号ルール 例 （2417 ページ）」を参照してください。

復号ルール 例

このセクションでは、復号ルールの例を示し、シスコのベストプラクティスについて説明します。

詳細については、次の項を参照してください。

関連トピック

プレフィルタするトラフィック （2418 ページ）
（2418 ページ）
：特定のトラフィックを復号する （2418 ページ）
低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない（2419ページ）

カテゴリの [復号-再署名（Decrypt - Resign）] ルールの作成 （2420 ページ）
復号ルール：証明書とプロトコルバージョンをブロックまたは監視する （2421 ページ）

プレフィルタするトラフィック

プレフィルタリングはアクセス制御の最初のフェーズで、よりリソース消費の大きい評価を実行する前に行われます。プレフィルタリングは、内部ヘッダーを使用した、より堅牢なインスペクション機能を備えた後続の評価と比較すると、シンプルかつ高速で、初期に実行されます。

プレフィルタリングは、セキュリティのニーズとトラフィックプロファイルに基づいて検討する必要があるため、以下を対象とするポリシーとインスペクションから除外する必要があります。

- Microsoft Outlook 365 などの一般的な社内アプリケーション
- サーバーバックアップなどのエレファントフロー

関連トピック

プレフィルタリングとアクセス コントロール （1894 ページ）
Fastpath プレフィルタリングのベストプラクティス （1897 ページ）

例の最初の復号ルールでは、内部ネットワーク（**intranet** として定義）に向かうトラフィックは復号されません。[復号しない（Do Not Decrypt）] ルールアクションは、ClientHello 中に一致するため、非常に高速に処理されます。

（注） 内部 DNS サーバーから内部 DNS リゾルバ（Cisco Umbrella 仮想アプライアンスなど）に向かうトラフィックがある場合は、それらのトラフィックにも [復号しない（Do Not Decrypt）] ルールを追加できます。内部 DNS サーバーで独自のログが記録される場合、それらをプレフィルタリングポリシーに追加することもできます。

ただし、インターネットルートサーバー（たとえば、Active Directory に組み込まれた Microsoft 内部 DNS リゾルバ）など、インターネットに向かう DNS トラフィックには、[復号しない（Do Not Decrypt）] ルールやプレフィルタリングを使用しないことを強く推奨します。そのような場合は、トラフィックを完全に検査するか、ブロックすることを検討する必要があります。

ルールの詳細：

：特定のトラフィックを復号する

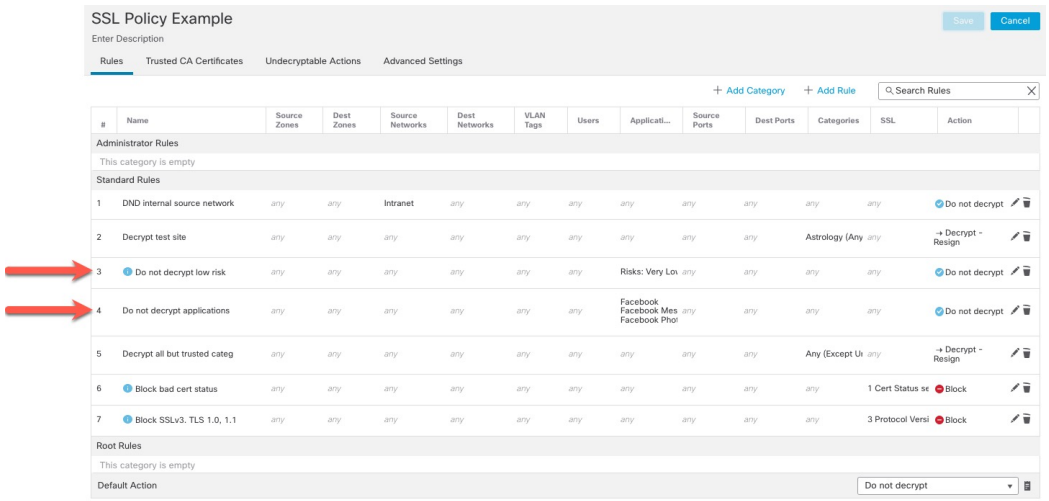
この例では、次のルールはオプションです。このルールは、限られたタイプのトラフィックを復号および監視してから、ネットワーク上で許可するか判断する場合に使用します。

ルールの詳細：

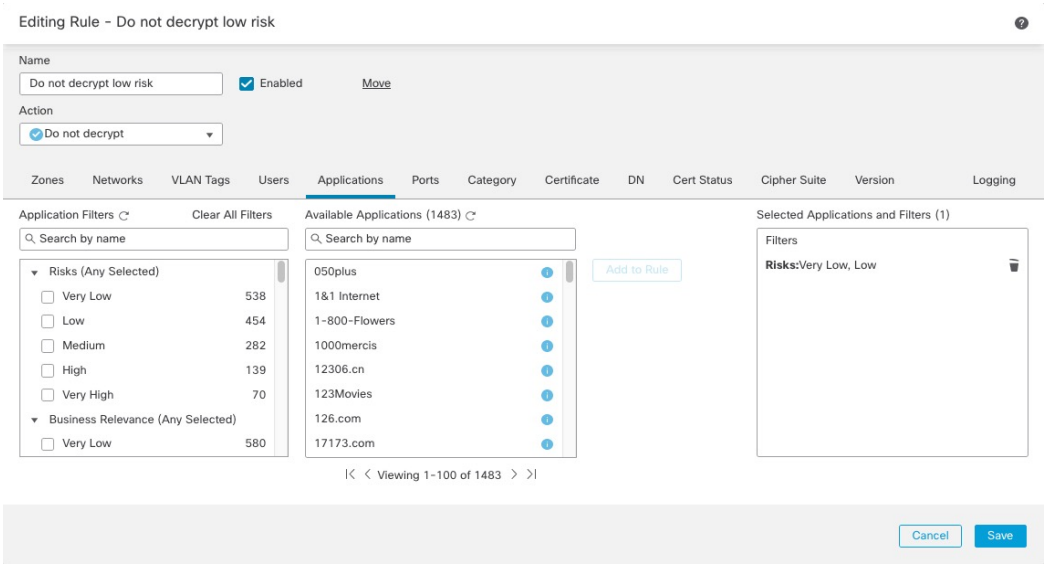
低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない

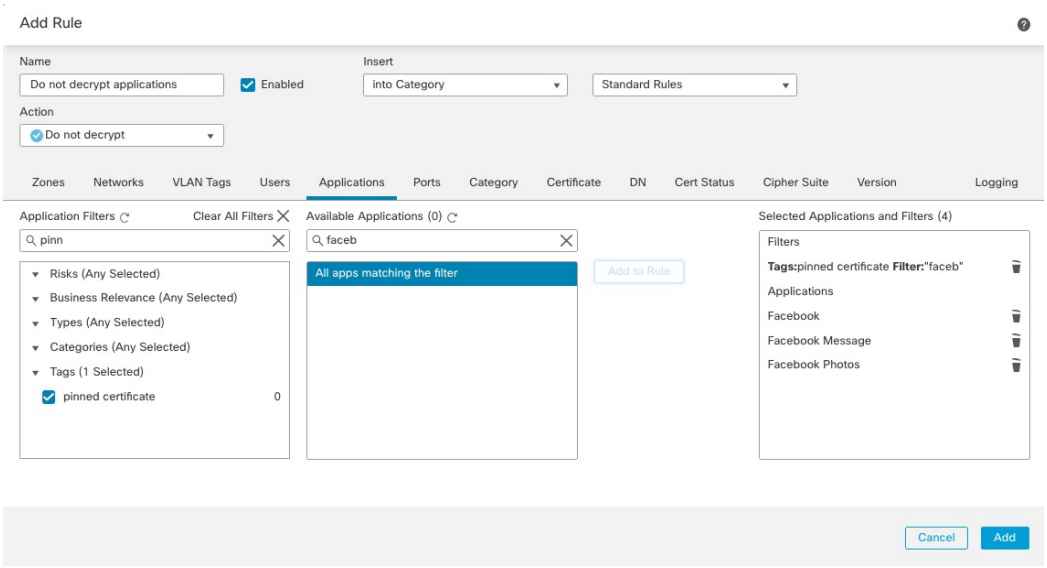
ネットワーク上のトラフィックを評価して、低リスクのカテゴリ、レピュテーション、またはアプリケーションに一致するトラフィックを判断し、[復号しない（Do Not Decrypt）]アクションを使用して、それらのルールを追加します。トラフィックの処理により多くの時間がかかるため、それらのルールは他のより具体的な [復号しない（Do Not Decrypt）] ルールの後に配置します。

次に例を示します。



ルールの詳細：





関連トピック

アプリケーション制御の設定のベストプラクティス （1732 ページ）
アプリケーション制御に関する推奨事項 （1729 ページ）

カテゴリの [復号-再署名（Decrypt - Resign）] ルールの作成

このトピックでは、未分類のサイトを除くすべてのサイトに対して、[復号-再署名（Decrypt - Resign）] アクションを使用して復号ルールを作成する例を示します。このルールでは、[キーのみを置換（Replace Key Only）] オプションを使用します。[復号-再署名（Decrypt - Resign）] ルールアクションでは常にこのオプションを使用することを推奨します。

[キーのみを置換（Replace Key Only）] オプションを使用すると、自己署名証明書を使用するサイトを参照した場合、Web ブラウザにセキュリティ警告が表示されるため、ユーザーはセキュリティで保護されていないサイトと通信していることに気付きます。

このルールを最下部に配置することで、両方の長所を活用でき、ルールをポリシーの前に配置した場合と同じようにパフォーマンスに影響を与えることなく、トラフィックを復号し、必要に応じて検査できます。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 内部認証局（CA）を Secure Firewall Management Center（**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**、次に**[PKI]** > **[内部CA（Internal CAs）]**）にアップロードします（まだアップロードしていない場合）。

ステップ 3 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[復号（Decryption）]** をクリックします。

ステップ 4 復号ポリシー の横にある [編集（Edit）]（✎） をクリックします。

ステップ 5 [ルールの追加（Add Rule）] をクリックします。

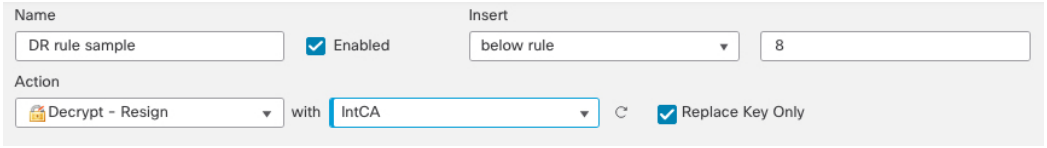
ステップ 6 [名前（Name）] フィールドにルールを識別する名前を入力します。

ステップ 7 [アクション（Action）] リストから、[復号-再署名（Decrypt - Resign）] をクリックします。

ステップ 8 [with] リストから、内部 CA の名前をクリックします。

ステップ 9 [キーのみを置換（Replace Key Only）] ボックスをオンにします。

次の図は例を示しています。



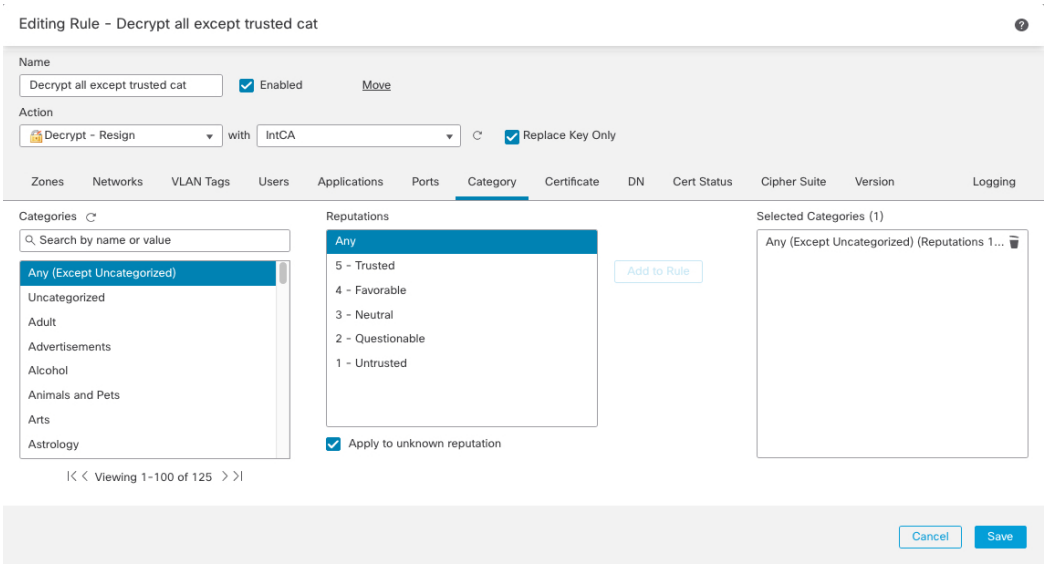
ステップ 10 [カテゴリ（Category）] タブページをクリックします。

ステップ 11 [カテゴリ（Categories）] リストの上部で、[任意（未分類を除く）（Any (Except Uncategorized)）] をクリックします。

ステップ 12 [レピュテーション（Reputations）] リストで、[任意（Any）] をクリックします。

ステップ 13 [ルールに追加（Add to Rule）] をクリックします。

次の図は例を示しています。



関連トピック

内部認証局オブジェクト （1354 ページ）

復号ルール：証明書とプロトコルバージョンをブロックまたは監視する

最後の復号ルールは、最も具体的で最も処理が必要なルールのため、不正な証明書と安全でないプロトコルバージョンを監視またはブロックするルールです。

ルールの詳細：

関連トピック

例：証明書ステータスを監視またはブロックする 復号ルール （2422 ページ）
例：プロトコルバージョンを監視またはブロックする 復号ルール （2423 ページ）
オプションの例：証明書識別名の監視またはブロックのマニュアル復号ルール （2425 ページ）

例：証明書ステータスを監視またはブロックする 復号ルール

最後の復号ルールは、最も具体的で最も処理が必要なルールのため、不正な証明書と安全でないプロトコルバージョンを監視またはブロックするルールです。このセクションの例は、証明書のステータスによってトラフィックを監視またはブロックする方法を示しています。

重要 [暗号スイート（Cipher Suite）] と [バージョン（Version）] のルール条件は、[ブロック（Block）] または [リセットしてブロック（Block with reset）] のルールアクションが使用されているルールでのみ使用します。[暗号スイート（Cipher Suite）] または [バージョン（Version）] を [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] ルールアクションとともに使用しないでください。ルールのこれらの条件を他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]** をクリックします。

ステップ 3 復号ポリシー の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 復号ルール の横にある [編集（Edit）]（✎） をクリックします。

ステップ 5 [ルールの追加（Add Rule）] をクリックします。

ステップ 6 [ルールの追加（Add Rule）] ダイアログボックスの [名前（Name）] フィールドに、ルールの名前を入力します。

ステップ 7 [証明書ステータス（Cert Status）] をクリックします。

ステップ 8 各証明書ステータスには次のオプションがあります。

- 該当する証明書ステータスが存在するときに照合する場合は、[はい（Yes）] をクリックします。
- 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ（No）]をクリックします。

- ルールが一致するときに条件をスキップする場合は、[任意（Any）] をクリックします。つまり、[任意（Any）] を選択すると、証明書ステータスの有無に関わらずルールは一致します。

ステップ 9 [アクション（Action）] リストで、[監視（Monitor）] をクリックしてルールに一致するトラフィックのみを監視してログに記録するか、[ブロック（Block）] または [リセットしてブロック（Block with Reset）] をクリックしてトラフィックをブロックし、必要に応じて接続をリセットします。

ステップ 10 ルールへの変更を保存するには、ページの下部にある [追加（Add）] をクリックします。

ステップ 11 ポリシーへの変更を保存するには、ページの上部にある [保存（Save）] をクリックします。

例

組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から提供された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。

次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合します。

次の例では、無効な発行者の証明書、自己署名された証明書、期限切れの証明書、および無効な証明書が着信トラフィックで使用されている場合、トラフィックはこのルール条件に一致します。

次の図は、要求の SNI がサーバー名に一致する、または CRL が有効でない場合に一致する証明書ステータスのルール条件を示しています。

例：プロトコルバージョンを監視またはブロックする 復号ルール

この例では、TLS 1.0、TLS 1.1、SSLv3 などのセキュアと見なされなくなったネットワーク上の TLS および SSL プロトコルをブロックする方法を示します。この例は、プロトコルバージョンルールがどのように機能するかについてもう少し詳細に説明するために含まれています。

非セキュアなプロトコルはすべてエクスプロイト可能なため、ネットワークから除外する必要があります。この例では、次のようになります。

- 復号ルール の [バージョン（Version）] ページを使用して、一部のプロトコルをブロックすることができます。

- SSLv2は復号不可と見なされるため、復号ポリシーの[復号不可のアクション（Undecryptable Actions）] を使用してブロックできます。
- 同様に、圧縮 TLS/SSL はサポートされていないため、ブロックする必要があります。

重要 [暗号スイート（Cipher Suite）] と [バージョン（Version）] のルール条件は、[ブロック（Block）] または [リセットしてブロック（Block with reset）] のルールアクションが使用されているルールでのみ使用します。[暗号スイート（Cipher Suite）] または [バージョン（Version）] を [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] ルールアクションとともに使用しないでください。ルールのこれらの条件を他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[復号（Decryption）]** をクリックします。

ステップ 3 復号ポリシー の横にある [編集（Edit）]（） をクリックします。

ステップ 4 復号ルール の横にある [編集（Edit）]（） をクリックします。

ステップ 5 [ルールの追加（Add Rule）] をクリックします。

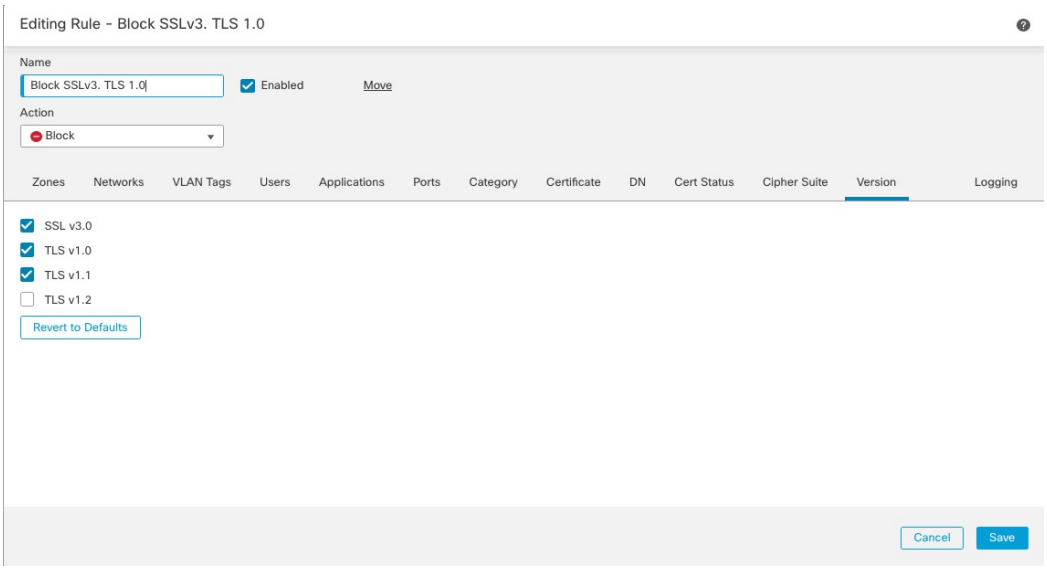
ステップ 6 [ルールの追加（Add Rule）] ダイアログボックスの [名前（Name）] フィールドに、ルールの名前を入力します。

ステップ 7 [アクション（Action）] リストから [ブロック（Block）] または [リセットしてブロック（Block with reset）] をクリックします。

ステップ 8 [バージョン（Version）] ページをクリックします。

ステップ 9 **SSL v3.0**、**TLS 1.0**、**TLS 1.1** など、セキュアでなくなったプロトコルのチェックボックスをオンにします。引き続きセキュアと見なされているプロトコルのチェックボックスをオフにします。

次の図は例を示しています。



ステップ 10 必要に応じて他のルール条件を選択します。

ステップ 11 **[追加（Add）]** をクリックします。

オプションの例：証明書識別名の監視またはブロックのマニュアル 復号ルール

このルールは、サーバー証明書の識別名に基づいてトラフィックを監視またはブロックする方法についてのアイデアを提供し、もう少し詳細に説明するために含まれています

識別名は、国コード、共通名、組織、および組織単位で構成できますが、通常は共通名のみで構成されます。たとえば、`https://www.cisco.com` の証明書の共通名は `cisco.com` です。（ただし、これは必ずしも単純ではありません。一般的な名前を見つける方法については、「*Cisco Secure Firewall Management Center* デバイス設定ガイド」の識別名（DN）のルール条件（2373 ページ）を参照してください）。

クライアント要求の URL のホスト名部分は、サーバー名指定（SNI）です。クライアントは、TLS ハンドシェイクの SNI 拡張を使用して、接続するホスト名（たとえば、`auth.amp.cisco.com`）を指定します。次に、サーバーは、単一の IP アドレスですべての証明書をホストしながら、接続を確立するために必要な、対応する秘密キーと証明書チェーンを選択します。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[復号（Decryption）]** をクリックします。

ステップ 3 復号ポリシー の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 復号ルール の横にある [編集（Edit）]（✎） をクリックします。

ステップ 5 [ルールの追加（Add Rule）] をクリックします。

ステップ 6 [ルールの追加（Add Rule）] ダイアログボックスの [名前（Name）] フィールドに、ルールの名前を入力します。

ステップ 7 [アクション（Action）] リストから [ブロック（Block）] または [リセットしてブロック（Block with reset）] をクリックします。

ステップ 8 [DN] をクリックします。

ステップ 9 [使用可能な DN（Available DNs）] で、追加する識別名を探します。

- ここで識別名オブジェクトを作成してリストに追加するには（後で条件に追加できます）、[使用可能なDN（Available DNs）] リストの上にある [追加（Add）] (＋) をクリックします。
- 追加する識別名オブジェクトおよびグループを検索するには、[使用可能なDN（Available DNs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

ステップ 10 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 11 [サブジェクトに追加（Add to Subject）] または [発行元に追加（Add to Issuer）] をクリックします。

ヒント
選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 12 手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。[Subject DNs] または [Issuer DNs] リストの下にある [Enter DN or CN] プロンプトをクリックし、共通名または識別名を入力して [Add] をクリックします。

どちらのリストにも CN または DN を追加できますが、[サブジェクトDN（Subject DNs）] リストに追加するのが一般的です。

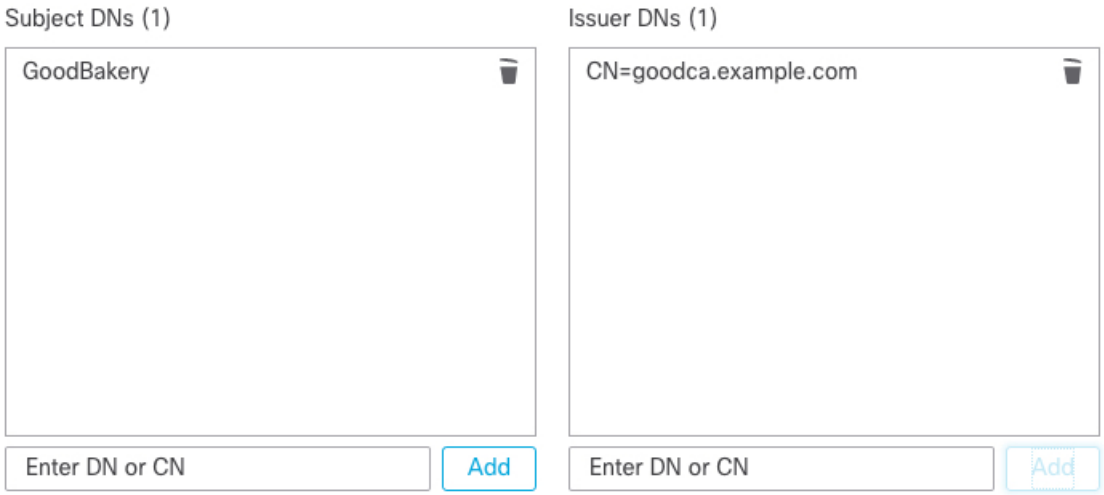
ステップ 13 ルールを追加するか、編集を続けます。

ステップ 14 終了したら、ルールへの変更を保存し、ページの下部にある [追加（Add）] をクリックします。

ステップ 15 ポリシーへの変更を保存するには、ページの上部にある [保存（Save）] をクリックします。

例

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセス コントロールにより制御されます。



復号ルール の設定

復号ルール に推奨されるベストプラクティス設定の設定方法。

復号ルール：[復号しない（Do Not Decrypt）] ルールアクションが使用されるルールを除く、すべてのルールのロギングを有効にします。（これは任意です。復号されていないトラフィックに関する情報を表示する場合は、そのルールのロギングも有効にします。）

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]** をクリックします。

ステップ 3 復号ポリシー の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 復号ルール の横にある [編集（Edit）]（✎） をクリックします。

ステップ 5 [ロギング（Logging）] タブをクリックします。

ステップ 6 [接続の終了時にロギングする（Log at End of Connection）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 ページ最上部にある [保存（Save）] をクリックします。

第 XI 部

ユーザー ID

- ユーザーアイデンティティの概要 （2431 ページ）
- [Realms] （2451 ページ）
- ISE/ISE-PIC によるユーザーの制御 （2497 ページ）
- キャプティブポータルによるユーザーの制御 （2519 ページ）
- リモートアクセス VPN によるユーザーの制御 （2543 ページ）
- TS エージェントによるユーザーの制御 （2549 ページ）
- ユーザー アイデンティティ ポリシー （2553 ページ）

第 64 章

ユーザーアイデンティティの概要

次のトピックでは、ユーザー ID について説明します。

- ユーザー アイデンティティについて （2431 ページ）
- Firepower システムのホストとユーザーの制限 （2443 ページ）
- アイデンティティ レルムの制限 （2447 ページ）
- Microsoft Azure Active Directory レルムのユーザー制限 （2447 ページ）

ユーザー アイデンティティについて

ユーザアイデンティティ情報を使用すると、ポリシー違反、攻撃、ネットワークの脆弱性の発生源を特定し、特定のユーザまで遡って追跡することができます。たとえば、以下について決定できます。

- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者。
- 内部攻撃またはポートスキャンを開始した人物。
- 特定のホストへの不正アクセスを試みている人物。
- 過度に大量の帯域幅を使用している人物。
- 重要なオペレーティング システム更新を適用しなかった人物。
- 会社のポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物。
- ネットワーク上の侵害の兆候に関連付けられている人物。

この情報を入手すれば、システムの他の機能を使用して、リスクを軽減し、アクセス制御を実行し、他のユーザーを破壊行為から保護するためのアクションを実行できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザー アイデンティティ ソースを設定してユーザー データを収集すると、ユーザー認識とユーザー制御を実行できます。

アイデンティティソースの詳細については、ユーザーアイデンティティ ソースについて（2433 ページ）を参照してください。

関連トピック

アイデンティティの用語 （2432 ページ）
ユーザー アイデンティティ ソースについて （2433 ページ）
アイデンティティ導入 （2437 ページ）
アイデンティティ ポリシーの設定方法 （2438 ページ）

アイデンティティの用語

このトピックでは、ユーザアイデンティティおよびユーザ制御の一般的な用語について説明します。

ユーザー認識

アイデンティティソース（TSエージェントなど）を使用して、ネットワーク上のユーザーを識別します。ユーザー認識によって、権限のあるソース（Active Directory など）および権限のないソース（アプリケーションベース）の両方からユーザーを識別できます。Active Directory をアイデンティティ ソースとして使用するには、レルムおよびディレクトリを設定する必要があります。詳細については、ユーザー アイデンティティ ソースについて（2433 ページ）を参照してください。

ユーザー制御

アクセス コントロール ポリシーに関連付けるアイデンティティ ポリシーを構成します。（アイデンティティ ポリシーは、アクセス コントロール サブポリシーと呼ばれるようになります。）アイデンティティ ポリシーはアイデンティティ ソースを指定し、オプションで、そのソースに属するユーザおよびグループを指定します。

アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けることで、ネットワークのトラフィックでユーザまたはユーザアクティビティをモニタ、信頼、ブロックまたは許可するかどうかを決定します。詳細については、アクセス制御ポリシー（1745 ページ）を参照してください。

権限のあるアイデンティティ ソース

信頼できるサーバによってユーザ ログインが検証されています（たとえば、Active Directory）。権限のあるログインから取得したデータを使用すると、ユーザー認識とユーザー制御を実行できます。権限のあるユーザー ログインは、パッシブ認証とアクティブ認証から得られます。

- パッシブ認証は、ユーザーが外部リポジトリ経由で認証されるときに発生します。サポートされているパッシブ認証ユーザーリポジトリは、ISE/ISE-PIC、TS エージェント、および Microsoft Active Directory です。
- アクティブ認証は、ユーザが事前設定済みの管理対象デバイス経由で認証されるときに発生します。アクティブ認証はキャプティブポータルとも呼ばれます。アクティブ認証は通常、パッシブ認証と同じユーザーリポジトリを使用します（例外として、ISE/ISE-PIC、 および TS エージェントはパッシブのみです）。

権限のないアイデンティティ ソース

ユーザー ログインの検証を行った不明または信頼できないサーバー。トラフィックベースの検出は、システムでサポートされている唯一の権限のないアイデンティティ ソースです。権限のないログインから取得されたデータを使用すると、ユーザー認識を実行できます。

ユーザー アイデンティティ ソースについて

次の表に、システムでサポートされているユーザー アイデンティティ ソースの概要を示します。各アイデンティティ ソースは、ユーザー認識のためのユーザーの記憶域を提供します。これらのユーザーは、アイデンティティおよびアクセス コントロール ポリシーで制御できます。

ユーザーアイデンティティ ソース	サーバー要件	ログインタイプ	認証タイプ（Authentication Type）	ユーザ制御	詳細については、次を参照してください。
キャプティブ ポータル	OpenLDAP Microsoft Active Directory	権威あり	アクティブ	はい	キャプティブ ポータルのアイデンティティ ソース（2519ページ）
パッシブ認証	OpenLDAP Microsoft Active Directory	権威なし	アクティブ	はい	LDAP レルムまたは Active Directory レルムおよびレルム ディレクトリの作成（2452 ページ）
TS エージェントによるパッシブ認証	Microsoft Windows Terminal Server	権威あり	パッシブ	はい	ターミナル サービス（TS）エージェントのアイデンティティ ソース（2549ページ）
リモート アクセス VPN	OpenLDAP または Microsoft Active Directory	権威あり	アクティブ	はい	リモート アクセス VPN アイデンティティ ソース（2543 ページ）
	RADIUS	権威あり	Active	非対応、認識のみ	
ISE/ISE-PIC	Microsoft Active Directory	権威あり	パッシブ	はい	ISE/ISE-PIC アイデンティティ ソース（2497ページ）

ユーザーアイデンティティ ソース	サーバー要件	ログインタイプ	認証タイプ（Authentication Type）	ユーザ制御	詳細については、次を参照してください。
トラフィック ベースの検出 （ネットワーク検出ポリシーで設定）。	—	権威なし	—	非対応、認識のみ	トラフィック ベース検出のアイデンティティ ソース（2668 ページ）

展開するアイデンティティ ソースを選択する際には、以下を検討してください。

- 非 LDAP ユーザー ログインにはトラフィック ベースの検出を使用する必要があります。
- 失敗したログインまたは認証アクティビティを記録するには、トラフィック ベースの検出またはキャプティブ ポータルを使用する必要があります。失敗したログインまたは認証試行で新しいユーザーがデータベース内のユーザーのリストに追加されることはありません。
- キャプティブ ポータルのアイデンティティ ソースには、ルーテッド インターフェイスを備えた管理対象デバイスが必要です。キャプティブ ポータルでインライン（タップ モードとも呼ばれます）インターフェイスを使用することはできません。

これらのアイデンティティ ソースからのデータは、Secure Firewall Management Center のユーザー データベースとユーザー アクティビティ データベースに格納されます。Secure Firewall Management Center サーバー ユーザー ダウンロードを設定して、新しいユーザー データがデータベースに自動的かつ定期的にダウンロードされるようにできます。

必要なアイデンティティ ソースを使用してアイデンティティ ルールを設定したら、各ルールにアクセス コントロール ポリシーを関連付け、ポリシーを有効にするために管理対象デバイスに展開する必要があります。アクセス コントロール ポリシーおよび展開の詳細については、アクセス制御への他のポリシーの関連付け（1765 ページ）を参照してください。

ユーザーアイデンティティの一般情報については、ユーザーアイデンティティについて（2431 ページ）を参照してください。

ユーザーアイデンティティのベストプラクティス

アイデンティティポリシーを設定する前に、次の情報を確認することを推奨します。

- ユーザー制限を把握します
- ヘルスモニター
- ISE/ISE-PIC の最新バージョン、2 種類の修復を使用します
- ユーザーエージェントのサポートは 6.7 で終了します
- キャプティブポータルには、ルーテッドインターフェイスと、いくつかの個別のタスクが必要です

Microsoft Active Directory および LDAP

システムは、ユーザーの認識および管理のために、Active Directory、LDAP などのユーザーレポジトリをサポートしています。Active Directory または LDAP リポジトリと Secure Firewall Management Center の間の関連付けは、レルムと呼ばれます。LDAP サーバーまたは Active Directory ドメインごとに 1 つのレルムを作成する必要があります。サポートされているバージョンの詳細については、レルムがサポートされているサーバー（2461 ページ）を参照してください。

LDAP でサポートされるユーザー アイデンティティ ソースは、キャプティブポータルのみです。（ISE/ISE-PIC を除く）他のアイデンティティソースを使用するには、Active Directory を使用する必要があります。

Active Directory の場合のみ：

- ドメインコントローラごとに 1 つのディレクトリを作成します。

  詳細については、「LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）」を参照してください。

- 2 つのドメイン間の信頼関係にあるユーザーとグループは、すべての Active Directory ドメインとドメインコントローラを、それぞれレルムとディレクトリとして追加した場合にサポートされます。

  詳細については、レルムおよび信頼できるドメイン （2458 ページ）を参照してください。

ヘルスモニター

Secure Firewall Management Center ヘルスモニターは、次のようなさまざまな Secure Firewall Management Center 機能のステータスに関する重要な情報を提供します。

- ユーザー/レルムの不一致
- Snort メモリ使用率
- ISE 接続のステータス

ヘルスモジュールの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Health Modules」を参照してください。

ヘルスモジュールをモニターするポリシーを設定するには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Creating Health Policies」を参照してください。

デバイス固有のユーザー制限

すべての物理または仮想 Firewall Management Center デバイスには、ダウンロードできるユーザー数に制限があります。ユーザー制限に達すると、Firewall Management Center がメモリを使い果たし、結果として機能の信頼性が低下する可能性があります。

ユーザー制限については、Microsoft Active Directory のユーザー制限 （2445 ページ）で説明しています。

ISE/ISE-PIC アイデンティティソースを使用する場合は、オプションで、アイデンティティ ポリシーの作成（2555ページ）で説明されているようにアイデンティティマッピングフィルタを使用して、Firewall Management Center がモニターするサブネットを制限し、メモリ使用率を減らすことができます。

ISE/ISE-PIC の最新バージョンの使用

ISE/ISE-PIC アイデンティティソースを使用する場合は、常に最新バージョンを使用して、最新の機能とバグ修正を確実に入手することを強く推奨します。

pxGrid 2.0（バージョン 2.6 パッチ 6 以降、または 2.7 パッチ 2 以降で使用）も、ISE/ISE-PIC で使用される修復を、エンドポイント保護サービス（EPS）から適応型ネットワーク制御（ANC）に変更します。ISE/ISE-PIC をアップグレードする場合は、修復ポリシーを EPS から ANC に移行する必要があります。

ISE/ISE-PIC の使用に関する詳細については、ISE/ISE-PIC の注意事項と制限事項（2500ページ）を参照してください。

ISE/ISE-PIC アイデンティティソースを設定するには、ユーザー制御用 ISE/ISE-PIC の設定方法（2503 ページ）を参照してください。

キャプティブポータルの情報

TS エージェントの情報

TS エージェントのユーザー アイデンティティ ソースは、Windows Terminal Server 上のユーザーセッションを識別するために必要です。『Cisco Terminal Services (TS) Agent Guide』で説明されているように、TS エージェントソフトウェアをターミナルサーバーマシンにインストールする必要があります。また、TS エージェントサーバーと Secure Firewall Management Center の時計を同期させる必要があります。

TS エージェントのデータは [ユーザ（Users）] テーブル、[ユーザ アクティビティ（User Activity）] テーブル、および [接続イベント（Connection Event）] テーブルに表示され、ユーザ認識とユーザ制御に使用できます。

詳細については、TS エージェントのガイドライン （2550 ページ）を参照してください。

アイデンティティポリシーとアクセス コントロール ポリシーの関連付け

レルム、ディレクトリ、およびユーザーアイデンティティ ソースを設定したら、アイデンティティポリシーでアイデンティティルールを設定する必要があります。ポリシーを有効にするには、アイデンティティポリシーとアクセス コントロール ポリシーを関連付ける必要があります。

アイデンティティポリシーの作成の詳細については、アイデンティティ ポリシーの作成（2555ページ）を参照してください。

アイデンティティルールの作成の詳細については、アイデンティティ ルールの作成（2565ページ）を参照してください。

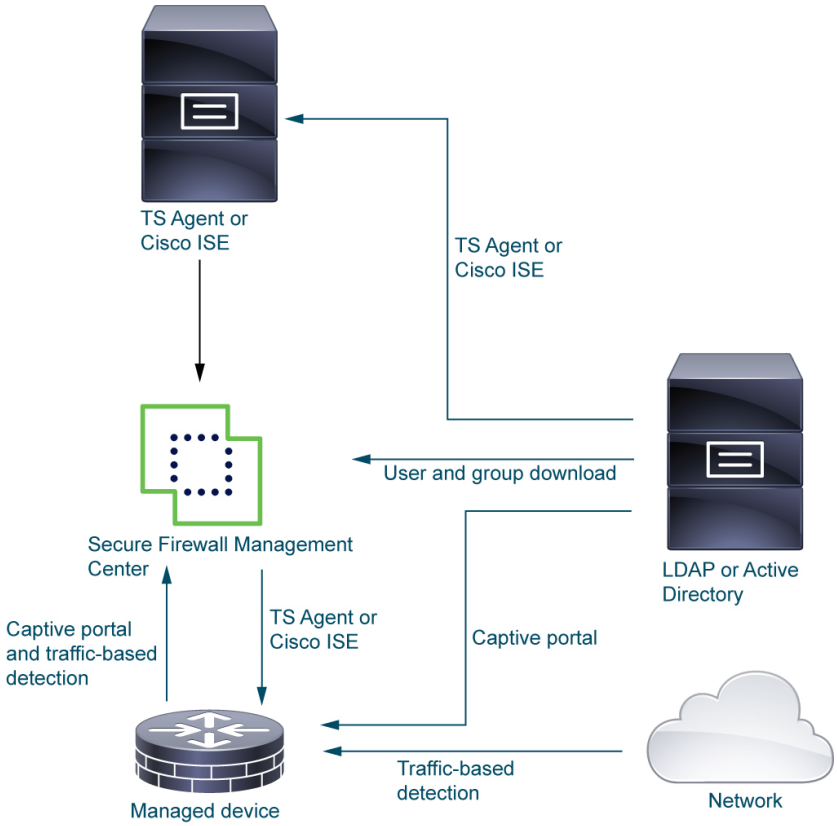
アイデンティティポリシーとアクセス コントロール ポリシーを関連付けるには、アクセス制御への他のポリシーの関連付け （1765 ページ）を参照してください。

アイデンティティ導入

システムがユーザー ログイン、またはアイデンティティ ソースからのユーザー データを検出すると、そのログインからのユーザーは、Secure Firewall Management Center ユーザー データベース内のユーザーのリストに照らしてチェックされます。ログインユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

ユーザーは Secure Firewall Management Center で確認されるとすぐに、そのユーザーが属するグループと関連付けられます。

次の図は、ユーザーデータの収集および保存の仕組みを示しています。



アイデンティティ ポリシーの設定方法

このトピックでは、使用可能な任意のユーザー アイデンティティ ソース（TS エージェント、ISE/ISE-PIC、キャプティブポータルを使用してアイデンティティポリシーを設定する方法の概要を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意）レルムとディレクトリを作成します。ユーザー制御で使用するユーザーを含むフォレスト内のドメインごとに1つのレルムを作成します。また、ドメインコントローラごとに1つのディレクトリを作成します。アイデンティティポリシーでは、対応する Firewall Management Center レルムとディレクトリを持つユーザーとグループのみを使用できます。	次のいずれかに該当する場合、レルム、レルムディレクトリの作成はオプションです。 • SGT ISE 属性条件を設定することを計画しているものの、ユーザー、グループ、レルム、エンドポイントロケーション、エンドポイントプロファイルの条件の設定は計画していない。 • ネットワークトラフィックをフィルタ処理するためだけにアイデンティティポリシーを使用している。 レルムとは、信頼されたユーザおよびグループの領域で、Microsoft Active Directory リポジトリなどがあります。Firewall Management Center は、指定した間隔でユーザーとグループをダウンロードします。ユーザとグループは、ダウンロードに含めることも、ダウンロードから除外することもできます。 LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452ページ）を参照してください。レルムを作成するためのオプションの詳細については、レルム フィールド（2464ページ）を参照してください。 ディレクトリとは、コンピュータ ネットワークのユーザーとネットワーク共有に関する情報を編成する Active Directory ドメイン コントローラのことです。Active Directory コントローラはレルムにディレクトリ サービスを提供します。

	コマンドまたはアクション	目的
		Active Directory は、ユーザー オブジェクトやグループ オブジェクトを複数のドメイン コントローラ間に分散させます。これらのドメインコントローラは、ディレクトリ サービスを使用してローカルの変更を互いに伝達するピアです。詳細については、MSDN の『Active Directory technical specification glossary』[英語] を参照してください。 1 つのレルムに複数のディレクトリを指定できます。この場合、ユーザー制御用のユーザー クレデンシャルとグループ クレデンシャルを照合するために、そのレルムの [ディレクトリ（Directory）] タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。 （注） SGT ISE 属性条件の設定を計画しているものの、ユーザー、グループ、レルム、エンドポイントロケーション、またはエンドポイントプロファイルの条件の設定は計画していない場合、レルムまたはレルムシーケンスの設定はオプションです。
ステップ 2	レルムからユーザーとグループを同期します。	ユーザーとグループを制御するには、それらを Firewall Management Center と同期する必要があります。必要に応じて手動でユーザーとグループと同期することも、指定した間隔でシステムがそれらと同期するように設定することもできます。 ユーザーとグループを同期するときに、例外を指定できます。たとえば、そのレルムのすべてのユーザー制御から Engineering というグループを除外したり、Engineering グループに適用されるユーザー制御から **joe.smith** というユーザーを除外したりできます。 参照先ユーザーとグループの同期（2475 ページ）

	コマンドまたはアクション	目的
ステップ 3	（任意）レルムシーケンスを作成します。	レルムシーケンスは、レルムの順序付きリストであり、アイデンティティポリシーで使用すると、システムは指定された順序でレルムを検索して、ルールに一致するユーザーを見つけます。レルムシーケンスの作成（2476ページ）を参照してください。
ステップ 4	ユーザ データやグループ データを取得するための手法（アイデンティティ ソース）を作成します。	レルムに保存されたデータを使用してユーザーやグループを制御するには、固有の設定を使ってアイデンティティソースをセットアップします。アイデンティティソースには、TSエージェント、キャプティブポータル、またはリモートVPNが含まれます。次のいずれかを参照してください。 • ユーザー制御のためのキャプティブポータルの設定方法（2524ページ） • ユーザー制御用 RA VPN の設定（2544 ページ）
ステップ 5	アイデンティティ ポリシーを作成します。	アイデンティティポリシーには、1つ以上のアイデンティティ ルールが含まれており、 必要に応じてこれらをカテゴリにまとめることができます。アイデンティティポリシーの作成（2555ページ）を参照してください。 （注） SGT ISE 属性条件を設定することを計画しているものの、ユーザー、グループ、レルム、エンドポイントロケーション、エンドポイントプロファイルの条件の設定は計画していない場合、または ID ポリシーのみを使用してネットワークトラフィックをフィルタ処理する場合、レルムまたはレルムシーケンスの設定はオプションです。
ステップ 6	1つ以上のアイデンティティ ルールを作成します。	アイデンティティルールを使用すると、認証の種類、ネットワークゾーン、ネットワークまたは地理位置情報、レルム、レルムシーケンスなど、多数の一致条件

	コマンドまたはアクション	目的
		を指定できます。アイデンティティ ルールの作成（2565 ページ）を参照してください。
ステップ 7	アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます。	アクセス コントロール ポリシーはトラフィックをフィルタリングし、必要に応じてトラフィックを検査します。アイデンティティ ポリシーを有効にするには、アクセス コントロール ポリシーを関連付ける必要があります。アクセス制御への他のポリシーの関連付け（1765 ページ）を参照してください。
ステップ 8	少なくとも 1 つの管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを使用してユーザー アクティビティを制御するには、クライアントの接続先となる管理対象デバイスにそのポリシーを展開する必要があります。設定変更の展開（172 ページ）を参照してください。
ステップ 9	ユーザー アクティビティをモニターします。	ユーザー アイデンティティ ソースによって収集されたアクティブ セッションの一覧、またはユーザー アイデンティティ ソースによって収集されたユーザー情報の一覧を確認します。Cisco Secure Firewall Management Center アドミニストレーション ガイド の「ワークフローの使用」を参照してください。 次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。 • ISE/ISE-PIC アイデンティティ ソースを使用できます。 • アクセス コントロール ポリシーのユーザまたはグループは使用しません。 • アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較」を参照してください。

関連トピック

トラフィックに基づくユーザー検出の設定 （2670 ページ）

ユーザー アクティビティ データベース

Secure Firewall Management Center のユーザ アクティビティ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたネットワーク上のユーザ アクティビティのレコードが含まれています。システムがイベントを記録するのは以下のような状況です。

- 個別のログインまたはログオフを検出したとき。
- 新しいユーザを検出したとき。
- システム管理者が手動でユーザを削除したとき。
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ数の制限に達したためにそのユーザを追加できなかったとき。
- ユーザーに関連付けられている侵害の兆候を解決したとき、またはユーザーに対して侵害の兆候ルールを有効または無効にしたとき。

（注） TS エージェントが別のパッシブ認証のアイデンティティ ソース（ISE/ISE-PIC など）と同じユーザーをモニターする場合、Firewall Management Center では TS エージェントのデータを優先します。同じ IP アドレスからの同じアクティビティが TS エージェントと別のパッシブ ソースから報告される場合、TS エージェントのデータだけが Firewall Management Center に記録されます。

システムで検出されたユーザーアクティビティは、Secure Firewall Management Centerを使用して表示できます（**[分析（Analysis）] > [ユーザー（Users）] 見出し > [ユーザーアクティビティ（User Activity）]**）。

ユーザ データベース

Secure Firewall Management Center のユーザー データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたユーザーごとのレコードが含まれています。権限のあるソースから取得したデータをユーザ制御に使用できます。

サポートされている権限のないアイデンティティ ソースと権限のあるアイデンティティ ソースの詳細については、ユーザー アイデンティティ ソースについて （2433 ページ） を参照してください。

Microsoft Active Directory のユーザー制限 （2445 ページ） で説明されているように、Secure Firewall Management Center で保存できるユーザーの合計数は Secure Firewall Management Center のモデルによって異なります。ユーザ制限に達した後、システムは、アイデンティティ ソースに基づいて未検出ユーザ データを次のように優先順位付けします。

- 新しいユーザーが権限のないアイデンティティ ソースからである場合、ユーザーはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザーが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザーを削除し、データベースに新しいユーザーを追加します。

アイデンティティ ソースが特定のユーザ名を除外するように設定されている場合、それらのユーザ名のユーザ アクティビティ データは Secure Firewall Management Center に報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。システムによって保存されるデータのタイプの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*User Data*」を参照してください。

Firewall Management Center の高可用性が設定済みで、プライマリに障害が発生した場合、キャプティブポータル、ISE/ISE-PIC、TS エージェント、またはリモートアクセス VPN デバイスから報告されるログインはフェールオーバーダウンタイム中に識別不能になります（ユーザーが以前に確認されて Firewall Management Center にダウンロードされている場合も同様）。識別されていないユーザーは、Firewall Management Center で [不明（Unknown）] のユーザーとして記録されます。ダウンタイム後、不明のユーザーはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

（注） TS エージェントが別のパッシブ認証の ID ソース（ISE/ISE-PIC）と同じユーザーをモニターしている場合、Firewall Management Center は TS エージェントのデータを優先します。同じ IP アドレスからの同じアクティビティが TS エージェントと別のパッシブソースから報告される場合、TS エージェントのデータだけが Firewall Management Center に記録されます。

システムが新しいユーザ セッションを検出すると、そのユーザ セッションのデータは、次のいずれかが発生するまでユーザ データベースに残ります。

- Firewall Management Center のユーザーが手動でユーザーセッションを削除した。
- アイデンティティ ソースがそのユーザー セッションのログオフを報告した。
- レルムがレルムの [ユーザーセッションのタイムアウト：認証されたユーザー（User Session Timeout: Authenticated Users）] 設定、[ユーザーセッションのタイムアウト：認証に失敗したユーザー（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザーセッションのタイムアウト：ゲスト ユーザー（User Session Timeout: Guest Users）] 設定で指定されているユーザー セッションを終了した。

Firepower システムのホストとユーザーの制限

Secure Firewall Management Center モデルにより、展開でモニターできる個別のホストの数、モニターし、ユーザー制御を実行するために使用できるユーザーの数が決定されます。

ホスト制限（Host Limit）

システムは（ネットワーク検出ポリシーで定義されている）モニタ対象ネットワークで IP アドレスに関連付けられたアクティビティを検出すると、ネットワークマップにホストを追加します。Secure Firewall Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。

表 *193 : Secure Firewall Management Center* モデル別のホスト制限

Firewall Management Center モデル	ホスト
MC1000	50,000
MC1600	50,000
MC2500	150,000
MC2600	150,000
MC4500	600,000
MC4600	600,000
仮想	50,000

ネットワーク マップに存在しないホストのコンテキスト データは表示できません。ただし、アクセス制御は実行できます。たとえば、コンプライアンス allow リストを使用してホストのネットワーク コンプライアンスをモニターできない場合でも、ネットワークマップに存在しないホストとの間のトラフィックでアプリケーション制御を実行できます。

（注） システムでは、IPアドレスとMACアドレスの両方によって識別されるホストとは別に、MAC専用ホストがカウントされます。1つのホストに関連付けられているすべてのIPアドレスは、まとめて 1 つのホストとしてカウントされます。

ホスト制限への到達とホストの削除

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または非アクティブになっている期間が最も長いホストを置換することができます。また、システムが非アクティブであるためネットワークからホストを削除するまでの期間を設定できます。ホスト、サブネット全体、またはすべてのホストをネットワークマップから手動で削除できますが、システムは、削除されたホストに関連付けられたアクティビティを検出した場合は、ホストを再追加します。

関連トピック

ネットワーク検出のデータ ストレージ設定 （2677 ページ）

Microsoft Active Directory のユーザー制限

ユーザー制限について

Firewall Management Center モデルにより、モニターできる個々のユーザー数が決まります。ユーザーは、次の場合に Firewall Management Center ユーザーデータベースに追加されます。

- ユーザーはレルムからダウンロードされます。
- キャプティブポータルまたは RA-VPN のユーザーがログインします。
- ユーザーは、任意のアイデンティティソース（たとえば、TS エージェント）から検出されます。

権限のあるユーザのみがアクセス コントロール ポリシーによるユーザ制御を使用できます。

次の点に注意してください。

- ダウンロードユーザーの最大数は、Firewall Management Center モデルによって異なります。
- 同時ユーザーセッション（つまり、ログイン）の最大数は、管理対象デバイスモデルによって異なります。1 人のユーザーが、異なる固有の IP アドレスから複数のセッションを持つことができます。

（注） システムは、すべてのユーザーセッションをすべての Firewall Threat Defense デバイスにダウンロードします。異なるユーザーの同時ユーザーセッション制限を持つデバイスがある場合、メモリが設定された制限に達すると、制限が最小である Firewall Threat Defense が正常性警告を報告します。（たとえば、Firewall Management Center が Firepower 2110 と 4125 を管理している場合、同時ユーザーセッション数が最大の 64,000 に近づくと、2110 が正常性警告を報告します。）

Microsoft Active Directory のユーザー制限

表 *194 : Firewall Threat Defense* 別の最大同時ユーザーログイン制限

Firewall Threat Defense モデル	レルムあたりの最大同時ユーザーログイン数
Firewall Threat Defense Virtual 5、10、20、30、50（サポートされる任意のハイパーバイザ）	64,000
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130 Cisco Secure Firewall 3105、3110、3120	64,000

Firewall Threat Defense モデル	レルムあたりの最大同時ユーザーログイン数
Firepower 2140 Cisco Secure Firewall 3130、3140 Firepower 4112、4115、4125	150,000
Firepower 4145 Firepower 9300	300,000

ユーザー制限は、Microsoft Active Directory レルムごとに適用されます。1 つのレルムに最大ユーザー数を超えるユーザーをダウンロードしようとした場合、最大数に達するとダウンロードが停止し、正常性アラートが表示されます。一方、最大ユーザー数を超えるユーザーを複数のレルムにダウンロードする場合は、ダウンロードは成功します（いずれか 1 つのレルムのユーザー数が 150,000 を超える場合を除きます。この場合、そのレルムのダウンロードは失敗します）。

表 *195 : Firewall Management Center* モデルごとの最大ダウンロードユーザー数

Firewall Management Center モデル	最大ダウンロードユーザー数
FMC 1000	50,000
FMC 1600	50,000
FMC 2500	150,000
FMC 2600	150,000
FMC 4500	600,000
FMC 4600	600,000
Firewall Management Center Virtual（サポートされる任意のハイパーバイザ）	50,000
Firewall Management Center Virtual 300（サポートされる任意のハイパーバイザ）	150,000

制限に達してから、新しい、以前検出されなかったユーザーをシステムが検出すると、アイデンティティ ソースに基づいてユーザー データに優先順位が付けられます。

- 新しいユーザが権限のないソースからである場合、権限のないユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動でユーザを削除するか、データベースを消去する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しい権限のあるユーザを追加します。

権限のあるユーザー以外いない場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザーを削除し、データベースに新しいユーザーを追加します。

トラブルシューティング情報は、ユーザー制御のトラブルシューティング（2569ページ）にあります。

ヒント　トラフィック ベースの検出を使用している場合、プロトコルによるユーザー ロギングを制限すると、ユーザー名の散乱を最小限に抑え、データベースのスペースを残しておくことができます。たとえば、システムが AIM、POP3、および IMAP トラフィックで検出されたユーザーを追加できないようにすることができます（モニターを望んでいない特定の契約業者または訪問者からのトラフィックであることがわかっているため）。

アイデンティティ レルムの制限

Firewall Threat Defense モデルに関係なく、最大 25 のレルムに制限されます。同じ制限が クラウド提供型 Firewall Management Center にも適用されます。

システムにダウンロードできる ユーザー の数は、次に記載されている情報に従って制限されます。

Microsoft Active Directory のユーザー制限 （2445 ページ）

Microsoft Azure Active Directory レルムのユーザー制限

Microsoft Azure Active Directory のユーザー制限

ユーザー制限について

Firewall Management Center モデルにより、モニターできる個々のユーザー数が決まります。

次の点に注意してください。

- ダウンロードユーザーの最大数は、Firewall Management Center モデルによって異なります。
- 同時ユーザーセッション（つまり、ログイン）の最大数は、管理対象デバイスモデルによって異なります。1 人のユーザーが、異なる固有の IP アドレスから複数のセッションを持つことができます。

（注） システムは、すべてのユーザーセッションをすべての Firewall Threat Defense デバイスにダウンロードします。異なるユーザーの同時ユーザーセッション制限を持つデバイスがある場合、メモリが設定された制限に達すると、制限が最小である Firewall Threat Defense が正常性警告を報告します。（たとえば、Firewall Management Center が Firepower 2110 と 4125 を管理している場合、同時ユーザーセッション数が最大の 64,000 に近づくと、2110 が正常性警告を報告します。）

次の表を参照してください。

表 *196 : Firewall Management Center* モデルごとの最大ダウンロードユーザー数[1]

Firewall Management Center モデル	Cisco Secure 動的属性コネクタ コネクタの数	最大ダウンロードユーザー数
FMC1600、FMC1700	10	50,000
FMC2600、FMC2700	20	150,000
FMC4600、FMC4700	30	600,000
Firewall Management Center Virtual（サポートされる任意のハイパーバイザ）	10	50,000
Firewall Management Center Virtual 300（サポートされる任意のハイパーバイザ）	20	150,000

[1]：Firewall Management Center モデルは、生産終了および販売終了の対象となります。詳細については、サポート終了と販売終了のお知らせを参照してください。

表 *197 : Firewall Threat Defense* 別の最大同時ユーザーログイン制限

Firewall Threat Defense モデル	最大同時ユーザ ログイン
Firewall Threat Defense Virtual 5、10、20、30、50（サポートされる任意のハイパーバイザ）	50,000
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130 Secure Firewall 3110、3120、3130、3140	50,000
Firepower 2140 Cisco Secure Firewall 3130、3140	150,000

Firewall Threat Defense モデル	最大同時ユーザ ログイン
Firepower 4140、4145、4150 Firepower 9300	225,000

第 65 章

[Realms]

次のトピックでは、レルムとアイデンティティ ポリシーについて説明します。

- レルムのライセンス要件 （2451 ページ）
- レルムの要件と前提条件 （2451 ページ）
- LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）
- レルムシーケンスの作成 （2476 ページ）
- クロスドメイン信頼のために Firewall Management Center を設定する：セットアップ （2477 ページ）
- レルムの管理 （2486 ページ）
- レルムの比較 （2486 ページ）
- レルムとユーザーのダウンロードのトラブルシュート （2487 ページ）
- レルムの履歴 （2496 ページ）

レルムのライセンス要件

Threat Defense ライセンス

いずれか（Any）

従来のライセンス

Control

レルムの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成

レルムなしで ISE/ISE-PIC を設定する場合は、Secure Firewall Management Centerでのユーザーの表示方法に影響するユーザー セッション タイムアウトがあることに注意してください。詳細については、レルム フィールド （2464 ページ）を参照してください。

次の手順では、レルム（Firewall Management Center と Active Directory レルム間の接続）とディレクトリ（Firewall Management Center と LDAP サーバーまたは Active Directory ドメインコントローラ間の接続）を作成できます。

（推奨）Firewall Management Center から Active Directory サーバーに安全に接続するには、まず次のタスクを実行します。

- Active Directory サーバーのルート証明書のエクスポート （2473 ページ）
- Active Directory サーバーの名前の検索 （2472 ページ）

Microsoft 社は、2020 年に Active Directory サーバーで LDAP バインディングと LDAP 署名の適用を開始すると発表しました。Microsoft 社がこれらを要件にするのは、デフォルト設定で Microsoft Windows を使用する場合に権限昇格の脆弱性が存在するために、中間者攻撃者が認証要求を Windows LDAP サーバーに正常に転送できる可能性があるからです。詳細については、Microsoft 社のサポートサイトで「2020 LDAP channel binding and LDAP signing requirement for Windows」を参照してください。

レルムおよびディレクトリの設定フィールドに関する詳細については、レルム フィールド（2464 ページ）と[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド（2468 ページ）を参照してください。

クロスドメイン信頼を使用してレルムを設定する段階的手順の例については、クロスドメイン信頼のために Firewall Management Center を設定する：セットアップ （2477 ページ）を参照してください。

Active Directory グローバルカタログサーバーは、レルムディレクトリとしてサポートされていません。グローバルカタログサーバーの詳細については、learn.microsoft.com の「Global Catalog」を参照してください。

（注） すべての Microsoft Active Directory（AD）レルムに固有の [ADプライマリドメイン（AD Primary Domain）] を指定する必要があります。異なる Microsoft AD レルムに同じ [ADプライマリドメイン（AD Primary Domain）] を指定することはできますが、システムが適切に機能しなくなります。これは、システムにより各レルム内のすべてのユーザーとグループに 1 つの固有 ID が割り当てられるためです。そのため、システムは特定のユーザまたはグループを明確に識別することができません。ユーザーとグループが適切に識別されないため、同じ [ADプライマリドメイン（AD Primary Domain）] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザーとグループに割り当てるために発生します。そのため、システムは特定のユーザーまたはグループを明確に識別できません。

レルムなしで ISE/ISE-PIC を設定する場合は、Secure Firewall Management Centerでのユーザーの表示方法に影響するユーザー セッション タイムアウトがあることに注意してください。詳細については、レルム フィールド （2464 ページ）を参照してください。

始める前に

キャプティブポータルにKerberos認証を使用している場合は、開始する前に次のセクションを参照してください：Kerberos 認証の前提条件 （2463 ページ）。

重要 Secure Firewall Management Center と Active Directory ドメインコントローラ間の遅延を削減するには、地理的に Secure Firewall Management Center にできるだけ近いレルムディレクトリ（つまり、ドメインコントローラ）を構成することを強くお勧めします。

たとえば、Secure Firewall Management Center が北米にある場合は、同様に北米にあるレルムディレクトリを構成します。このように構成しないと、ユーザーやグループのダウンロードがタイムアウトするなどの問題が発生する可能性があります。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 3 新しいレルムを作成するには、[レルムの追加（Add Realm）] ドロップダウンリストから選択します。

ステップ 4 その他のタスク（レルムの有効化、無効化、削除など）を実行する場合は、レルムの管理 （2486 ページ）を参照してください。

ステップ 5 レルム フィールド （2464 ページ）で説明したように、レルム情報を入力します。

ステップ 6 [ディレクトリサーバー設定（Directory Server Configuration）] セクションで、[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド （2468 ページ）の説明に従ってディレクトリを入力します。

ステップ 7 （オプション）このレルムに別のドメインを設定するには、[Add another directory] をクリックします。

ステップ 8 [Configure Groups and Users] をクリックします。
次の情報を入力します。

[Information]	説明
AD Primary Domain	ユーザー認証が必要となる Active Directory サーバーのドメインです。詳細については、レルム フィールド（2464 ページ）を参照してください。 ドメインの代替ユーザープリンシパル名（UPN）サフィックスではなく、ドメインの元のドメイン名を使用してレルムを作成する必要があります。そうしない場合、ユーザーとグループはダウンロードに失敗し、アイデンティティポリシーは適用されません。たとえば、元のドメインが `domain.example.com` で、代替の UPN 名が `domain2.mydomain.com` の場合は、`domain.example.com` を使用するようにレルムを設定する必要があります。代替の UPN サフィックスの設定の詳細については、learn.microsoft.com の「Configuring Alternate Login ID」などのリソースを参照してください。
ベース DN（Base DN）	Firewall Management Center がユーザー データの検索を開始するサーバーのディレクトリ ツリー。
Group DN	Firewall Management Center がグループデータの検索を開始するサーバーのディレクトリツリー。
[Load Groups]	クリックして、Active Directory サーバーからグループをロードします。グループが表示されない場合は、[AD Primary Domain]、[Base DN]、および [Group DN] フィールドに情報を入力するか、または情報を編集して、[Load Groups] をクリックします。 これらのフィールドの詳細については、レルム フィールド（2464 ページ）を参照してください。
[Available Groups] セクション	[含めるグループとユーザー（Included Groups and Users）] または [除外するグループとユーザー（Excluded Groups and Users）] リストにグループを移動して、ポリシーで使用するグループを制限します。 たとえば、1 つのグループを [含めるグループとユーザー（Included Groups and Users）] リストに移動すると、そのグループのみポリシーで使用し、他のグループはすべて除外できます。 [除外するグループとユーザー（Excluded Groups and Users）] のグループ、およびそれらに含まれるユーザーは、ユーザー認識と制御から除外されます。他のすべてのグループとユーザーは利用できます。 詳細については、[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド（2468 ページ）を参照してください。

ステップ 9 [レルム設定（Realm Configuration）] タブをクリックします。

ステップ 10 [Group Attribute] を入力し、（キャプティブポータルにケルベロス認証を使用する場合）[AD Join Username] と [AD Join Password] を入力します。詳細については、[レルムディレクトリ（Realm Directory）]および[同期（Synchronize）]フィールド（2468 ページ）を参照してください。

ステップ 11 Kerberos 認証を使用する場合は、[テスト（Test）] をクリックします。テストが失敗した場合は、少し待ってから再試行してください。

ステップ 12 [ISE/ISE-PICユーザー（ISE/ISE-PIC Users）]、[ターミナルサーバーエージェントユーザー（Terminal Server Agent Users）]、[キャプティブポータルユーザー（Captive Portal Users）]、[失敗したキャプティブポータルユーザー（Failed Captive Portal Users）]、および [ゲストキャプティブポータルユーザー（Guest Captive Portal Users）] のユーザー セッション タイムアウト値を分単位で入力します。

ステップ 13 レルムの設定が完了したら、[Save] をクリックします。

次のタスク

- クロスドメイン信頼のために Firewall Management Center を設定する：セットアップ （2477 ページ）
- ユーザーとグループの同期 （2475 ページ）
- レルムの編集、削除、有効化、または無効化を行います。レルムの管理 （2486 ページ）を参照してください
- レルムの比較 （2486 ページ）.
- 必要に応じて、タスクのステータスをモニターします。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Viewing Task Messages*」を参照してください。

レルムとレルムシーケンスについて

レルムとは、Secure Firewall Management Center とモニタリング対象のサーバー上にあるユーザーアカウントの間の接続です。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。レルムでは次のことを実行できます。

- アクティビティをモニターするユーザーとユーザー グループを指定する。
- 権限のあるユーザー、および権限のない一部のユーザー（トラフィックベースの検出で検出された POP3 および IMAP ユーザー、およびトラフィックベースの検出、TS エージェント、ISE/ISE-PIC によって検出されたユーザー）のユーザーメタデータについてユーザーリポジトリをクエリする。

レルムシーケンスは、アイデンティティポリシーで使用する 2 つ以上の Active Directory レルムの順序付きリストです。レルムシーケンスをアイデンティティルールに関連付けると、レルム

シーケンスで指定されている順序で、最初から最後まで Active Directory ドメインが検索されます。

レルム内のディレクトリとして複数のドメインコントローラを追加できますが、同じ基本レルム情報を共有する必要があります。レルム内のディレクトリは、LDAP サーバのみ、または Active Directory（AD）サーバのみである必要があります。レルムを有効にすると、保存された変更は次回 Secure Firewall Management Centerがサーバに照会するときに適用されます。

ユーザ認識を行うには、サポートされるすべてのサーバタイプのレルムを設定する必要があります。システムは、これらの接続を使用して、POP3 および IMAP ユーザーに関連するデータについてサーバーにクエリし、トラフィック ベースの検出で検出された LDAP ユーザーに関するデータを収集します。

システムは、POP3 および IMAP ログイン内の電子メールアドレスを使用して、Active Directory または OpenLDAP 上の LDAP ユーザーに関連付けます。たとえば、LDAP ユーザーと電子メール アドレスが同じユーザーの POP3 ログインを管理対象デバイスが検出すると、システムは LDAP ユーザーのメタデータをそのユーザーに関連付けます。

ユーザー制御を実行するために以下のいずれかを設定できます。

- Active Directoryサーバー、または ISE/ISE-PIC のレルムまたはレルムシーケンス

（注） SGT ISE 属性条件を設定する予定で、ユーザー、グループ、レルム、エンドポイントロケーション、エンドポイントプロファイルの条件を設定する予定はない場合、または ID ポリシーのみを使用してネットワークトラフィックをフィルタ処理する場合、Microsoft AD レルムやレルムシーケンスの設定は任意です。

- TS エージェント用の Microsoft AD サーバーのレルムまたはレルムシーケンス。
- キャプティブポータルの場合は、LDAP レルム。

  LDAP 用のレルムシーケンスはサポートされていません。

未定の ネストできます。 Secure Firewall Management Center はそれらのグループとグループに含まれるユーザーをダウンロードします。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452ページ）の説明に従い、必要に応じて、ダウンロードするグループとユーザーを制限できます。

ユーザーの同期について

次のような特定の検出されたユーザーに関して、ユーザーとユーザーグループのメタデータを取得するために、Firewall Management Center と LDAP サーバーまたは Microsoft AD サーバー間の接続を確立するためのレルムまたはレルムシーケンスを設定できます。

- キャプティブポータルで認証されたか、または ISE/ISE-PIC で報告された LDAP および Microsoft AD のユーザー。このメタデータは、ユーザ認識とユーザ制御に使用できます。

- トラフィック ベースの検出で検出された POP3 と IMAP ユーザー ログイン（ユーザーが LDAP または AD ユーザーと同じ電子メール アドレスを持つ場合）。このメタデータは、ユーザ認識に使用できます。

Firewall Management Centerは、ユーザーごとに次の情報とメタデータを取得します。

- LDAP ユーザー名
- 姓と名
- 電子メール アドレス（Email address）
- 部署名（Department）
- 電話番号（Telephone number）

重要 Secure Firewall Management Center と Active Directory ドメインコントローラ間の遅延を削減するには、地理的に Secure Firewall Management Center にできるだけ近いレルムディレクトリ（つまり、ドメインコントローラ）を構成することを強くお勧めします。

たとえば、Secure Firewall Management Center が北米にある場合は、同様に北米にあるレルムディレクトリを構成します。このように構成しないと、ユーザーやグループのダウンロードがタイムアウトするなどの問題が発生する可能性があります。

ユーザ アクティビティ データについて

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザのアイデンティティ データはユーザ データベースに保存されます。アクセス制御で保存できる使用可能なユーザーの最大数は Firewall Management Center モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス制御パラメータの範囲が広すぎる場合、Firewall Management Center はできるだけ多くのユーザーに関する情報を取得し、取得できなかったユーザーの数をメッセージセンターの [タスク（Tasks）] タブ ページで報告します。

オプションで、管理対象デバイスがユーザー認識データを監視するサブネットを制限するには、Cisco Secure Firewall Threat Defense コマンドリファレンスで説明されている **configure identity-subnet-filter** コマンドを使用できます。

（注） ユーザー リポジトリからシステムによって検出されたユーザーを削除しても、Firewall Management Center はユーザー データベースからそのユーザーを削除しません。そのため、手動で削除する必要があります。ただし、LDAP に対する変更は、次に権限のあるユーザーのリストを Firewall Management Center が更新したときにアクセス 制御ルールに反映されます。

レルムおよび信頼できるドメイン

Firewall Management Center で Microsoft Active Directory（AD）レルムを構成すると、Microsoft Active Directory または LDAP ドメインに関連付けられます。

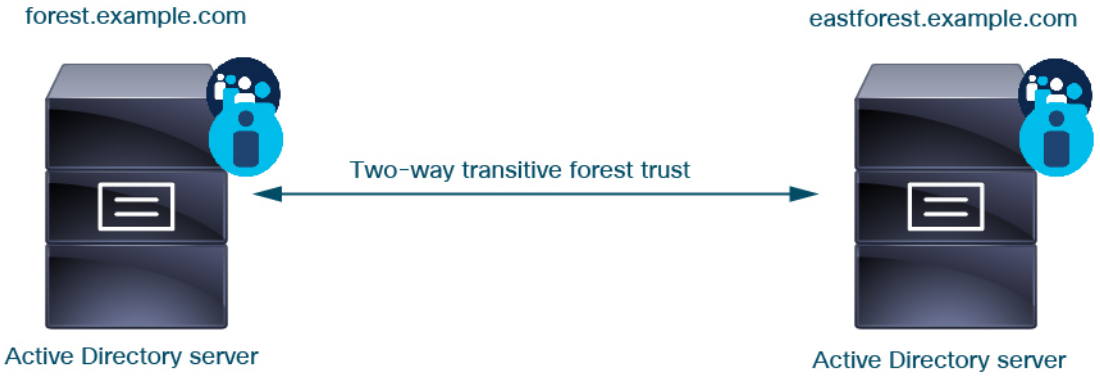
互いに信頼する Microsoft Active Directory（AD）ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザー アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。

システムと信頼できるドメイン

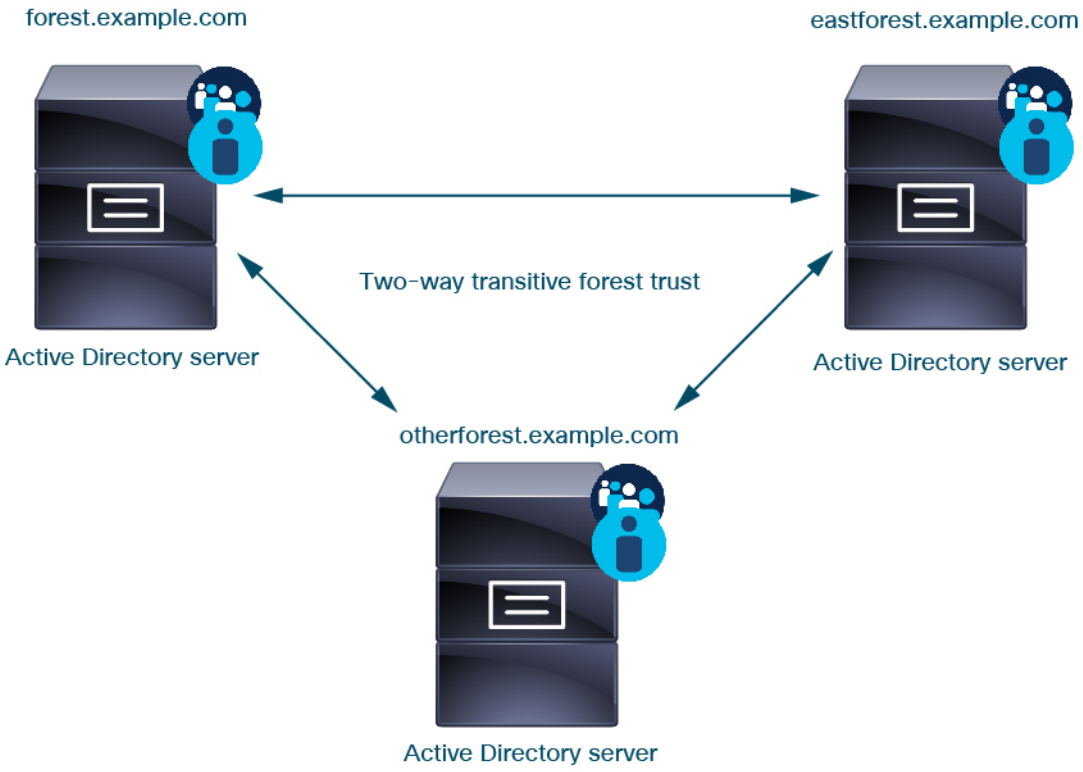
システムは、信頼関係で設定されている AD フォレストをサポートします。信頼関係にはいくつかのタイプがあります。このガイドでは、双方向の推移的なフォレストの信頼関係について説明します。次の簡単な例は、2 つのフォレストを示しています。**forest.example.com** と **eastforest.example.com** 各フォレスト内のユーザーとグループは、他のフォレスト内の AD によって認証されます（フォレストをそのように設定している場合）。

ドメインごとに 1 つのレルムとドメインコントローラごとに 1 つのディレクトリを使用して設定したシステムでは、最大 100,000 の外部セキュリティプリンシパル（ユーザーとグループ）を検出できます。これらの外部セキュリティプリンシパルが別のレルムでダウンロードされたユーザーと一致する場合は、アクセス コントロール ポリシーで使用できます。

アクセス コントロール ポリシーで使用するユーザーが存在しないドメインには、レルムを設定する必要はありません。

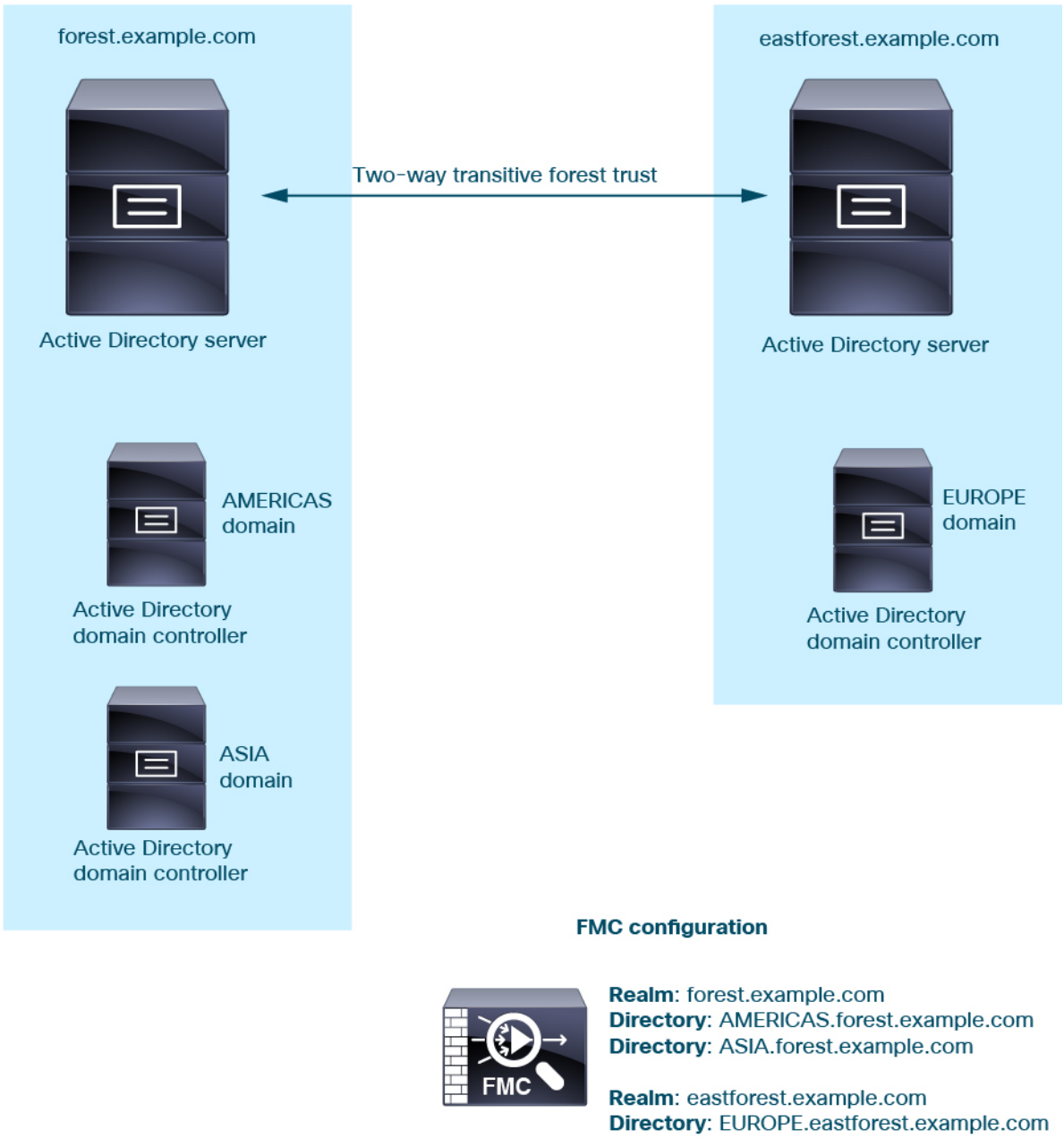


この例を続けるために、3 つの AD フォレスト（1 つはサブドメインまたは独立したフォレスト）があり、すべてが双方向の推移的なフォレストの関係として設定されていて、すべてのユーザーとグループが 3 つすべてのフォレストとシステムで使用可能だとします。（前述の例のように、3 つすべての AD ドメインをレルムとして設定し、すべてのドメインコントローラをそれらのレルムのディレクトリとして設定する必要があります）。



最後に、双方向の推移的なフォレストの信頼関係を持つ2フォレストシステムのユーザーとグループに ID ポリシーを適用できるように Firewall Management Center を設定することが可能です。各フォレストに少なくとも 1 つのドメインコントローラがあり、それぞれが異なるユーザーとグループを認証するとします。Firewall Management Center がこれらのユーザーとグループに ID ポリシーを適用できるようにするには、関連するユーザーを含む各ドメインを Firewall Management Center レルムとして、また各ドメインコントローラをそれぞれのレルムの Firewall Management Center ディレクトリとして設定する必要があります。

Firewall Management Center を正しく設定しないと、一部のユーザーとグループがポリシーで使用できなくなります。この場合、ユーザーとグループの同期を試みると警告が表示されます。



前述の例を使用して、Firewall Management Center を次のように設定します。

- アクセス コントロール ポリシーで制御するユーザーを含む **forest.example.com** のドメインのレルム
  - **AMERICAS.forest.example.com** のレルム内のディレクトリ
  - **ASIA.forest.example.com** のレルム内のディレクトリ
- アクセス コントロール ポリシーで制御するユーザーを含む **eastforest.example.com** のドメインのレルム

- **EUROPE.eastforest.example.com** のレルム内のディレクトリ

（注） Firewall Management Center は AD フィールド **msDS-PrincipalName** を使用して参照を解決し、各ドメインコントローラでユーザー名とグループ名を検索します。**msDS-PrincipalName** は NetBIOS 名を返します。

レルムがサポートされているサーバー

レルムを設定して次のサーバータイプに接続すると、Firewall Management Centerからの TCP/IP アクセスを提供できます。

サーバー タイプ（**Server Type**）	**ISE/ISE-PIC** によるデータ取得のサポート	**TS** エージェントによるデータ取得のサポート	キャプティブ ポータルによるデータ取得のサポート
Windows Server 2012、2016、および 2019 上の Microsoft Active Directory	はい	はい	はい
Linux 上の OpenLDAP	いいえ	非対応	はい

Active Directory グローバルカタログサーバーは、レルムディレクトリとしてサポートされていません。グローバルカタログサーバーの詳細については、learn.microsoft.com の「Global Catalog」を参照してください。

（注） TS エージェントが別のパッシブ認証 ID ソース（ISE/ISE-PIC）と共有されている Windows Server 上の Microsoft Active Directory にインストールされている場合、Firewall Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firewall Management Center に記録されます。

サーバー グループの設定に関して次の点に注意してください。

- ユーザー グループまたはグループ内のユーザーに対してユーザー制御を実行するには、LDAP または Active Directory サーバーでユーザー グループを設定する必要があります。
- グループ名は LDAP で内部的に使用されているため、`s-` で開始することはできません。

  グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用すると、それらのグループまたは組織

単位内のユーザーはダウンロードされず、アイデンティティポリシーでは使用できません。

- サーバー上のサブグループのメンバーであるユーザーを含む（または除外する）Active Directory レルムを設定するには、Windows Server 2012 では、Active Directory のグループあたりのユーザー数が 5000 人以下であることが Microsoft により推奨されていることに注意してください。詳細については、MSDN の「Active Directory Maximum Limits—Scalability」を参照してください。

  必要に応じて、より多くのユーザーをサポートするため、このデフォルトの制限を引き上げるよう Active Directory サーバーの設定を変更できます。

- リモート デスクトップ サービス環境でサーバーにより報告されるユーザーを一意に識別するには、Cisco Terminal Services（TS）エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザーに別個のポートを割り当て、システムはこれらのユーザーを一意に識別できるようになります。（Microsoft により、ターミナル サービスという名称はリモート デスクトップ サービスに変更されました）。

  TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

サポートされているサーバー オブジェクト クラスと属性名

Secure Firewall Management Center がサーバからユーザ メタデータを取得できるようにするには、レルム内のサーバが、次の表に記載されている属性名を使用する必要があります。サーバ上の属性名が正しくない場合、Secure Firewall Management Center はその属性の情報を使ってデータベースに入力できなくなります。

表 *198 : Secure Firewall Management Center* フィールドへの属性名のマップ

メタデータ（Metadata）	Firewall Management Center 属性	LDAP オブジェクト クラス	Active Directory 属性	OpenLDAP 属性
LDAP ユーザー名	Username	• user • inetOrgPerson	samaccountname	cn uid
名	First Name		givenname	givenname
姓	Last Name		sn	sn
電子メール アドレス	Email		mail userprincipalname（mail に値が設定されていない場合）	mail
department	部署名		部署 distinguishedname（department に値が設定されていない場合）	ou
telephone number	Phone		telephonenumber	telephonenumber

（注） グループの LDAP オブジェクト クラスは、`group`、`groupOfNames`（Active Directory の場合は `group-of-names`）、または `groupOfUniqueNames` です。

オブジェクト クラスと属性の詳細については、次のリファレンスを参照してください。

- Microsoft Active Directory：
  - オブジェクト クラス：MSDN の「All Classes」
  - 属性：MSDN の「All Attributes」
- OpenLDAP：RFC 4512

Kerberos 認証の前提条件

キャプティブ ポータル ユーザーの認証に Kerberos を使用している場合は、次の点に注意してください。

ホスト名の文字の制限

Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります（Windows で設定されている NetBIOS の制限）。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に設定します。詳細については、Microsoft のマニュアルサイト「Naming conventions in Active Directory for computers, domains, sites, and OUs」で、次のような記事を参照してください。

DNS 応答の文字の制限

DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、RFC 6891 セクション 6.2.5 で説明されています。

レルム フィールド

次のフィールドを使用して、レルムを設定します。

レルムの設定（Realm Configuration）フィールド

これらの設定は、レルム内のすべての Active Directory サーバまたはドメイン コントローラ（別名ディレクトリ）に適用されます。

Name

レルムの一意の名前。

- アイデンティティ ポリシーにレルムを使用する場合、英数字や特殊文字に対応しています。
- RA VPN 設定でレルムを使用する場合は、英数字、ハイフン（-）、下線（_）、プラス（+）に対応しています。

説明

（オプション）レルムの説明を入力します。

タイプ

レルムのタイプで、Microsoft Active Directory 用の [AD]、その他のサポートされている LDAP リポジトリ用の [LDAP]、または [Local] です。サポートされている LDAP リポジトリの一覧については、レルムがサポートされているサーバー（2461 ページ）を参照してください。LDAP リポジトリを使用してキャプティブ ポータル ユーザーを認証できます。他はすべて Active Directory が必要です。

（注） キャプティブ ポータルのみ、LDAP レルムをサポートします。

レルムタイプ LOCAL は、ローカルユーザー設定の設定に使用されます。LOCAL レルムは、リモートアクセスユーザーの認証で使用されます。

LOCAL レルムの次のローカルユーザー情報を追加します。

- [Username]：ローカルユーザーの名前。
- [Password]：ローカルユーザーのパスワード。
- [Confirm Password]：ローカルユーザーのパスワードを確認します。

（注） LOCAL レルムにユーザーを追加するには、[Add another local user] をクリックします。

レルムの作成後にユーザーを追加し、ローカルユーザーのパスワードを更新できます。複数の LOCAL レルムも作成できますが、無効にすることはできません。

AD プライマリ ドメイン（AD Primary Domain）

Microsoft Active Directory レルム専用です。ユーザー認証が必要となる Active Directory サーバーのドメインです。

（注） すべての Microsoft Active Directory（AD）レルムに固有の [ADプライマリドメイン（AD Primary Domain）] を指定する必要があります。異なる Microsoft AD レルムに同じ [ADプライマリドメイン（AD Primary Domain）] を指定することはできますが、システムが適切に機能しなくなります。これは、システムにより各レルム内のすべてのユーザーとグループに 1 つの固有 ID が割り当てられるためです。そのため、システムは特定のユーザまたはグループを明確に識別することができません。ユーザーとグループが適切に識別されないため、同じ [ADプライマリドメイン（AD Primary Domain）] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザーとグループに割り当てるために発生します。そのため、システムは特定のユーザーまたはグループを明確に識別できません。

AD 参加ユーザー名（AD Join Username）、AD 参加パスワード（AD Join Password）
（レルムの編集時に [Realm Configuration] タブページで使用できます）。

Kerberos キャプティブ ポータル アクティブ認証を目的とした Microsoft Active Directory レルムでは、Active Directory ドメインでドメイン コンピュータ アカウントを作成するための適切な権限を持つ Active Directory ユーザーの識別用のユーザー名とパスワード。

次の点を考慮してください。

- DNS は、ドメイン名を Active Directory ドメイン コントローラの IP アドレスに解決できる必要があります。
- 指定するユーザは、コンピュータを Active Directory ドメインに参加させることができる必要があります。
- ユーザー名は完全修飾名である必要があります（たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します）。

Kerberos（またはKerberosをオプションとする場合に**HTTP ネゴシエート**）を、アイデンティティルールの [認証プロトコル（Authentication Protocol）] として選択する場合、選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行するように、[AD参加ユーザー名（AD Join Username）] と [AD参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） SHA-1 ハッシュアルゴリズムでは Active Directory サーバーにパスワードが保存されて安全ではないため、使用しないでください。詳細については、Open Web Application Security Project の Web サイトにある「Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet」や「Password Storage Cheat Sheet」などの参考資料を参照してください。

Active Directory との通信には SHA-256 を使用することを推奨します。

[ディレクトリ ユーザー名（Directory Username）] と [ディレクトリ パスワード（Directory Password）]

取得するユーザ情報に適切なアクセス権を持っているユーザの識別用のユーザ名とパスワード。

次の点に注意してください。

- Microsoft Active Directory の一部のバージョンでは、ユーザーとグループを読み取るために特定の権限が必要な場合があります。詳細については、Microsoft Active Directory に付属しているマニュアルを参照してください。
- OpenLDAP では、ユーザーのアクセス権限は、OpenLDAP の仕様書のセクション 8 で説明されている `<level>` パラメータにより決定されます。ユーザーの `<level>` は、`auth` 以上にする必要があります。
- ユーザ名は完全修飾名である必要があります（たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します）。

（注） SHA-1 ハッシュアルゴリズムでは Active Directory サーバーにパスワードが保存されて安全ではないため、使用しないでください。詳細については、Open Web Application Security Project の Web サイトにある「Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet」や「Password Storage Cheat Sheet」などの参考資料を参照してください。

Active Directory との通信には SHA-256 を使用することを推奨します。

ベース DN（Base DN）

（オプション）Secure Firewall Management Centerがユーザー データの検索を開始するサーバーのディレクトリ ツリー。ベースDNを指定しない場合、サーバーに接続できる場合、システムは最上位 DN を取得します。

通常、ベース識別名（DN）には企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、**ou=security,dc=example,dc=com** となります。

Group DN

（オプション）Secure Firewall Management Centerがグループ属性を持つユーザーを検索するサーバーのディレクトリ ツリー。サポートされているグループ属性の一覧については、サポートされているサーバー オブジェクト クラスと属性名 （2462 ページ）を参照してください。グループ DN を指定しない場合、サーバーに接続できる場合、システムは最上位 DN を取得します。

（注） 次に、ディレクトリサーバーのユーザー、グループ、DN でシステムがサポートする文字のリストを示します。次に示す文字以外を使用すると、システムがユーザーとグループをダウンロードできなくなる可能性があります。

エンティティ	サポートされている文字
ユーザー名	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
グループ名	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
ベース DN とグループ DN	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

ユーザー名では、どの場所でも（末尾を含む）スペースはサポートされていません。

既存のレルムを編集する場合、次のフィールドを使用できます。

[ユーザー セッション タイムアウト（User Session Timeout）]
（レルムの編集時に [Realm Configuration] タブページで使用できます）。

ユーザーセッションがタイムアウトするまでの分数を入力します。デフォルトは、ユーザのログイン イベントから 1440 分（24 時間）後です。このタイムアウトを過ぎると、ユーザーのセッションは終了します。ユーザーが再度ログインせずにネットワークにアクセスし続けている場合、ユーザーは Secure Firewall Management Center により不明として認識されます（[失敗したキャプティブポータルユーザー（Failed Captive Portal Users）] を除く）。

さらに、レルムなしで ISE/ISE-PIC を設定し、タイムアウトを超えた場合は、回避策が必要です。詳細については、Cisco TAC にお問い合わせください。

次のタイムアウト値を設定できます。

- [ユーザーエージェントおよびISE/ISE-PICユーザー（User Agent and ISE/ISE-PIC Users）]：パッシブ認証タイプであるユーザー エージェントまたは ISE/ISE-PIC によってトラッキングされるユーザーのタイムアウト。

  指定したタイムアウト値は、pxGrid SXP セッション トピック サブスクリプション（宛先 SGT マッピングなど）には適用されません。代わりに、ISE からの特定のマッピングの削除または更新メッセージがない限り、セッション トピック マッピングは保持されます。

ISE/ISE-PIC の詳細については、ISE/ISE-PIC アイデンティティ ソース （2497 ページ）を参照してください。

- [ターミナルサービスエージェントユーザー（Tterminal Services Agent Users）]：パッシブ認証タイプである TS エージェントによってトラッキングされるユーザーのタイムアウト。詳細については、ターミナル サービス（TS）エージェントのアイデンティティ ソース （2549 ページ）を参照してください。
- [キャプティブポータルユーザ（Captive Portal Users）]：アクティブ認証タイプであるキャプティブポータルを使用して正常にログインしたユーザのタイムアウト。詳細については、キャプティブ ポータルのアイデンティティ ソース （2519ページ）を参照してください。
- [失敗したキャプティブポータルユーザ（Failed Captive Portal Users）]：キャプティブポータルを使用して正常にログインしていないユーザのタイムアウト。Secure Firewall Management Center によってユーザが認証失敗ユーザとして認識されるまでの、[最大ログイン試行回数（Maximum login attempts）] を設定できます。アクセス コントロール ポリシーを使用して、認証失敗ユーザにネットワークへのアクセス権を付与することもできます。この場合は、そのユーザにこのタイムアウト値が適用されます。

  失敗したキャプティブ ポータル ログインの詳細については、キャプティブ ポータル フィールド （2536 ページ）を参照してください。
- [ゲストキャプティブポータルユーザ（Guest Captive Portal Users）]：キャプティブ ポータルにゲスト ユーザとしてログインしているユーザのタイムアウト。詳細については、「キャプティブ ポータルのアイデンティティ ソース （2519ページ）」を参照してください。

[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド

レルムのディレクトリ フィールド（Realm Directory Fields）

これらの設定は、レルム内の個々のサーバー（Active Directory ドメイン コントローラなど）に適用されます。

ホスト名/IP アドレス（Hostname/IP Address）

Active Directory ドメインコントローラマシンの完全修飾ホスト名。完全修飾名を確認するには、Active Directory サーバーの名前の検索 （2472 ページ）を参照してください。

キャプティブポータルの認証に Kerberos を使用している場合は、次のことも理解してください。

Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります（Windows で設定されている NetBIOS の制限）。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に設定します。詳細については、Microsoft のマニュアルサイト「Naming conventions

in Active Directory for computers, domains, sites, and OUs」で、次のような記事を参照してください。

DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、RFC 6891 セクション 6.2.5 で説明されています。

ポート

サーバーのポート。

暗号化（Encryption）

（強く推奨）使用する暗号化方式。

- **STARTTLS**：暗号化 LDAP 接続
- **LDAPS**：暗号化 LDAP 接続
- **なし**：非暗号化 LDAP 接続（保護されていないトラフィック）

Active Directory サーバーと安全に通信するには、Active Directory または LDAP に安全に接続する （2471 ページ）を参照してください。

CA Certificate

サーバーへの認証に使用する TLS/SSL 証明書。TLS/SSL 証明書を使用するために、**STARTTLS** または **LDAPS** を [暗号化（Encryption）] タイプとして設定できます。

認証に証明書を使用する場合、証明書のサーバー名は、サーバーの [Hostname/IP Address] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で **computer1.example.com** を使用している場合は、接続が失敗します。

ディレクトリサーバーへの接続に使用されるインターフェイス

Secure Firewall Threat Defense が Active Directory サーバーに安全に接続できるように、RA VPN 認証にのみ必要です。ただし、このインターフェイスは、ユーザーおよびグループのダウンロードには使用されません。

ルーテッド インターフェイス グループだけを選択できます。詳細については、インターフェイス（Interface） （1346 ページ）を参照してください。

次のいずれかをクリックします。

- ルートルックアップによる解決：ルーティングを使用して Active Directory サーバーに接続します。
- [インターフェイスの選択（Choose an interface）]：Active Directory サーバーに接続する特定の管理対象デバイス インターフェイス グループを選択します。

ユーザーの [同期（Synchronize）] フィールド

AD プライマリ ドメイン（AD Primary Domain）

Microsoft Active Directory レルム専用です。ユーザー認証が必要となる Active Directory サーバーのドメインです。

（注） すべての Microsoft Active Directory（AD）レルムに固有の [ADプライマリドメイン（AD Primary Domain）] を指定する必要があります。異なる Microsoft AD レルムに同じ [ADプライマリドメイン（AD Primary Domain）] を指定することはできますが、システムが適切に機能しなくなります。これは、システムにより各レルム内のすべてのユーザーとグループに 1 つの固有 ID が割り当てられるためです。そのため、システムは特定のユーザまたはグループを明確に識別することができません。ユーザーとグループが適切に識別されないため、同じ [ADプライマリドメイン（AD Primary Domain）] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザーとグループに割り当てるために発生します。そのため、システムは特定のユーザーまたはグループを明確に識別できません。

ユーザーとグループを検索するクエリを入力してください

[Base DN]：

（オプション）Firewall Management Center がユーザー データの検索を開始するサーバーのディレクトリ ツリー。

通常、ベース識別名（DN）には企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、**`ou=security,dc=example,dc=com`** となります。

[Group DN]：

（オプション）Firewall Management Center がグループ属性を持つユーザーを検索するサーバーのディレクトリ ツリー。サポートされているグループ属性の一覧については、サポートされているサーバーオブジェクトクラスと属性名（2462 ページ）を参照してください。

（注） グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用した場合、それらのグループのユーザーはダウンロードされず、ID ポリシーで使用できないためです。

[Load Groups]

ユーザー認識用およびユーザー制御用にユーザーとグループをダウンロードできるようになります。

[使用可能なグループ（Available Groups）]、[含むに追加する（Add to Include）]、[除外するに追加する（Add to Exclude）]

ポリシーで使用できるグループを制限します。

- [使用可能なグループ（Available Groups）] フィールドに表示されているグループは、グループを [含めるグループとユーザー（Included Groups and Users）] または [除外するグループとユーザー（Excluded Groups and Users）] フィールドに移動しない限り、ポリシーで利用できます。
- グループを [含めるグループとユーザー（Included Groups and Users）] フィールドに移動させた場合は、それらのグループとそれらのグループに含まれるユーザーだけがダウンロードされ、ユーザーデータはユーザー認識やユーザー制御に利用できます。
- グループを [除外するグループとユーザー（Excluded Groups and Users）] フィールドに移動させた場合は、それ以外のすべてのグループとそれらのグループに含まれるユーザーがダウンロードされ、ユーザー認識やユーザー制御に利用できます。
- 含まれないグループのユーザーを含めるには、[ユーザーの包含（User Inclusion）] の下のフィールドにそのユーザー名を入力し、[追加（Add）] をクリックします。
- 除外されないグループのユーザーを除外するには、[ユーザーの除外（User Exclusion）] の下のフィールドにそのユーザー名を入力し、[追加（Add）] をクリックします。

（注） Firewall Management Center にダウンロードされるユーザーは、数式 **R = I - (E+e) + i** を使用して計算されます。

- R はダウンロードしたユーザーのリストです。
- I は含まれているグループです。
- E は除外されているグループです。
- e は除外されているユーザーです。
- i は含まれているユーザーです。

[Synchronize Now]
クリックして、グループとユーザーを AD と同期します。

自動同期の開始時間
AD からユーザーとグループをダウンロードする時間と時間間隔を入力します。

Active Directory または LDAP に安全に接続する

Active Directory または LDAP サーバーおよび Secure Firewall Management Center（強く推奨）間でセキュアな接続を確立するには、次のすべてのタスクを実行する必要があります。

- サーバーのルート証明書をエクスポートします。
- ルート証明書を信頼できる CA 証明書（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**）として Secure Firewall Management Center にインポートします。
- サーバーの完全修飾名を検索します。

- レルムディレクトリを作成します。

詳細については、次のいずれかのタスクを参照してください。

関連トピック

Active Directory サーバーのルート証明書のエクスポート （2473 ページ）
Active Directory サーバーの名前の検索 （2472 ページ）
LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）

Active Directory サーバーの名前の検索

Firewall Management Center でレルムディレクトリを設定するには、次の手順で説明するように、完全修飾サーバー名を把握しておく必要があります。

これらのタスクは、Microsoft Active Directory にのみ適用されます。LDAP を使用する場合は、手順について適切な参考資料を参照してください。

始める前に

コンピュータの名前を表示できる権限を持つユーザーとして Active Directory サーバーにログインする必要があります。

手順

ステップ 1 Active Directory サーバーにログインします。
ステップ 2 [開始（Start）] をクリックします。
ステップ 3 [この PC（This PC）] を右クリックします。
ステップ 4 [プロパティ（Properties）] をクリックします。
ステップ 5 [Advanced System Settings] をクリックします。
ステップ 6 [コンピュータ名（Computer Name）] タブをクリックします。
ステップ 7 [フルコンピュータ名（Full computer name）] の値をメモします。
Firewall Management Center でレルムディレクトリを構成する際は、この正確な名前を入力する必要があります。

次のタスク

LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）。

関連トピック

Active Directory サーバーのルート証明書のエクスポート （2473 ページ）

Active Directory サーバーのルート証明書のエクスポート

次のタスクでは、Active Directory サーバーのルート証明書をエクスポートする方法について説明します。これは、ユーザーアイデンティティ情報を取得するために Firewall Management Center に安全に接続する際に必要になります。

これらのタスクは、Microsoft Active Directory にのみ適用されます。LDAP を使用する場合は、手順について適切な参考資料を参照してください。

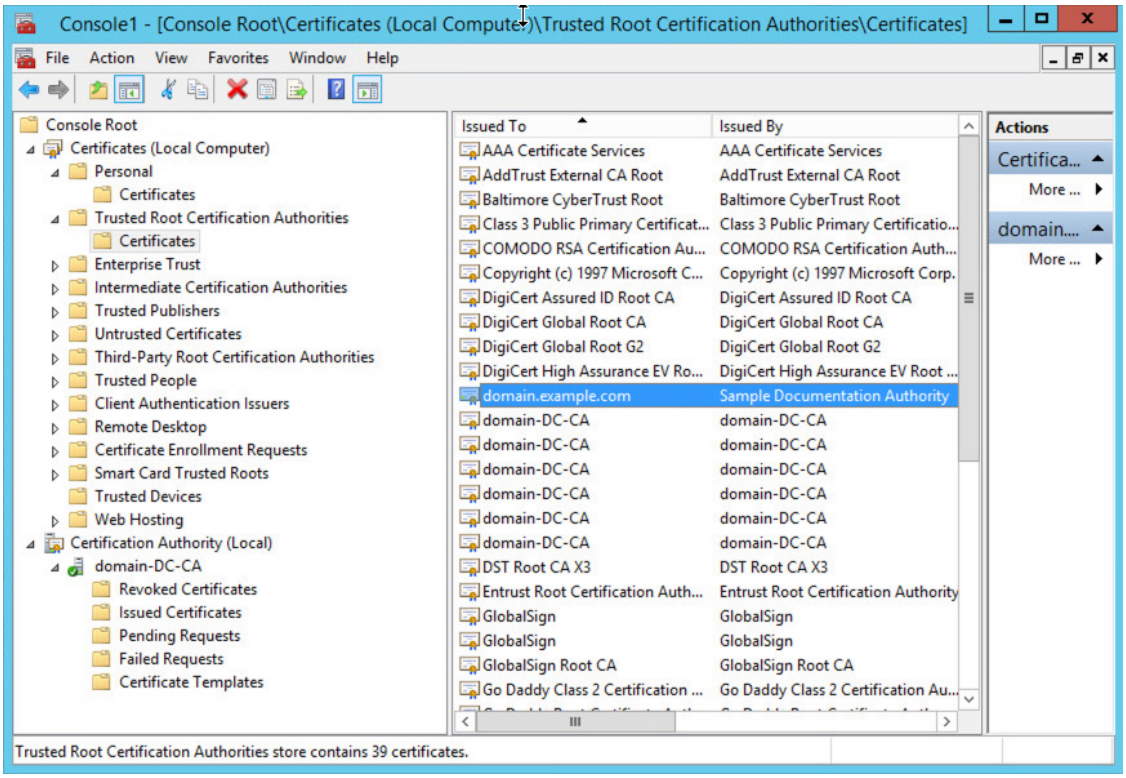
始める前に

Active Directory サーバーのルート証明書の名前が分かっている必要があります。ルート証明書の名前がドメインと同じである場合も異なっている場合もあります。次の手順は、名前を確認する一つの方法を示しています。ただし、他の方法も考えられます。

手順

ステップ 1 以下は、Active Directory サーバーのルート証明書の名前を確認する一つの方法です。詳細については、Microsoft 社のドキュメントを参照してください。

a) Microsoft 管理コンソールを実行する権限を持つユーザーとして Active Directory サーバーにログインします。
b) [開始（Start）] をクリックして、**mmc** を入力します。
c) **[ファイル（File）]** > **[スナップインの追加と削除（Add/Remove Snap-in）]** をクリックします。
d) 左側のペインにある [使用可能なスナップイン（Available Snap-ins）] リストから、[証明書（ローカル）（Certificates (local)）] をクリックします。
e) [追加（Add）] をクリックします。
f) [証明書スナップイン（Certificates snap-in）] ダイアログボックスで、[コンピュータアカウント（Computer Account）] をクリックし、[次へ（Next）] をクリックします。
g) [コンピュータの選択（Select Computer）] ダイアログボックスで [ローカルコンピュータ（Local Computer）] をクリックし、[終了（Finish）] をクリックします。
h) Windows Server 2012 のみ。前の手順を繰り返して、証明機関スナップインを追加します。
i) **[コンソールルート（Console Root）]** > **[信頼された証明機関（Trusted Certification Authorities）]** > **[証明書（Certificates）]** をクリックします。
サーバーの信頼できる証明書が右側のペインに表示されます。次の図は Windows Server 2012 の例であり、環境によっては異なっている可能性があります。



ステップ 2 **certutil** コマンドを使用して証明書をエクスポートします。

これは、証明書をエクスポートする一つの方法に過ぎません。これは、証明書をエクスポートする便利な方法です。特に、Web ブラウザを実行して Active Directory サーバーから Firewall Management Center に接続できる場合に便利です。

a) [開始（Start）] をクリックして、**cmd** を入力します。

b) **certutil -ca.cert** *certificate-name* コマンドを入力します。
サーバーの証明書が画面に表示されます。

c) **-----BEGIN CERTIFICATE-----** で始まり **-----END CERTIFICATE-----** で終わる（これらの文字列を含む）証明書全体をクリップボードにコピーします。

次のタスク

信頼できる CA オブジェクトの追加 （1359 ページ） の説明に従って、Active Directory サーバーの証明書を信頼できる CA 証明書として Firewall Management Center にインポートします。

関連トピック

Active Directory サーバーの名前の検索 （2472 ページ）

ユーザーとグループの同期

ユーザーとグループの同期とは、グループとグループ内のユーザーに対して設定したレルムとディレクトリに対して、Firewall Management Center がクエリを実行することを意味します。Firewall Management Center が検出したすべてのユーザーを ID ポリシーで使用できます。

問題が見つかった場合は、Firewall Management Center がロードできないユーザーとグループを含むレルムを追加する必要があります。詳細は、レルムおよび信頼できるドメイン（2458 ページ）を参照してください。

始める前に

各 Active Directory ドメインの Secure Firewall Management Center レルムと、各フォレストの Active Director ドメインコントローラごとの Firewall Management Center ディレクトリを作成します。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452 ページ） を参照してください。

ユーザー制御で使用するユーザーを含むドメインに対してのみレルムを作成する必要があります。

未定の ネストできます。 Secure Firewall Management Center はそれらのグループとグループに含まれるユーザーをダウンロードします。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452ページ）の説明に従い、必要に応じて、ダウンロードするグループとユーザーを制限できます。

ドメインの代替ユーザープリンシパル名（UPN）サフィックスではなく、ドメインの元のドメイン名を使用してレルムを作成する必要があります。そうしない場合、ユーザーとグループはダウンロードに失敗し、アイデンティティポリシーは適用されません。たとえば、元のドメインが `domain.example.com` で、代替の UPN 名が `domain2.mydomain.com` の場合は、`domain.example.com` を使用するようにレルムを設定する必要があります。代替の UPN サフィックスの設定の詳細については、learn.microsoft.com の「Configuring Alternate Login ID」などのリソースを参照してください。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** をクリックします。

ステップ 3 各レルムの横にある [ダウンロード（download）]（ ） をクリックします。

ステップ 4 結果を表示するには、[Sync Results] タブをクリックします。
[Realms] 列に、Active Directory フォレスト内のユーザーとグループの同期に関する問題の有無が示されます。各レルムの横にある次のインジケータを探します。

[Realms] 列のインジケータ	意味
（なし）	エラーなく同期されたすべてのユーザーとグループ。対処不要です。
黄色い三角形（ ）	ユーザーとグループの同期中に問題が発生しました。各 Active Directory ドメインのレルムと各 Active Directory ドメインコントローラのディレクトリを追加したことを確認します。 詳細については、クロスドメイン信頼のトラブルシュート （2492 ページ）を参照してください。

レルムシーケンスの作成

次の手順で、レルムシーケンスを作成できます。レルムシーケンスは、システムがアイデンティティポリシーを適用するときに検索するレルムの順序付きリストです。レルムを追加する場合とまったく同じ方法で、アイデンティティルールにレルムシーケンスを追加します。違いは、システムがアイデンティティポリシーを適用するときに、レルムシーケンスで指定された順序ですべてのレルムが検索されることです。

始める前に

Active Directory サーバーとの接続にそれぞれ対応する、少なくとも 2 つのレルムを作成して有効にする必要があります。LDAP レルムのレルムシーケンスは作成できません。

LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）の説明に従って、レルムを作成します。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [レルムシーケンス（Realm Sequences）]** をクリックします。

ステップ 3 [レルムシーケンス（Realm Sequences）] タブをクリックします。

ステップ 4 [シーケンスを追加（Add Sequence）] をクリックします。

ステップ 5 [Name] フィールドに、レルムシーケンスを識別するための名前を入力します。

ステップ 6 （オプション）[Description] フィールドに、レルムシーケンスの説明を入力します。

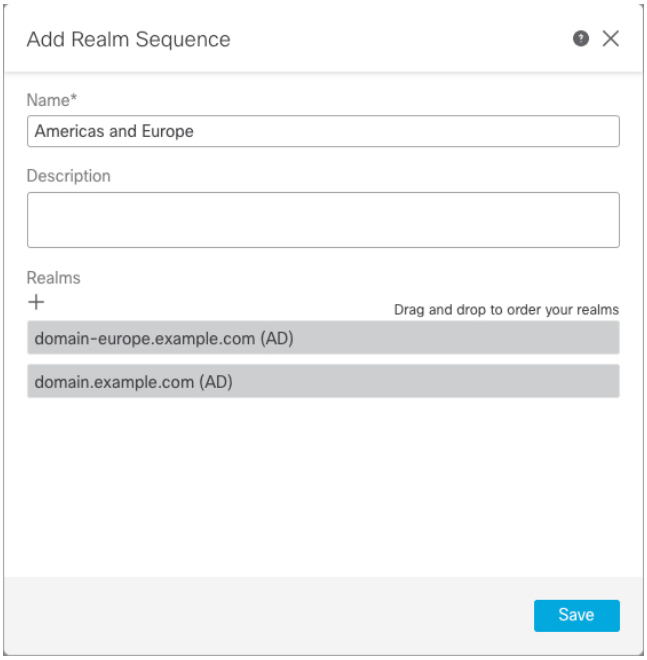
ステップ 7 [Realms]で、[追加（Add）] (＋) をクリックします。

ステップ 8 シーケンスに追加する各レルムの名前をクリックします。

検索を絞り込むには、[Filter] フィールドにレルム名のすべてまたは一部を入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Add Realm Sequence] ダイアログボックスで、システムが検索する順序でレルムをドラッグアンドドロップします。
次の図に、2 つのレルムで構成されるレルムシーケンスの例を示します。
domain-europe.example.com レルムは、**domain.example.com** レルムの前にユーザーに対して検索されます。



ステップ 11 [Save] をクリックします。

次のタスク

「アイデンティティ ポリシーの作成 （2555 ページ）」を参照してください。

クロスドメイン信頼のために Firewall Management Center を設定する：セットアップ

ここでは、いくつかのトピックを通じて、クロスドメイン信頼を持つ2つのレルムを使用した Firewall Management Center の設定方法を解説します。

この段階的な手順の例には、2 つのフォレスト：**forest.example.com** と **eastforest.example.com** が含まれます。フォレストは、各フォレスト内の特定のユーザーおよびグループが他のフォレスト内の Microsoft AD によって認証されるように設定されます。

次に、この例で使用する設定例を示します。

前述の例を使用して、Firewall Management Center を次のように設定します。

- アクセス コントロール ポリシーで制御するユーザーを含む **forest.example.com** 内の任意のドメインのレルムとディレクトリ
- アクセス コントロール ポリシーで制御するユーザーを含む **eastforest.example.com** 内の任意のドメインのレルムとディレクトリ

この例の各レルムには、Firewall Management Center でディレクトリとして設定されている 1 つのドメインコントローラがあります。この例のディレクトリは、次のように設定されています。

- **forest.example.com**
  - ユーザーのベース識別名（DN）：**ou=UsersWest,dc=forest,dc=example,dc=com**
  - グループのベース DN：**ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - ユーザーのベース DN：**ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - グループのベース DN：**ou=EastEngineering,dc=eastforest,dc=example,dc=com**

関連トピック

クロスドメイン信頼のために Secure Firewall Management Center を設定する。ステップ 1：レルムとディレクトリの設定 （2478 ページ）

クロスドメイン信頼のために Secure Firewall Management Center を設定する。ステップ 1：レルムとディレクトリの設定

これは、クロスドメインの信頼関係で設定された Active Directory サーバーを認識するように Firewall Management Center を設定する方法を説明する、段階的な手順の最初のタスクです。この設定は、企業組織で一般的になりつつあります。この設定例の概要については、クロスドメ

イン信頼のために Firewall Management Center を設定する：セットアップ（2477 ページ）を参照してください。

ドメインごとに 1 つのレルムとドメインコントローラごとに 1 つのディレクトリを使用して設定したシステムでは、最大 100,000 の外部セキュリティプリンシパル（ユーザーとグループ）を検出できます。これらの外部セキュリティプリンシパルが別のレルムでダウンロードされたユーザーと一致する場合は、アクセス コントロール ポリシーで使用できます。

始める前に

Microsoft Active Directory サーバーは、クロスドメインの信頼関係で設定する必要があります。詳細については、レルムおよび信頼できるドメイン （2458 ページ）を参照してください。

LDAP でユーザーを認証する場合、この手順は使用できません。

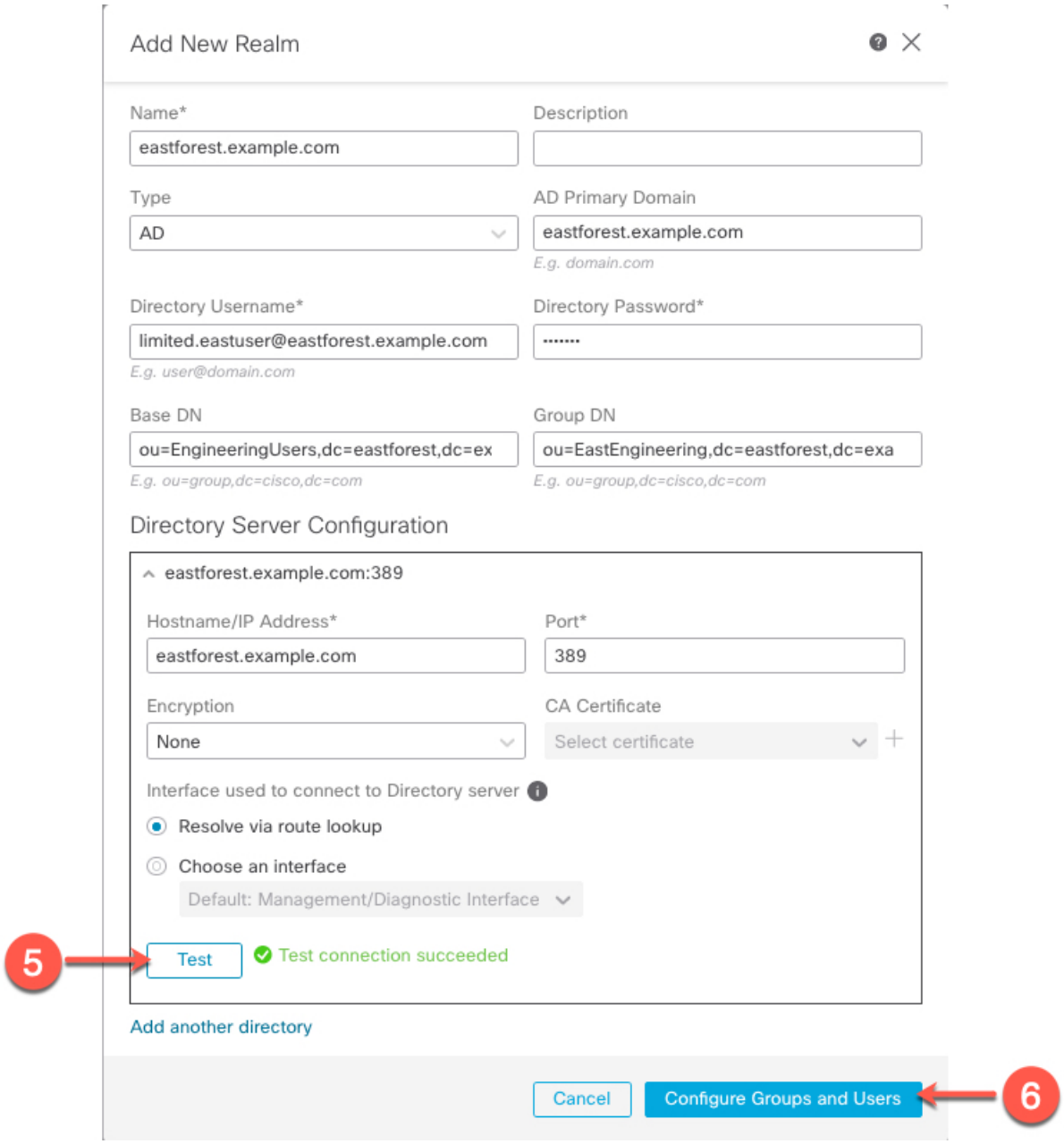
手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 3 **[レルムを追加（Add Realm）] > [Active Directory/LDAP]** をクリックします。

ステップ 4 **forest.example.com** を設定するために、次の情報を入力します。



（注）

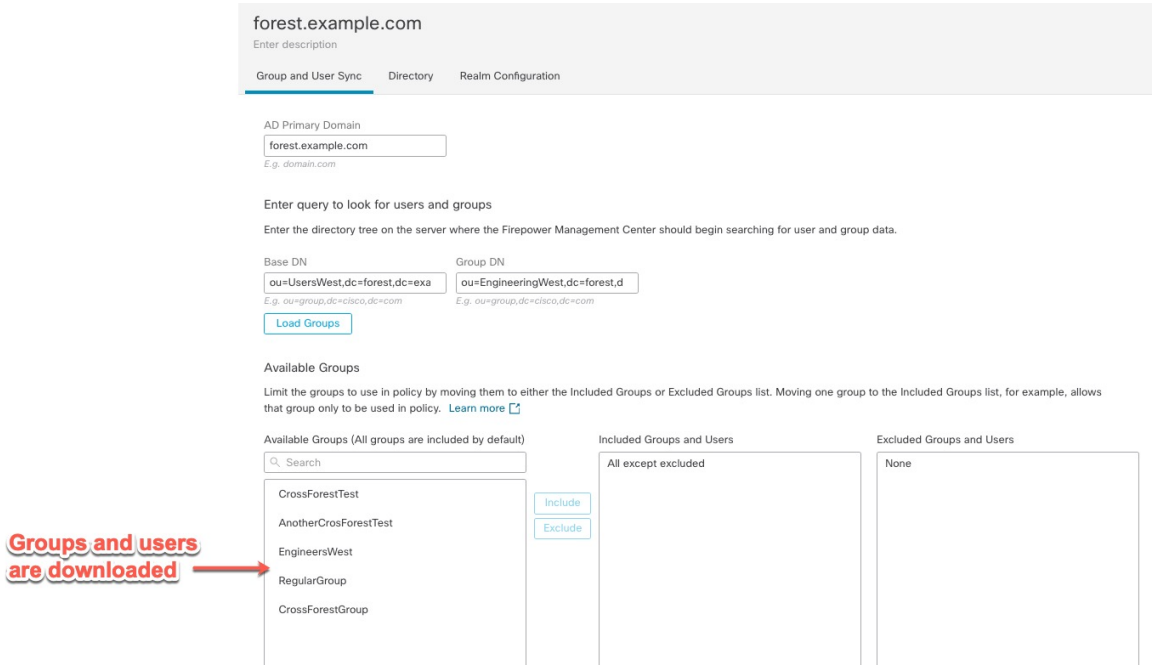
[Directory Username] には、Active Directory ドメイン内の任意のユーザーを指定できます。特別な権限は必要ありません。

ディレクトリサーバーへの接続に使用されるインターフェイスは、Active Directory サーバーに接続できる任意のインターフェイスです。

ステップ 5 [Test] をクリックし、テストが成功することを確認してから続行します。

ステップ 6 [Configure Groups and Users] をクリックします。

ステップ 7　設定が成功すると、次のようなページが表示されます。



（注）
グループとユーザーがダウンロードされていない場合は、[Base DN] フィールドと [Groups DN] フィールドの値を確認し、[Load Groups] をクリックします。

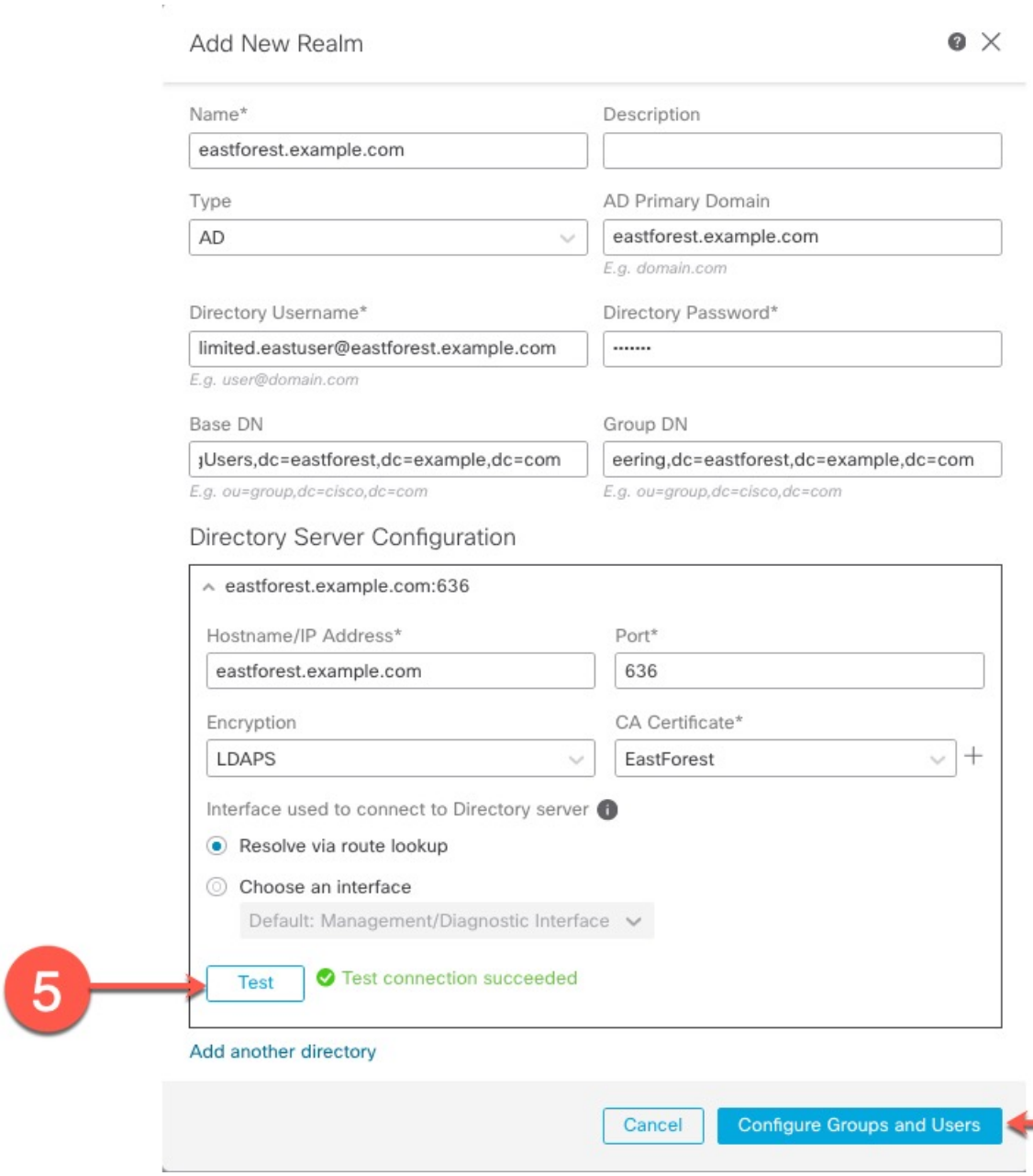
このページでは、その他のオプション設定を使用できます。詳細については、レルム フィールド（2464 ページ）および[レルムディレクトリ（Realm Directory）]および[同期（Synchronize）]フィールド（2468 ページ）を参照してください。

ステップ 8　このページまたはタブページで変更を行った場合は、[Save] をクリックします。

ステップ 9　**[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 10　[レルムを追加（Add Realm）] をクリックします。

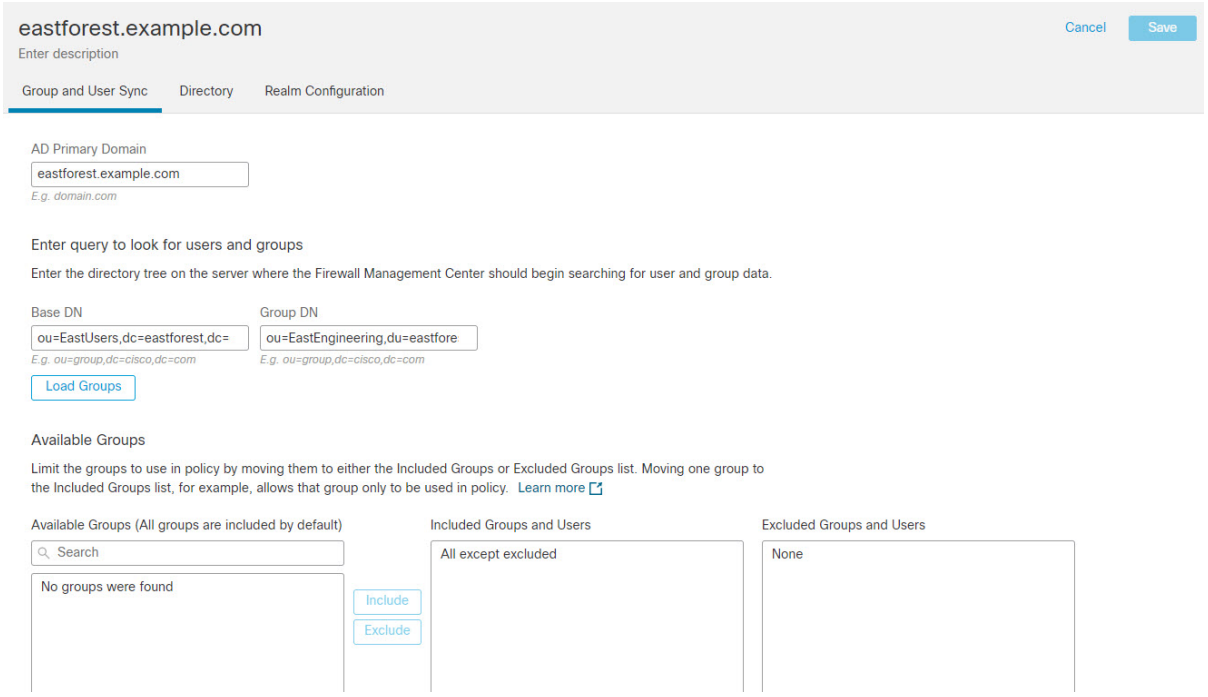
ステップ 11　**eastforest.example.com** を設定するために、次の情報を入力します。



ステップ 12 [Test] をクリックし、テストが成功することを確認してから続行します。

ステップ 13 [Configure Groups and Users] をクリックします。

ステップ 14 設定が成功すると、次のようなページが表示されます。



関連トピック

クロスドメイン信頼のための Secure Firewall Management Center の設定。ステップ 2：ユーザーとグループの同期 （2483 ページ）

クロスドメイン信頼のための Secure Firewall Management Center の設定。ステップ 2：ユーザーとグループの同期

クロスドメインの信頼関係を持つ 2 つ以上の Active Directory サーバーを設定したら、ユーザーとグループをダウンロードする必要があります。このプロセスでは、Active Directory の設定で問題が発生する可能性があります（一方の Active Directory ドメインにはグループまたはユーザーがダウンロードされていて、もう一方にはダウンロードされていない場合など）。

始める前に

クロスドメイン信頼のために Secure Firewall Management Center を設定する。ステップ 1：レルムとディレクトリの設定 （2478 ページ） で説明されている作業を実行したことを確認します。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** をクリックします。

ステップ 3 クロスドメイン信頼の任意のレルムの行の末尾で、[今すぐダウンロード（Download Now）]（ ）をクリックし、[はい（Yes）] をクリックします。

ステップ 4 **チェックマーク**（ ）（[Notifications]）> [Tasks] をクリックします。

グループとユーザーのダウンロードに失敗した場合は、再試行してください。後続の試行が失敗した場合は、レルムフィールド（2464ページ）および[レルムディレクトリ（Realm Directory）]および[同期（Synchronize）]フィールド（2468ページ）の説明に従い、レルムとディレクトリの設定を確認します。

ステップ 5 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [結果を同期（Sync Results）]** をクリックします。

関連トピック

クロスドメイン信頼のための Secure Firewall Management Center の設定。ステップ 3：問題の解決 （2484 ページ）

クロスドメイン信頼のための Secure Firewall Management Center の設定。ステップ 3：問題の解決

Firewall Management Center でクロスドメイン信頼を設定する最後の手順は、ユーザーとグループがエラーなしでダウンロードされるようにすることです。ユーザーとグループが適切にダウンロードされない一般的な理由は、ユーザーとグループが属するレルムが Firewall Management Center にダウンロードされていないことです。

このトピックでは、ドメインコントローラ階層でグループを検索するようにレルムが設定されていないため、1 つのフォレストで参照されているグループをダウンロードできないことを診断する方法について説明します。

始める前に

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

[Realms] 列で、レルムの名前の横に **黄色い三角形**（ ）が表示されている場合、解決する必要がある問題があります。表示されていない場合、正しく設定されているため、終了できます。

ステップ 3 問題を表示するレルムからユーザーとグループを再度ダウンロードします。

a) [Realms] タブをクリックします。

b) [(Download Now)] をクリックし、[Yes] をクリックします。

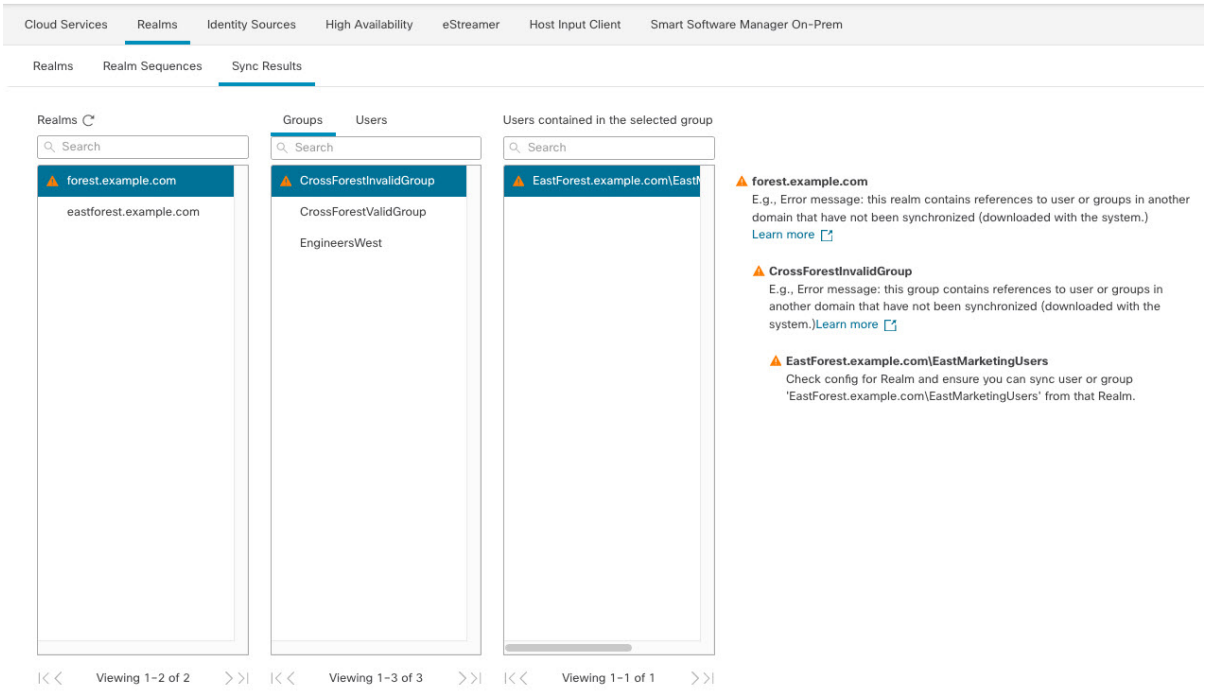
ステップ 4 [Sync Results] タブページをクリックします。

[Realms] カラムに **黄色い三角形**（⚠） が表示されている場合は、問題のあるレルムの横にある **黄色い三角形**（⚠） をクリックします。

ステップ 5 中央の列で、[Groups] または [Users] をクリックして詳細情報を検索します。

ステップ 6 [Groups] または [Users] タブページで、**黄色い三角形**（⚠） をクリックして詳細情報を表示します。

右側の列には、問題の原因を特定できる十分な情報が表示されます。



前述の例では、**forest.example.com** には、Firewall Management Center によってダウンロードされていない別のグループ **EastMarketingUsers** を含むクロスドメイングループ **CrossForestInvalidGroup** が含まれています。**eastforest.example.com** レルムを再度同期した後、エラーが解決しない場合は、Active Directory ドメインコントローラに **EastMarketingUsers** が含まれていない可能性があります。

この問題を解決するには、次を実行します。

- **CrossForestInvalidGroup** から **EastMarketingUsers** を削除し、**forest.example.com** レルムを再度同期して、再確認します。
- **eastforest.example.com** レルムの [Group DN] から **ou=EastEngineering** 値を削除します。これにより、Firewall Management Center は Active Directory 階層の最上位レベルからグループを取得し、**eastforest.example.com** を同期して再確認します。

レルムの管理

この項では、[レルム（Realms）]ページ上のコントロールを使用して、レルムに関するさまざまなメンテナンスタスクを実行する方法について説明します。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。。 代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 3 レルムを削除するには、[削除（Delete）]（） をクリックします。

ステップ 4 レルムを編集するには、レルムの横にある [編集（Edit）]（） をクリックし、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）の説明に従って変更を行います。

ステップ 5 レルムを有効にするには、[状態（State）] を右にスライドします。レルムを無効にするには、左にスライドします。

ステップ 6 ユーザーおよびユーザーグループをダウンロードするには、[ダウンロード（download）]（）をクリックします。

ステップ 7 レルムをコピーするには、[コピー（Copy）]（） をクリックします。

ステップ 8 レルムを比較する方法については、レルムの比較 （2486 ページ）を参照してください。

レルムの比較

このタスクを実行するには、管理者、アクセス管理者、ネットワーク管理者、またはセキュリティ承認者である必要があります。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 3 [レルムの比較（Compare Realms）] をクリックします。

ステップ 4 [比較対象（Compare Against）] リストから [レルムの比較（Compare Realm）] を選択します。

ステップ 5 [レルム A（Realm A）] および [レルム B（Realm B）] リストから比較するレルムを選択します。

ステップ 6 [OK] をクリック

ステップ 7 個々の変更を選択するには、タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックします。

ステップ 8 （オプション）[比較レポート（Comparison Report）] をクリックして、レルム比較レポートを生成します。

ステップ 9 （オプション）[新しい比較（New Comparison）] をクリックして、新しいレルム比較ビューを生成します。

レルムとユーザーのダウンロードのトラブルシュート

予期しないサーバー接続の動作に気付いたら、レルム設定、デバイス設定、またはサーバー設定の調整を検討してください。関連の他のトラブルシューティングについては、次を参照してください。

- ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング （2514 ページ）
- TS エージェント アイデンティティ ソースのトラブルシューティング （2551 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （2539 ページ）
- リモートアクセス VPN アイデンティティ ソースのトラブルシューティング （2545 ページ）
- ユーザー制御のトラブルシューティング （2569 ページ）

症状: レルムとグループはレポートされますが、ダウンロードされません

Secure Firewall Management Center のヘルスモニターは、ユーザーまたはレルムの不一致を通知します。これらは次のように定義されています。

- ユーザーの不一致：ユーザーは、ダウンロードされることなく Secure Firewall Management Center に報告されます。

  ユーザーの不一致の一般的な理由は、ユーザーが Secure Firewall Management Center へのダウンロードから除外されたグループに属していることです。Review the information discussed in Cisco Secure Firewall Management Center デバイス構成ガイド.

- レルムの不一致：ユーザーが、Firewall Management Center に認識されていないレルムに対応するドメインにログインした場合に不一致が起きます。

たとえば、Firewall Management Center で **domain.example.com** というドメインに対応するレルムを定義していても、**another-domain.example.com** というドメインからログインがレポートさ

れる場合、これはレルムの不一致となります。このドメイン内のユーザーはFirewall Management Centerによって[不明（Unknown）]と識別されます。

あるヘルス警告がトリガーされると、パーセンテージの不一致のしきい値を設定します。次に例を示します。

- 50%のデフォルトの不一致のしきい値を使用すると、2つのミスマッチ レルム8つの着信セッションでは、不一致割合は、25%と警告はトリガーされません。
- 30%の不一致のしきい値を設定すると、3つのミスマッチ レルム5つの着信セッションでは、不一致割合は、60%および警告がトリガーされます。

不明なユーザーアイデンティティルールに一致しないには、ポリシーに適用されていません。（不明ユーザーに対してアイデンティティルールをセットアップすることはできますが、ユーザーとレルムを正確に識別することによってルールの数を最小限に保つことをお勧めします。）

詳細については、レルムまたはユーザーの不一致の検出（2491ページ）を参照してください。

症状：ユーザがダウンロードされない

考えられる原因は次のとおりです。

- レルムの[タイプ（Type）]が正しく設定されていない場合は、システムにより必要とされる属性とリポジトリにより提供される属性が一致しないため、ユーザーとグループをダウンロードできません。たとえば、Microsoft Active Directory レルムの[タイプ（Type）]を[LDAP]として設定すると、システムでは`uid`属性が必要になり、この属性はActive Directoryでは`none`に設定されています。（Active Directory リポジトリでは、ユーザ ID に`sAMAccountName`が使用されます。）

  ソリューション：レルムの[タイプ（Type）]フィールドを適切に設定します。Microsoft Active Directoryの場合は[AD]に設定し、サポートされている別のLDAPリポジトリの場合は[LDAP]に設定します。

- グループ名または組織単位名に特殊文字が使用されているActive Directoryグループのユーザーは、アイデンティティポリシールールで使用できない可能性があります。たとえば、グループ名または組織単位名にアスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字が含まれている場合、これらのグループ内のユーザーはダウンロードされず、アイデンティティ ポリシーで使用できません。

  解決策：グループ名または組織単位名から特殊文字を削除します。

重要 Secure Firewall Management Centerと Active Directoryドメインコントローラ間の遅延を削減するには、地理的にSecure Firewall Management Centerにできるだけ近いレルムディレクトリ（つまり、ドメインコントローラ）を構成することを強くお勧めします。

たとえば、Secure Firewall Management Centerが北米にある場合は、同様に北米にあるレルムディレクトリを構成します。このように構成しないと、ユーザーやグループのダウンロードがタイムアウトするなどの問題が発生する可能性があります。

症状：レルム内の一部のユーザーがダウンロードされない

考えられる原因は次のとおりです。

- 1 つのレルムで最大数を超えるユーザーをダウンロードしようとすると、最大ユーザー数でダウンロードが停止し、正常性アラートが表示されます。ユーザーダウンロードの制限は、Secure Firewall Management Center モデルごとに設定されています。詳細については、Microsoft Active Directory のユーザー制限 （2445 ページ）を参照してください。
- すべてのユーザーは、グループのメンバーである必要があります。グループのメンバーでないユーザーはダウンロードされません。

症状：アクセス コントロール ポリシーがグループのメンバーシップと一致しない

この解決策は、他の AD ドメインとの信頼関係にある AD ドメインに適用されます。以下の説明で、外部ドメイン ドメインは、ユーザーがログインするドメイン以外のドメインを指します。

ユーザーが信頼されている外部ドメインで定義されたグループに属している場合、Secure Firewall Management Center は外部ドメインのメンバーシップを追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン コントローラ 1 と 2 は相互に信頼している
- グループ A はドメイン コントローラ 2 で定義されている
- コントローラ 1 のユーザー `mparvinder` はグループ A のメンバーである

ユーザー `mparvinder` はグループ A に属しているものの、メンバーシップグループ A を指定する Secure Firewall Management Center のアクセス コントロール ポリシー ルールが一致しません。

解決策：グループ A に属する、すべてのドメイン 1 のアカウントを含むドメイン コントローラ 1 に同様のグループを作成します。グループ A またはグループ B のすべてのメンバーに一致するように、アクセス コントロール ポリシー ルールを変更します。

症状：アクセス コントロール ポリシーが子ドメインのメンバーシップと一致しない

ユーザーが親ドメインの子であるドメインに属している場合、Firepower はドメイン間の親/子関係を追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン `child.parent.com` はドメイン `parent.com` の子である
- ユーザー `mparvinder` は `child.parent.com` で定義されている

ユーザー `mparvinder` が子ドメインに属しているが、`parent.com` と一致する Firepower アクセス コントロール ポリシーが `child.parent.com` ドメインの `mparvinder` と一致しません。

解決策：`parent.com` または `child.parent.com` のいずれかのメンバーシップに一致するようにアクセス コントロール ポリシー ルールを変更します。

症状：レルムまたはレルム ディレクトリのテストが失敗する

ディレクトリ ページの [テスト（Test）] ボタンは、入力したホスト名または IP アドレスに LDAP クエリを送信します。失敗した場合は、次を確認してください。

- 入力した [ホスト名（Hostname）] が、LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- 入力した [IPアドレス（IP Address）] が有効である。

レルム設定ページの **[AD参加のテスト（Test AD Join）]** ボタンは、次のことを確認します。

- DNS が、[ADプライマリドメイン（AD Primary Domain）] を LDAP サーバーまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- [AD参加ユーザ名（AD Join Username）] と [AD参加パスワード（AD Join Password）] が正しい。

  [AD参加ユーザ名（AD Join Username）] は完全修飾名である必要があります（たとえば、**`administrator`** ではなく **`administrator@mydomain.com`** を使用します）。
- ドメイン内にコンピュータを作成し、ドメインに Secure Firewall Management Center をドメインコンピュータとして参加させるための十分な権限がユーザーにある。

症状：予期しない時間にユーザー タイムアウトが発生する

予期しない間隔でユーザータイムアウトが実行されていることに気付いたら、ISE/ISE-PIC サーバーの時間が Secure Firewall Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザーのタイムアウトが実行される可能性があります。

予期しない間隔でユーザータイムアウトが実行されていることに気付いたら、ISE/ISE-PIC、または TS エージェントサーバーの時間が Secure Firewall Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザーのタイムアウトが実行される可能性があります。

症状：未知の ISE/ISE-PIC ユーザーのユーザーデータが Web インターフェイスで表示されない

システムはデータがまだデータベースにない ISE/ISE-PIC または TS エージェントユーザーのアクティビティを検出すると、サーバーからそれらに関する情報を取得します。状況によっては、システムが Microsoft Windows サーバーからこの情報を正常に取得するためにさらに時間がかかることもあります。データ取得が成功するまで、ISE/ISE-PIC または TS エージェントユーザーから見えるアクティビティは Web インターフェイスに表示されません。

これにより、アクセスコントロールルールを使ったユーザートラフィックの処理も妨げられることがある点に注意してください。

症状：イベントのユーザ データが想定外の内容になる

ユーザーやユーザーアクティビティイベントに想定外の IP アドレスが含まれる場合は、レルムを確認します。複数のレルムに同一の [AD プライマリ ドメイン（AD Primary Domain）] の値を設定することはできません。

症状：ターミナル サーバからログインしたユーザが、システムによって一意に識別されない

導入されている構成にターミナルサーバーが含まれ、これに接続されている 1 つまたは複数のサーバーにレルムが設定されている場合は、ターミナルサーバー環境でのユーザーログインを正確に報告するため Cisco Terminal Services（TS）エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザーに別個のポートを割り当て、システムはこれらのユーザーを Web インターフェイスで一意に識別できるようになります。

TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

レルムまたはユーザーの不一致の検出

この項では、レルムまたはユーザーの不一致を検出する方法について説明します。これらは次のように定義されています。

- ユーザーの不一致：ユーザーは、ダウンロードされることなく Secure Firewall Management Center に報告されます。

  ユーザーの不一致の一般的な理由は、ユーザーが Secure Firewall Management Center へのダウンロードから除外されたグループに属していることです。Review the information discussed in Cisco Secure Firewall Management Center デバイス構成ガイド.

- レルムの不一致：ユーザーが、Firewall Management Center に認識されていないレルムに対応するドメインにログインした場合に不一致が起きます。

詳細については、レルムとユーザーのダウンロードのトラブルシュート（2487ページ）を参照してください。

不明なユーザーアイデンティティルールに一致しないには、ポリシーに適用されていません。（不明ユーザーに対してアイデンティティルールをセットアップすることはできますが、ユーザーとレルムを正確に識別することによってルールの数を最小限に保つことをお勧めします。）

手順

ステップ 1 レルムまたはユーザーの不一致の検出を有効にします。

a) Management Center にログインしていない場合はログインします。
b) **[System]** > **[Health]** > **[Policy]** をクリックします。
c) 新しいヘルス ポリシーを作成するか、または既存のポリシーを編集します。

d) [ポリシーの編集（Editing Policy）]ページで、[ポリシーのランタイムの間隔（Policy Runtime Interval）] を設定します。
これは、すべてのヘルス モニター タスクが実行される頻度です。
e) 左側のペインで、[レルム（Realm）] をクリックします。
f) 次の情報を入力します。

- [有効（Enabled）] : [オン（On）] をクリックします
- **警告のユーザーに一致のしきい値 %**: ヘルス モニターに警告をトリガーするレルムの不一致またはユーザーの不一致のいずれかの割合。詳細については、レルムとユーザーのダウンロードのトラブルシュート （2487 ページ）を参照してください。

g) ページの下部で [ポリシーを保存して終了（Save Policy & Exit）] をクリックします。
h) Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Applying Health Policies*」で説明したように、管理対象デバイスに正常性ポリシーを適用します。

ステップ 2 次の方法のいずれかでユーザーとレルムの不一致を表示します。

- 警告しきい値を超過した場合は、Firewall Management Center の上部のナビゲーションで [警告（Warning）] > [ヘルス（Health）] の順にクリックします。これにより、ヘルス モニターが開きます。
- **[システム（System）] > [ヘルス（Health）] > [モニタ（Monitor）]** をクリックします。

ステップ 3 [ヘルス モニター（Health Monitor）] ページの [表示（Display）] 列で、[レルム：ドメイン（Realm: Domain）] または [レルム：ユーザー（Realm: User）] を展開し、不一致に関する詳細を表示します。

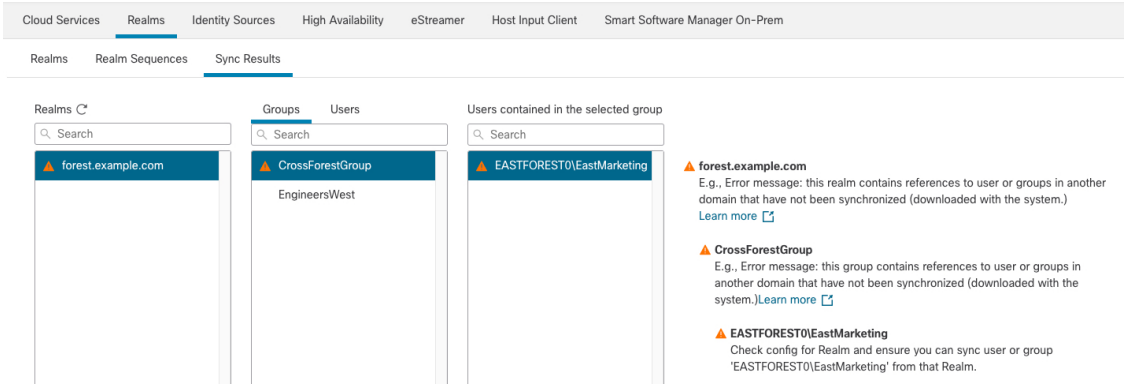
クロスドメイン信頼のトラブルシュート

クロスドメイン信頼の Management Center 設定のトラブルシューティングに関する一般的な問題は次のとおりです。

- 共有グループを持つすべてのフォレストにレルムまたはディレクトリを追加していない。
- ユーザーをダウンロード対象から除外し、除外したユーザーが別のレルムのグループで参照されるようにレルムを設定します。
- 特定の一時的な問題。

問題を理解する

Management Center がユーザーとグループを Active Directory フォレストと同期できる問題が存在する場合、次のような [Sync Results（同期結果）] タブページが表示されます。



次の表で、情報の解釈方法について説明します。

列	意味
[Realms]	システムに設定されているすべてのレルムを表示します。**[更新（Refresh）]**（） をクリックして、レルムのリストを更新します。 **黄色い三角形**（） はレルムの問題を示すために表示されます。 すべてのユーザーとグループが正常に同期された場合、レルムの横には何も表示されません。
Groups	[Groups] をクリックして、レルム内のすべてのグループを表示します。 レルムと同様、**黄色い三角形**（） は問題を示すために表示されます。 **黄色い三角形**（） をクリックして、問題の詳細を表示します。
ユーザー	[Users] をクリックして、すべてのユーザーをグループ別にソートして表示します。
選択したグループに含まれるユーザー	[Groups] 列で選択したグループ内のすべてのユーザーを表示します。 **黄色い三角形**（） をクリックすると、テーブルの右側に詳細情報が表示されます。
選択したユーザーを含むグループ	選択したユーザーが属するすべてのグループを表示します。**黄色い三角形**（） をクリックすると、テーブルの右側に詳細情報が表示されます。

列	意味
エラーの詳細情報（テーブルの右側に表示）。	同期できなかったNetBIOSフォレスト名とグループ名が表示されます。ユーザーとグループを同期できない一般的な理由は次のとおりです。 • 問題：グループとユーザーを含むフォレストに、Management Centerで設定されている対応するレルムがありません。 解決策：LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452ページ）の説明に従って、グループを含むフォレストのレルムを追加します。 • 問題：グループをManagement Centerへのダウンロード対象から除外しました。 解決策：[Realms]タブページをクリックして、[編集（Edit）]（✎）をクリックし、[Excluded Groups and Users]リストから指定されたグループまたはユーザーを移動します。

ユーザーとグループのダウンロードを再試行してください。

問題が一時的なものである可能性がある場合は、すべてのレルムのユーザーとグループをダウンロードします。

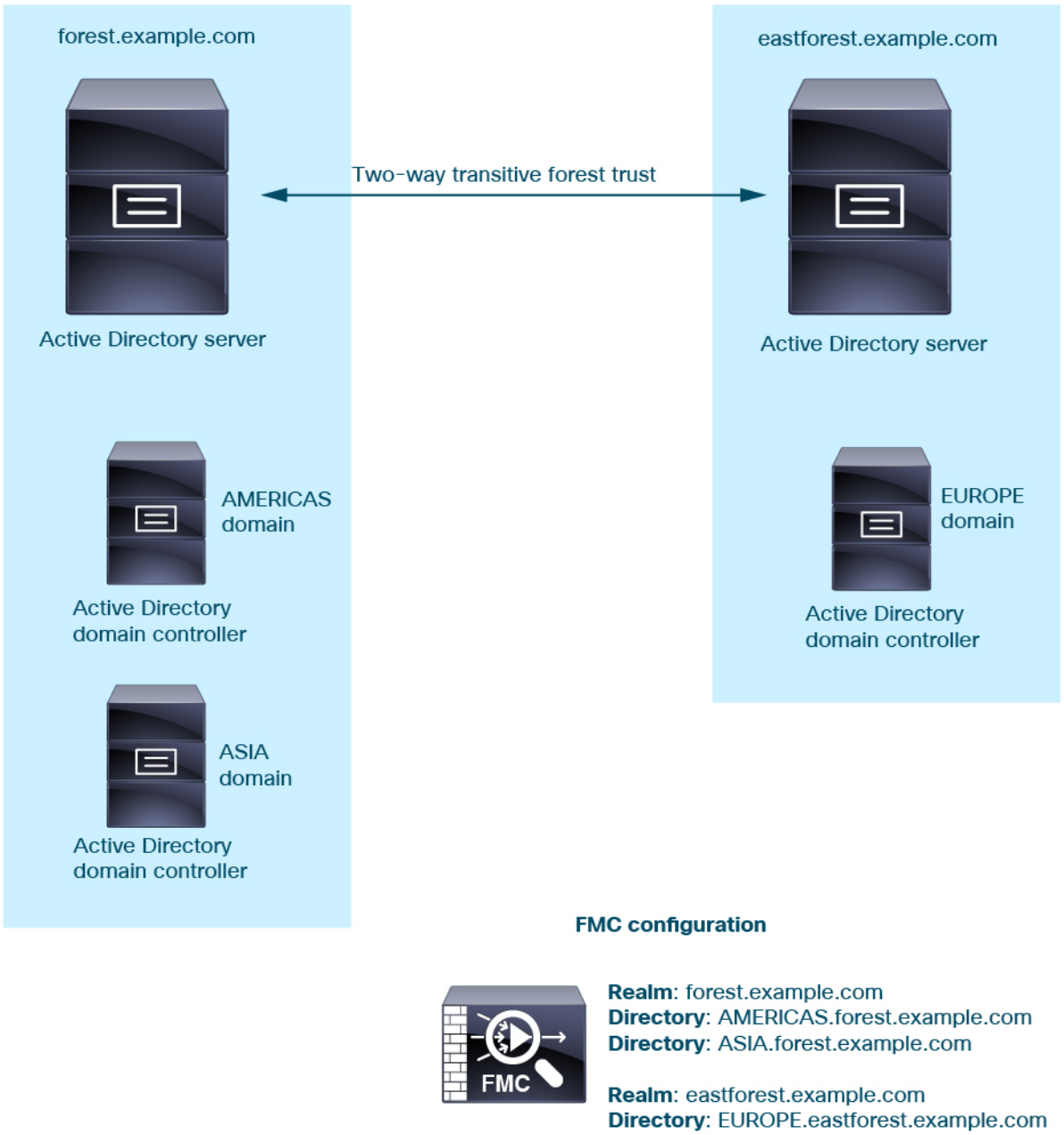
1. まだ Management Center にログインしていない場合は、ログインします。
2. **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** をクリックします。
3. [ダウンロード（download）]（⬇）をクリックします。
4. [Sync Results] タブページをクリックします。
5. [Realms]列のエントリに対するインジケータが表示されない場合、問題は解決しています。

すべてのフォレストのレルムを追加する

次の設定を確認します。

- ID ポリシーで使用するユーザーが存在する各フォレストの Management Center レルム。
- ID ポリシーで使用するユーザーを含むフォレスト内の各ドメインコントローラの Management Center ディレクトリ。

次の図は例を示しています。


forest.example.com
eastforest.example.com
Two-way transitive forest trust
Active Directory server
Active Directory server
AMERICAS
domain
Active Directory
domain controller
EUROPE
domain
Active Directory
domain controller
ASIA
domain
Active Directory
domain controller
FMC configuration
FMC
Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

レルムの履歴

表 *199 :*

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
プロキシシーケンス。	7.2.0	7.2.0	プロキシシーケンスは、レルムシーケンスと同様に、Cisco Defense Orchestrator が LDAP または Active Directory サーバーと通信できない場合に Cisco Defense Orchestrator と通信できる、1 つ以上の管理対象デバイスです。 新規/変更された画面：**[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [プロキシシーケンス（Proxy Sequence）]**
Active Directory ドメインのクロスドメイン信頼。	7.2.0	7.0.0	互いに信頼する Microsoft Active Directory（AD）ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザー アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。 Firewall Management Center は、アイデンティティルールのために Active Directory フォレストからユーザーを取得できます。
レルムシーケンス。	7.2.0	6.7.0	レルムシーケンスは、アイデンティティルールを適用する 2 つ以上のレルムの順序付きリストです。レルムシーケンスをアイデンティティポリシーに関連付けると、Firepower システムは、レルムシーケンスで指定されている順序で、最初から最後まで Active Directory ドメインを検索します。 新規/変更された画面：**[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [レルムシーケンス（Realm Sequences）][システム（System）] > [統合（Integration）] > [レルム（Realms）] > [レルムシーケンス（Realm Sequences）]**
ユーザー制御用のレルム。	7.2.0	すべて	レルムは、Firewall Management Center と、Active Directory または LDAP のユーザーリポジトリ間の接続です。

第 66 章

ISE/ISE-PIC によるユーザーの制御

次のトピックでは、ISE/ISE-PIC によりユーザー認識とユーザー制御を実行する方法について説明します。

- ISE/ISE-PIC アイデンティティ ソース （2497 ページ）
- ISE/ISE-PIC のライセンス要件 （2500 ページ）
- ISE/ISE-PIC の要件と前提条件 （2500 ページ）
- ISE/ISE-PIC の注意事項と制限事項 （2500 ページ）
- ユーザー制御用 ISE/ISE-PIC の設定方法 （2503 ページ）
- ISE/ISE-PIC の設定 （2507 ページ）
- ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング （2514 ページ）
- ISE/ISE-PIC の履歴 （2516 ページ）

ISE/ISE-PIC アイデンティティ ソース

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開をシステムと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、またはRSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE/ISE-PIC は、ISE ゲスト サービス ユーザーの失敗したログイン試行またはアクティビティは報告しません。

ユーザーの認識と制御に加えて、ISE Cisco ISE を使用してセキュリティグループタグ（SGT）を定義して使用する場合は、送信元と宛先の両方の一致基準として SGT を使用するアクセス コントロールルールを作成できます。これにより、IP アドレスまたはネットワーク オブジェクトではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。詳細については、「ダイナミック属性の条件の設定（1799ページ）」を参照してください。 を使用する場合は「ISE/ISE-PICの注意事項と制限事項（2500ページ）」も参照してください。

（注） システムはIEEE 802.1xマシン認証を解析しませんが、802.1xユーザー認証を解析します。ISEで802.1xを使用している場合は、ユーザー認証を含める必要があります。802.1xマシン認証は、ポリシーで使用できるFirewall Management Centerにユーザーアイデンティティを提供しません。

Cisco ISE/ISE-PICの詳細については、『Cisco Identity Services Engine Passive Identity Connector管理者ガイド』または『Cisco Identity Services Engine Administrator Guide』を参照してください。

（注） 最新バージョンのISE/ISE-PICを使用して、最新の機能セットと最大数の問題修正を入手することを強くお勧めします。

送信元および宛先セキュリティグループタグ（SGT）の照合

Cisco ISEを使用してセキュリティグループタグ（SGT）を定義して使用する場合は、送信元と宛先の両方の一致基準としてSGTを使用するアクセスコントロールルールを作成できます。これにより、IPアドレスまたはネットワーク オブジェクトではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。詳細については、「ダイナミック属性の条件の設定 （1799 ページ）」を参照してください。 を使用する場合、

SGT タグの照合には、次の利点があります。

- Firewall Management Center は、ISE から Security Group Tag eXchange Protocol（SXP）マッピングに登録できます。

  ISE は SXP を使用して、IP-to-SGT マッピング データベースを管理対象デバイスに伝搬します。ISE サーバーを使用するように Firewall Management Center を設定する場合は、ISE から SXP トピックをリッスンするオプションを有効にします。有効にすると、Firewall Management Center は ISE から直接セキュリティグループタグとマッピングについて学習します。次に、Firewall Management Center は SGT とマッピングを管理対象デバイスにパブリッシュします。

  SXP トピックは、ISE と他の SXP 準拠デバイス（スイッチなど）の間の SXP プロトコルを通じて学習した静的マッピングと動的マッピングに基づいてセキュリティグループタグを受信します。

  ISE でセキュリティ グループ タグを作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。また、ユーザアカウントに SGT を割り当て、SGT がユーザのトラフィックに割り当てられるようにすることもできます。ネットワーク内のスイッチとルータがそのように設定されている場合、これらのタグは、ISE、Cisco TrustSec クラウドによって制御されるネットワークに入るときに、パケットに割り当てられます。

  SXP は ISE-PIC ではサポートされていません。

- Firewall Management Center および管理対象デバイスは、追加のポリシーを展開しなくても、SGT マッピングについて学習できます（つまり、アクセス コントロール ポリシーを展開しなくても SGT マッピングの接続イベントを表示できます）。
- Cisco TrustSec をサポートしているため、ネットワークをセグメント化して重要なビジネス資産を保護することができます。
- 管理対象デバイスは、ルールのトラフィック一致基準として、SGT を強化し、次の優先度を使用します。

  1. パケット内で定義されている送信元 SGT タグ（存在する場合）。

     SGT タグがパケットに含まれるようにするには、ネットワーク内のスイッチおよびルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。

     SGT タグがパケットに含まれるようにするには、ネットワーク内のスイッチおよびルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。

  2. ISE セッションディレクトリからダウンロードされる、ユーザセッションに割り当てられた SGT。SGT は、送信元または宛先と照合することができます。
  3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが、SGT の範囲内である場合は、トラフィックは、そのSGT を使用するトラフィックと一致します。SGT は、送信元または宛先と照合することができます。

次に例を示します。

- ISE で、Guest Users という名前の SGT タグを作成し、それを 192.0.2.0/24 ネットワークに関連付けます。

  たとえば、Guest Users をアクセス コントロール ルール内の送信元 SGT 条件として使用し、ネットワークにアクセスするすべてのユーザーによる特定の URL、Web サイト カテゴリ、またはネットワークへのアクセスを制限することができます。

- ISE で、Restricted Networks という名前の SGT タグを作成し、それを 198.51.100.0/8 ネットワークに関連付けます。

  たとえば、Restricted Networks を宛先 SGT ルール条件として使用し、Guest Users や、ネットワークへのアクセスを許可されていないユーザーを持つ他のネットワークからのアクセスをブロックすることができます。

関連トピック

ISE/ISE-PIC の注意事項と制限事項 （2500 ページ）

ISE/ISE-PIC のライセンス要件

Threat Defense ライセンス

いずれか（Any）

従来のライセンス

Control

ISE/ISE-PIC の要件と前提条件

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

ISE/ISE-PIC の注意事項と制限事項

ISE/ISE-PIC を構成する際に、このセクションで説明されているガイドラインを使用してください。

ISE/ISE-PIC バージョンと設定の互換性

ご使用の ISE/ISE-PIC バージョンと構成は、次のように Secure Firewall Management Center との統合や相互作用に影響を及ぼします。

- 最新バージョンの ISE/ISE-PIC を使用して最新の機能セットを入手することを強くお勧めします。
- ISE/ISE-PIC サーバーと Secure Firewall Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザーのタイムアウトを実行する可能性があります。
- ISE または ISE-PIC データを使用してユーザー制御を実装するには、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452 ページ） の説明に従って、pxGrid のペルソナを想定して ISE サーバーのレルムを構成し、有効にします。

- ISE サーバーに接続する各 Secure Firewall Management Center ホスト名は一意である必要があります。そうでない場合、Secure Firewall Management Center のいずれかへの接続は廃棄されます。
- 多数のユーザーグループをモニターするように ISE/ISE-PIC を設定した場合、システムは管理対象デバイスのメモリ制限のためにグループに基づいてユーザーマッピングをドロップすることがあります。その結果、レルムまたはユーザー条件を使用するルールが想定どおりに実行されない可能性があります。

  6.7 以降を実行しているデバイスの場合、**configure identity-subnet-filter** コマンドを使用して、管理対象デバイスがモニタするサブネットを制限することもできます。詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

  または、ネットワークオブジェクトを設定し、そのオブジェクトを ID ポリシーのアイデンティティマッピングフィルタとして適用できます。アイデンティティ ポリシーの作成 （2555 ページ）を参照してください。

システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、Cisco Firepower Compatibility Guideを参照してください。

IPv6 のサポート

- ISE/ISE-PIC のバージョン 2.x の互換性のあるバージョンには、IPv6 対応エンドポイントのサポートが含まれています。
- ISE/ISE-PIC のバージョン 3.0（パッチ 2）以降では、ISE/ISE-PIC と Firewall Management Center 間の IPv6 通信が可能です。

ISE でのクライアントの認証

ISE サーバーと Firewall Management Center 間の接続を確立するには、ISE のクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。

到達不能なセッションは削除されます。

ISE/ISE-PIC のユーザーセッションが到達不能として報告された場合、[>] ではそのセッションがプルーニングされ、同じ IP を持つ別のユーザーは到達不能なユーザーのアイデンティティルールに一致できません。
[プロバイダー（Providers）]>[エンドポイントプローブ（Endpoint Probes）] に移動し、次のいずれかをクリックして、ISE/ISE-PIC でこの動作を制御できます。

- [有効（Enabled）] にすると、ISE/ISE-PIC がエンドポイント接続を監視し、Secure Firewall Management Center で到達不能なユーザーからのセッションをプルーニングできます。
- [無効（Disabled）] にすると、ISE/ISE-PIC はエンドポイント接続を無視します。

セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）

セキュリティグループタグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス（SGA）と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティグループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。

セキュリティ グループ タグは、アクセス制御ルール内の送信元および宛先の両方の一致基準として使用できます。

（注） ISE SGT 属性タグのみを使用してユーザー制御を実装する場合、ISE サーバーのレルムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザー制御とみなされず、アイデンティティ ソースとして ISE/ISE-PIC を使用しない場合にのみ機能します。カスタム SGT 条件 を参照してください。

送信元 SGT タグに加えて宛先 SGT タグを照合するには、次の条件が適用されます。

必要な ISE バージョン：2.6 パッチ 6 以降、2.7 パッチ 2 以降

ルータのサポート：イーサネットを介した SGT インライン タギングをサポートする任意のシスコ ルータ。詳細については、『Cisco Group Based Policy Platform and Capability Matrix Release』などの参考資料を参照してください。

制限事項

- サービス品質（QoS）ポリシーは、送信元 SGT 照合のみを使用し、宛先 SGT 照合は使用しません。
- RA-VPN は、RADIUS を介した SGT マッピングの直接の受信はしません。

ISE と高可用性

プライマリ ISE/ISE-PIC サーバーで障害が発生すると、次のようなことが起きます。

pxGrid v2 との統合の結果として、Secure Firewall Management Center は、一方が接続を受け入れるまで設定された両方の ISE ホスト間のラウンドロビンを行います。

接続が失われると、Secure Firewall Management Center は接続されたホストへのラウンドロビンの試行を再開します。

エンドポイント ロケーション（Endpoint Location）（またはロケーション IP（Location IP））

[エンドポイント ロケーション（Endpoint Location）] 属性は、ISE によって識別される、ユーザーの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

[エンドポイント ロケーション（Endpoint Location）]（[ロケーション IP（Location IP）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ISE 属性

ISE 接続を設定すると、ISE 属性データが Secure Firewall Management Center データベースに入力されます。ユーザー認識とユーザー制御に使用できる ISE 属性は、次のとおりです。 これは、ISE-PIC ではサポートされません。

エンドポイント プロファイル（Endpoint Profile）（またはデバイス タイプ（Device Type））

[エンドポイント プロファイル（Endpoint Profile）] 属性は、ISE によって識別されるユーザーのエンドポイント デバイス タイプです。

[エンドポイント プロファイル（Endpoint Profile）]（[デバイス タイプ（Device Type）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ユーザー制御用 ISE/ISE-PIC の設定方法

ISE/ISE-PIC は、次の設定のいずれかで使用できます。

- レルム、アイデンティティ ポリシー、および関連付けられたアクセス コントロール ポリシーを使用。

  レルムを使用して、ポリシー内のネットワーク リソースへのユーザー アクセスを制御します。ポリシーでは、ISE/ISE-PIC セキュリティ グループ タグ（SGT）のメタデータを引き続き使用できます。

- アクセス コントロール ポリシーのみを使用。レルムまたはアイデンティティ ポリシーは必要ありません。

  SGT メタデータのみを使用してネットワーク アクセスを制御するには、この方法を使用します。

関連トピック

レルムを使用しない ISE/ISE-PIC の設定方法 （2503 ページ）
レルムを使用したユーザー制御用 ISE/ISE-PIC の設定方法 （2505 ページ）

レルムを使用しない ISE/ISE-PIC の設定方法

このトピックでは、SGT タグを使用してネットワークへのアクセスを許可またはブロックできるように ISE を設定するために必要なタスクの概要について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	SGT 照合：ISE で SXP を有効にします。	これにより、SGT メタデータの変更時に Secure Firewall Management Center が ISE から更新を受信できるようになります。
ステップ 2	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバー、および Secure Firewall Management Center の間で安全に接続するために必要です（「Firewall Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート（2510 ページ）」を参照）。
ステップ 3	Secure Firewall Management Center に証明書をインポートします。	証明書は次のようにインポートする必要があります。 • pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト** > **オブジェクト管理** > **PKI** > **内部証明書**） • pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**） • MNT 証明書：信頼できる CA
ステップ 4	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザー アクティビティを制御できます。
ステップ 5	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元および宛先の SGT メタデータを使用できます。アクセス コントロール ルールの概要（1775 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 6	管理対象デバイスにアクセスコントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。「設定変更の展開 （172 ページ）」を参照してください。

次のタスク

Firewall Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （2510 ページ）

レルムを使用したユーザー制御用 ISE/ISE-PIC の設定方法

始める前に

このトピックでは、ユーザ制御用 ISE/ISE-PIC を設定し、ユーザまたはグループによるネットワークへのアクセスを許可またはブロックできるようにするために必要なタスクの概要について説明します。ユーザーおよびグループは、レルムがサポートされているサーバー （2461 ページ）に記載されている任意のサーバーに保存できます。

手順

	コマンドまたはアクション	目的
ステップ 1	宛先 SGT のみ：ISE で SXP を有効にします。	これにより、SGT メタデータの変更時に Secure Firewall Management Center が ISE から更新を受信できるようになります。
ステップ 2	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバー、および Secure Firewall Management Center の間で安全に接続するために必要ですその場合は、次のトピックを参照してください。 • pxGrid サーバーおよび MNT サーバー証明書：Firewall Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （2510 ページ） • pxGrid クライアント証明書：自己署名証明書の生成 （2512 ページ）

	コマンドまたはアクション	目的
ステップ 3	Secure Firewall Management Center に証明書をインポートします。	証明書は次のようにインポートする必要があります。 • pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト** > **オブジェクト管理** > **PKI** > **内部証明書**） • pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**） • MNT 証明書：信頼できる CA
ステップ 4	レルムを作成します。	レルムの作成は、選択したユーザーおよびグループによるネットワークへのアクセスを制御するためにのみ必要です。 LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成（2452 ページ）を参照してください。
ステップ 5	ユーザーおよびグループをダウンロードし、レルムを有効にします。	ユーザーおよびグループをダウンロードすると、それらをアクセス コントロール ルールで使用できるようになります。ユーザーとグループの同期（2475 ページ）を参照してください。
ステップ 6	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザー アクティビティを制御できます。
ステップ 7	アイデンティティ ポリシーを作成します。	アイデンティティ ポリシーは、1 つ以上のアイデンティティ ルールのコンテナです。アイデンティティ ポリシーの作成（2555 ページ）を参照してください。
ステップ 8	アイデンティティ ルールを作成します。	アイデンティティ ルールは、ユーザーおよびグループによるネットワークへのアクセスを制御するためにレルムがどのように使用されるかを指定しま

	コマンドまたはアクション	目的
		す。アイデンティティ ルールの作成（2565 ページ）を参照してください。
ステップ 9	アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます。	これにより、アクセス コントロール ポリシーがレルム内のユーザーとグループを使用できるようになります。
ステップ 10	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元および宛先の SGT メタデータを使用できます。アクセス コントロール ルールの概要（1775 ページ）を参照してください。
ステップ 11	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。「設定変更の展開（172 ページ）」を参照してください。

次のタスク

Firewall Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート（2510 ページ）

ISE/ISE-PIC の設定

次のトピックでは、Firewall Management Center のアイデンティティポリシーで使用するように ISE/ISE-PIC サーバーを設定する方法について説明します。

このトピックでは、次の方法について説明します。

- Firewall Management Center で認証するために ISE/ISE-PIC サーバーから証明書をエクスポートします。
- Firewall Management Center を ISE サーバーのセキュリティグループタグ（SGT）で更新できるように、SXP トピックを公開します。

関連トピック

ISE でのセキュリティグループと SXP パブリッシングの設定（2508 ページ）

Firewall Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート（2510 ページ）

ISE でのセキュリティグループと SXP パブリッシングの設定

Cisco Identity Services Engine（ISE）では、TrustSec ポリシーとセキュリティ グループ タグ（SGT）を作成するために実行を必要とする設定が多数あります。TrustSecの実装の詳細については、ISEのマニュアルを参照してください。

次の手順では、Firewall Threat Defense デバイスがスタティック SGT から IP アドレスへのマッピングをダウンロードして適用できるようにするためにISEで設定する必要があるコア設定のハイライトを示します。これは、アクセス制御ルールでの送信元と宛先 SGT の照合に使用できます。詳細については、ISEのマニュアルを参照してください。

この手順のスクリーンショットは、ISE 2.4に基づいています。これらの機能にアクセスするための正確な手順は後続のリリースで変更される可能性がありますが、概念と要件は同じです。ISE 2.4 以降、特に 2.6 以降が推奨されますが、ISE 2.2 パッチ 1 以降でもこの設定は動作します。

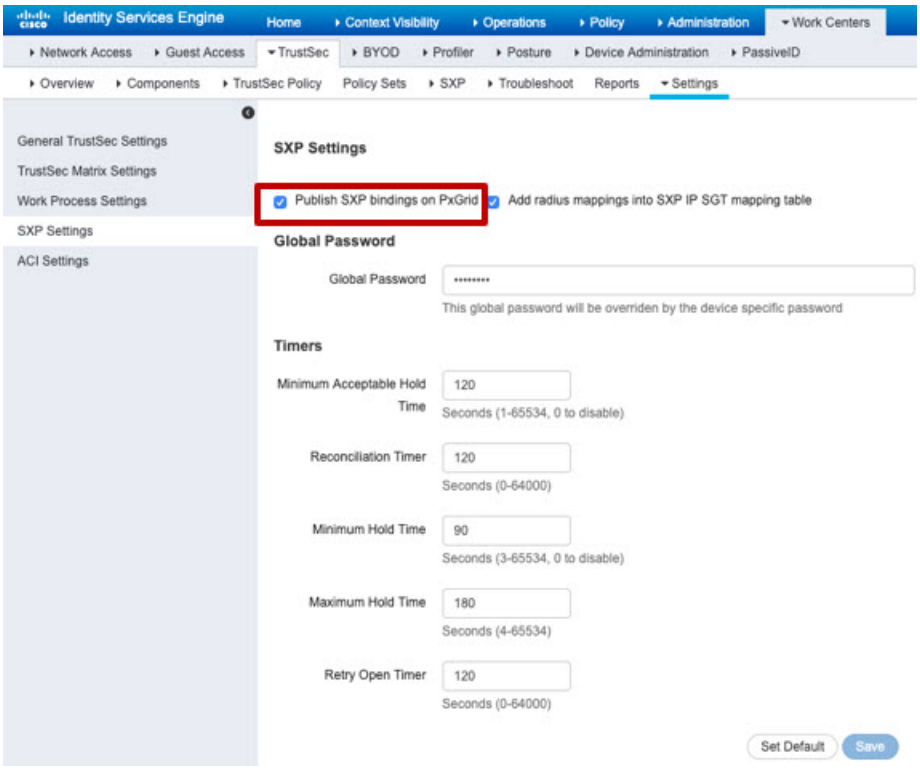
始める前に

SGT から IP アドレスへのスタティックマッピングを公開し、ユーザセッションからと SGT へのマッピングを取得して Firewall Threat Defense デバイスがそれらを受信できるようにするには、ISE Plus ライセンスが必要です。

手順

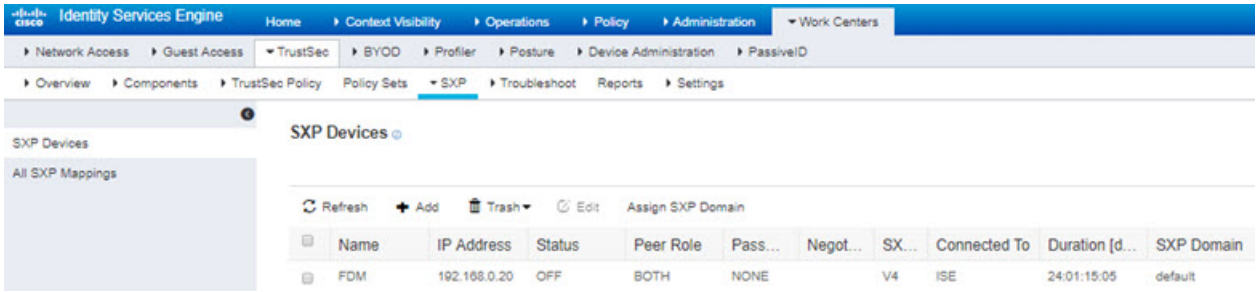
ステップ 1 **[ワークセンター（Work Centers）]** > **[TrustSec]** > **[設定（Settings）]** > **[SXP 設定（SXP Settings）]** を選択し、**[PxGrid で SXP バインディングを公開（Publish SXP Bindings on PxGrid）]** オプションを選択します。

このオプションにより、ISEはSXPを使用してSGTマッピングを送信します。リストからSXPトピックまでを "確認する" には、Firewall Threat Defense デバイスに対してこのオプションを選択する必要があります。このオプションは、Firewall Threat Defenseデバイスが静的SGT-to-IPアドレスマッピング情報を取得するために選択する必要があります。単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

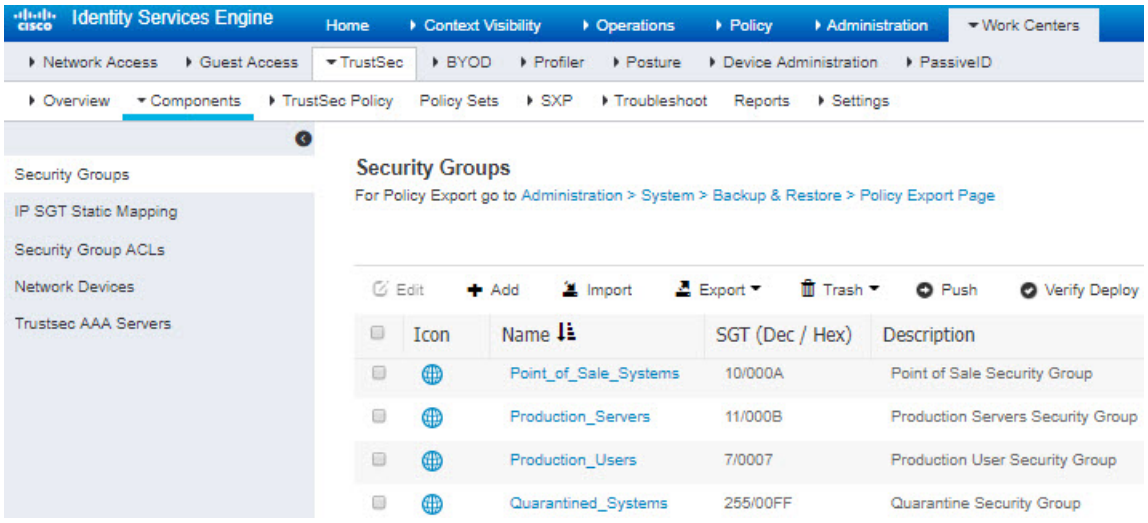


ステップ 2 **[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）]** を選択し、デバイスを追加します。

これは実際のデバイスである必要はありませんが、Firewall Threat Defense デバイスの管理 IP アドレスを使用することもできます。このテーブルには、ISEが静的SGT-to-IPアドレスマッピングをパブリッシュするためのデバイスが1つ以上必要です。単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

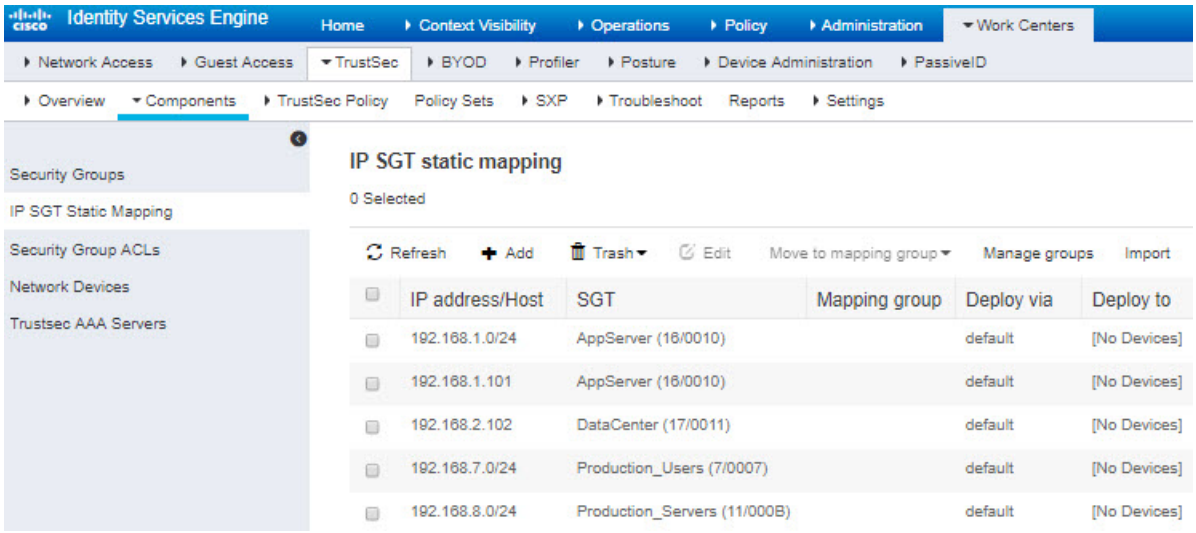


ステップ 3 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]** の順に選択し、セキュリティグループタグが定義されていることを確認します。必要に応じて新しいタグを作成します。



ステップ 4 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGT スタティックマッピング（IP SGT Static Mapping）]** を選択し、ホストとネットワーク IP アドレスをセキュリティ グループ タグにマッピングします。

単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。



Firewall Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート

ここでは、次のことを行う方法について説明します。

- ISE/ISE-PIC サーバーからシステム証明書をエクスポートします。

これらの証明書は、ISE/ISE-PIC サーバーに安全に接続するために必要です。ISE システムの設定に応じ、次のうち 1 つまたは最大 3 つの証明書をエクスポートする必要があります。

- pxGrid サーバー用の証明書
- モニタリング（MNT）サーバー用の証明書
- pxGrid クライアント（つまり、Firewall Management Center）用の証明書（秘密キーを含む）

  最初の 2 つの証明書とは異なり、これは自己署名証明書です。

- これらの証明書を Firewall Management Center にインポートします。
  - pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト** > **オブジェクト管理** > **PKI** > **内部証明書**）
  - pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**）
  - MNT 証明書：信頼できる CA

関連トピック

システム証明書のエクスポート
ISE/ISE-PIC 証明書のインポート （2513 ページ）

システム証明書のエクスポート

システム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

手順

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]**。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント

値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他の Cisco ISE ノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）]をクリックして、クライアントブラウザを実行しているファイルシステムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は PEM 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は PEM 形式の証明書と暗号化された秘密キーファイルを含む .zip ファイルとしてエクスポートされます。

自己署名証明書の生成

自己署名証明書を生成することで、新しいローカル証明書を追加します。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境に Cisco ISE を展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

（注） 自己署名証明書を使用しており、Cisco ISE ノードのホスト名を変更する場合は、 Cisco ISE ノードの管理ポータルにログインし、古いホスト名が使用されている自己署名証明書を削除してから、新しい自己署名証明書を生成します。そうしないと、Cisco ISE は古いホスト名が使用された自己署名証明書を引き続き使用します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

手順

ステップ 1 Cisco ISE GUI で、[Menu] アイコン（☰）をクリックし、**[Administration]** > **[System]** > **[Certificates]** > **[System Certificates]**を選択します。

セカンダリノードから自己署名証明書を生成するには、**[管理（Administration）]** > **[システム（System）]** > **[サーバー証明書（Server Certificate）]** を選択します。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[証明書（Certificates）]** > **[システム証明書（System Certificates）]**。

ステップ 3 [自己署名証明書の生成（Generate Self Signed Certificate）] をクリックし、表示されるウィンドウに詳細を入力します。

ステップ 4 この証明書を使用するサービスに基づいて [使用方法（Usage）] 領域のチェックボックスをオンにします。

ステップ 5 証明書を生成するには、[送信（Submit）] をクリックします。

CLI からセカンダリノードを再起動するには、次の順序で次のコマンドを入力します。

a) **application stop ise**
b) **application start ise**

ISE/ISE-PIC 証明書のインポート

この手順は任意です。

始める前に

システム証明書のエクスポート（2511 ページ）の説明に従って、ISE/ISE-PIC サーバから証明書をエクスポートします。証明書とキーは、Secure Firewall Management Center へのログイン元のマシンに存在している必要があります。

次のように証明書をインポートする必要があります。

- pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト** > **オブジェクト管理** > **PKI** > **内部証明書**）
- pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**）
- MNT 証明書：信頼できる CA

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** をクリックします。

ステップ 3 [PKI] を展開します。

ステップ 4 [内部証明書（Internal Cert）] をクリックします。

ステップ 5 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 6 画面の指示に従って、証明書と秘密キーをインポートします。

ステップ 7 [信頼できるCA（Add Trusted CAs）] をクリックします。

ステップ 8 [信頼できるCAの追加（Add Trusted CA）] をクリックします。

ステップ 9 画面の指示に従って、pxGrid サーバー証明書をインポートします。

ステップ 10 必要に応じ、上記の手順を繰り返して MNT サーバーの信頼できる CA をインポートします。

ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング

Cisco TrustSec の問題のトラブルシューティング

デバイスインターフェイスでは、ISE / ISE-PIC またはネットワーク上のシスコデバイスからセキュリティグループタグ（SGT）を伝達するように設定できます（Cisco TrustSec と呼ばれます）。デバイス管理ページ（[デバイス（Devices）] > [デバイス管理（Device Management）]）では、デバイスの再起動後にインターフェイスの[セキュリティグループタグの伝達（Propagate Security Group Tag）] チェックボックスがオンになります。>インターフェイスが TrustSec データを伝播しないようにするには、このボックスをオフにします。

ISE /ISE-PIC の問題のトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザーのダウンロードのトラブルシュート（2487 ページ）およびユーザー制御のトラブルシューティング（2569 ページ）を参照してください。

ISE または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE とシステムを正常に統合するには、ISE 内の pxGrid アイデンティティマッピング機能を有効にする必要があります。
- プライマリ サーバーが失敗した場合は、セカンダリをプライマリに手動で昇格させる必要があります。自動でフェール オーバーすることはありません。
- ISE サーバーと Firewall Management Center 間の接続を確立するには、ISE のクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

  Cisco Identity Services Engine Administrator Guideの「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。
- [pxGridクライアント証明書（pxGrid Client Certificate）][FMCサーバー証明書（FMC Server Certificate）] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。
- ISE サーバの時刻は、Secure Firewall Management Center の時刻と同期している必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードが含まれている場合は、

- 両方のノードの証明書が、同じ認証局によって署名される必要があります。
- ホスト名で使用されるポートが、ISE サーバーと Secure Firewall Management Center の両方から到達可能である必要があります。

- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ユーザーから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングを ISE から受信するときに、サブネットを除外するには **configure identity-subnet-filter** {**add** | **remove**} コマンドを使用します。通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。

ISE または ISE-PIC によって報告されたユーザ データに問題がある場合は、次の項目に注意します。

- システムは、データベース にデータがない ISE ユーザのアクティビティを検出すると、サーバからそのユーザに関する情報を取得します。ISE ユーザから見えるアクティビティは、システムがユーザのダウンロードで情報の取得に成功するまでアクセス コントロール ルールで処理されず、Web インターフェイスに表示されません。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Secure Firewall Management Centerは、ISE ゲスト サービス ユーザのユーザ データは受信しません。
- ISE が TS エージェントと同じユーザーをモニターする場合、Secure Firewall Management Center は TS エージェントのデータを優先します。TS エージェントと ISE が同じ IP アドレスによる同一のアクティビティを報告した場合は、TS エージェントのデータのみが Secure Firewall Management Center に記録されます。
- 使用する ISE のバージョンと設定は、システムでの ISE の使用方法に影響を与えます。詳細については、ISE/ISE-PIC アイデンティティ ソース （2497 ページ）を参照してください。
- Secure Firewall Management Center の高可用性が設定されているとプライマリが失敗する場合は、ISE/ISE-PIC の注意事項と制限事項 （2500 ページ）の ISE と高可用性に関する項を参照してください。
- ISE-PIC は ISE 属性のデータを提供しません。
- ISE-PIC は ISE ANC の修復を実行できません。
- Active FTP sessions are displayed as the **Unknown** user in events. これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバーが接続を開始し、FTP サーバーには関連付けられているユーザー名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

サポートされている機能に問題がある場合は、ISE/ISE-PIC アイデンティティ ソース （2497 ページ）で詳細を参照してバージョンの互換性を確認してください。

ISE/ISE-PIC ユーザータイムアウト

レルムなしで ISE/ISE-PIC を設定する場合は、Secure Firewall Management Centerでのユーザーの表示方法に影響するユーザー セッション タイムアウトがあることに注意してください。詳細については、レルム フィールド （2464 ページ）を参照してください。

ISE/ISE-PIC の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
pxGrid 2.0 は、サポートされている ISE/ISE-PIC バージョンのデフォルトです	6.7.0	6.7.0	次の点に注意してください。 • サポートされる ISE/ISE-PIC バージョン：2.6 パッチ 6 以降、2.7 パッチ 2 以降 • 適応型ネットワーク制御（ANC）ポリシーは、Endpoint Protection Service（EPS; エンドポイント保護サービス）の修復に取って代わります。Firewall Management Center で EPS ポリシーが設定されている場合は、それらを移行して ANC を使用する必要があります。
必要に応じて、ユーザーから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングを ISE から受信するときに、サブネットを除外します。通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。	6.7.0	6.7.0	新しいコマンド：**configure identity-subnet-filter** {**add** | **remove**}

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
宛先セキュリティ グループ タグ（SGT）の照合	6.5.0	6.5.0	導入された機能。アクセス コントロール ルール内の送信元および宛先の両方の一致基準に ISE SGT タグを使用できるようにします。 SGT タグは、ISE によって取得されたタグからホスト/ネットワークへのマッピングです。 新規/変更された画面： • 宛先 SGT 照合を設定するための新しいオプション： **[システム（System）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）] > [ISE/ISE-PIC]** • [セッションディレクトリのトピック（Session Directory Topic）]：ISE ユーザー セッションの情報をサブスクライブします。 • [SXP トピック（SXP Topic）]：ISE サーバでの SGT タグの更新をサブスクライブします。 • **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** の新しい列および名前が変更された列 • 名前の変更：[セキュリティグループタグ（Security Groups Tags）] が [送信元SGT（Source SGT）] に名称変更されました • 新規：[宛先SGT（Destination SGT）]
ISE-PIC との統合	6.2.1	6.2.1	ISE-PIC のデータを使用できるようになりました。
ユーザ制御用の SGT タグ。	6.2.1	6.2.0	ISE セキュリティ グループ タグ（SGT）データに基づいてユーザ制御を実行するために、レルムまたはアイデンティティ ポリシーを作成する必要がなくなりました。
ISE との統合。	6.0	6.0	導入された機能。シスコの Platform Exchange Grid（PxGrid）に登録することで、Firepower Management Center で追加のユーザー データ、デバイス タイプ データ、デバイス ロケーション データ、およびセキュリティ グループ タグ（SGT：ネットワーク アクセス コントロールを提供するために ISE によって使用される方式）をダウンロードできます。

第 67 章

キャプティブポータルによるユーザーの制御

- キャプティブ ポータルのアイデンティティ ソース （2519 ページ）
- キャプティブポータルのライセンス要件 （2520 ページ）
- キャプティブポータルの要件と前提条件 （2520 ページ）
- キャプティブ ポータルのガイドラインと制約事項 （2521 ページ）
- ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （2539 ページ）
- キャプティブ ポータルの履歴 （2541 ページ）

キャプティブ ポータルのアイデンティティ ソース

キャプティブポータルは、システムでサポートされる権限のあるアイデンティティソースの 1 つです。キャプティブポータルは、ユーザーがネットワークに対し、管理対象デバイスを使用して認証を行うアクティブ認証方式です。（RA-VPN は別のタイプのアクティブ認証です）。認証レルム（Microsoft AD など）に照会してユーザーを認証するパッシブ認証とは異なり、アクティブ認証では、ユーザーに対して、管理対象デバイスによってログインページが表示されます。

通常、キャプティブポータルを使用して、インターネットにアクセスするため、または制限されている内部リソースにアクセスするための認証を要求します。必要に応じて、リソースへのゲスト アクセスを設定することができます。システムはキャプティブ ポータル ユーザを認証した後、それらのユーザのトラフィックをアクセス制御ルールに従って処理します。キャプティブ ポータルは、HTTP および HTTPS のトラフィックのみで認証を行います。

（注） キャプティブ ポータルが認証を実行する前に、HTTPS トラフィックを復号する必要があります。

キャプティブ ポータルはまた、失敗した認証の試行を記録します。失敗した試行で新しいユーザーがデータベース内のユーザーのリストに追加されることはありません。キャプティブ ポータルで報告される失敗した認証アクティビティのユーザー アクティビティ タイプは [認証失敗ユーザー（Failed Auth User）] です。

キャプティブ ポータルから取得された認証データはユーザー認識とユーザー制御に使用できます。

関連トピック

ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）

ホスト名のリダイレクトについて

（Snort 3 のみ。）アクティブ認証アイデンティティルールは、設定されたインターフェイスを使用してキャプティブポータルポートにリダイレクトします。通常、リダイレクトは IP アドレスに対して行われるため、信頼できない証明書エラーが発生する場合があります。この動作は中間者攻撃に似ているため、ユーザーは信頼できない証明書を受け入れることに消極的である可能性があります。

この問題を回避するために、管理対象デバイスの完全修飾ドメイン名（FQDN）を使用するようにキャプティブポータルを設定できます。適切に設定された証明書を使用すると、ユーザーは信頼できない証明書エラーを受け取ることがなくなり、認証がよりシームレスになり、安全性が向上します。

関連トピック

ホスト名ネットワークルール条件にリダイレクト （2559 ページ）

キャプティブポータルのライセンス要件

Threat Defense ライセンス

いずれか（Any）

従来のライセンス

Control

キャプティブポータルの要件と前提条件

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

キャプティブ ポータルのガイドラインと制約事項

アイデンティティポリシーでキャプティブポータルを設定して展開すると、指定されたレルムのユーザーはFirewall Threat Defenseを使用して認証を行ってからネットワークにアクセスします。

（注） リモート アクセス VPN ユーザーがセキュア ゲートウェイとして機能している管理対象デバイスを介してアクティブに認証されている場合、アイデンティティ ポリシーで設定されている場合でも、キャプティブ ポータルのアクティブ認証は実行されません。

キャプティブポータルとポリシー

アイデンティティ ポリシーのキャプティブ ポータルを設定し、アイデンティティ ルールのアクティブ認証を呼び出します。アイデンティティポリシーはアクセス コントロール ポリシーに関連付けられ、アクセス コントロール ポリシーはネットワーク内のリソースへのアクセスを定義します。たとえば、US-West/Finance グループのユーザーを Engineering サーバーへのアクセスから除外したり、ユーザーがネットワーク上の安全でないアプリケーションにアクセスするのを禁止したりできます。

キャプティブ ポータルのいくつかのアイデンティティ ポリシー設定はアイデンティティポリシーの [アクティブ認証（Active Authentication）] タブページで行い、残りの設定はアクセス コントロール ポリシーに関連付けられたアイデンティティルールで行います。

アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれます。それぞれのケースで、システムは TLS/SSL 復号を透過的に有効化/無効化し、これにより Snort プロセスが再起動します。

注意 TLS/SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに 復号ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

キャプティブポータルがアイデンティティルールに一致するユーザーを認証する場合、ダウンロードされていない Microsoft Active Directory または LDAP グループ内のユーザーは不明として識別されます。ユーザーが不明として識別されるのを回避するには、キャプティブポータルで認証するすべてのグループのユーザーをダウンロードするようにレルムを設定します。不明なユーザーは、関連付けられたアクセス コントロール ポリシーに従って処理されます。アクセス コントロール ポリシーが不明なユーザーをブロックするように構成されている場合、これらのユーザーはブロックされます。

システムによってレルム内のすべてのユーザーが確実にダウンロードされるようにするには、グループがレルムの設定の [使用可能グループ（Available Groups）] リストに含まれていることを確認します。

ユーザーとグループの同期の詳細については、ユーザーとグループの同期 （2475 ページ）を参照してください。

必要なルーテッドインターフェイス

キャプティブ ポータル アクティブ認証を実行できるのは、ルーテッド インターフェイスが設定されているデバイスのみです。キャプティブポータルにアイデンティティルールを設定していて、キャプティブ ポータル デバイスにインラインインターフェイスとルーテッドインターフェイスが含まれている場合は、デバイス上のルーテッドインターフェイスのみを対象とするインターフェイスルール条件をアクセス コントロール ポリシーで設定する必要があります。

アクセス コントロール ポリシーと関連づけられたアイデンティティポリシーに、1 つ以上のキャプティブ ポータル アイデンティティ ルールが含まれており、ルーテッドインターフェイスが設定されている 1 つ以上のデバイスを管理する Secure Firewall Management Center にポリシーを展開すると、ポリシーの展開は成功し、ルーテッドインターフェイスはアクティブ認証を実行します。

必要な証明書と認証局

ユーザーの制御および認識のためにキャプティブポータルを使用する前に、以下のすべてが必要です。

- Microsoft AD で認証する場合は、サーバーのルート証明書をエクスポートし、信頼できる CA 証明書として Secure Firewall Management Center にインポートします。
- アイデンティティポリシーが展開されている管理対象デバイスで認証するための、内部証明書オブジェクト。

- 必要な復号ルールの内部認証局。

キャプティブポータルの要件と制約事項

以下の要件と制約事項に注意してください。

- キャプティブポータルは HTTP/3 QUIC 接続をサポートしていません。
- システムがサポートするキャプティブ ポータル ログインの数は 1 秒あたり最大 20 です。
- 最大ログイン試行回数のカウントに数えられるログイン試行の失敗から次の失敗までには制限があり、最大 5 分です。5 分の制限の設定は変更できません

  （最大ログイン試行回数は **[分析（Analysis）]** > **[接続（Connections）]** > **[イベント（Events）]** で接続イベントに表示されます）。

  ログイン失敗の間に 5 分以上の間隔がある場合は、ユーザーは認証のためにキャプティブポータルにリダイレクトされ、失敗したログインユーザーまたはゲストユーザーには指定されず、Secure Firewall Management Center に報告されることはありません。
- キャプティブ ポータルは、TLS v1.0 接続をネゴシエートしません。

  TLS v1.1、v1.2、および TLS 1.3 接続のみがサポートされています。
- キャプティブポータルでレルムシーケンスを使用することはできません。
- ユーザーをキャプティブポータルから安全にログアウトし、ユーザーが再度ログインできないようにするために、管理者はセッションを閉じることができます : **[分析（Analysis）]**> **[ユーザー（Users）] 見出し** > **[アクティブセッション（Active Sessions）]**。ユーザーがブラウザを閉じた場合も、ブラウザは自動的に再認証されません。
- 親ドメインのレルムを作成し、管理対象デバイスがその親ドメインの子へのログインを検出した場合、管理対象デバイスはそのユーザーのその後のログアウトを検出しません。
- アクセス制御ルールは、キャプティブポータルに使用する予定のデバイスの IP アドレスおよびポートを宛先とするトラフィックを許可する必要があります。
- キャプティブ ポータル アクティブ認証を HTTPS トラフィックで行う場合、復号ポリシーを使用して、認証対象のユーザーからのトラフィックを復号する必要があります。キャプティブ ポータル ユーザーの Web ブラウザと管理対象デバイス上のキャプティブ ポータル デーモンとの間の接続では、トラフィックを復号できません。この接続は、キャプティブ ポータル ユーザーの認証に使用されます。
- 管理対象デバイスの通過が許可されている HTTP 以外のトラフィックまたは HTTPS トラフィックの量を制限するには、アイデンティティ ポリシーの [ポート（Ports）] タブ ページで一般的な HTTP ポートと HTTPS ポートを入力する必要があります。

  管理対象デバイスは、着信要求に HTTP プロトコルまたは HTTPS プロトコルが使用されていないと判断した場合、以前に非表示にしたユーザーを [保留中（Pending）] から [不明（Unknown）] に変更します。管理対象デバイスがユーザーを [保留中（Pending）] から別の状態に変更するとすぐに、そのトラフィックにはアクセス制御、QoS、および復号ポリシー を適用できます。他のポリシーで HTTP 以外のトラフィックまたは HTTPS トラ

フィックが許可されていない場合は、キャプティブポータルのポートにアイデンティティポリシーを設定することによって、望ましくないトラフィックが管理対象デバイスを通過できないようにします。

Kerberos の前提条件

Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります（Windows で設定されている NetBIOS の制限）。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に設定します。詳細については、Microsoft のマニュアルサイト「Naming conventions in Active Directory for computers, domains, sites, and OUs」で、次のような記事を参照してください。

DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、RFC 6891 セクション 6.2.5 で説明されています。

ユーザー制御のためのキャプティブポータルの設定方法

始める前に

アクティブ認証にキャプティブポータルを使用するには、LDAP レルムか、Microsoft AD レルム、Microsoft Azure AD（SAML） レルム、アクセス コントロール ポリシー、アイデンティティポリシー、復号ポリシー をセットアップし、アイデンティポリシーと 復号ポリシー を同じアクセス コントロール ポリシーに関連付ける必要があります。最後にポリシーを管理対象デバイスに展開します。このトピックでは、このタスクのハイレベルな概要について説明します。

最初に次のタスクを実行します。

- 「ルーテッド」インターフェイスが設定された 1 つ以上のデバイスが Secure Firewall Management Center によって管理されていることを確認します。
- キャプティブポータルで暗号化認証を使用するには、Secure Firewall Management Center のアクセス元となるマシンで証明書データとキーを使用できるようにするか、管理対象デバイスを認証するための PKI オブジェクトを作成します。PKI オブジェクトの作成方法については、PKI （1352 ページ） を参照してください。

手順

ステップ 1 次のトピックに記載されているように、LDAP レルムか、Microsoft AD レルムを作成し、有効化します。

- LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）
- ユーザーとグループの同期 （2475 ページ）

レルムシーケンスは、キャプティブポータルではサポートされていません。

システムによってレルム内のすべてのユーザーが確実にダウンロードされるようにするには、グループがレルムの設定の [使用可能グループ（Available Groups）] リストに含まれていることを確認します。

詳細については、「ユーザーとグループの同期 （2475 ページ）」を参照してください。

ステップ 2 必要な証明書と認証局を取得します。
以下のすべてが必要です。

- Microsoft AD で認証する場合は、サーバーのルート証明書をエクスポートし、信頼できる CA 証明書として Secure Firewall Management Center にインポートします。
- アイデンティティポリシーが展開されている管理対象デバイスで認証するための、内部証明書オブジェクト。
- 必要な復号ルールの内部認証局。

ステップ 3 関連付けられた信頼できる認証局を使用してネットワークオブジェクトを作成します。

キャプティブポータルの設定パート 1：ネットワークオブジェクトの作成 （2526 ページ） を参照してください。

ステップ 4 アクティブ認証ルールを含むアイデンティティポリシーを作成します。

アイデンティティ ポリシーによって、キャプティブ ポータルで認証後にレルム アクセス リソースで選択したユーザを有効にします。

詳細については、キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成 （2528 ページ）を参照してください。

ステップ 5 キャプティブ ポータル ポート（デフォルトでは TCP 885）上のトラフィックを許可するキャプティブ ポータルに関するアクセス コントロール ルールを設定します。

キャプティブ ポータルが使用可能な TCP ポートのいずれかを選択できます。どれを選択しても、そのポートでトラフィックを許可するルールを作成する必要があります。

詳細については、キャプティブポータルの設定パート 3：TCP ポートアクセス コントロール ルールの作成 （2530 ページ）を参照してください。

ステップ 6 別のアクセスコントロールルールを追加して、選択したレルムのユーザーがキャプティブポータルを使用してリソースにアクセスできるようにします。

詳細については、キャプティブポータルの設定パート 4：ユーザー アクセス コントロール ルールの作成 （2532 ページ）を参照してください。

ステップ 7 キャプティブ ポータル ユーザーが HTTPS プロトコルを使用して Web ページにアクセスできるように、[不明（Unknown）] なユーザー用の [復号-再署名（Decrypt - Resign）] ルールを用いて 復号ポリシー を設定します。

HTTPS トラフィックがキャプティブ ポータルへ送信される前に復号される場合のみ、キャプティブ ポータルはユーザを認証できます。システムは、キャプティブポータル自体を [不明（Unknown）] ユーザーと認識します。

キャプティブポータルの例：アウトバウンドルールを使用した復号ポリシーの作成（2533 ページ）

ステップ 8 アイデンティティと 復号ポリシー をアクセス コントロール ポリシーに関連付けます（ステップ 3）。

この最後の手順により、システムはキャプティブ ポータルを使用してユーザーを認証します。

詳細については、キャプティブポータルの設定パート 6：アクセス コントロール ポリシーへのアイデンティティと 復号ポリシー の関連付け （2535 ページ）を参照してください。

次のタスク

を参照してくださいキャプティブポータルの設定パート 1：ネットワークオブジェクトの作成（2526 ページ）。

関連トピック

キャプティブ ポータルからのアプリケーションの除外 （2537 ページ）
PKI （1352 ページ）
キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （2539 ページ）
Snort 再起動のシナリオ （162 ページ）

キャプティブポータルの設定パート 1：ネットワークオブジェクトの作成

このタスクでは、アイデンティティソースとしてのキャプティブポータルの設定を開始する方法について説明します。

始める前に

（Snort 3 のみ。）DNS サーバーを使用して完全修飾ホスト名（FQDN）を作成し、Firewall Threat Defense の内部証明書を Management Center にアップロードします。これまでに行ったことがない場合は、このようなリソースを参照できます。Management Center で管理されるデバイスの 1 つにあるルーテッドインターフェイスの IP アドレスを指定します。

ネットワークオブジェクトの詳細については、ホスト名ネットワークルール条件にリダイレクト （2559 ページ）を参照してください。

手順

ステップ 1 まだ Management Center にログインしていない場合は、ログインします。

ステップ 2 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** をクリックします。

ステップ 3 [PKI] を展開します。

ステップ 4 [内部証明書（Internal Cert）] をクリックします。

ステップ 5 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 6 [名前（Name）] フィールドに、内部証明書を識別する名前を入力します（たとえば、**`MyCaptivePortal`**）。

ステップ 7 [証明書データ（Certificate Data）] フィールドで、証明書を貼り付けるか、[参照（Browse）] ボタンを使用して検索します。

証明書の共通名は、キャプティブ ポータル ユーザーの認証に使用する FDQN と正確に一致する必要があります。

ステップ 8 [キー（Key）] フィールドで、証明書の秘密キーを貼り付けるか、[参照（Browse）] ボタンを使用して検索します。

ステップ 9 証明書が暗号化されている場合は、[暗号化（Encrypted）] チェックボックスをオンにして、隣のフィールドにパスワードを入力します。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 [ネットワーク（Network）] をクリックします。

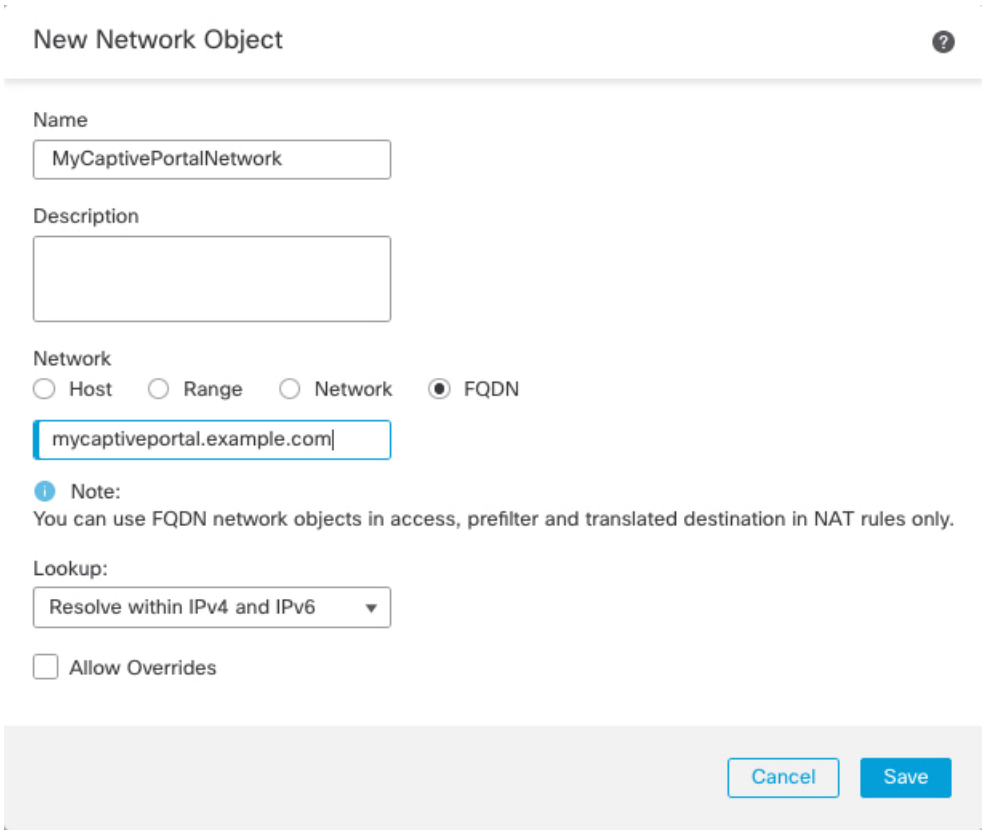
ステップ 12 **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

ステップ 13 [名前（Name）] フィールドに、オブジェクトを識別する名前を入力します（たとえば、**`MyCaptivePortalNetwork`**）。

ステップ 14 [FDQN] をクリックし、フィールドにキャプティブポータルの FDQN の名前を入力します。

ステップ 15 [ルックアップ（Lookup）] のオプションをクリックします。

次の図は例を示しています。



ステップ 16 [保存（Save）] をクリックします。

次のタスク

キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成 （2528 ページ）

キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成

始める前に

複数のパートに分かれたこの手順では、デフォルトの TCP ポート 885 を使用するとともに、キャプティブポータルと TLS/SSL 復号の両方に Management Center サーバー証明書を使用して、キャプティブポータルを設定する方法を示します。この例の各パートでは、キャプティブポータルでアクティブ認証を実行できるようにするために必要なタスクについて説明します。

すべての手順を実行すると、ドメイン内のユーザ用に機能するようにキャプティブポータルを設定できます。必要に応じて、手順の各パートで説明されている追加のタスクを実行できます。

手順全体の概要については、ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）を参照してください。

手順

ステップ 1 Management Center にログインしていない場合はログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [アイデンティティ（Identity）]** の順にクリックして、アイデンティティ ポリシーを作成または編集します。

ステップ 3 （オプション）[カテゴリの追加（Add Category）] をクリックし、そのキャプティブ ポータル アイデンティティ ルール用にカテゴリを追加して、カテゴリの [名前（Name）] を入力します。

ステップ 4 [アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 5 リストから適切なルート**サーバー証明書**を選択するか、[追加（Add）] (＋) をクリックして、証明書を追加します。

詳細については、Active Directory または LDAP に安全に接続する （2471 ページ）を参照してください。

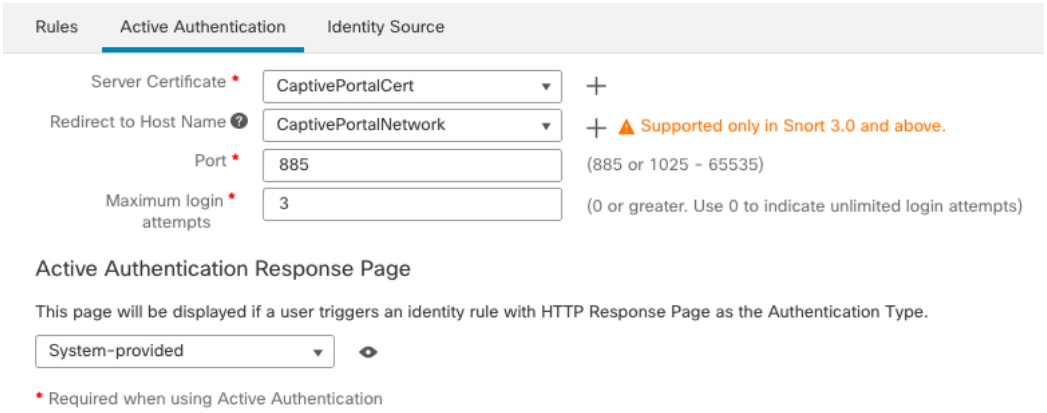
（注）
キャプティブ ポータルは、デジタル署名アルゴリズム（DSA）証明書または楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用をサポートしていません。

ステップ 6 [ホスト名へのリダイレクト（Redirect to Host Name）] フィールドで、前に作成したネットワークオブジェクトをクリックするか、[追加（Add）] (＋) をクリックします。

ステップ 7 [ポート（Port）] フィールドに **885** と入力し、[最大ログイン試行回数（Maximum login attempts）] を指定します。

ステップ 8 （オプション）キャプティブ ポータル フィールド （2536 ページ）の説明に従って、[アクティブ認証応答ページ（Active Authentication Response Page）] を選択します。

次の図は例を示しています。



ステップ 9 [保存（Save）] をクリックします。

ステップ 10 **[ルール（Rules）]** をクリックします。

ステップ 11 [ルールの追加（Add Rule）] をクリックして新しいキャプティブ ポータル アイデンティティ ポリシー ルールを追加するか、[編集（Edit）]（✎） をクリックして既存のルールを編集します。

ステップ 12 ルールの [名前（Name）] を入力します。

ステップ 13 [アクション（Action）] リストから [アクティブ認証（Active Authentication）] を選択します。

ステップ 14 [レルムおよび設定（Realm & Settings）] をクリックします。

ステップ 15 [レルム（Realms）] 一覧から、ユーザー認証に使用するレルムを選択します。

レルムシーケンスはサポートされていません。

ステップ 16 （オプション）[認証でユーザーを識別できない場合はゲストとして識別する（Identify as Guest if authentication cannot identify user）] をオンにします。詳細については、キャプティブ ポータル フィールド （2536 ページ）を参照してください。

ステップ 17 リストから [認証プロトコル（Authentication Protocol）] を 1 つ選択します。

ステップ 18 （オプション）キャプティブ ポータルから特定のアプリケーション トラフィックを除外する方法については、キャプティブ ポータルからのアプリケーションの除外 （2537 ページ）を参照してください。

ステップ 19 アイデンティティルールの条件 （2558 ページ）の説明に従って、ルールに条件を追加します（ポートやネットワークなど）。

ステップ 20 [追加（Add）] をクリックします。

ステップ 21 ページの上部にある [保存（Save）] をクリックします。

次のタスク

キャプティブポータルの設定パート 3：TCP ポートアクセス コントロール ルールの作成 （2530 ページ）に進みます。

キャプティブポータルの設定パート3：TCPポートアクセスコントロール ルールの作成

この手順では、キャプティブ ポータルのデフォルト ポートである TCP ポート 885 を使用して、キャプティブポータルがクライアントと通信できるようにするアクセス コントロール ルールを作成する方法を示します。必要に応じて別のポートを選択できますが、キャプティブポータルの設定パート2：アイデンティティポリシーおよびアクティブ認証ルールの作成 （2528 ページ）で選択したポートと一致している必要があります。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）を参照してください。

手順

ステップ 1 Management Center にログインしていない場合はログインします。

ステップ 2 PKI （1352 ページ）の説明に従って、キャプティブポータルの証明書を作成します（まだ作成していない場合）。

ステップ 3 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [アクセスコントロール（Access Control）]** をクリックして、アクセス コントロール ポリシーを作成または編集します。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

ステップ 5 ルールの [名前（Name）] を入力します。

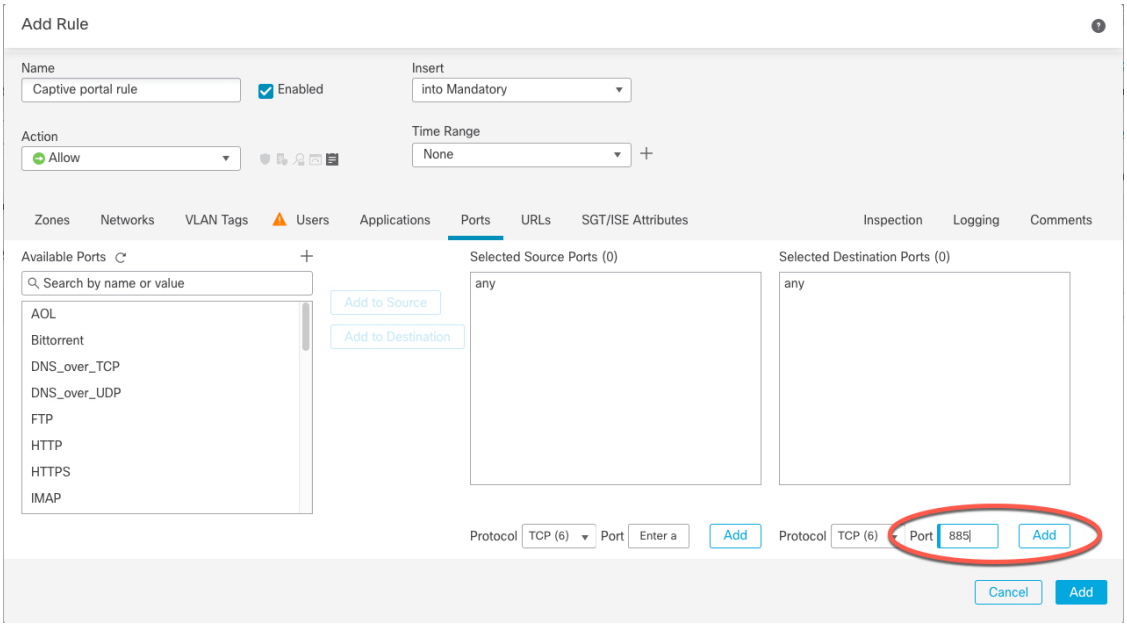
ステップ 6 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

ステップ 7 [ポート（Ports）] をクリックします。

ステップ 8 [選択した宛先ポート（Selected Destination Ports）] フィールドの [プロトコル（Protocol）] 一覧から、[TCP] を選択します。

ステップ 9 [ポート（Port）] フィールドに **885** と入力します。

ステップ 10 [ポート（Port）] フィールドの横にある [追加（Add）] をクリックします。
次の図は例を示しています。



ステップ 11 ページ下部の [追加（Add）] をクリックします。

次のタスク

キャプティブポータルの設定パート 4：ユーザー アクセス コントロール ルールの作成 （2532 ページ）に進みます。

キャプティブポータルの設定パート 4：ユーザー アクセス コントロール ルールの作成

この手順では、レルム内のユーザがキャプティブ ポータルを使用して認証できるようにするアクセス コントロール ルールを追加する方法について説明します。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）を参照してください。

手順

ステップ 1 ルール エディタで、[ルールの追加（Add Rule）] をクリックします。

ステップ 2 ルールの [名前（Name）] を入力します。

ステップ 3 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

ステップ 4 [ユーザー（Users）] をクリックします。

ステップ 5 [使用可能なレルム（Available Realms）] 一覧で、許可するレルムをクリックします。

ステップ 6 レルムが表示されない場合は、[更新（Refresh）]（ ） をクリックします。

ステップ 7 [使用可能なユーザー（Available Users）] 一覧で、ルールに追加するユーザーを選択し、[ルールに追加（Add to Rule）] をクリックします。

ステップ 8 （オプション）アイデンティティルールの条件 （2558 ページ）の説明に従って、アクセス コントロール ポリシーに条件を追加します。

ステップ 9 [追加（Add）] をクリックします。

ステップ 10 [アクセス制御ルール（access control rule）] ページで、[保存（Save）] をクリックします。

ステップ 11 ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。ルールには1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

次のタスク

キャプティブポータルの例：アウトバウンドルールを使用した復号ポリシーの作成（2533 ページ）

キャプティブポータルの例：アウトバウンドルールを使用した復号ポリシーの作成

この手順では、トラフィックがキャプティブポータルに到達する前に、トラフィックを復号して再署名する 復号ポリシー を作成する方法について説明します。キャプティブ ポータルは、トラフィックが復号された後にのみトラフィックを認証できます。

始める前に

アウトバウンドサーバー（つまり、キャプティブポータルユーザーの認証のためにトラフィックを復号する管理対象デバイス）の内部認証局（CA）が必要です。この証明書は、管理対象デバイスでキャプティブポータルを認証するために使用する内部証明書とは異なる必要があります。

手順

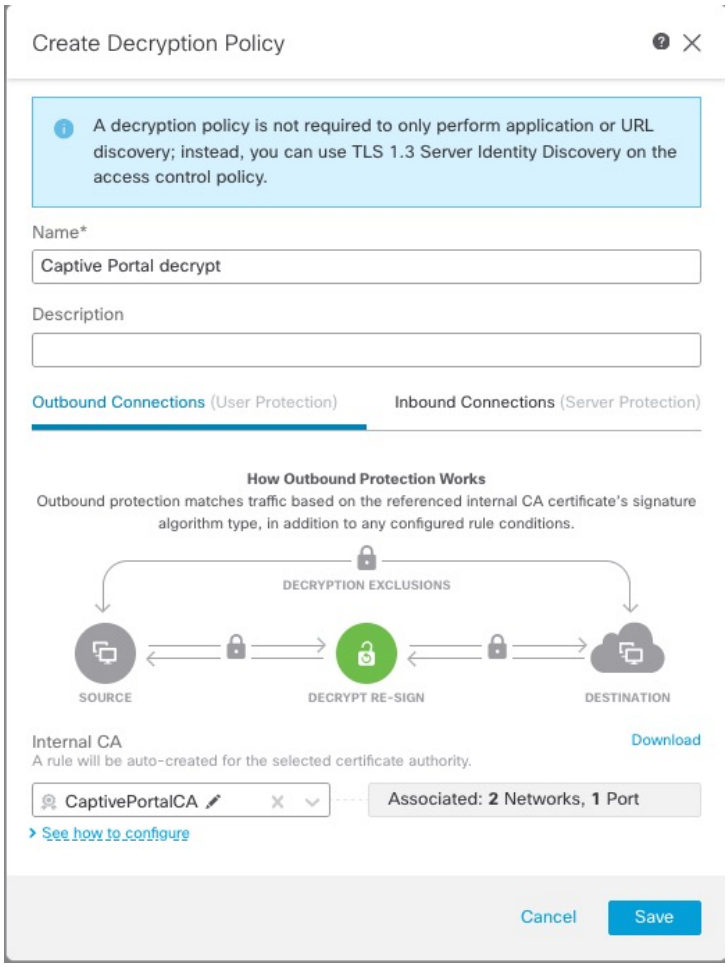
ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]** をクリックします。

ステップ 3 [新しいポリシー（New Policy）] をクリックします。

ステップ 4 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

ステップ 5 [アウトバウンド接続（Outbound Connections）] タブをクリックします。



ステップ 6 ルールの証明書をアップロードまたは選択します。

CA とネットワーク/ポートの各組み合わせに対して 1 つのルールが作成されます。

ステップ 7 （任意）ネットワークとポートを選択します。

詳細については、次を参照してください。

- 復号ルール 条件 （2365 ページ）
- ネットワークルール条件 （816 ページ）
- ポートルールの条件 （819 ページ）

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 作成した復号ポリシーの横にある [編集（Edit）]（✎）をクリックします。

ステップ 10 キャプティブポータルの復号ルールの横にある [編集（Edit）]（✎）をクリックします。

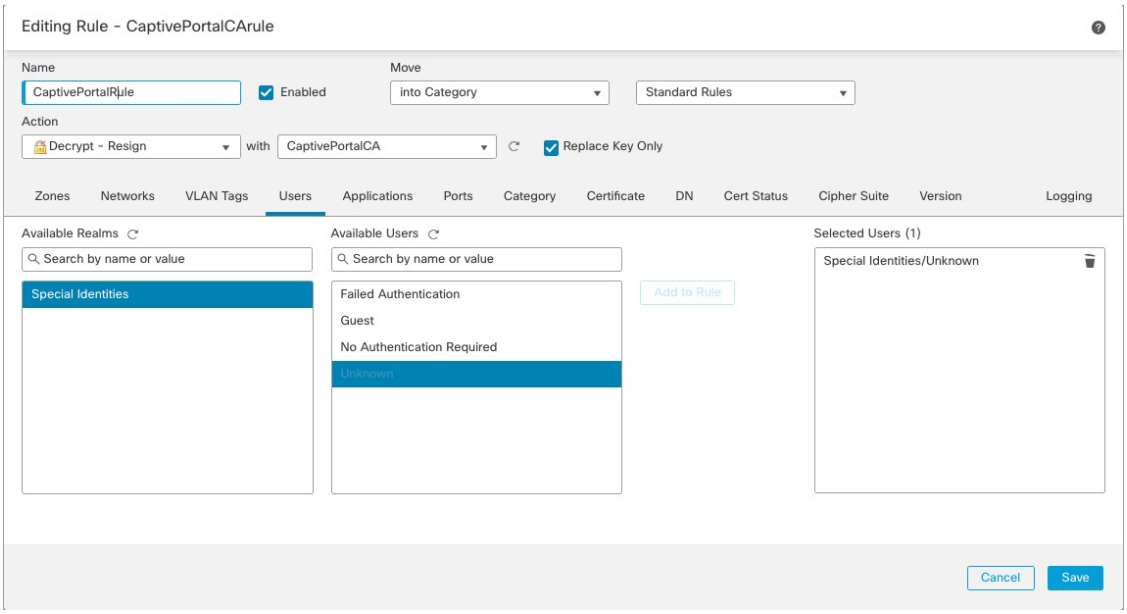
ステップ 11 [ユーザー（Users）] をクリックします。

ステップ 12 [使用可能なレルム（Available Realms）] 一覧の上にある [更新（Refresh）]（） をクリックします。

ステップ 13 [使用可能なレルム（Available Realms）] 一覧で、[特殊なアイデンティティ（Special Identities）] をクリックします。

ステップ 14 [使用可能なユーザー（Available Users）] 一覧で、[不明（Unknown）] をクリックします。

ステップ 15 [ルールに追加（Add to Rule）] をクリックします。
次の図は例を示しています。



ステップ 16 （オプション）復号ルール 条件 （2365 ページ）の説明に従って、他のオプションを設定します。

ステップ 17 **[追加（Add）]** をクリックします。

次のタスク

キャプティブポータルの設定パート 6：アクセス コントロール ポリシーへのアイデンティティと 復号ポリシー の関連付け （2535 ページ）

キャプティブポータルの設定パート 6：アクセス コントロール ポリシーへのアイデンティティと 復号ポリシー の関連付け

この手順では、アイデンティティポリシーと TLS/SSL [復号-再署名（Decrypt - Resign）] ルールを、以前に作成したアクセス コントロール ポリシーに関連付ける方法について説明します。この手順を実行すると、ユーザーはキャプティブ ポータルを使用して認証できるようになります。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセス制御（Access Control）]** をクリックして、キャプティブポータルの設定パート 3：TCP ポートアクセス コントロール ルールの作成（2530 ページ）の説明に従い作成したアクセス コントロール ポリシーを編集します。 代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 新しいアクセス コントロール ポリシーを作成するか、既存のポリシーを編集します。

ステップ 3 ページ上部の [アイデンティティ（Identity）] という文字をクリックします。

ステップ 4 一覧から、使用するアイデンティティ ポリシーの名前を選択し、ページ上部にある [保存（Save）] をクリックします。

ステップ 5 上記の手順を繰り返して、使用するキャプティブポータル復号ポリシーをアクセス コントロール ポリシーに関連付けます。

ステップ 6 アクセス コントロール ポリシーのターゲット デバイスの設定（1757 ページ）の説明に従って、管理対象デバイスでそのポリシーをターゲットにします（この手順をまだ行っていない場合）。

次のタスク

- 設定変更の展開（172 ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- 『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「*Using Workflows*」の説明に従ってユーザーアクティビティをモニターします。

キャプティブ ポータル フィールド

次のフィールドを使用して、アイデンティティポリシーの [Active Authentication] タブページでキャプティブポータルを設定します。「アイデンティティ ルール フィールド（2567 ページ）」および「キャプティブ ポータルからのアプリケーションの除外（2537 ページ）」も参照してください。

サーバー証明書（Server Certificate）

キャプティブ ポータル デーモンが示す内部証明書。

（注） キャプティブ ポータルは、デジタル署名アルゴリズム（DSA）証明書または楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用をサポートしていません。

[ポート（Port）]

キャプティブポータル接続のために使用するポート番号。キャプティブポータルに使用する TCP ポートを使用してアクセス制御ルールを設定し、アイデンティティポリシーをそのアクセス コントロール ポリシーに関連付ける必要があります。詳細については、キャプティブポータルの設定パート 3：TCP ポートアクセス コントロール ルールの作成（2530 ページ）を参照してください。

最大ログイン試行回数（Maximum login attempts）

ユーザのログイン要求がシステムによって拒否されるまでに許容されるログイン試行失敗の最大数。

アクティブ認証回答ページ（Active Authentication Response Page）

キャプティブ ポータル ユーザーに対して表示される、システム提供またはカスタムの HTTP 応答ページ。アイデンティティ ポリシーのアクティブ認証設定で [アクティブ認証応答ページ（Active Authentication Response Page）] を選択した後、[HTTP 応答ページ（TTP Response Page）] で 1 つ以上のアイデンティティ ルールを [認証プロトコル（Authentication Protocol）] として設定する必要があります。

システム提供の HTTP 応答ページには、[ユーザー名（Username）] および [パスワード（Password）] フィールドに加え、[ゲストとしてログイン（Login as guest）] ボタンがあり、ユーザーはゲストとしてネットワークにアクセスできます。単一のログイン方法を表示するには、カスタム HTTP 応答ページを設定します。

次のオプションから選択します。

- 汎用的な応答を使用する場合は、[システム提供（System-provided）] をクリックします。[表示（View）]（）をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[カスタム（Custom）] をクリックします。システム提供コードを示すウィンドウが表示され、これを置換または変更できます。完了したら、変更を保存します。カスタムページは、[編集（Edit）]（）をクリックすると編集できます。

関連トピック

内部証明書オブジェクト （1362 ページ）

キャプティブ ポータルからのアプリケーションの除外

アプリケーション（HTTP `User-Agent` 文字列によって指定される）を選択し、キャプティブ ポータル アクティブ認証から除外することができます。これにより、選択されたアプリケーションからのトラフィックが認証を受けずにアイデンティティ ポリシーを通過できるようになります。

（注） このリストに表示されるのは、**User-Agent Exclusion タグ**が付けられたアプリケーションのみです。

手順

ステップ 1 まだ Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（Identity）]** をクリックします。

ステップ 3 キャプティブポータルルールを含むアイデンティティポリシーを編集します。

ステップ 4 [レルムと設定（Realm & Settings）] タブページで、[HTTPユーザーエージェントの除外（HTTP User Agent Exclusions）] を展開します。

- 最初の列で、アプリケーションをフィルタリングする各項目の横にあるチェックボックスをオンにしてから、1 つ以上のアプリケーションを選択し、[Add to Rule] をクリックします。

  チェックボックスはまとめて AND 結合されます。

- 表示されるフィルタを絞り込むには、[Search by name] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、[クリア（Clear）]（×） をクリックします。

- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、**リロード**（↻）をクリックします。

（注）
リストには一度に 100 のアプリケーションが表示されます。

ステップ 5 [Available Applications] リストから、フィルタに追加するアプリケーションを選択します。

- 表示される個別のアプリケーションを絞り込むには、[名前で検索（Search by name）] フィールドに検索文字列を入力します。検索をクリアするには、[クリア（Clear）]（×）をクリックします。

- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページングアイコンを使用します。

- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、**リロード**（↻） をクリックします。

ステップ 6 外部認証から除外する、選択したアプリケーションを追加します。クリックしてドラッグするか、[ルールに追加（Add to Rule）] をクリックできます。結果は、選択したアプリケーションフィルタの組み合わせになります。

次のタスク

- アイデンティティ ルールの作成（2565 ページ）の説明に従ってアイデンティティ ルールの設定を続けます。

キャプティブポータルのアイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザーのダウンロードのトラブルシュート（2487 ページ）およびユーザー制御のトラブルシューティング（2569 ページ）を参照してください。

キャプティブ ポータルに関する問題が発生した場合は、次の点を確認してください。

- キャプティブポータル管理対象デバイスの時刻は、Firewall Management Center の時刻と同期している必要があります。
- 設定済みの DNS 解決があり、**Kerberos**（または Kerberos をオプションとする場合は **HTTP ネゴシエート**）キャプティブ ポータルを実行するアイデンティティ ルールを作成する場合は、キャプティブ ポータルデバイスの完全修飾ドメイン名（FQDN）を解決するように DNS サーバを設定する必要があります。FQDN は、DNS 設定時に指定したホスト名と一致する必要があります。

  詳細については、ホスト名のリダイレクトについて（2520 ページ）を参照してください。
- Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります（Windows で設定されている NetBIOS の制限）。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に設定します。詳細については、Microsoft のマニュアルサイト「Naming conventions in Active Directory for computers, domains, sites, and OUs」で、次のような記事を参照してください。
- DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、RFC 6891 セクション 6.2.5 で説明されています。
- キャプティブポータルが正しく設定されていても、IP アドレスまたは完全修飾ドメイン名（FQDN）へのリダイレクトが失敗する場合は、エンドポイントセキュリティ ソフトウェアを無効にします。このタイプのソフトウェアは、リダイレクトを妨げる可能性があります。

- **Kerberos**（または Kerberos をオプションとする場合は **HTTP Negotiate**）をアイデンティティルールの [Authentication Type] として選択する場合は、選択する [Realm] には、Kerberos キャプティブ ポータル アクティブ認証を実行できるようにするため、[AD Join Username] および [AD Join Password] が設定されている必要があります。
- アイデンティティルールの [Authentication Type] として [HTTP Basic] を選択した場合、ネットワーク上のユーザーはセッションがタイムアウトしたことを認識しない場合があります。ほとんどの Web ブラウザは、**HTTP 基本**ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。
- Firewall Management Center と管理対象デバイスとの間の接続に障害が発生した場合、ユーザーが以前に認識され Firewall Management Center にダウンロードされた場合を除き、デバイスによって報告されたすべてのキャプティブ ポータル ログインはダウンタイム中に特定できません。識別されていないユーザーは、Firewall Management Center で [不明（Unknown）] のユーザーとして記録されます。ダウンタイム後、不明のユーザーはアイデンティティ ポリシーのルールに従って再確認され、処理されます。
- キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッドインターフェイスの両方が含まれる場合、キャプティブ ポータルデバイス上でルーテッドインターフェイスだけを対象とするようにキャプティブ ポータル アイデンティティ ルールでゾーン条件を設定する必要があります。
- Kerberos認証が成功するには、管理対象デバイスのホスト名が 15 文字未満である必要があります。
- ユーザーをキャプティブポータルから安全にログアウトし、ユーザーが再度ログインできないようにするために、管理者はセッションを閉じることができます：**[分析（Analysis）]** > **[ユーザー（Users）] 見出し** > **[アクティブセッション（Active Sessions）]**。ユーザーがブラウザを閉じた場合も、ブラウザは自動的に再認証されません。
- Active FTP sessions are displayed as the **Unknown** user in events. これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバーが接続を開始し、FTP サーバーには関連付けられているユーザー名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。
- キャプティブポータルがアイデンティティルールに一致するユーザーを認証する場合、ダウンロードされていない Microsoft Active Directory または LDAP グループ内のユーザーは不明として識別されます。ユーザーが不明として識別されるのを回避するには、キャプティブポータルで認証するすべてのグループのユーザーをダウンロードするようにレルムを設定します。不明なユーザーは、関連付けられたアクセス コントロール ポリシーに従って処理されます。アクセス コントロール ポリシーが不明なユーザーをブロックするように構成されている場合、これらのユーザーはブロックされます。

  システムによってレルム内のすべてのユーザーが確実にダウンロードされるようにするには、グループがレルムの設定の [使用可能グループ（Available Groups）] リストに含まれていることを確認します。

  詳細については、「ユーザーとグループの同期 （2475 ページ）」を参照してください。

キャプティブ ポータルの履歴

機能	最小 Firewall Management CenterFirewall Management Center	最小 Firewall Threat Defense	詳細
ホスト名のリダイレクト。	7.1.0	7.1.0（Snort 3）	キャプティブポータルをアクティブな認証要求に使用できるインターフェイスの完全修飾ホスト名（FQDN）を含むネットワークオブジェクトを使用できます。
ゲスト ログイン。	6.1.0	6.1.0	ユーザは、キャプティブ ポータルを使用してゲストとしてログインできます。
キャプティブ ポータル。	6.0.0	6.0.0	導入された機能。キャプティブ ポータルを使用して、ブラウザ ウィンドウにプロンプトが表示されたときにクレデンシャルを入力するよう、ユーザに要求することができます。このマッピングでは、ユーザーまたはユーザーのグループに基づいたポリシーを使用することもできます。

第 68 章

リモートアクセス VPN によるユーザーの制御

次のトピックでは、リモート アクセス VPN によりユーザー認識とユーザー制御を実行する方法について説明します。

- リモート アクセス VPN アイデンティティ ソース （2543 ページ）
- ユーザー制御用 RA VPN の設定 （2544 ページ）
- リモートアクセス VPN アイデンティティ ソースのトラブルシューティング （2545 ページ）
- RA VPN の履歴 （2548 ページ）

リモート アクセス VPN アイデンティティ ソース

Secure Client はエンドポイントデバイスでサポートされている唯一のクライアントで、Firewall Threat Defense デバイスへのリモート VPN 接続が可能です。

新しいリモートアクセス VPN ポリシーの作成 （1572 ページ）の説明に従って安全な VPN ゲートウェイを設定する場合、ユーザーが Active Directory リポジトリ内にいる場合は、それらのユーザーのアイデンティティ ポリシーを設定して、アクセス コントロール ポリシーにアイデンティティ ポリシーを関連付けることができます。

（注） ユーザーアイデンティティと RADIUS をアイデンティティソースとしてリモートアクセス VPN を使用する場合は、レルムを設定する必要があります（[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAA サーバー（AAA Server）] > [RADIUS サーバーグループ（RADIUS Server Group）]）。

リモート ユーザーから提供されるログイン情報は、LDAP または AD レルムまたは RADIUS サーバー グループによって検証されます。これらのエンティティは、Secure Firewall Threat Defense セキュア ゲートウェイと統合されます。

（注） ユーザーが認証ソースとして Active Directory を使用してリモートアクセス VPN で認証を受ける場合、ユーザーは自分のユーザー名を使用してログインする必要があります。`domain\username` または `username@domain` 形式は失敗します。（Active Directory はこのユーザー名をログオン名、または場合によっては `sAMAccountName` と呼んでいます）。詳細については、MSDN でユーザーの命名属性 [英語] を参照してください。

認証に RADIUS を使用する場合、ユーザーは前述のどの形式でもログインできます。

VPN 接続経由で認証されると、リモート ユーザーには *VPN ID* が適用されます。この VPN ID は、そのリモート ユーザーに属しているネットワーク トラフィックを認識し、フィルタリングするために Secure Firewall Threat Defense のセキュア ゲートウェイ上のアイデンティティ ポリシーで使用されます。

アイデンティティ ポリシーはアクセス コントロール ポリシーと関連付けられ、これにより、誰がネットワーク リソースにアクセスできるかが決まります。リモート ユーザーがブロックされるか、またはネットワーク リソースにアクセスできるかはこのようにして決まります。

関連トピック

VPN の概要 （1469 ページ）
リモート アクセス VPN の概要 （1557 ページ）
VPN の基本 （1470 ページ）
リモート アクセス VPN の機能 （1558 ページ）
リモート アクセス VPN のガイドラインと制限事項 （1566 ページ）
新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）

ユーザー制御用 RA VPN の設定

始める前に

- LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）の説明に従って、レルムを作成します。
- 認証、認可、および監査（AAA）を使用するには、RADIUS サーバーグループの追加 （1314 ページ）の説明に従って RADIUS サーバー グループを設定します。

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** の順にクリックします。

ステップ 3 新しいリモート アクセス VPN ポリシーの作成 （1572 ページ）を参照してください。

次のタスク

- アイデンティティ ポリシーの作成（2555 ページ）の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付け （1765 ページ）の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 設定変更の展開 （172 ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- VPN セッションとユーザー情報 （1701 ページ）の説明に従って、VPN ユーザートラフィックをモニターします。

リモート アクセス VPN アイデンティティ ソースのトラブルシューティング

- 関連の他のトラブルシューティングについては、レルムとユーザーのダウンロードのトラブルシュート （2487 ページ）およびユーザー制御のトラブルシューティング （2569 ページ）を参照してください。
- リモート アクセス VPN の問題が発生した場合は、Firewall Management Center と管理対象デバイスとの間の接続を確認します。接続に障害が発生している場合、ユーザが既に認識されて Firewall Management Center にダウンロードされている場合を除き、デバイスによって報告されたすべてのリモート アクセス VPN ログインはダウンタイム中に識別されません。

  識別されていないユーザは、Firewall Management Center で [不明（Unknown）] のユーザとして記録されます。ダウンタイム後、[不明（Unknown）] ユーザーはアイデンティティ ポリシーのルールに従って再び識別され、処理されます。
- Kerberos認証が成功するには、管理対象デバイスのホスト名が 15 文字未満である必要があります。
- Active FTP sessions are displayed as the **Unknown** user in events. これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバーが接続を開始し、FTP サーバーには関連付けられているユーザー名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

VPN 統計の設定が正しくない

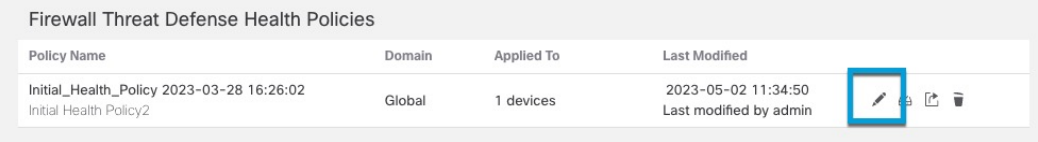
このタスクでは、正常性ポリシーで [VPN統計（VPN Statistics）] 設定を有効または無効にした後に実行する必要がある手順について説明します。このタスクを実行しない場合は、管理対象デバイスの正常性ポリシーの設定が正しくないことを意味します。

手順

ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 [システム（System）]（⚙）>**[正常性（Health）]**>**[ポリシー（Policy）]** をクリックします。

ステップ 3 [Firewall Threat Defense正常性ポリシー（Firewall Threat Defense Health Policies）] で、編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。



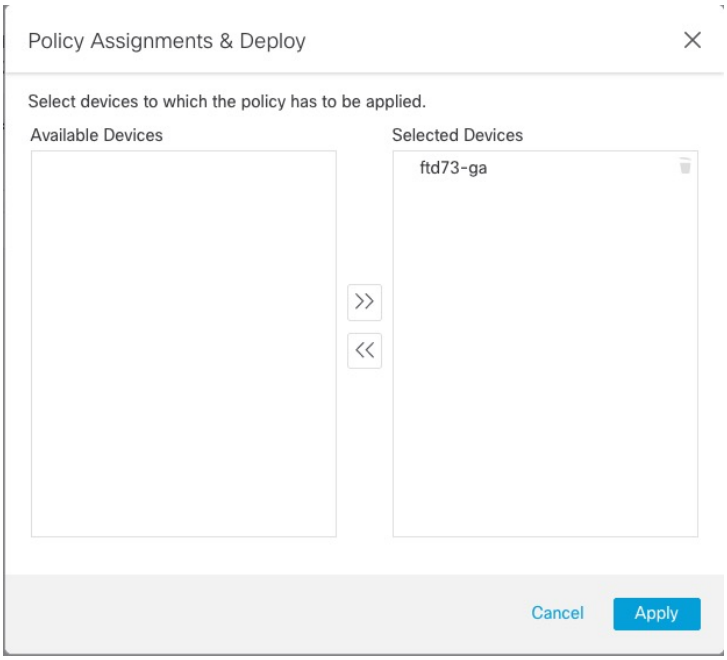
ステップ 4 [正常性モジュール（Health Modules）] タブページで、下にスクロールして [VPN統計（VPN Statistics）] を見つけます。

ステップ 5 VPN 統計の設定が正しいことを確認するか、必要に応じて変更します。

ステップ 6 設定を変更した場合は、[保存（Save）] をクリックし、[キャンセル（Cancel）] をクリックして正常性ポリシーに戻ります。

ステップ 7 [Firewall Threat Defense正常性ポリシー（Firewall Threat Defense Health Policies）]で、 [正常性ポリシーの展開（Deploy health policy）]（📥） をクリックしてポリシーを適用します。

ステップ 8 [ポリシーの割り当てと展開（Policy Assignments & Deploy）] ダイアログボックスで、正常性ポリシーを展開するデバイスを [選択したデバイス（Selected Devices）] フィールドに移動します。



ステップ 9 [適用（Apply）] をクリックします。
正常性ポリシーが展開されると、メッセージが表示されます。

ステップ 10 正常性ポリシーの展開が完了したら、**[ポリシー（Policies）]**>**[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** をクリックしてアクセス コントロール ポリシーを編集します。

ステップ 11 編集するポリシーの横にある編集 [編集（Edit）]（） をクリックします。

ステップ 12 名前の変更など、ポリシーにマイナー変更を加えます。

ステップ 13 アクセス コントロール ポリシーを保存します。

ステップ 14 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。。

RA VPN の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
リモート アクセス VPN	6.2.1	いずれか	導入された機能。RA VPN により、インターネットに接続されたラップトップまたはデスクトップ コンピュータや、Android または Apple iOS モバイル デバイスを使用して、個々のユーザがリモート ロケーションからプライベート ビジネス ネットワークに接続することができます。リモートユーザーは、共有メディアやインターネットを介してデータを転送するために不可欠な暗号化技術を使用して、セキュアに機密性を保持してデータを転送します。

第 69 章

TS エージェントによるユーザーの制御

TS エージェントをユーザー認識およびユーザー制御用のアイデンティティソースとして使用するには、Cisco ターミナルサービス（TS）エージェントガイドの説明に従って TS エージェントソフトウェアをインストールして設定します。

次に行う作業：

- アイデンティティ ポリシーの作成（2555 ページ）の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付け（1765 ページ）の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 設定変更の展開（172 ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「*Using Workflows*」の説明に従って、ユーザーアクティビティをモニターします。

- ターミナル サービス（TS）エージェントのアイデンティティ ソース （2549 ページ）
- TS エージェントのガイドライン （2550 ページ）
- TS エージェントによるユーザーの制御 （2550 ページ）
- TS エージェント アイデンティティ ソースのトラブルシューティング （2551 ページ）
- TS エージェントの履歴 （2552 ページ）

ターミナルサービス（TS）エージェントのアイデンティティ ソース

TS エージェントはパッシブ認証方式であり、システムでサポートされる権限のあるアイデンティティソースの 1 つです。Windows Terminal Server が認証を実行し、TS エージェントがスタンドアロンまたはハイ アベイラビリティの Firewall Management Center にその認証の実行を報告します。

TS エージェントは、Windows Terminal Server にインストールされると、個々のユーザーがモニター対象ネットワークにログインまたはログアウトする際にそのユーザーに固有のポート範囲を割り当てます。Firewall Management Center では、この固有のポートを使用してシステムの個々のユーザーを識別します。1 つの TS エージェントを使用して、1 つの Windows Terminal Server 上のユーザ アクティビティをモニタし、暗号化データを Firewall Management Center に送信できます。

TS エージェントは失敗したログイン試行を報告しません。TS エージェントから取得されたデータは、ユーザー認識とユーザー制御に使用できます。

TS エージェントのガイドライン

TS エージェントには段階的な設定が必要で、次のものがあります。

1. TS エージェントがインストールおよび設定された Windows Terminal Server。
2. サーバがモニタするユーザを対象とする 1 つ以上のアイデンティティ レルム。

TS エージェントは、Microsoft Windows Terminal Server にインストールします。段階的な TS エージェントのインストールと設定、およびサーバーと Firepower システムの要件の詳細については、Cisco ターミナルサービス（TS）エージェントガイドを参照してください。

TS エージェントのデータは [ユーザー（Users）] テーブル、[ユーザー アクティビティ（User Activity）] テーブル、および [接続イベント（Connection Event）] テーブルに表示され、ユーザー認識とユーザー制御に使用できます。

（注） TS エージェントが別のパッシブ認証の ID ソース（ISE/ISE-PIC）と同じユーザーをモニターしている場合、Firewall Management Center は TS エージェントのデータを優先します。同じ IP アドレスによるアクティビティが TS エージェントと別のパッシブ アイデンティティ ソースから報告される場合、TS エージェントのデータだけが Firewall Management Center に記録されます。

TS エージェントによるユーザーの制御

TS エージェントをユーザー認識およびユーザー制御用のアイデンティティ ソースとして使用するには、Cisco ターミナルサービス（TS）エージェントガイドの説明に従って TS エージェントソフトウェアをインストールして設定します。

次に行う作業：

- アイデンティティ ポリシーの作成（2555 ページ）の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付け（1765 ページ）の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。

- 設定変更の展開（172 ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「*Using Workflows*」の説明に従って、ユーザーアクティビティをモニターします。

TS エージェント アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザーのダウンロードのトラブルシュート（2487 ページ）およびユーザー制御のトラブルシューティング（2569 ページ）を参照してください。

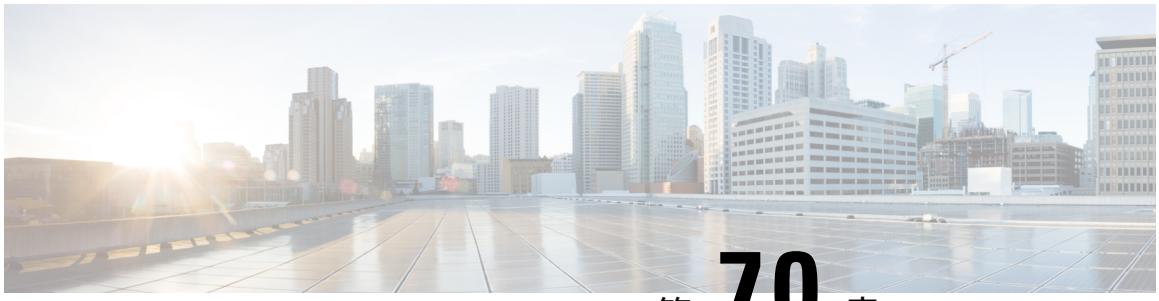
TS エージェントの統合で問題が発生した場合は、次のことを確認してください。

- TS エージェントサーバーと Firewall Management Center の時計を同期させる必要があります。
- TS エージェントが別のパッシブ認証の ID ソース（ISE/ISE-PIC）と同じユーザーをモニターしている場合、Firewall Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firewall Management Center に記録されます。
- Active FTP sessions are displayed as the **Unknown** user in events. これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバーが接続を開始し、FTP サーバーには関連付けられているユーザー名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

トラブルシューティングの詳細については、Cisco ターミナルサービス（TS）エージェントガイドを参照してください。

TS エージェントの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ユーザ制御用の TS エージェント。	7.2.0	6.2.0	導入された機能。FirePOWER が、Citrix の仮想デスクトップ インフラストラクチャ（VDI）などの共有環境で個々のユーザをより正確に識別して、ファイアウォールにユーザ ベースのポリシー ルールを正確に適用できるようになりました。ユーザは使用されるポートによって識別されます。 TS エージェント ソフトウェアは、Firepower Management Center とは独立して更新されます。詳細については、以下を参照してください。 • cisco.com で利用可能な『*Cisco Terminal Services (TS) Agent Guide*』 • 『Cisco Firepower Compatibility Guide』



第 70 章

ユーザー アイデンティティ ポリシー

次のトピックでは、アイデンティティ ルールとアイデンティティ ポリシーの作成方法と管理方法について説明します。

- アイデンティティ ポリシーについて （2553 ページ）
- アイデンティティポリシーのライセンス要件 （2554 ページ）
- アイデンティティポリシーの要件と前提条件 （2555 ページ）
- アイデンティティ ポリシーの作成 （2555 ページ）
- アイデンティティルールの条件 （2558 ページ）
- アイデンティティ ルールの作成 （2565 ページ）
- アイデンティティ ポリシーの管理 （2568 ページ）
- アイデンティティ ルールの管理 （2569 ページ）
- ユーザー制御のトラブルシューティング （2569 ページ）

アイデンティティ ポリシーについて

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

次の段落の最後に記載されている例外を除き、使用する予定のレルムと認証方式は、アイデンティティルールで起動する前に設定する必要があります。

- **[システム（System）] > [統合（Integration）] > [レルム（Realms）]** でアイデンティティ ポリシー外のレルムを設定します。詳細については、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）を参照してください。
- パッシブ認証のアイデンティティソースである ISE/ISE-PIC は、**[システム（System）] > [統合（Integration）] > [アイデンティティソース（Identity Sources）]**で設定します。
- パッシブ認証のアイデンティティソースである TS エージェントについては、システムの外で設定します。詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

- アクティブ認証のアイデンティティ ソースであるキャプティブ ポータルについては、アイデンティティ ポリシー内で設定します。詳細については、ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）を参照してください。
- リモート アクセス VPN ポリシー内では、アクティブな認証アイデンティティ ソースであるリモート アクセス VPN を設定します。詳細については、リモート アクセス VPN 認証（1561 ページ）を参照してください。

単一のアイデンティティ ポリシーに複数のアイデンティティ ルールを追加した後、ルールの順番を決めます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールがそのトラフィックを処理するルールです。

ネットワークオブジェクトでトラフィックをフィルタ処理することもできます。これにより、デバイスがメモリ制限に達しているか、または制限に近い状態の場合に、各デバイスがモニターするネットワークが制限されます。

1 つ以上のアイデンティティ ポリシーを設定した後、1 つのアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付ける必要があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致する場合、システムはトラフィックを指定されたレルムと関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザーを認証します。

アイデンティティ ポリシーを設定しない場合、システムはユーザー認証を実行しません。

アイデンティティ ポリシーの作成に関する例外

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE/ISE-PIC アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較」を参照してください。

関連トピック

アイデンティティ ポリシーの設定方法 （2438 ページ）

アイデンティティポリシーのライセンス要件

Threat Defense ライセンス

いずれか（Any）

従来のライセンス

Control

アイデンティティポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

アイデンティティ ポリシーの作成

このタスクでは、アイデンティティポリシーの作成方法について説明します。

始める前に

アイデンティティ ポリシーは、アクセス コントロール ポリシーのレルムでユーザやグループを使用するために必要です。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）の説明に従って 1 つ以上のレルムを作成し、有効にします。

（オプション）多数のユーザーグループをモニターする特定の管理対象デバイスの場合、管理対象デバイスのメモリ制限のためにグループに基づいてユーザーマッピングがドロップされることがあります。その結果、レルムまたはユーザー条件を使用するルールが想定どおりに実行されない可能性があります。デバイスがバージョン6.7以降を実行している場合は、1つのネットワークまたはネットワーク グループ オブジェクトのみによってトラフィックをモニターするアイデンティティルールを設定できます。ネットワークオブジェクトの作成については、ネットワーク オブジェクトの作成 （1351 ページ）を参照してください。

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE/ISE-PIC アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較」を参照してください。

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（Identity）]** をクリックし、[新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ポリシーにルールを追加するには、アイデンティティ ルールの作成 （2565 ページ）で説明されているように、[ルールの追加（Add Rule）] をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 7 キャプティブポータルのアクティブ認証を設定するには、[アクティブ認証（Active Authentication）] をクリックし、キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成 （2528 ページ） を参照します。

ステップ 8 （オプション）ネットワークオブジェクトでトラフィックをフィルタ処理するには、[Identity Source] タブをクリックします。リストから、この ID ポリシーのトラフィックのフィルタ処理に使用するネットワークオブジェクトをクリックします。新しいネットワークオブジェクトを作成するには、[追加（Add）] (+) をクリックします。

ステップ 9 [保存（Save）] をクリックして、アイデンティティ ポリシーを保存します。

次のタスク

- 照合するユーザーおよび他のオプションを指定するルールを、アイデンティティ ポリシーに追加します（アイデンティティ ルールの作成 （2565 ページ）を参照）。
- 指定したリソースへのアクセスを特定のユーザーに許可またはブロックするには、このアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付け （1765 ページ）を参照）。
- 設定変更を管理対象デバイスに展開します（設定変更の展開 （172 ページ）を参照）。

問題が発生した場合は、ユーザー制御のトラブルシューティング （2569ページ）を参照してください。

関連トピック

キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成 （2528 ページ）
キャプティブ ポータル フィールド （2536 ページ）
ユーザー制御のトラブルシューティング （2569 ページ）
アイデンティティ マッピング フィルタの作成 （2557 ページ）

アイデンティティ マッピング フィルタの作成

アイデンティティマッピングフィルタを使用して、アイデンティティルールが適用されるネットワークを制限できます。たとえば、Management Center がメモリ量の限られた FTD を管理している場合、モニターするネットワークを制限できます。

IPv4 アドレスと IPv6 アドレスに対して個別のアイデンティティ マッピング フィルタを作成する必要があります。

必要に応じて、以下からサブネットを除外することもできます。

- ユーザーから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングを ISE から受信する。

通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。

始める前に

次の作業を実行します。

1. アイデンティティポリシーに必要なレルムを作成します。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）を参照してください。
2. アイデンティティ ポリシーを作成します。アイデンティティ ポリシーの作成 （2555 ページ）を参照してください。
3. ネットワーク オブジェクトの作成 （1351 ページ） の説明に従って、ネットワークオブジェクトまたはネットワーク グループ オブジェクトを作成します。作成するネットワークオブジェクトまたはグループでは、管理対象デバイスがアイデンティティポリシーでモニターするネットワークを定義する必要があります。

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** をクリックします。

ステップ 3 [編集（Edit）]（✎） をクリックします。

ステップ 4 [アイデンティティの送信元（Identity Source）] タブをクリックします。

ステップ 5 [アイデンティティ マッピング フィルタ（Identity Mapping Filter）] リストから、フィルタとして使用するネットワークオブジェクトの名前をクリックする。

新しいネットワークオブジェクトを作成するには、ネットワーク オブジェクトの作成 （1351 ページ）を参照してください。

（注）
トラフィックを IPv6 アドレスに制限するには、少なくとも 1 つのアドレス、ネットワーク、またはグループをフィルタに追加する必要があります。

ステップ 6 **[Save（保存）]** をクリックします。

ステップ 7 設定変更を管理対象デバイスに展開します（設定変更の展開 （172 ページ）を参照）。

次のタスク

アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付け （1765 ページ） を参照）。

ISEアイデンティティマッピングフィルタ（サブネットフィルタとも呼ばれる）を確認または変更するには、以下のコマンドを使用します。

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

アイデンティティルールの条件

ルール条件を使用すると、アイデンティティポリシーを微調整して、制御するユーザーとネットワークをターゲットにすることができます。詳細については、次の項を参照してください。

関連トピック

セキュリティゾーンルール条件 （1877 ページ）
ネットワークルール条件 （816 ページ）
VLAN タグルール条件 （1792 ページ）
ポートルールの条件 （819 ページ）
レルムと設定のルール条件 （2562 ページ）

セキュリティゾーンルール条件

セキュリティゾーンはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することで、トラフィックフローを管理、分類、および復号しやすくします。

セキュリティゾーンは、トラフィックをその送信元と宛先のセキュリティゾーンで制御または復号します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ヒント　ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

ネットワークルール条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注）　アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

ホスト名ネットワークルール条件にリダイレクト

（Snort 3.0 のみ）キャプティブポータルがアクティブな認証要求に使用できるインターフェイスの完全修飾ホスト名（FQDN）を含むネットワークオブジェクトを使用できます。

FQDN は、管理対象デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、管理対象デバイスの IP アドレスにリダイレクトされたときにユーザーに表示される信頼できない証明書の警告を回避できます。

証明書では、1 つの FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。

アイデンティティルールによりユーザーのアクティブ認証が要求されているが、リダイレクト FQDN を指定していない場合、ユーザーは、接続されている管理対象デバイスのインターフェイス上のキャプティブポータルポートにリダイレクトされます。

[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定しない場合、HTTP 基本、HTTP 応答ページ、および NTLM 認証方式では、インターフェイスの IP アドレスを使用してユーザーがキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、

ユーザーは完全修飾 DNS 名 *firewall-hostname.directory-server-domain-name* を使用してリダイレクトされます。[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定せずに HTTP ネゴシエートを使用するには、アクティブ認証が必要なすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバーを更新する必要もあります。そうでない場合は、リダイレクションが完了せず、ユーザは認証できません。

認証方式に関係なく一貫した動作を確保するために、[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を常に指定することを推奨します。

VLAN タグルール条件

（注） アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

ポートルールの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTD など）にも推奨されます。ポートベースのアクセス コントロールルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

ポート、プロトコル、および ICMP コードルールの条件

ポート条件により、送信元ポートと宛先ポートに基づいてトラフィックが照合されます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP と UDP のトラフィックは、ポートに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- プロトコル：ポートを使用しないその他のプロトコルを使用してトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスする

ように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーションフィルタリング基準を使用してトラフィックをターゲット指定します。なお、プレフィルタルールではアプリケーション フィルタリングを使用できません。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTP など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP と DNS over UDP の両方を 1 つのアクセスコントロールルールの宛先ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

ポートベースではないプロトコルを照合できます。デフォルトでは、ポート条件を指定しない場合は IP トラフィックを照合します。非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：クラシック デバイスの場合、GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して**すべての**トラフィックを照合します。Firewall Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。
- 復号ルール：これらのルールは TCP ポート条件のみをサポートします。
- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

レルムと設定のルール条件

[レルムと設定（Realm & Settings）] タブページでは、アイデンティティルールを適用するレルムまたはレルムシーケンスを選択できます。キャプティブポータルを使用している場合は、追加のオプションがあります。

認証レルム（Authentication Realm）

[レルム（Realm）] リストから、レルムまたはレルムシーケンスをクリックします。

[アクション（Action）] で指定されたアクションの実行対象になるユーザーが含まれるレルムまたはレルムシーケンス。アイデンティティルールのレルムまたはレルムシーケンスとして選択する前に、これを完全に設定する必要があります。

（注） リモート アクセス VPN が有効で、展開で VPN 認証に RADIUS サーバー グループを使用している場合は、この RADIUS サーバー グループに関連付けられているレルムを指定してください。

アクティブ認証のみ：その他のオプション

認証タイプとして [アクティブ認証（Active Authentication）] を選択するか、[パッシブまたはVPN IDを確立できない場合はアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] チェックボックスをオンにした場合、次のオプションがあります。

パッシブまたはVPN IDを確立できない場合はアクティブ認証を使用

（パッシブ認証ルールのみ）このオプションを選択すると、パッシブまたは VPN 認証でユーザーを識別できない場合にキャプティブ ポータルアクティブ認証を使用してユーザーが認証されます。このオプションを選択するには、アイデンティティポリシーでアクティブ認証ルールを設定する必要があります。（つまり、ユーザーはキャプティブポータルを使用して認証する必要があります）

このオプションを無効にすると、VPN ID を持たないユーザまたはパッシブ認証では識別できないユーザは、「不明（Unknown）」と識別されます。

このトピックで後述する**認証レルム**リストの説明も参照してください。

認証でユーザーを識別できない場合は特別 ID/ゲストとして識別する（Identify as Special Identities/Guest if authentication cannot identify user）

このオプションを選択すると、キャプティブ ポータル アクティブ認証に指定された回数失敗したユーザーがゲストとしてネットワークにアクセスできます。これらのユーザーは、Firewall Management Center 上ではユーザー名（ユーザー名が AD または LDAP サーバーに存在する場合）または[ゲスト（Guest）]（ユーザー名が不明の場合）で表示されます。これらのユーザーのレルムは、アイデンティティ ルールで指定されたレルムです。（デフォルトでは、失敗したログインの数は 3 回です。）

ルール アクションとして [アクティブ認証（Active Authentication）]（つまり、キャプティブ ポータル認証）を設定している場合にのみ、このフィールドが表示されます。

認証プロトコル（Authentication Protocol）

キャプティブ ポータル アクティブ認証を実行するために使用する方法です。。

選択は、レルム、LDAP、または AD のタイプによって異なります。

- 暗号化されていないHTTP基本認証（BA）接続を使用してユーザーを認証するには、[HTTP 基本（HTTP Basic）] を選択します。ユーザーはブラウザのデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。

  ほとんどの Web ブラウザは、**HTTP 基本**ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。

- NT LAN Manager（NTLM）接続を使用してユーザーを認証するには **NTLM** を選択します。この選択は AD レルムを選択するときにのみ使用できます。透過的な認証がユーザーのブラウザで設定されている場合、ユーザーは自動的にログインします。透過的な認証が設定されていない場合、ユーザーは各自のブラウザでデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。

- Kerberos 接続を使用してユーザーを認証する場合は、[Kerberos] を選択します。この選択は、セキュア LDAP（LDAPS）が有効になっているサーバーに対して AD レルムを選択する場合にのみ可能です。透過的な認証がユーザーのブラウザで設定されている場合、ユーザーは自動的にログインします。透過的な認証が設定されていない場合、ユーザーは各自のブラウザでデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。

（注） 選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行するために、[AD参加ユーザー名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） Kerberosキャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS解決は設定済みである場合は、キャプティブ ポータルデバイスの完全修飾ドメイン名（FQDN）を解決するDNSサーバーを設定する必要があります。FQDNは、DNS の設定時に指定したホスト名と一致する必要があります。

Firewall Threat Defense デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッドインターフェイスのIPアドレスに解決される必要があります。

- キャプティブ ポータル サーバーが認証接続に HTTP 基本認証、Kerberos、または NTLM を選択できるようにするには、[HTTP ネゴシエート（HTTP Negotiate）] を選択します。このタイプは AD レルムを選択するときにのみ使用できます。

（注） 選択する [レルム（Realm）] は、[HTTP ネゴシエート（HTTP Negotiate）] で Kerberos キャプティブ ポータル アクティブ認証を選択するために、[AD 参加ユーザー名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） [HTTP ネゴシエート（HTTP Negotiate）] キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバーを設定する必要があります。キャプティブ ポータルに使用するデバイスの FQDN は、DNS の設定時に入力したホスト名と一致している必要があります。

- ユーザーがログインするレルムを選択できるようにするには、[HTTP 応答ページ（HTTP Response Page）] を選択します。

  必要に応じて、応答ページをカスタマイズできます。たとえば、会社のスタイル標準に準拠できます。

アイデンティティ ルールの作成

アイデンティティ ルールの設定オプションに関する詳細については、アイデンティティ ルール フィールド （2567 ページ）を参照してください。

始める前に

レルムまたはレルムシーケンスを作成して有効にする必要があります。

- LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （2452 ページ）の説明に従って、Microsoft Azure Active Directory レルムおよびレルムディレクトリを作成します。
- ユーザーおよびグループをダウンロードし、ユーザーとグループの同期 （2475 ページ）で説明したようにレルムを有効にします。
- （オプション）レルムシーケンスの作成 （2476 ページ）の説明に従って、レルムシーケンスを作成します。
- ルールは、トップダウン方式で評価されます。特定のルールの指定されたネットワーク基準に一致する接続の場合、ユーザーは、ルールで指定されたアイデンティティレルムに対して評価されます。そのレルムの一部ではない場合、そのユーザーは不明としてマークさ

れ、アイデンティティポリシー内のそれ以上のルールは評価されません。そのため、評価する必要があるレルムが複数ある場合は、単一のレルムではなく、必ずレルムシーケンスを使用してください。

注意 TLS/SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに 復号ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれることに注意してください。

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（Identity）]** をクリックします。

ステップ 3 アイデンティティルールの追加先となるアイデンティティポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 指定されたルールを適用する場合は、[有効（Enabled）] チェックボックスをオンにします。

ステップ 7 既存のカテゴリにルールを追加するには、ルールを [挿入（Insert）] する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 8 一覧からルール [アクション（Action）] を選択します。

ステップ 9 キャプティブ ポータルを設定する場合は、ユーザー制御のためのキャプティブ ポータルの設定方法 （2524 ページ）を参照してください。

ステップ 10 （オプション）アイデンティティルールに条件を追加するには、アイデンティティルールの条件 （2558 ページ）を参照してください。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。ルールには1から番号が付け

られます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 13 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

Enabled

このオプションを有効にすると、ID ポリシーのアイデンティティルールが有効になります。このオプションの選択を解除すると、アイデンティティルールが無効になります。

Action

指定したレルムでユーザーに対して実行する認証のタイプを指定します。これには、[パッシブ認証（Passive Authentication）]（デフォルト）、[アクティブ認証（Active Authentication）]、または [認証なし（No Authentication）] があります。アイデンティティルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。

さらに、VPN が有効になっている場合（少なくとも 1 つの管理対象デバイスで設定されている場合）、リモートアクセス VPN セッションは VPN によってアクティブに認証されます。他のセッションはルール アクションを使用します。つまり、VPN が有効になっている場合は、選択したアクションに関係なく、すべてのセッションで VPN ID の判別が最初に行われます。指定されたレルム上に VPN ID が見つかった場合、これは使用されるアイデンティティ ソースになります。選択されていても、追加のキャプティブ ポータル アクティブ認証は実行されません。

VPN アイデンティティ ソースが見つからない場合は、指定されたアクションに従ってプロセスが続行されます。アイデンティティ ポリシーを VPN 認証のみに制限することはできません。VPN ID が見つからない場合は、選択されたアクションに従ってルールが適用されるためです。

⚠

注意 TLS/SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれることに注意してください。

使用中のシステムのバージョンでサポートされるパッシブおよびアクティブ認証方式の詳細については、ユーザー アイデンティティ ソースについて （2433 ページ）を参照してください。

アイデンティティ ポリシーの管理

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（Identity）]** をクリックします。

ステップ 3 ポリシーを削除するには、[削除（Delete）]（🗑） をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ポリシーを編集するには、ポリシーの横にある [編集（Edit）]（✎） をクリックし、アイデンティティ ポリシーの作成 （2555 ページ）の説明に従って変更を行います。 代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 5 ポリシーをコピーするには、[コピー（Copy）]（⧉） をクリックします。

ステップ 6 ポリシーのレポートを生成するには、現在のポリシーレポートの生成 （192 ページ）の説明に従って **[レポート（Report）]**（📄） をクリックします。

ステップ 7 ポリシーを比較する方法については、ポリシーの比較 （190 ページ）を参照してください。

ステップ 8 ポリシーを整理するフォルダを作成するには、[カテゴリの追加（Add Category）] をクリックします。

次のタスク

設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アイデンティティ ルールの管理

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（Identity）]** をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（ ）をクリックします。代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 アイデンティティルールを編集する場合は、[編集（Edit）]（）をクリックし、アイデンティティ ポリシーの作成 （2555 ページ）の説明に従って変更を行います。

ステップ 5 アイデンティティルールを削除するには、[削除（Delete）]（ ） をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックし、位置とルールを選択します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ユーザー制御のトラブルシューティング

ユーザー ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。その他の関連するトラブルシューティング情報については、以下を参照してください。

- ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング （2514 ページ）
- TS エージェント アイデンティティ ソースのトラブルシューティング （2551 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （2539 ページ）
- レルムとユーザーのダウンロードのトラブルシュート （2487 ページ）

レルム、ユーザー、またはユーザーグループを対象とするルールがトラフィックと一致しない

TS エージェントまたは ISE/ISE-PIC デバイスのモニター対象に多くのユーザーグループを設定した場合、またはネットワークでホストにマップされるユーザー数が非常に多い場合、Firewall Management Center のユーザー制限が原因で、システムがユーザーレコードをドロップすることがあります。その結果、ユーザー条件のルールが、一致することが想定されているトラフィックと一致しない可能性があります。

ユーザー グループまたはユーザー グループ内のユーザーを対象とするルールが、一致することが想定されているトラフィックと一致しない

ユーザー グループ条件を含むルールを設定する場合は、LDAP または Active Directory サーバーでユーザー グループを設定している必要があります。サーバーが基本的なオブジェクト階層でユーザーを整理している場合、システムはユーザー グループ制御を実行できません。

セカンダリ グループ内のユーザーを対象とするルールが、一致することが想定されているトラフィックと一致しない

Active Directory サーバーのセカンダリ グループのメンバーであるユーザーを含めるか除外するユーザー グループ条件を含むルールを設定する場合、サーバーは報告するユーザーの数を制限していることがあります。

デフォルトでは、Active Directory サーバーはセカンダリ グループから報告するユーザーの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザーが Firewall Management Center に報告され、ユーザー条件を含むルールでの使用に適するようにカスタマイズする必要があります。

ルールが、初めて表示されたユーザーと一致しない

システムは、以前に表示されていないユーザーからのアクティビティを検出すると、サーバーからそれらのユーザーに関する情報を取得します。システムがこの情報を正常に取得するまで、このユーザーに表示されるアクティビティは、一致するルールによって処理されません。代わりに、ユーザーセッションが、一致する次のルール（または該当する場合はポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザー グループのメンバーであるユーザーが、ユーザー グループ条件を含むルールに一致しない。
- ユーザーデータの取得に使用されたサーバーが Active Directory サーバーである場合、TS エージェントまたは ISE デバイスによって報告されたユーザーがルールと一致しない。

これにより、システムがユーザー データをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

ルールがすべての ISE/ISE-PIC ユーザーと一致しない

これは想定されている動作です。Active Directory ドメイン コントローラで認証された ISE/ISE-PIC ユーザーに対してユーザー制御を実行することができます。LDAP、RADIUS、または RSA ド

メイン コントローラで認証された ISE/ISE-PIC ユーザーに対するユーザー制御は実行できません。

ユーザーとグループによる大量のメモリの使用

ユーザーとグループの処理によって大量のメモリが使用されている場合、ヘルスアラートが表示されます。すべてのユーザーセッションが Firewall Management Center のすべての管理対象デバイスに伝達されることに注意してください。Firewall Management Center がメモリ容量の異なるデバイスを管理している場合、メモリ容量が最も小さいデバイスによって、システムがエラーなしで処理できるユーザーセッションの数が決まります。

アイデンティティプロセスに割り当てられたメモリを調整することはできません。デバイスに使用可能なメモリがある場合でも、メモリ不足の問題を報告することがあります。問題が解決しない場合、次の選択肢があります。

- 容量の小さい管理対象デバイスをサブネットに分離し、パッシブ認証データをそれらのサブネットに報告しないように ISE/ISE-PIC を設定します。

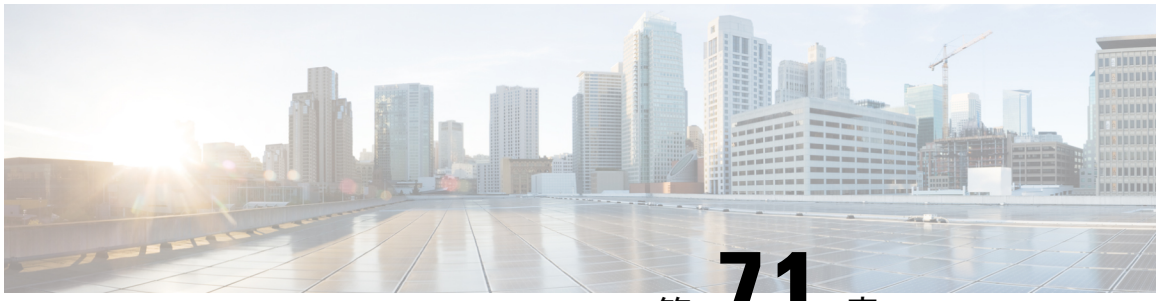
  『*Cisco Identity Services Engine Administrator Guide*』のネットワークデバイスの管理に関する章を参照してください。

- セキュリティグループタグ（SGT）の登録を解除します。
- 管理対象デバイスをメモリが大きなモデルにアップグレードします。

第 XII 部

ネットワーク検出

- ネットワーク検出の概要 （2575 ページ）
- ホスト アイデンティティ ソース （2585 ページ）
- アプリケーションの検出 （2631 ページ）
- ネットワーク検出ポリシー （2657 ページ）



第 71 章

ネットワーク検出の概要

次のトピックでは、ネットワーク検出について説明します。

- ホスト、アプリケーション、およびユーザーのデータの検出について （2575 ページ）
- ホストおよびアプリケーション検出の基礎 （2576 ページ）

ホスト、アプリケーション、およびユーザーのデータの検出について

システムは、ネットワーク検出およびアイデンティティポリシーを使用して、ネットワークトラフィックのホスト、アプリケーション、およびユーザーのデータを収集します。特定のタイプの検出およびアイデンティティデータを使用すると、ネットワークアセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

ホストおよびアプリケーション データ

ホストやアプリケーションデータは、ネットワーク検出ポリシーの設定に従ってホストのアイデンティティ ソースとアプリケーション ディテクタによって収集されます。管理対象デバイスは、指定したネットワーク セグメントのトラフィックを確認します。

詳細については、ホストおよびアプリケーション検出の基礎 （2576 ページ）を参照してください。

ユーザ データ（User Data）

ユーザ データはネットワーク検出およびアイデンティティ ポリシーの設定に従ってユーザのアイデンティティ ソースによって収集されます。データはユーザ認識とユーザ制御のために使用できます。

詳細については、ユーザー アイデンティティについて （2431 ページ）を参照してください。

検出データとアイデンティティデータをロギングすることにより、次のようなシステムのさまざまな機能を活用できます。

- ネットワーク アセットとトポロジの詳細を示すネットワーク マップを表示します。その際、ホストとネットワーク デバイス、ホスト属性、アプリケーション プロトコル、または脆弱性をグループ化して表示できます。
- アプリケーション、レルム、ユーザ、ユーザ グループ、およびISE属性の各条件を使ってアクセス コントロール ルールを作成することにより、アプリケーション制御およびユーザ制御を実行します。
- 検出されたホストで利用可能なすべての情報の完全なビューであるホストプロファイルを表示します。
- （さまざまな機能の 1 つとして）ネットワーク アセットとユーザ アクティビティの概要を示すダッシュボードを表示します。
- システムによって記録された検出イベントとユーザアクティビティに関する詳細情報を表示します。
- ホストおよびそこで実行されているサーバ/クライアントと、被害を及ぼす可能性のあるエクスプロイトとを関連付けます。

  これにより、脆弱性を特定して軽減したり、ネットワークに対する侵入イベントの影響を評価したり、ネットワークアセットを最大限に保護できるように侵入ルール状態を調整したりできます。
- システムで特定の影響フラグ付きの侵入イベントまたは特定のタイプの検出イベントが生成された場合に、電子メール、SNMP トラップ、またはsyslogによるアラートを発行します。
- 許可されたオペレーティングシステム、クライアント、アプリケーションプロトコル、およびプロトコルのallowリストを使用して組織のコンプライアンスをモニターします。
- システムが検出イベントを生成するかユーザーアクティビティを検出したときにトリガーして相関イベントを生成するルールを使って、相関ポリシーを作成します。
- 該当する場合、NetFlow 接続をロギングして使用します。

ホストおよびアプリケーション検出の基礎

ネットワーク検出ポリシーを設定すると、ホストおよびアプリケーション検出を実行できます。

詳細については、「概要：ホストのデータ収集 （2585ページ）」および「概要：アプリケーション検出 （2631 ページ）」を参照してください。

オペレーティング システムおよびホスト データのパッシブ検出

パッシブ検出は、システムがネットワーク トラフィック（およびエクスポートされたNetFlowデータ）を分析してネットワーク マップにデータを取り込む際のデフォルト方式です。パッシ

ブ検出では、ネットワーク アセットに関するコンテキスト情報（オペレーティング システムや実行中のアプリケーションなど）が提供されます。

モニタ対象のホストからのトラフィックが、ホストで実行されているオペレーティング システムを示す決定的証拠とならない場合、使用されている可能性が最も高いオペレーティングがネットワーク マップに表示されます。たとえば、複数のホストが NAT デバイスの「背後」にあることから、NAT デバイスが複数のオペレーティング システムを実行しているように表示される場合があります。この最も可能性の高いオペレーティングを決定するためにシステムが使用するのは、検出された各オペレーティング システムに割り当てられた信頼度の値と、検出されたオペレーティング システムの中でその特定のオペレーティング システムが使用されていることを裏付けるデータの量です。

（注） この決定を行う際、システムは「unknown」として報告されたアプリケーションとオペレーティング システムを考慮しません。

パッシブ検出でネットワーク アセットが正確に識別されない場合は、管理対象デバイスの配置について検討してください。また、システムのパッシブ検出機能をオペレーティング システムのカスタム フィンガープリントとカスタム アプリケーション ディテクタで増補することもできます。あるいは、アクティブ検出を使用するという方法もあります。アクティブ検出では、トラフィック分析をベースとするのではなく、スキャン結果やその他の情報ソースを使用して直接ネットワーク マップを更新できます。

オペレーティング システムおよびホスト データのアクティブ検出

アクティブ検出では、アクティブ ソースによって収集されたホスト情報をネットワーク マップに追加します。たとえば、Nmap スキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmap は、ホストでオペレーティング システムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワーク マップにホスト入力データをアクティブに追加することができます。ホスト入力データには 2 種類のカテゴリがあります。

- ユーザ入力データ：FirePOWER システム ユーザ インターフェイスで追加されたデータ。このユーザ インターフェイスを使用して、ホストのオペレーティング システムやアプリケーションの ID を変更できます。
- ホスト インポート入力データ：コマンド ライン ユーティリティを使用してインポートされたデータ。

システムは、それぞれのアクティブ ソースに対して 1 個の ID を保持します。たとえば、Nmap スキャン インスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmap スキャンを実行し、それらの結果をクライアントからのデータ（コマンド ラインを使用してインポートした結果）と交換する場合、システムは Nmap の結果の ID とインポート クライアントの ID の両方を保持します。システムは、ネットワーク検出ポリ

シーで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザーが入力したとしても、ユーザー入力は1 ソースと見なされることに注意してください。たとえば、UserA がホスト プロファイルを使用してオペレーティング システムを設定し、UserB がホスト プロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザー入力によって、他のアクティブ ソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

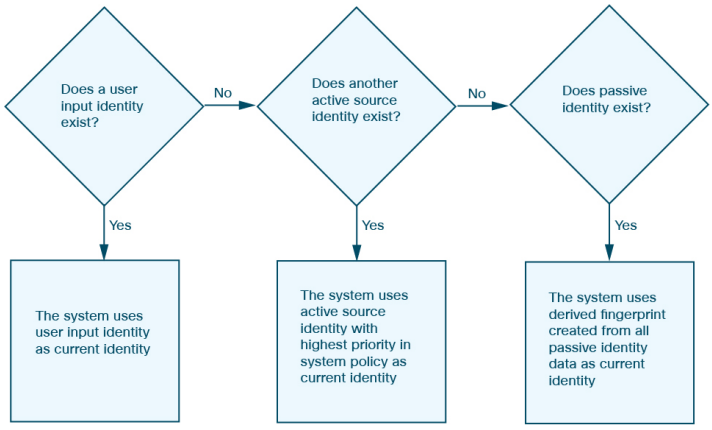
アプリケーションおよびオペレーティング システムの現在の ID

ホストのアプリケーションまたはオペレーティング システムの現在の *ID* は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティング システムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価
- オペレーティングシステムの識別、ホストプロファイルの認定、およびコンプライアンスのallowリストに対して記述された相関ルールの評価
- ワークフローのホストおよびサーバーのテーブル ビューでの表示
- ホスト プロファイルでの表示
- [検出統計情報（Discovery Statistics）]ページでのオペレーティング システムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティング システムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザーがホストでオペレーティング システムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱

性を狙った攻撃により大きな影響力があると見なされ、ホストプロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含められます。

データベースは、ホストのオペレーティング システムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティング システムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

1. ユーザー

2. スキャナとアプリケーション（ネットワーク検出ポリシーで設定）

3. 管理対象デバイス

4. ：NetFlow レコード

新しい優先順位の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合、現在の ID を上書きしません。

また、ID の競合が発生した場合、競合の解決はネットワーク検出ポリシーの設定または手動解決によります。

現在のユーザー ID

システムは、同じホストに対して異なるユーザーによる複数のログインを検出すると、特定のホストにログインするユーザーは一度に 1 人だけであり、ホストの現在のユーザーが最後の権限のあるユーザー ログインであると見なします。権限のないユーザ ログインだけがホストにログインしている場合は、最後にログインしたものが現在のユーザと見なされます。複数のユーザがリモートセッション経由でログインしている場合は、サーバによって報告された最後のユーザが Firewall Management Centerに報告されるユーザです。

システムは、同じホストに対して異なるユーザーによる複数のログインを検出すると、ユーザーが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

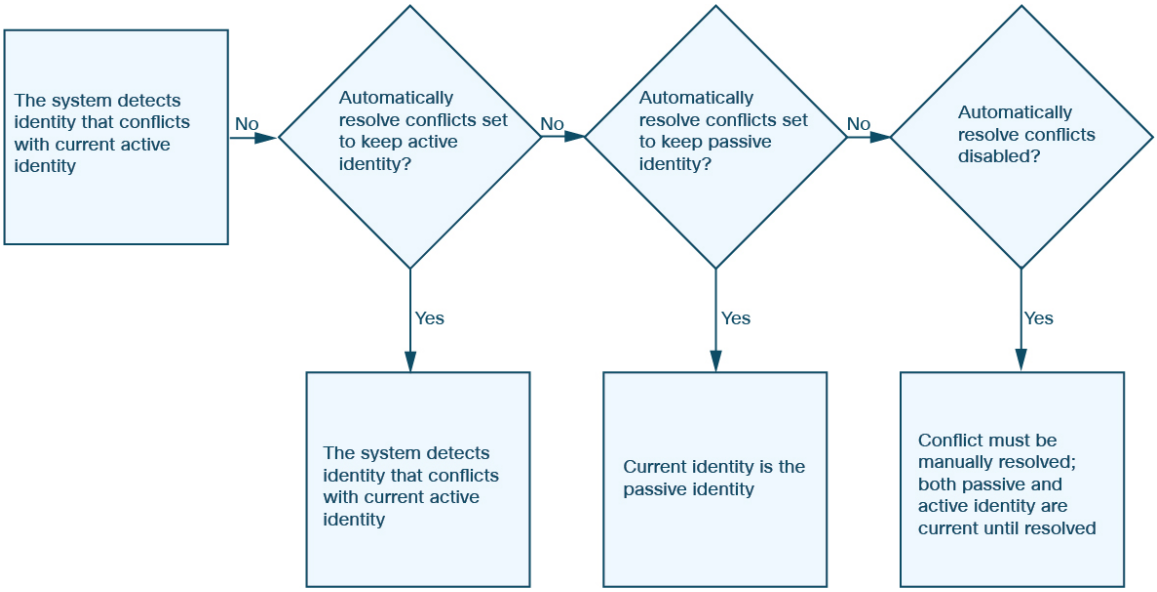
ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザーが再度ログインすると、その人物の新しいログインが記録されます。

アプリケーションおよびオペレーティング システムの ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、*ID* の競合が発生します。たとえば、オペレーティング システムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

ホストのオペレーティング システムまたはホスト上のいずれかのアプリケーションの ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザーは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、相関応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティング システムとアプリケーション データを取得します。

NetFlow データ

NetFlowは、ルータを通過するパケットの統計情報を提供する、Cisco IOS アプリケーションの 1 つです。NetFlow は Cisco ネットワーキング デバイスで使用できます。また、Juniper、FreeBSD、OpenBSD デバイスに組み込むことも可能です。

NetFlow がネットワーク デバイスで有効にされている場合、そのデバイス上のデータベース（NetFlow キャッシュ）に、ルータを通過するフローのレコードが格納されます。システムで接続と呼ばれるフローは、特定のポート、プロトコル、およびアプリケーションプロトコルを使用する送信元ホストと宛先ホスト間のセッションを表すパケットのシーケンスです。この NetFlowデータをエクスポートするようにネットワーク デバイスを設定できます。本書では、そのように設定されたネットワーク デバイスを NetFlow エクスポータと呼びます。

管理対象デバイスは、NetFlow エクスポータからレコードを収集して、それらのレコードに含まれるデータに基づいて単方向の接続終了イベントを生成し、それらのイベントを接続イベントデータベースに記録するためにFirewall Management Centerに送信するように設定できます。

また、NetFlow接続内の情報に基づいて、ホストとアプリケーションプロトコルに関する情報をデータベースに追加するためのネットワーク検出ポリシーを設定することもできます。

この検出データと接続データを使用して、管理対象デバイスによって直接収集されたデータを補完できます。これは、管理対象デバイスでモニターできないネットワークをNetFlowエクスポータにモニターさせる場合には特に有効です。

NetFlow データを使用するための要件

NetFlow データを分析するために Firepower System を設定する前に、ルータまたは使用する他の NetFlow が有効なネットワーク デバイス上で NetFlow 機能を有効にし、管理対象デバイスのセンシング インターフェイスを接続する宛先ネットワークへNetFlowデータをブロードキャストするようにデバイスを設定する必要があります。

Firepower System では、NetFlow バージョン 5 レコードと NetFlow バージョン 9 レコードをいずれも解析できます。Firepower Systemにデータをエクスポートするには、NetFlowエクスポータがいずれかのバージョンを使用する**必要があります**。さらに、このシステムでは、特定のフィールドがエクスポートされた NetFlow テンプレートとレコードに存在する必要があります。NetFlow エクスポータがカスタマイズ可能なバージョン 9 を使用している場合は、エクスポートされたテンプレートとレコードに次のフィールドが任意の順序で含まれていることを確認する必要があります。

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Firepower System は管理対象デバイスを使用して NetFlow データを分析するため、NetFlow エクスポータの監視可能な1つ以上の管理対象デバイスを展開に含める必要があります。この管理対象デバイス上の 1 つ以上のセンシング インターフェイスを、エクスポートされた NetFlow データを収集可能なネットワークに接続する必要があります。通常、管理対象デバイス上のセンシング インターフェイスには IP アドレスが割り当てられないため、システムは NetFlow レコードの直接収集をサポートしません。

一部のネットワーク デバイス上で使用可能な Sampled NetFlow 機能は、デバイスを通過するパケットのサブセットだけに基づく NetFlow 統計情報を収集することに注意してください。この機能を有効にすると、ネットワーク デバイス上の CPU 使用率が改善される可能性がありますが、Firepower System で分析するために収集されている NetFlow データに影響する場合があります。

NetFlow データと管理対象デバイス データの違い

NetFlow データで表示されるトラフィックは、直接的には分析されません。代わりに、エクスポートした NetFlow レコードを接続ログおよびホストとアプリケーションのプロトコルデータに変換します。

その結果、変換された NetFlow データと、管理対象デバイスによって直接収集された検出および接続データにはいくつかの違いがあります。以下のことを必要とする分析を実行する場合に、これらの違いを意識しなければなりません。

- 検出された接続数に基づく統計情報
- オペレーティング システムとその他のホスト関連情報（脆弱性を含む）
- クライアント情報、Web アプリケーション情報、ベンダーおよびバージョン サーバ情報を含むアプリケーション データ
- 接続内の発信側のホストと応答側のホストの認識

ネットワーク検出ポリシーとアクセス コントロール ポリシーの違い

接続ロギングを含む NetFlow データ収集は、ネットワーク検出ポリシー内のルールを使用して設定します。これを、アクセス コントロール ルールごとに設定した管理対象デバイスによって検出された接続の接続ロギングと比較してください。

接続イベントのタイプ

NetFlow データ収集はアクセス コントロール ルールではなくネットワークにリンクされているため、システムがログに記録する NetFlow 接続をきめ細かく制御することはできません。

NetFlow データは、セキュリティ インテリジェンス イベントを生成することはできません。

NetFlow ベースの接続イベントは、接続イベント データベースにのみ保存できます。システム ログまたは SNMP トラップ サーバに送信することはできません。

モニタ対象セッションごとに生成される接続イベントの数

管理対象デバイスによって直接検出された接続の場合は、アクセス コントロール ルールを設定して、接続の最初か最後またはその両方で双方向接続イベントをログに記録できます。

それに対し、エクスポートされた NetFlow レコードには単方向接続データが含まれているため、システムは処理する各 NetFlow レコードに対し少なくとも 2 つの接続イベントを生成します。これは、概要の接続数が NetFlow データに基づいた接続ごとに 2 ずつ増加することも意味しており、ネットワーク上で実際に発生している接続数が急増することになります。

接続がまだ実行中であっても、NetFlow エクスポータは固定間隔でレコードを出力するため、長時間実行しているセッションの場合は複数のエクスポートされたレコードが生成される場合があり、その各レコードが接続イベントを生成します。たとえば、NetFlow エクスポータが 5 分ごとにエクスポートする場合に、特定の接続が 12 分間続いている場合、システムはそのセッションに対し 6 つの接続イベントを生成します。

- 最初の 5 分間の 1 つのイベント ペア
- 次の 5 分間の 1 つのペア
- 接続が終了した時点の最後のペア

ホスト データとオペレーティング システム データ

NetFlow データからのネットワークマップに追加されたホストには、オペレーティングシステム、NetBIOS、またはホストタイプ（ホストまたはネットワーク デバイス）の情報がありません。ただし、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定できます。

アプリケーション データ

管理対象デバイスによって直接検出された接続の場合は、接続内のパケットを検査することによって、システムはアプリケーションプロトコル、クライアント、および Web アプリケーションを識別できます。

システムは NetFlow レコードを処理するときに、`/etc/sf/services` 内のポート関連付けを使用して、アプリケーション プロトコル ID を推測します。ただし、これらのアプリケーション プロトコルに関するベンダーまたはバージョン情報が存在しないため、接続ログにはセッションで使用されるクライアントまたは Web アプリケーションに関する情報が含まれません。しかし、ホスト入力機能を使用してこの情報を手動で提供できます。

単純なポート関連付けでは、非標準ポート上で動作しているアプリケーションプロトコルが特定されないまたは誤認される可能性があることに注意してください。加えて、関連付けが存在しない場合は、システムがそのアプリケーションプロトコルを接続ログで `unknown` としてマークします。

脆弱性マッピング

システムは、ホスト入力機能を使用してホストのオペレーティング システム ID またはアプリケーション プロトコル ID を手動で設定しない限り、NetFlow エクスポータによってモニタされるホストに脆弱性をマッピングできません。NetFlow 接続内にクライアント情報が存在しないため、クライアントの脆弱性を NetFlow データから作成されたホストに関連付けることはできないことに注意してください。

接続内の発信側情報と応答側情報

管理対象デバイスによって直接検出された接続の場合、システムは発信側または送信元のホストと応答側または宛先のホストを識別できます。ただし、NetFlow データには発信側または応答側の情報が含まれていません。

システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートがウェルノウンであるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。

- 使用されているポートの両方が既知のポートの場合、または、どちらも既知のポートでない場合、システムは番号の若い方のポートを使用しているホストを応答側と見なします。
- どちらかのホストだけが既知のポートを使用している場合は、システムがそのホストを応答側と見なします。

したがって、既知のポートは、1 ～ 1023 の番号が割り当てられたポートまたは管理対象デバイス上の `/etc/sf/services` にアプリケーション プロトコル情報が保存されているポートです。

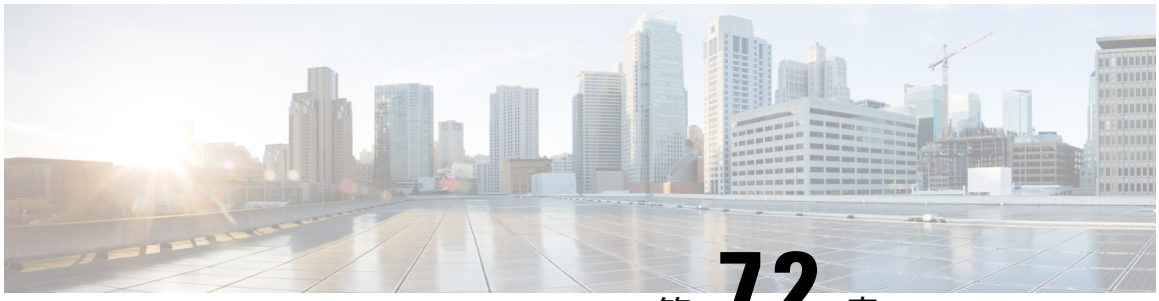
さらに、管理対象デバイスによって直接検出された接続の場合、システムは対応する接続イベントの 2 バイト数を記録します。

- [イニシエータ バイト数（Initiator Bytes）] フィールドは送信バイト数を記録します。
- [レスポンダ バイト数（Responder Bytes）] フィールドは受信バイト数を記録します。

単方向 NetFlow レコードに基づく接続イベントには、1 バイト数しか含まれておらず、ポートベース アルゴリズムに応じて、システムが [イニシエータ バイト数（Initiator Bytes）] または [レスポンダ バイト数（Responder Bytes）] に割り当てます。システムによって他のフィールドは 0 に設定されます。NetFlow レコードの接続の概要（集約接続データ）を表示している場合に、両方のフィールドに値が読み込まれる場合があることに注意してください。

NetFlow のみの接続イベント フィールド

いくつかのフィールドは、NetFlow レコードから生成された接続イベントでのみ表示されます（『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「*Information Available in Connection Event Fields*」を参照してください。



第 72 章

ホスト アイデンティティ ソース

次のトピックでは、ホスト ID ソースについて説明します。

- 概要：ホストのデータ収集 （2585 ページ）
- ホスト アイデンティティ ソースの要件と前提条件 （2586 ページ）
- システムが検出できるホスト オペレーティング システムの判別 （2586 ページ）
- ホスト オペレーティング システムの識別 （2587 ページ）
- カスタムフィンガープリント （2587 ページ）
- ホスト入力データ （2598 ページ）
- Nmap スキャン （2607 ページ）
- ホスト アイデンティティ ソースの履歴 （2630 ページ）

概要：ホストのデータ収集

Firepower システムはネットワークを通過するトラフィックを受動的に監視するため、ネットワーク トラフィックからの特定のパケット ヘッダー値とその他の固有データを設定された定義と比較して（フィンガープリントと呼ばれる）、ネットワーク上のホストに関する次の情報を判断します。

- ホストの台数と種類（ブリッジ、ルータ、ロード バランサ、NAT デバイスなどのネットワーク デバイスを含む）
- ネットワーク上の検出ポイントからホストまでのホップ数を含む、基本的なネットワーク トポロジ データ
- ホスト上で実行中のオペレーティング システム
- ホスト上のアプリケーションとそのアプリケーションに関連付けられているユーザ

システムがホストのオペレーティング システムを特定できない場合、カスタムのクライアントまたはサーバのフィンガープリントを作成できます。システムはこれらのフィンガープリントを使用して新しいホストを特定します。フィンガープリントを脆弱性データベース（VDB）内のシステムにマップすることにより、カスタム フィンガープリントを使用してホストが特定されるたびに適切な脆弱性情報を表示できます。

（注） システムはモニター対象のネットワーク トラフィックからだけでなく、エクスポートされた NetFlow レコードからもホスト データを収集することができ、また Nmap スキャンやホスト入力機能を使用してアクティブにホスト データを追加することもできます。

ホスト アイデンティティ ソースの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意（リーフ のみであるカスタムフィンガープリントを除く）。

ユーザの役割

- 管理者
- 検出管理者（Discovery Admin）（サードパーティデータとカスタムマッピングを除く）。

システムが検出できるホストオペレーティング システムの判別

システムがどのオペレーティング システムのフィンガープリントを作成できるかを確認するには、カスタム OS フィンガープリントの作成プロセス中に表示される、使用可能なフィンガープリントの一覧を表示します。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションにあるドロップダウン リスト内のオプションのリストを表示します。これらのオプションが、システムがフィンガープリントを作成できるオペレーティング システムになります。

次のタスク

必要に応じて、ホスト オペレーティング システムの識別（2587ページ）を参照してください。

ホスト オペレーティング システムの識別

システムがホストのオペレーティング システムを正しく識別しない場合（たとえばホスト プロファイル「不明」を示したり間違って識別したりする場合）には、下記の方法を試してください。

手順

次のいずれかの方法を試します。

- ネットワーク検出アイデンティティ競合設定を確認します。
- ホストのカスタム フィンガープリントを作成します。
- ホストに対して Nmap スキャンを実行します。
- ホスト入力機能を使用して、ネットワーク マップにデータをインポートします。
- オペレーティング システム情報を手動で入力します。

カスタムフィンガープリント

システムには、検出された各ホストのオペレーティングシステムを識別するためにシステムが使用するオペレーティングシステムのフィンガープリントが含まれます。しかし、オペレーティングシステムに一致するフィンガープリントがないため、システムがホストオペレーティングシステムを識別できない、または誤って識別することがあります。この問題を解決するために、不明または誤認されたオペレーティング システムに固有のオペレーティング システム特性のパターンを提供するカスタムフィンガープリントを作成し、識別用のオペレーティングシステムの名前を提供することができます。

システムはオペレーティングシステムのフィンガープリントから各ホストの脆弱性リストを取得するため、システムがホストのオペレーティングシステムを照合できない場合には、ホストの脆弱性を識別できません。たとえば、システムが Microsoft Windows を実行中のホストを検出した場合、そのシステムには保存された Microsoft Windows の脆弱性リストが存在します。このリストは、検出した Windows オペレーティング システムに基づいて、そのホストのホスト プロファイルに追加されます。

たとえば、ネットワーク上に Microsoft Windows の新しいベータ バージョンを実行中の複数のデバイスがある場合、システムはそのオペレーティングシステムを識別できず、脆弱性をそれ

らのホストにマッピングすることもできません。しかし、システムに Microsoft Windows に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行中の他のホストを識別できるように、いずれか 1 台のホストに対してカスタム フィンガープリントを作成できます。フィンガープリントに Microsoft Windows の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

カスタム フィンガープリントを作成すると Firewall Management Center は、同じオペレーティング システムを実行中のすべてのホストに関するそのフィンガープリントに関連付けられた脆弱性のセットをリストします。ユーザが作成したカスタム フィンガープリントに脆弱性マッピングが 1 つも存在しない場合、システムはフィンガープリントを使用して、フィンガープリントで提供するカスタム オペレーティング システムの情報を割り当てます。以前に検出されたホストからの新しいトラフィックが確認されると、システムはそのホストを新しいフィンガープリント情報で更新します。さらに、そのオペレーティング システムを実行する新しいホストの最初の検出時に、新しいフィンガープリントを使用して識別します。

カスタム フィンガープリントを作成する前に、ホストが正しく識別されない理由を特定して、カスタム フィンガープリントが実行可能なソリューションであるかどうかを判断する必要があります。

以下の 2 種類のフィンガープリントを作成できます。

- クライアントのフィンガープリント。ネットワーク上の別のホストで実行中の TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。
- サーバのフィンガープリント。実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。

（注） クライアントとサーバの両方のフィンガープリントが同じホストに一致する場合、クライアントのフィンガープリントが使用されます。

フィンガープリントを作成した後、システムがフィンガープリントをホストに関連付けるには、その前に、フィンガープリントを有効化する必要があります。

関連トピック

クライアント用のカスタム フィンガープリントの作成 （2591 ページ）
サーバー用のカスタム フィンガープリントの作成 （2594 ページ）

フィンガープリントの管理

フィンガープリントを作成してアクティブにした後、フィンガープリントを編集して変更を加えたり、脆弱性マッピングを追加したりできます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。システムがフィンガープリントを作成するデータを待機している場合、フィンガープリントが作成されるまで 10 秒ごとに自動的に更新されます。

ステップ 3 カスタムのフィンガープリントを管理します。

- アクティブ化/非アクティブ化：フィンガープリントをアクティブ化または非アクティブ化します。詳細については、フィンガープリントのアクティブおよび非アクティブの設定（2589 ページ）を参照してください。
- 作成：フィンガープリントを作成します。詳細については、クライアント用のカスタムフィンガープリントの作成（2591 ページ）およびサーバー用のカスタムフィンガープリントの作成 （2594 ページ）を参照してください。
- 編集：フィンガープリントを編集します。詳細については、アクティブなフィンガープリントの編集（2590ページ）および非アクティブなフィンガープリントの編集（2590ページ）を参照してください。
- 削除：削除するフィンガープリントの横にある[削除（Delete）]（ ）をクリックして、確認のために [OK] をクリックします。削除できるのは、非アクティブ化したフィンガープリントのみです。

フィンガープリントのアクティブおよび非アクティブの設定

ホストを識別するためにシステムがカスタム フィンガープリントを使用できるようにするには、その前に、カスタムフィンガープリントをアクティブにする必要があります。新しいフィンガープリントがアクティブにされた後は、以前に検出したホストを再識別し、新しいホストを検出するために使用されます。

フィンガープリントの使用を停止する場合は、それを非アクティブにすることができます。フィンガープリントを非アクティブにすると、フィンガープリントは使用できなくなりますが、システム上で維持できます。フィンガープリントを非アクティブにすると、オペレーティングシステムは、フィンガープリントを使用しているホストに対して不明としてマークされます。ホストが再度検出され、別のアクティブなフィンガープリントに一致すると、ホストはそのアクティブなフィンガープリントによって識別されます。

フィンガープリントを削除すると、システムから完全に削除されます。フィンガープリントを非アクティブにした後に削除できます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするフィンガープリントの横にあるスライダをクリックします。

（注）
アクティブ化オプションは、作成したフィンガープリントが有効である場合に限り使用できます。スライダが使用できない場合、フィンガープリントを再作成してください。

アクティブなフィンガープリントの編集

フィンガープリントがアクティブである場合、フィンガープリントの名前、説明、オペレーティングシステムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

フィンガープリントの名前、説明、オペレーティングシステムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある[編集（Edit）]（✎）をクリックします。

ステップ 4 必要に応じて、フィンガープリントの名前、説明、およびカスタム OS 表示を変更します。

ステップ 5 脆弱性マッピングを削除する場合は、ページの [事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] セクションのマッピングの横にある [削除（Delete）] をクリックします。

ステップ 6 脆弱性マッピングにその他のオペレーティングシステムを追加する場合は、[製品（Product）] を選択し（該当する場合は [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および[拡張（Extension）] も選択します）、[OS 定義の追加（Add OS Definition）] をクリックします。

脆弱性マッピングが、[事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] リストに追加されます。

ステップ 7 [保存（Save）] をクリックします。

非アクティブなフィンガープリントの編集

フィンガープリントが非アクティブである場合は、フィンガープリントのすべての要素を変更し、それらを Secure Firewall Management Center に再送信できます。これには、フィンガープリントのタイプ、ターゲットの IP アドレスとポート、脆弱性マッピングなど、フィンガープリントの作成時に指定したすべてのプロパティが含まれます。非アクティブのフィンガープリン

トを編集および送信すると、システムに再送信されます。また、それがクライアントのフィンガープリントである場合、アクティブにする前に、アプライアンスにトラフィックを再送信する必要があります。非アクティブのフィンガープリントに対して選択できる脆弱性マッピングは1つだけであることに注意してください。フィンガープリントをアクティブにした後、追加のオペレーティング システムおよびバージョンを脆弱性リストにマッピングすることができます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある[編集（Edit）]（✎）をクリックします。

ステップ 4 必要に応じてフィンガープリントを変更します。

- クライアントのフィンガープリントを変更している場合は、クライアント用のカスタム フィンガープリントの作成 （2591 ページ）を参照してください。
- サーバーのフィンガープリントを変更している場合は、サーバー用のカスタム フィンガープリントの作成 （2594 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- クライアントのフィンガープリントを変更した場合は、ホストからフィンガープリントを収集しているアプライアンスにトラフィックを必ず送信してください。

クライアント用のカスタム フィンガープリントの作成

クライアントのフィンガープリントは、クライアントがネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

Firewall Management Centerが監視対象ホストと直接通信することがない場合は、クライアントのフィンガープリントのプロパティを指定するときに、Firewall Management Centerによって管理され、フィンガープリントを作成するホストに最も近いデバイスを指定することができます。

フィンガープリント作成プロセスを開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用する Firewall Management Center またはデバイスの間のネットワーク ホップの数。（Cisco では、ホストが接続されている同じサブネットに Firewall Management Center またはデバイスを直接接続することを強く推奨します）。

- ホストが存在するネットワークに接続されているネットワーク インターフェイス（Firewall Management Center またはデバイス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- クライアント トラフィックを生成するためのホストへのアクセス。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [デバイス（Device）] ドロップダウンリストから、フィンガープリントを収集するために使用する Firewall Management Center またはデバイスを選択します。

ステップ 5 [フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6 [フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7 [フィンガープリント タイプ（Fingerprint Type）] リストから、[クライアント（Client）] を選択します。

ステップ 8 [ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザーが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

ステップ 9 [ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意
これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10 [インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意
Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシングインターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合（またはフィンガープリントを作成するホストが [OS 脆弱性マッピング（OS Vulnerability Mappings）]セクションに存在しない場合）、[カスタムOS表示の使用（Use Custom OS Display）]を選択して、次に示すように表示する値を指定します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 12 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションで[ベンダー（Vendor）]と [製品（Product）] の値名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、[ベンダー（Vendor）] および [製品（Product）] の値のみを指定します。

（注）
[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

たとえば、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、メジャー バージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 13 [作成（Create）] をクリックします。

ステータスは一時的に [新規（New）] になってから、[保留中（Pending）] に切り替わります。フィンガープリントのトラフィックが確認されるまで、このステータスが維持されます。トラフィックが確認されると、[使用可（Ready）] に切り替わります。

当該のホストからデータを受信するまで、[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新されます。

ステップ 14 ターゲット IP アドレスとして指定した IP アドレスを使用して、フィンガープリントを作成しようとしているホストにアクセスし、アプライアンスへの TCP 接続を開始します。

正確なフィンガープリントを作成するためには、トラフィックがフィンガープリントを収集するアプライアンスで認識される**必要**があります。スイッチを経由して接続している場合は、アプライアンス以外のシステムへのトラフィックはシステムによって認識されない場合があります。

例：

フィンガープリントを作成しようとしているホストから Firewall Management Center の Web インターフェイスにアクセスするか、ホストから SSH で Firewall Management Center にアクセスします。SSH を使用する場合は、次に示すコマンドを使用します。このコマンドの localIPv6address は、現在ホストに割り当てられているステップ 7 で指定した IPv6 アドレスです。DCmanagementIPv6address は、Firewall Management Center の管理 IPv6 アドレスです。[カスタム フィンガープリント（Custom Fingerprint）] ページが [使用可（Ready）] ステータスでリロードされるようになります。

```
ssh -b localIPv6address DCmanagementIPv6address
```

次のタスク

- フィンガープリントのアクティブおよび非アクティブの設定（2589ページ） で説明するように、フィンガープリントをアクティブにします。

サーバー用のカスタム フィンガープリントの作成

サーバーのフィンガープリントは、実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するアプライアンスの間のネットワーク ホップの数。Cisco では、ホストが接続されている同じサブネットにアプライアンスの使用されていないインターフェイスを直接接続することを強く推奨します。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（アプライアンス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- 現在使用されておらず、ホストが存在するネットワーク上で許可されている IP アドレス。

ヒント　Firewall Management Center が監視対象ホストと直接通信することがない場合は、サーバーのフィンガープリントのプロパティを指定するときに、フィンガープリントを作成するホストに最も近い管理対象デバイスを指定することができます。

手順

ステップ 1　**[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2　[カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3　[カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4　[デバイス（Device）] リストから、フィンガープリントを収集するために使用する Firewall Management Center または管理対象デバイスを選択します。

ステップ 5　[フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6　[フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7　[フィンガープリント タイプ（Fingerprint Type）] リストから、サーバーのフィンガープリント作成オプションを表示する [サーバー（Server）] を選択します。

ステップ 8　[ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザーが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

注意
バージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。

ステップ 9　[ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意
これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10　[インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意
Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシングインターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのイン

ターフェイスがデバイスのセンシングインターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 [アクティブなポートを取得（Get Active Ports）] をクリックします。

ステップ 12 [サーバー ポート（Server Port）] フィールドに、フィンガープリントを収集するように選択したデバイスが通信を開始するポートを入力します。または、[アクティブ ポートの取得（Get Active Ports）] ドロップダウンリストからポートを選択します。

ホストでオープンしていると判明しているすべてのサーバー ポートを使用できます（たとえば、ホストで Web サーバーを実行している場合は 80）。

ステップ 13 [送信元 IP アドレス（Source IP Address）] フィールドで、ホストとの通信を試行するために使用する IP アドレスを入力します。

ネットワークでの使用が許可されていて、現在未使用の送信元 IP アドレス（たとえば、現在使用されていない DHCP プール アドレス）を使用する必要があります。これにより、フィンガープリントの作成中に、別のホストを一時的にオフラインにすることを防ぎます。

フィンガープリントを作成している間は、その IP アドレスをネットワーク検出ポリシーでモニタリングから除外する必要があります。そうしていないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。

ステップ 14 [送信元サブネット マスク（Source Subnet Mask）] フィールドには、ユーザーが使用している IP アドレスのサブネット マスクを入力します。

ステップ 15 [送信元ゲートウェイ（Source Gateway）] フィールドが表示されたら、ホストへのルートを確立するために使用するデフォルトのゲートウェイ IP アドレスを入力します。

ステップ 16 フィンガープリントを作成したホストのホストプロファイルのカスタム情報を表示する場合、または使用するフィンガープリントの名前が [OS 定義（OS Definition）] セクションに存在しない場合、[カスタム OS 表示（Custom OS Display）] セクションの [カスタム OS 表示の使用（Use Custom OS Display）] を選択します。

以下のように、ホスト プロファイルで表示する値を入力します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 17 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。

（注）
[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 18 [作成（Create）] をクリックします。
[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新され、[使用可（Ready）] ステータスでリロードされます。

（注）
ターゲット システムがフィンガープリント作成プロセス中に応答を停止した場合、ステータスにはメッセージ「エラー：応答がありません（ERROR: No Response）」が示されます。このメッセージが表示された場合は、フィンガープリントを再度送信します。3 ～ 5 分間（時間はターゲットシステムによって異なる場合があります）待機して、[編集（Edit）]（✎）をクリックし、[カスタムフィンガープリント（Custom Fingerprint）] ページにアクセスしてから [作成（Create）] をクリックします。

次のタスク

- フィンガープリントのアクティブおよび非アクティブの設定（2589ページ） で説明するように、フィンガープリントをアクティブにします。

ホスト入力データ

サードパーティからネットワーク マップ データをインポートすることで、ネットワーク マップを増強することができます。また、Web インターフェイスを使用して、オペレーティング システムまたはアプリケーションの ID を変更するか、アプリケーション プロトコル、プロトコル、ホスト属性、クライアントを削除することによって、ホスト入力機能を使用することができます。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。

ネットワーク マップから影響を受けるホストを削除すると、サードパーティの脆弱性を除くすべてのデータは破棄されます。スクリプトまたはインポート ファイルの設定方法の詳細については、『*Firepower* システムホスト入力 *API* ガイド』を参照してください。

影響の関連付けにインポートしたデータを含めるには、データベースのオペレーティング システムおよびアプリケーション定義にデータをマッピングする必要があります。

サードパーティのデータを使用するための要件

ネットワーク上のサードパーティのシステムから検出データをインポートできます。ただし、シスコの推奨、adaptive profile updates、影響評価などの侵入データおよび検出データを共に使用する機能を有効にするには、対応する定義に対して、可能な限り多くのエレメントをマッピングする必要があります。サードパーティのデータを使用するには、以下の要件を考慮してください：

- サードパーティのシステムにネットワーク アセット上に特定のデータがある場合、ホスト入力機能によりそのデータをインポートできます。しかし、サードパーティが異なる製品名をつける可能性があることから、対応する Cisco 製品の定義に対して、サードパーティ ベンダー、製品、バージョンをマッピングする必要があります。製品をマッピング後、Firewall Management Center 設定の影響を評価するために脆弱性のマッピングを有効にして、影響相関を可能にします。バージョンまたはベンダーに関係のないアプリケーション プロトコルでは、Firewall Management Center 設定におけるアプリケーション プロトコルの脆弱性をマッピングする必要があります。
- サードパーティからパッチ情報をインポートし、そのパッチで修正されたすべての脆弱性に無効とマークする場合は、サードパーティの修正名をデータベースの修正定義にマッピングする必要があります。修正によって解決された脆弱性はすべて、その修正を加えるホストから排除されます。
- オペレーティング システムやアプリケーション プロトコルの脆弱性をサードパーティからインポートし、これらを影響相関に使用する場合、サードパーティの脆弱性識別文字列をデータベース内の脆弱性にマッピングする必要があります。多くのクライアントは、脆弱性と関連があり、影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートし、マッピングすることはできない点にご注意ください。脆弱性のマッピング後、Firewall Management Center 設定の影響評価のためにサードパーティの脆弱性のマッ

ピングを有効にします。ベンダー情報やバージョン情報のないアプリケーションプロトコルを脆弱性にマッピングするには、管理ユーザは、Firewall Management Center 設定のアプリケーションの脆弱性もマッピングする必要があります。

- アプリケーションデータをインポートし、そのデータを影響相関に使用する場合、各アプリケーションプロトコルのベンダー文字列を対応する Cisco アプリケーションプロトコルの定義にマッピングする必要があります。

関連トピック

サードパーティの製品のマッピング （2599 ページ）
サード パーティ製品の修正のマッピング （2601 ページ）
サードパーティの脆弱性のマッピング （2602 ページ）
カスタム製品マッピングの作成 （2603 ページ）

サードパーティ製品のマッピング

ユーザ入力機能を使用して各サードパーティからのデータをネットワーク マップに追加する場合、サードパーティで使用するベンダー、製品、およびバージョンの各名前を Cisco 製品定義にマッピングする必要があります。各製品を Cisco の定義にマッピングすると、これらの定義に基づいて脆弱性が割り当てられます。

同様に、パッチ管理製品などのサードパーティからのパッチ情報をインポートする場合、その修正の名前をデータベース内の適切なベンダー、製品、および対応する修正にマッピングする必要があります。

サードパーティの製品のマッピング

サード パーティからデータをインポートする場合、そのデータを使用して脆弱性を指定したり、影響の関連付けを行ったりするために、シスコの製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性情報をサードパーティ製品の名前に関連付けます。これにより、システムはそのデータを使用して影響の関連付けを行うことができます。

ホスト入力のインポート機能を使用してデータをインポートする場合、AddScanResult 機能を使用して、インポート中にサードパーティ製品をオペレーティング システムとアプリケーションの脆弱性にマップピングすることもできます。

たとえば、Apache Tomcat をアプリケーションとしてリストしているサード パーティのデータをインポートする場合で、それがバージョン 6 の Apache Tomcat であれば、以下のように設定し、サード パーティのマッピングを追加します。

- ベンダー名を [Apache] に設定します。
- プロダクト名に [Tomcat] 設定します。
- ベンダーのドロップダウン リストから [Apache] を選択します。
- 製品のドロップダウン リストから [Tomcat] を選択します。

- バージョンのドロップダウン リストから [6] を選択します。

このマッピングによって、Apache Tomcat 6 のすべての脆弱性が、Apache Tomcat をアプリケーションとしてリストアップするホストに割り当てられます。

バージョン情報やベンダー情報のないのアプリケーションの場合、Secure Firewall Management Center構成のアプリケーション タイプで脆弱性をマッピングする必要があります。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響アセスメントに使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。

ヒント すでに別の Secure Firewall Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この Firewall Management Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]**を選択します。

ステップ 2 [ユーザー サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- [作成（Creat）] : 新しいマップセットを作成するには、[製品マップセットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）] : 既存のマップセットを編集するには、変更するマップセットの横にある [編集（Edit）]（✎）をクリックします。 代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 次の 2 つの選択肢があります。

- [作成（Creat）] : サード パーティ製品をマッピングするには、[製品マップの追加（Add Product Map）] をクリックします。
- [編集（Edit）] : 既存のサードパーティ製品マップを編集するには、変更するマップセットの横にある[編集（Edit）]（✎）をクリックします。 代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 7 サードパーティの製品で使用される [ベンダーの文字列（Vendor String）] を入力します。

ステップ 8 サードパーティの製品で使用される [製品の文字列（Product String）] を入力します。

ステップ 9 サードパーティの製品で使用される [バージョン文字列（Version String）] を入力します。

ステップ 10 製品マッピング セクションで、ベンダーの脆弱性のマッピングに使用するオペレーティング システム、製品、製品バージョンを、以下の項目から選択します。[ベンダー（Vendor）]、[製品（Product）]、[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[改訂バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、[拡張子（Extension）]。

例：

名前がサードパーティの文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性マッピングを使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Red Hat Linux]、バージョンとして [9] を選択します。

ステップ 11 [保存（Save）] をクリックします。

サード パーティ製品の修正のマッピング

修正名をデータベースの特定の修正セットにマッピングする場合、サードパーティのパッチ管理アプリケーションからデータをインポートし、修正を一連のホストに適用することができます。修正名がホストにインポートされると、システムはその修正によって解決されるすべての脆弱性をそのホストに対して無効としてマークします。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]**を選択します。

ステップ 2 [ユーザー サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- [作成（Creat）] : 新しいマップセットを作成するには、[製品マップセットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）] : 既存のマップセットを編集するには、変更するマップセットの横にある [編集（Edit）]（✎）をクリックします。 代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 次の 2 つの選択肢があります。

- 作成：サードパーティ製品をマッピングするには、[修正マップの追加（Add Fix Map）] をクリックします。
- 編集：既存のサードパーティ製品マップを編集するには、その横にある[編集（Edit）]（✎）をクリックします。 代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 7 [サードパーティの修正名（Third-Party Fix Name）] フィールドにマッピングする修正の名前を入力します。

ステップ 8 [製品マッピング（Product Mappings）] セクションで、次のフィールドから修正マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

- **Vendor**
- **製品**
- **メジャー バージョン**
- **マイナー バージョン**
- **リビジョン バージョン**
- **ビルド（Build）**
- **パッチ**
- **内線番号（Extension）**

例：

Red Hat Linux 9 からパッチが適用されるホストにマッピングで修正を割り当てる場合は、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 9 [保存（Save）] をクリックして、修正マップを保存します。

サードパーティの脆弱性のマッピング

サードパーティからの脆弱性情報を VDB に追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存の SVID、Bugtraq、または SID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。

サードパーティの脆弱性に対する影響の関連付けを有効にし、関連付けの実行を可能にする必要があります。バージョンレスまたはベンダーレスのアプリケーションの場合、Secure Firewall Management Center の設定でアプリケーション タイプの脆弱性をマッピングする必要もあります。

多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性は影響評価に使用できません。

ヒント すでに別の Secure Firewall Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この Firewall Management Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーションディテクタ（Application Detectors）]**を選択します。

ステップ 2 [ユーザー サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- 作成：新しい脆弱性セットを作成するには、[脆弱性マップセットの作成（Create Vulnerability Map Set）] をクリックします。
- 編集：既存の脆弱性セットを編集するには、脆弱性セットの横にある[編集（Edit）]（✎）をクリックします。 代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [脆弱性マップの追加（Add Vulnerability Map）] をクリックします。

ステップ 5 [脆弱性 ID（Vulnerability ID）] フィールドに脆弱性のサードパーティ ID を入力します。

ステップ 6 [脆弱性の説明（Vulnerability Description）] を入力します。

ステップ 7 必要に応じて、次の操作を実行します。

- [Snort 脆弱性 ID マッピング（Snort Vulnerability ID Mappings）] フィールドに [Snort ID] を入力します。
- [SVID マッピング（SVID Mappings）] フィールドに、レガシー脆弱性 ID を入力します。
- [Bugtraq脆弱性IDマッピング（Bugtraq Vulnerability ID Mappings）] フィールドに、Bugtraq ID 番号を入力します。

ステップ 8 **[追加（Add）]** をクリックします。

関連トピック

ネットワーク検出の脆弱性影響評価の有効化 （2675 ページ）

カスタム製品マッピング

製品マッピングを使用して、サードパーティによるサーバ入力が適切なシスコ定義に関連付けられていることを確認できます。製品マッピングを定義し有効化した後、マッピングされたベンダー文字列を持つモニタ対象ホスト上のすべてのサーバまたはクライアントが、カスタム製品マッピングを使用します。したがって、サーバーのベンダー、製品、バージョンを明示的に設定する代わりに、特定のベンダー文字列でネットワーク マップのすべてのサーバーの脆弱性をマップすることをお勧めします。

カスタム製品マッピングの作成

システムが VDB のベンダーおよび製品にサーバーをマッピングできない場合は、手動でマッピングを作成できます。カスタム製品マッピングをアクティブにすると、システムは指定され

たベンダーおよび製品の脆弱性を、そのベンダー文字列が発生するネットワーク マップのすべてのサーバーにマッピングします。

（注） カスタム製品マッピングは、アプリケーションデータのソース（Nmap、ホスト入力機能、またはシステム自体など）に関係なく、アプリケーションプロトコルのすべての出現に適用されます。ただし、ホスト入力機能を使用してインポートしたデータのサードパーティの脆弱性マッピングが、カスタム製品マッピングを介して設定したマッピングと競合する場合、サードパーティの脆弱性マッピングはカスタム製品マッピングをオーバーライドし、入力が発生したときにサードパーティの脆弱性マッピング設定を使用します。

製品マッピング リストを作成し、各リストをアクティブ化/非アクティブ化することによって、複数のマッピングの同時使用を有効にするか、無効にします。マッピングするベンダーを指定すると、そのベンダーによって作成された製品のみを含むように製品リストが更新されます。

カスタム製品マッピングを作成した後で、カスタム製品マッピング リストをアクティブにする必要があります。カスタム製品マッピング リストをアクティブにすると、指定されたベンダー文字列が発生するすべてのサーバーが更新されます。ホスト入力機能を介してインポートされるデータでは、このサーバーの製品マッピングをすでに明示的に設定していない限り、脆弱性が更新されます。

たとえば、組織が Apache Tomcat Web サーバーのバナーの文字列を `Internal Web Server` に変更した場合、ベンダー文字列 `Internal Web Server` をベンダー **Apache** および製品 **Tomcat** にマッピングできます。その後、そのマッピングを含むリストをアクティブにすると、`Internal Web Server` とラベル付けされたサーバーが存在するすべてのホストのデータベースに Apache Tomcat の脆弱性が想定されます。

ヒント この機能を使用して、もう 1 つの脆弱性にルールの SID をマッピングすることによって、ローカルの侵入ルールに脆弱性をマッピングすることができます。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーションディテクタ（Application Detectors）]**を選択します。

ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。

ステップ 3 [カスタム製品マッピング リストの作成（Create Custom Product Mapping List）] をクリックします。

ステップ 4 [カスタム製品マッピング リスト名（Custom Product Mapping List Name）] を入力します。

ステップ 5 [ベンダー文字列の追加（Add Vendor String）] をクリックします。

ステップ 6 [ベンダー文字列（Vendor String）] フィールドに、選択したベンダーおよび製品値にマッピングする必要があるアプリケーションを識別するベンダー文字列を入力します。

ステップ 7 [ベンダー（Vendor）] ドロップダウン リストから、マッピングするベンダーを選択します。

ステップ 8 [製品（Product）] ドロップダウン リストから、マッピングする製品を選択します。

ステップ 9 [追加（Add）] をクリックして、マッピングしたベンダー文字列をリストに追加します。

ステップ 10 オプションで、さらにベンダー文字列のマッピングをリストに追加するには、必要に応じて手順 4 ～ 8 を繰り返します。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- カスタム製品マッピング リストをアクティブにします。詳細については、「カスタム製品マッピングのアクティブ化と非アクティブ化 （2605 ページ）」を参照してください。

カスタム製品マッピング リストの編集

ベンダー文字列を追加または削除したり、リスト名を変更したりして、既存のカスタム製品マッピング リストを変更できます。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーションディテクタ（Application Detectors）]**を選択します。

ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。

ステップ 3 編集する製品マッピングリストの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 カスタム製品マッピングの作成 （2603 ページ）の説明に従って、リストを変更します。

ステップ 5 終了したら、[保存（Save）] をクリックします。

カスタム製品マッピングのアクティブ化と非アクティブ化

カスタム製品マッピング リスト全体の使用を一度に有効または無効にすることができます。カスタム製品マッピング リストをアクティブにすると、そのリストの各マッピングが、管理対象デバイスによって検出されたか、またはホスト入力機能を介してインポートされたかに関わらず、指定したベンダー文字列を持つすべてのアプリケーションに適用されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーションディテクタ（Application Detectors）]**を選択します。

ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするカスタム製品のマッピング リストの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ホスト入力クライアントの設定

ホスト入力機能を使用すると、別のアプライアンスで実行されているクライアントプログラムから Firewall Management Center のネットワーク マップを更新できます。たとえば、ネットワーク マップからホストを追加または削除したり、ホスト OS およびサービス情報を更新したりできます。詳細については、*Firepower* システムホスト入力 *API* ガイドを参照してください。

リモート クライアントを実行するには、その前に、[ホスト入力クライアント（Host Input Client）] ページから Firewall Management Center のピア データベースにクライアントを追加する必要があります。また、Firewall Management Center によって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了すると、クライアントは Firewall Management Center に接続できます。

マルチドメイン展開では、すべてのドメインにクライアントを作成できます。認証証明書を使用すると、クライアントは、クライアント証明書のドメインに関連付けられているリーフ ドメインにネットワーク マップ アップデートを送信できます。先祖ドメインの証明書を作成した場合（または後で証明書ドメインが子孫ドメインの追加後に先祖ドメインになった場合）、その証明書を使用するクライアントは、*Firepower* システムホスト入力 *API* ガイドで説明するように、すべてのトランザクションのターゲット リーフ ドメインを指定する必要があります。

[ホスト入力クライアント（Host Input Client）] には、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは失効させるには、クライアントが作成されたドメインに切り替えます。

この接続では TLS 1.2 を使用します。

手順

ステップ 1 **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。

ステップ 2 [ホスト入力クライアント（Host Input Client）] をクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）]フィールドに、ホスト入力クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注）
DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[Password] フィールドにパスワードを入力します。

ステップ 6 [**Save**] をクリックします。
ホスト入力サービスは、ホストが Firewall Management Center 上のポート 8307 にアクセスすることを許可し、クライアント/サーバー認証時に使用する認証証明書を作成します。

ステップ 7 証明書ファイルの横にある[ダウンロード（download）]（）をクリックします。

ステップ 8 SSL/TLS認証のためにクライアントが使用するディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある[削除（Delete）]（）をクリックします。

Nmap スキャン

Firepower システムは、ネットワークのトラフィックをパッシブ分析してネットワーク マップを構築します。このパッシブ分析によって取得される情報は、システムの状態によっては不完全なことがよくあります。ただし、ホストをアクティブにスキャンすることで、完全な情報を取得できます。たとえば、オープンポート上で実行中のサーバがホストにあり、システムによるネットワークのモニタリング中にそのサーバがトラフィックを送受信しなかった場合、システムではそのサーバに関する情報をネットワークマップに追加しません。しかし、アクティブスキャナを使用して直接そのホストをスキャンすると、サーバの存在を検出できます。

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。

Nmap を使用してホストをスキャンすると、システムは以下のように動作します。

- 前に検出されていないオープン ポート上のサーバを、該当するホストのホスト プロファイルの [サーバ（Servers）] リストに追加します。ホスト プロファイルの [スキャン結果（Scan Results）] セクションには、フィルタ処理されていたり閉じていたりしている TCP ポートやUDPポート上で検出されたサーバがリストされます。デフォルトでは、Nmapは 1660 を超える TCP ポートをスキャンします。

  Nmap スキャンで識別されたサーバがシステムで認識され、対応するサーバ定義がシステムにある場合、システムは Nmap がそのサーバに使用する名前を、対応する Cisco サーバ定義にマップします。

- スキャン結果と 1500 を超える既知のオペレーティング システムのフィンガープリントを比較して、オペレーティング システムを判別し、それぞれにスコアを割り当てます。最高スコアのオペレーティング システムのフィンガープリントが、ホストに割り当てられるオペレーティング システムになります。

システムはNmapのオペレーティング システム名をCiscoのオペレーティング システム定義にマップします。

- 追加されたサーバおよびオペレーティング システムのホストに脆弱性を割り当てます。

（注）

- ホストがネットワーク マップ内になければ、Nmapは結果をホストプロファイルに追加することはできません。
- ホストがネットワーク マップから削除されると、そのホストに関するNmapスキャン結果が破棄されます。

ヒント　スキャン オプションによっては（ポートスキャンなど）低帯域幅のネットワークに非常に負荷をかけることがあります。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

スキャンに使用される基礎的なNmapテクノロジーの詳細については、http://insecure.org/ にあるNmapのマニュアルを参照してください。

Nmap 修復オプション

Nmap修復を作成して、Nmapスキャンの設定を定義します。Nmap修復は、相関ポリシー内で応答として使用したり、オンデマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。

Nmapにより提供されるサーバーやオペレーティング システムのデータは、もう1度Nmapスキャンを実行するまで静的な状態のままであることに注意してください。Nmapを使用してホスト内でオペレーティング システムやサーバーのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmapによって提供されるオペレーティング システムやサーバーのデータを最新に保つこともできます。

次の表に、Nmap修復で設定可能なオプションを示します。

表 *200 : Nmap* 修復オプション

オプション	説明	対応する Nmap オプション
[スキャンの開始元イベント（Scan Which Address(es) From Event?）]	Nmap スキャンを相関ルールに対する応答として使用する場合、イベント内の送信元ホスト、宛先ホスト、またはその両方のどのアドレスをスキャンするのか制御する次のいずれかのオプションを選択します。 • [送信元アドレスと宛先アドレスのスキャン（Scan Source and Destination Addresses）] は、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンします。 • [送信元アドレスのみのスキャン（Scan Source Address Only）] は、イベントの送信元 IP アドレスによって表されるホストをスキャンします。 • [宛先アドレスのみのスキャン（Scan Destination Address Only）] は、イベントの宛先 IP アドレスによって表されるホストをスキャンします。	該当なし
Scan Types	Nmap がポートをスキャンする方法を選択します。 • [TCP Syn] スキャンは、完全な TCP ハンドシェイクを使用せずに数千のポートにただちに接続します。このオプションを使用すると、TCP 接続が開始されますが完了はしていない状態で、`admin` アカウントが raw パケット アクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードでクイック スキャンできます。ホストが TCP Syn スキャンで送信される SYN パケットを確認応答すると、Nmap は接続をリセットします。 • [TCP 接続（TCP Connect）] スキャンは、`connect()` システム コールを使用して、ホスト上のオペレーティング システムを介して接続を開きます。TCP Connect スキャンは、Firewall Management Center 上の `admin` ユーザーや管理対象デバイスがホストに対する raw パケット特権を持っていない場合や、IPv6 ネットワークをスキャンしている場合に使用できます。つまり、このオプションは TCP Syn スキャンを使用できない状況で使用します。 • [TCP ACK] スキャンは、ACK パケットを送信して、ポートがフィルタ処理されているかいないかを検査します。 • [TCP Window] スキャンは、TCP ACK スキャンと同じ機能に加えて、ポートが開いているか閉じているかも判別します。 • [TCP Maimon] スキャンは、FIN/ACK プローブを使用して BSD 派生システムを識別します。	**TCP Syn**：`-sS` **TCP Connect**：`-sT` **TCP ACK**：`-sA` **TCP Window**：`-sW` **TCP Maimon**：`-sM`

オプション	説明	対応する Nmap オプション
Scan for UDP ports	TCP ポートに加えて UDP ポートのスキャンも有効にします。UDP ポートのスキャンには時間がかかることがあるので、クイック スキャンする場合はこのオプションを使用しないように注意してください。	`-sU`
Use Port From Event	相関ポリシー内で応答として修復を使用する計画の場合に、修復によるスキャンの対象として、相関応答をトリガーするイベントで指定されたポートのみを有効にします。 • 相関イベント内のポートをスキャンし、Nmap 修復構成中に指定するポートをスキャンしない場合は、[オン（On）] を選択します。相関イベント内のポートをスキャンする場合は、Nmap 修復構成中に指定する IP アドレス上のポートが修復によりスキャンされることに注意してください。これらのポートも修復の動的スキャンのターゲットに追加されます。 • Nmap 修復構成中に指定するポートのみスキャンするには、[オフ（Off）] を選択します。 Nmap がオペレーティング システムやサーバーに関する情報を収集するかどうかも制御できます。新しいサーバーに関連付けられたポートをスキャンするには、[Use Port From Event] オプションを有効にします。	該当なし
Scan from reporting detection engine	ホストを報告した検出エンジンがあるアプライアンスからホストへのスキャンを有効にします。 • レポート検出エンジンを実行しているアプライアンスからスキャンするには、[オン（On）] を選択します。 • 修復内で設定されているアプライアンスからスキャンするには、[オフ（Off）] を選択します。	該当なし
Fast Port Scan	スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内にある `nmap-services` ファイルにリストされている TCP ポートのみに対するスキャンを有効にし、その他のポート設定を無視できるようにします。このオプションと [ポート範囲とスキャンの順序（Port Ranges and Scan Order）] オプションを併用できないことに注意してください。 • スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内の `nmap-services` ファイルにリストされているポートのみスキャンし、その他のポート設定を無視するには、[オン（On）] を選択します。 • すべての TCP ポートをスキャンするには、[オフ（Off）] を選択します。	`-F`

オプション	説明	対応する Nmap オプション
Port Ranges and Scan Order	Nmap ポート仕様シンタックスを使用して、スキャンする特定のポートを設定し、スキャンする順序も設定します。このオプションと [Fast Port Scan] オプションを併用できないことに注意してください。	`-p`
Probe open ports for vendor and version information	サーバー ベンダーとバージョン情報の検出を有効にします。オープン ポートでサーバー ベンダーとバージョン情報を調査する場合、Nmap はサーバーの識別に使用するサーバー データを取得します。次に、シスコのサーバー データをそのサーバーに置き換えます。 • ホスト上のオープン ポートでサーバー情報をスキャンして、サーバー ベンダーとバージョンを識別するには、[オン（On）] を選択します。 • ホストのシスコのサーバー情報を使用して続行するには、[オフ（Off）] を選択します。	`-sV`
Service Version Intensity	サービス バージョンに対する Nmap プローブの強度を選択します。 • 選択する数値が大きいほど使用するプローブの数が増えるので、スキャンは長時間になり精度が上がります。 • 選択する数値が小さいほど、使用するプローブの数が減るので、スキャンは高速になり精度が下がります。	`--version-intensity` <intensity>
[オペレーティング システムの検出（Detect Operating System）]	ホストのオペレーティング システム情報の検出を有効にします。 ホストでのオペレーティング システムの検出を設定した場合、Nmap はホストをスキャンし、その結果を使用してオペレーティング システムごとに評価を作成します。この評価は、ホスト上でそのオペレーティング システムが実行されている可能性を反映します。 • ホストに対してオペレーティング システムを識別する情報をスキャンするには、[オン（On）] を選択します。 • ホストに関するシスコのオペレーティング システム情報を使い続ける場合は、[オフ（Off）] を選択します。	`-o`

オプション	説明	対応する Nmap オプション
Treat All Hosts As Online	ホストディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを有効にします。このオプションを有効にすると、Nmap は [ホストディスカバリ方式（Host Discovery Method）] と [ホストディスカバリポート リスト（Host Discovery Port List）] の設定を無視するので注意してください。 • ホストディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを実行するには、[オン（On）] を選択します。 • [ホスト ディスカバリ方式（Host Discovery Method）] と [ホスト ディスカバリ ポート リスト（Host Discovery Port List）] の設定を使用してホスト ディスカバリを実行し、使用不能なホスト上でのポート スキャンを省略するには、[オフ（Off）] を選択します。	`-PN`
Host Discovery Method	ホスト ディスカバリを、ターゲット範囲内のすべてのホストに対して実行するか、[Host Discovery Port List] にリストされているポートを経由して実行するか、または、ポートがリストされていない場合にそのホストディスカバリ方式のデフォルト ポートを経由するかを選択します。 ここで、[Treat All Hosts As Online] も有効にすると、[Host Discovery Method] オプションは無効になり、ホスト ディスカバリが実行されないことに注意してください。 ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。 • [TCP SYN] オプションは、SYN フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP SYN はポート 80 をスキャンします。TCP SYN スキャンは、ステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [TCP ACK] オプションは、ACK フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP ACK もポート 80 をスキャンします。TCP ACK スキャンは、ステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [UDP] オプションは、UDP パケットを送信し、クローズ ポートからポート到達不能応答が戻されるとホストが利用可能であると想定します。デフォルトでは UDP はポート 40125 をスキャンします。	**TCP SYN**：`-PS` **TCP ACK**：`-PA` **UDP**：`-PU`

オプション	説明	対応する Nmap オプション
Host Discovery Port List	ホスト ディスカバリの実行時にスキャンするポートを、カスタマイズしたカンマ区切りリストで指定します。	ホストディスカバリ方式に応じたポート リスト
Default NSE Scripts	ホストディスカバリを行い、サーバー、オペレーティング システム、脆弱性を検出する Nmap スクリプトのデフォルト セットを実行できるようにします。デフォルト スクリプトのリストについては、https://nmap.org/nsedoc/categories/default.html を参照してください。 • Nmap スクリプトのデフォルト セットを実行するには、[オン（On）] を選択します。 • Nmap スクリプトのデフォルト セットを省略するには、[オフ（Off）] を選択します。	`-sC`
Timing Template	スキャン プロセスのタイミングを選択します。選択する数値が大きいほど、スキャンは高速になり包括的ではなくなります。	**0**：`T0`（paranoid） **1**：`T1`（sneaky） **2**：`T2`（polite） **3**：`T3`（normal） **4**：`T4`（aggressive） **5**：`T5`（insane）

Nmap スキャンのガイドライン

アクティブ スキャンにより重要な情報が得られることがありますが、Nmap などのツールを多用すると、ネットワーク リソースに負荷がかかり、重要なホストがクラッシュすることさえあります。アクティブ スキャナを使用する際には、以下のガイドラインに従ってスキャン戦略を作成し、スキャンする必要があるホストとポートのみスキャンするようにしてください。

適切なスキャン ターゲットの選択

Nmap を設定する際に、スキャン対象のホストを識別するスキャン ターゲットを作成できます。スキャン ターゲットには 1 つの IP アドレス、IP アドレスの CIDR ブロックまたはオクテット範囲、IP アドレス範囲、スキャンする IP アドレスまたは範囲のリスト、および 1 つ以上のホスト上のポートが含まれます。

次の方法でターゲットを指定できます。

- IPv6 ホストの場合：
  - 正確な IP アドレス（`2001:DB8:1::178:ABCD` など）

- IPv4 ホストの場合：
  - 厳密な IP アドレス（192.168.1.101 など）またはカンマかスペースで区切った IP アドレスのリスト
  - CIDR 表記を使用した IP アドレス ブロック（たとえば、192.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）
  - オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、192.168.0-255.1-254 は、192.168.x.x の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
  - ハイフンを使用した IP アドレス範囲（たとえば、192.168.1.1 - 192.168.1.5 は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
  - カンマかスペースで区切ったアドレスか範囲のリスト（たとえば、192.168.1.0/24, 194.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

理想的な Nmap スキャンのスキャン ターゲットには、システムで識別できないオペレーティング システムがあるホスト、識別されていないサーバがあるホスト、最近ネットワーク上で検出されたホストが含まれます。ネットワーク マップ内にないホストに関する Nmap 結果は、ネットワーク マップに追加できないことに注意してください。

⚠

注意

- Nmap によって提供されるサーバーやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。
- ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。
- ターゲットをスキャンする権限を持っていることを確認してください。Nmap を使用して自分や自社に属さないホストをスキャンすると違法になる場合があります。

スキャン対象にする適切なポートの選択

設定するスキャン ターゲットごとに、スキャン対象のポートを選択できます。各ターゲット上でスキャンする必要があるポートのセットを正確に識別するため、個々のポート番号、ポート範囲、または一連のポート番号やポート範囲を指定できます。

デフォルトでは、Nmap は 1 から 1024 までの TCP ポートをスキャンします。相関ポリシー内で応答として修復を使用する計画の場合は、相関応答をトリガーするイベントで指定されたポートのみを修復でスキャンできます。オンデマンドまたはスケジュール済みタスクとして修復を実行する場合、または Use Port From Event を使用しない場合は、その他のポート オプションを使用して、スキャンするポートを決定できます。nmap-services ファイルにリストされている TCP ポートのみスキャンし、その他のポート設定を無視するよう選択できます。TCP ポートの他に UDP ポートもスキャンできます。UDP ポートに対するスキャンには時間がかかるこ

とがあるので、すばやくスキャンする場合はこのオプションを使用しないように注意してください。スキャン対象として特定のポートかポート範囲を選択するには、Nmap ポート仕様シンタックスを使用してポートを識別します。

ホスト ディスカバリ オプションの設定

ホストに対してポート スキャンを始める前にホスト ディスカバリを実行するかどうかを決めるか、またはスキャンを計画しているすべてのホストがオンラインであると想定できます。すべてのホストをオンラインとして扱わないことを選択した場合、使用するホストディスカバリ方式を選択でき、必要に応じて、ホストディスカバリ時のスキャン対象ポートのリストをカスタマイズできます。ホストディスカバリ時には、リストされているポートでオペレーティングシステムやサーバの情報は調査されません。特定のポートを経由する応答を使用して、ホストがアクティブで使用可能かどうかのみを判別します。ホストディスカバリを実行して、ホストが利用可能でなかった場合には、そのホスト上のポートは Nmap でスキャンされません。

例：Nmap を使用した不明なオペレーティング システムの解決

この例では、不明なオペレーティング システムを解決するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、Nmap スキャンの管理 （2618 ページ） を参照してください。

システムでネットワーク上のホストのオペレーティング システムを判別できない場合、Nmap を使用してホストをアクティブ スキャンできます。Nmap は、スキャンから得られた情報を利用して、使用されている可能性のあるオペレーティング システムを評価します。次に、最高の評価のオペレーティング システムを、ホストのオペレーティング システムを識別したものとして使用します。

Nmap を使用して新しいホストにオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシステムによるそのデータのモニタリングは非アクティブになります。Nmap を使用してホスト検出を実行し、システムにより不明なオペレーティング システムがあるとマークが付けられたホストのサーバ オペレーティング システムを検出すると、同種のホストのグループを識別できる場合があります。その場合、それらのホストのうちの 1 つに基づいたカスタム フィンガープリントを作成し、システムでそのフィンガープリントを、Nmap スキャンに基づいてそのホスト上で実行されていると判明したオペレーティング システムと関連付けるようにすることができます。可能な限り、Nmap などのサードパーティ製の静的データを入力するよりも、カスタム フィンガープリントを作成してください。カスタム フィンガープリントを使用すると、システムはホストのオペレーティング システムを継続してモニタし、必要に応じて更新できるからです。

この例では、次のことを実行します。

1. Nmap スキャン インスタンスの追加 （2619 ページ） の説明に従って、スキャン インスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
   - [イベントからのポートを使用（Use Port From Event）] を有効にして、新しいサーバーに関連付けられたポートをスキャンします。

- [オペレーティング システムの検出（Detect Operating System）] を有効にして、ホストのオペレーティング システムの情報を検出します。
- [ベンダーおよびバージョン情報に関するオープン ポートのプローブ（Probe open ports for vendor and version information）] を有効にして、サーバー ベンダーとバージョン情報を検出します。
- ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。

3. システムで不明なオペレーティング システムがあるホストが検出されたときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生**し、**ホストの OS 情報が変更**されており、**OS 名が不明**という条件が満たされている場合にトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. ネットワーク マップ上のホストを消去し、強制的にネットワーク検出が再起動されてネットワーク マップが再構築されるようにします。
8. 1 日後か 2 日後に、相関ポリシーによって生成されたイベントを検索します。Nmap 結果から、ホスト上で検出されたオペレーティング システムを分析し、システムで認識されない特定のホスト設定がネットワーク上にあるかどうか調べます。
9. 不明なオペレーティング システムがあるホストが複数検出され、Nmap 結果が同一の場合は、それらのホストの 1 つに対してカスタム フィンガープリントを作成し、将来類似のホストを識別する際に使用します。

関連トピック

Nmap 修復の作成 （2623 ページ）
Nmap スキャンの結果 （2627 ページ）
クライアント用のカスタム フィンガープリントの作成 （2591 ページ）

例：Nmap を使用した新しいホストへの応答

この例では、新しいホストに応答するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、Nmap スキャンの管理 （2618 ページ） を参照してください。

システムにより、侵入の可能性があるサブネット内で新しいホストが検出された場合、そのホストをスキャンして、そのホストの脆弱性に関する正確な情報を入手できます。

そのためには、このサブネット内に新しいホストが出現した時点で検出し、そのホスト上で Nmap スキャンを実行する修復を起動する相関ポリシーを作成してアクティブにします。

そのためには、次のことを実行します。

1. Nmap スキャンインスタンスの追加（2619 ページ）の説明に従って、スキャンインスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
   - [イベントからのポートを使用（Use Port From Event）] を有効にして、新しいサーバーに関連付けられたポートをスキャンします。
   - [オペレーティング システムの検出（Detect Operating System）] を有効にして、ホストのオペレーティング システムの情報を検出します。
   - [ベンダーおよびバージョン情報に関するオープン ポートのプローブ（Probe open ports for vendor and version information）] を有効にして、サーバー ベンダーとバージョン情報を検出します。
   - ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。
3. システムが特定のサブネット上で新しいホストを検出したときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生**し、**新しいホストが検出**されたときにトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. 新しいホストが通知されたら、ホスト プロファイルを調べて Nmap スキャンの結果を確認し、ホストに適用されている脆弱性に対処します。

このポリシーをアクティブにした後で、修復状態の表示（**[分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）]**）を定期的に検査して、修復が起動された時点を調べることができます。修復の動的なスキャン ターゲットには、サーバ検出の結果としてスキャンされたホストの IP アドレスを含める必要があります。これらのホストのホスト プロファイルを調べて、Nmap によって検出されたオペレーティング システムとサーバに基づいて、対処する必要がある脆弱性がホストにあるかどうか確認します。

注意 大規模なネットワークや動的なネットワークがある場合、新しいホストの検出は頻繁に発生するので、スキャンを使用して応答するには不向きな場合があります。リソースの過負荷を避けるために、頻繁に発生するイベントへの応答として Nmap スキャンを使用しないでください。また、Nmap を使用して新しいホストのオペレーティング システムやサーバーの情報を要求すると、スキャン対象のホストに対するによるそのデータのシスコ モニタリングが非アクティブになることに注意してください。

関連トピック

Nmap 修復の作成 （2623 ページ）

Nmap スキャンの管理

Nmap スキャンを使用するには、少なくとも 1 つの Nmap スキャン インスタンスと 1 つの Nmap 修復を設定する必要があります。Nmap スキャン ターゲットの設定はオプションです。

手順

ステップ 1 Nmap スキャンを設定します。

- Nmap スキャン インスタンスを追加します。詳細については、Nmap スキャン インスタンスの追加 （2619 ページ）を参照してください。
- Nmap 修復を作成します。詳細については、Nmap 修復の作成 （2623 ページ）を参照してください。
- 必要に応じて、Nmap スキャン ターゲットを追加します。詳細については、Nmap スキャン ターゲットの追加 （2621 ページ）を参照してください。

ステップ 2 Nmap スキャンを実行します。

- オンデマンド Nmap スキャンを実行します。詳細については、オンデマンド Nmap スキャンの実行 （2626 ページ）を参照してください。
- Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Nmap Scan Automation*」の説明に従い、自動 Nmap スキャンを設定します。
- Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Scheduling an Nmap Scan*」の説明に従い、自動 Nmap スキャンをスケジュールします。

次のタスク

- 関連タスクを表示することで、進行中の Nmap スキャンをモニターします。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Viewing Task Messages*」を参照してください。
- 必要に応じて、次に示すようにスキャンを調整します。
  - Nmap スキャン インスタンスを編集します。詳細については、Nmap スキャン インスタンスの編集 （2620 ページ）を参照してください。
  - Nmap スキャン ターゲットを編集します。詳細については、Nmap スキャン ターゲットの編集 （2622 ページ）を参照してください。
  - Nmap 修復を編集します。詳細については、Nmap 修復の編集 （2625 ページ）を参照してください。

Nmap スキャン インスタンスの追加

脆弱性についてネットワークをスキャンするのに使用する Nmap モジュールごとに別々のスキャン インスタンスをセットアップできます。Secure Firewall Management Center 上のローカル Nmap モジュールか、リモートでスキャンを実行するために使用するデバイスに対してスキャン インスタンスをセットアップできます。各スキャンの結果は常に Firewall Management Center に保存されます。リモートデバイスからスキャンを実行する場合でも、この場所でスキャンを設定できます。ミッションクリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスは追加できません。

手順

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- **[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**を選択します。
- **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 以下の場合、修復を追加します。

- 上記の最初の方法でリストにアクセスした場合は、[新しいインスタンスの追加（Add a New Instance）] セクションを探し、ドロップダウン リストから Nmap 修復モジュールを選択し、[追加（Add）] をクリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、[Nmap インスタンスの追加（Add Nmap Instance）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] を入力します。

ステップ 4 [説明（Description）] を入力します。

ステップ 5 オプションで、**[除外されたホスト（Exempted hosts）]** フィールドで、このスキャンインスタンスがスキャンしないホストまたはネットワークを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて `192.168.1.1` から `192.168.1.254` の間の 254 個のホストをスキャンします）
- 感嘆符（!）を使用してアドレス値の否定はできないことに注意してください。

（注）
ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。

ステップ 6 オプションで、Firewall Management Centerの代わりにリモート デバイスからスキャンを実行するには、そのデバイスの IP アドレスか名前を指定します。この情報は、Firewall Management Center Web インターフェイス内のそのデバイスに関する [Information] ページの [Remote Device Name] フィールドに表示されます。

ステップ 7 [作成（Create）] をクリックします。
システムがインスタンスの作成を終えると、編集モードでこのインスタンスが表示されます。

ステップ 8 必要に応じて、インスタンスに Nmap の修復を追加します。そのためには、インスタンスの [設定されている修復（Configured Remediations）] を探し、[追加（Add）] をクリックし、Nmap 修復の作成 （2623 ページ）の説明に従って修復を作成します。

ステップ 9 インスタンスのリストに戻るには、[キャンセル（Cancel）] をクリックします。

（注）
[スキャナ（Scanners）] オプションにより Nmap スキャンインスタンスのリストにアクセスした場合は、インスタンスの修復も併せて追加しないと追加したインスタンスは表示されません。修復が追加されていないインスタンスをすべて表示するには、[インスタンス（Instances）] メニュー オプションを使ってリストにアクセスします。

Nmap スキャン インスタンスの編集

スキャン インスタンスを編集する場合、インスタンスに関連付けられている修復を表示、追加、および削除できます。インスタンス内でプロファイルが作成されたNmapモジュールを使用しなくなった場合には、Nmapスキャンインスタンスを削除します。スキャンインスタンスを削除すると、そのインスタンスを使用する修復も削除されることに注意してください。

手順

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- **[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**を選択します。
- **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 編集するインスタンスの横にある[表示（View）]（👁）をクリックします。

ステップ 3 Nmap スキャン インスタンスの追加 （2619 ページ）の説明に従って、スキャンインスタンスの設定を変更します。

ステップ 4 **[Save（保存）]** をクリックします。

ステップ 5 [Done] をクリックします。

次のタスク

- 必要に応じて、スキャン インスタンスに新しい修復を追加します。次を参照してください。 Nmap 修復の作成 （2623 ページ）
- 必要に応じて、インスタンスに関連付けられている修復を編集します。Nmap 修復の編集（2625 ページ）を参照してください。
- 必要に応じて、インスタンスに関連付けられる修復を削除します。オンデマンド Nmap スキャンの実行 （2626 ページ）を参照してください。
- 必要に応じて、その横にある[削除（Delete）]（）をクリックして、スキャンインスタンスを削除します。

Nmap スキャン ターゲットの追加

Nmapモジュールを設定する際にスキャン ターゲットを作成して保存できます。スキャン ターゲットは、オンデマンドまたはスケジュール済みのスキャンの実行時にターゲットにするホストとポートを識別します。これにより、毎回新しいスキャン ターゲットを作成する必要がなくなります。スキャン ターゲットには、スキャンする 1 つの IP アドレスか IP アドレスのブロック、および 1 つ以上のホスト上のポートが含まれます。Nmap ターゲットの場合、オクテット範囲による Nmap のアドレッシングや IP アドレスの範囲も使用できます。Nmap のオクテット範囲によるアドレッシングの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

（注）

- スキャン ターゲットに多数のホストが含まれている場合、スキャンに要する時間が延びる場合があります。回避策として、一度にスキャンするホストを減らしてください。
- Nmap によって提供されるサーバーやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。

ステップ 3 [スキャン ターゲットの作成（Create Scan Target）] をクリックします。

ステップ 4 [名前（Name）] フィールドに、このスキャン ターゲットに使用する名前を入力します。

ステップ 5 [IP 範囲（IP Range）] テキスト ボックスで、Nmap スキャンのガイドライン （2613 ページ）で説明しているシンタックスを使用して、スキャンする 1 つ以上のホストを指定します。

（注）

スキャン ターゲット内の IP アドレスか範囲のリストでカンマを使用した場合、ターゲットを保存する際にカンマはスペースに変換されます。

ステップ 6 [ポート（Ports）] フィールドで、スキャンするポートを指定します。

1 から 65535 までの値を使用して、次のいずれかを入力できます。

- 1 つのポート番号
- カンマで区切ったポートのリスト
- ハイフンで区切ったポート番号の範囲
- ハイフンで区切ったポート番号の複数の範囲をカンマで区切ったもの

ステップ 7 [保存（Save）] をクリックします。

Nmap スキャン ターゲットの編集

ヒント 修復を使用して特定の IP アドレスをスキャンするつもりがないのに、修復を起動した相関ポリシー違反にホストが関係していたためにその IP アドレスがターゲットに追加された場合は、修復の動的スキャン ターゲットを編集できます。

スキャンターゲットにリストされているホストをスキャンする必要がなくなった場合は、そのスキャン ターゲットを削除します。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。

ステップ 3 編集するスキャンターゲットの横にある[編集（Edit）]（✎）をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 必要に応じて変更を加えます。詳細については、「Nmap スキャン ターゲットの追加（2621 ページ）」を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 必要に応じて、その横にある[削除（Delete）]（🗑）をクリックして、スキャンターゲットを削除します。

Nmap 修復の作成

Nmap 修復は、既存の Nmap スキャン インスタンスに修復を追加することによってのみ作成できます。修復では、スキャンの設定を定義します。これは相関ポリシーで応答として使用したり、オンデマンドで実行したり、スケジュール タスクとして特定の時刻に実行したりできます。

Nmap によって提供されるサーバーやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

始める前に

- Nmap スキャン インスタンスの追加 （2619 ページ） の説明に従って、Nmap スキャンインスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある[表示（View）]（👁）をクリックします。

ステップ 3 [設定済みの修復（Configured Remediations）] セクションで、[追加（Add）] をクリックします。

ステップ 4 [修復名（Remediation Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 侵入イベント、接続イベント、ユーザーイベントをトリガーする相関ルールに応じてこの修復を使用する場合は、[スキャンするイベントのアドレス（Scan Which Address(es) From Event?）] オプションを設定します。

ヒント
ディスカバリ イベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

（注）
トラフィック プロファイルの変更に対してトリガーする相関ルールへの応答として Nmap 修復を割り当て**ないでください**。

ステップ 7 [スキャン タイプ（Scan Type）] オプションを設定します。

ステップ 8 オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[UDP ポートのスキャン（Scan for UDP ports）] オプションで [オン（On）] を選択します。

ヒント
UDP ポートスキャンは TCP ポートスキャンよりも時間がかかります。スキャン時間を短縮するには、このオプションを無効のままにします。

ステップ 9 相関ポリシー違反への応答としてこの修復を使用する計画の場合は、[イベントからポートを使用（Use Port From Event）] オプションを設定します。

ステップ 10 相関ポリシー違反への応答としてこの修復を使用する計画で、イベントを検出した検出エンジンを実行しているアプライアンスを使用してスキャンを実行するには、[レポート検出エンジンからスキャン（Scan from reporting detection engine）] オプションを設定します。

ステップ 11 [高速ポート スキャン（Fast Port Scan）] オプションを設定します。

ステップ 12 [ポート範囲およびスキャン順序（Port Ranges and Scan Order）] フィールドに、デフォルトでスキャンするポートを入力します。Nmap ポート指定シンタックスを使用し、ポートをスキャンする順序で入力します。

次の形式を使用します。

- 1 から 65535 までの値を指定します。
- ポートを区切るには、カンマかスペースを使用します。
- ポート範囲を示すには、ハイフンを使用します。
- TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。

（注）
手順 8 で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[イベントからポートを使用（Use Port From Event）] オプションによりこの設定が上書きされます。

例：

UDP トラフィックのポート 53 と 111 をスキャンしてから、TCP トラフィックのポート 21 から 25 までスキャンするには、`U:53,111,T:21-25` と入力します。

ステップ 13 開いているポートでサーバー ベンダーおよびバージョン情報をプローブするには、[ベンダーおよびバージョン情報に関するオープン ポートのプローブ（Probe open ports for vendor and version information）] を設定します。

ステップ 14 開いているポートをプローブすることにした場合、[サービス バージョンの強さ（Service Version Intensity）] ドロップダウン リストから数値を選択することにより、使用されるプローブの数を設定します。

ステップ 15 オペレーティング システム情報をスキャンするには、[オペレーティング システムの検出（Detect Operating System）] 設定を行います。

ステップ 16 ホストディスカバリが行われるかどうか、およびポートのスキャンが使用可能なホストのみに対して実行されるかどうかを決めるには、[すべてのホストをオンラインとして扱う（Treat All Hosts As Online）] を設定します。

ステップ 17 Nmap でホストの使用可能性をテストする際に使用する方法を設定するには、[ホスト ディスカバリ方式（Host Discovery Method）] ドロップダウン リストから方式を選択します。

ステップ 18 ホストディスカバリ時にポートのカスタムリストをスキャンする場合は、選択したホストディスカバリ方式に適したポートのリストを、[ホストディスカバリ ポート リスト（Host Discovery Port List）] フィールドにカンマで区切って入力します。

ステップ 19 [デフォルト NSE スクリプト（Default NSE Scripts）] オプションを設定して、ホスト ディスカバリおよび、サーバー、オペレーティング システム、脆弱性のディスカバリに Nmap スクリプトのデフォルト セットを使用するかどうかを制御します。

ヒント
デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

ステップ 20 スキャン プロセスのタイミングを設定するには、[タイミング テンプレート（Timing Template）] ドロップダウン リストからタイミング テンプレート番号を選択します。

より高速だが、包括的でないスキャンを実行する場合は大きい番号を選択し、低速で、より包括的なスキャンを実行する場合は小さい番号を選択します。

ステップ 21 [作成（Create）] をクリックします。
修復の作成が完了すると、修復が編集モードで表示されます。

ステップ 22 [完了（Done）] をクリックして、関連インスタンスに戻ります。

ステップ 23 [キャンセル（Cancel）] をクリックすると、インスタンス リストに戻ります。

関連トピック

Nmap 修復オプション （2608 ページ）

Nmap 修復の編集

Nmap 修復に加えた変更は、進行中のスキャンには影響しません。新しい設定は、次回スキャンが開始されたときに有効になります。Nmap 修復が不要になったら削除します。

手順

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- **[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**を選択します。
- **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 編集する修復にアクセスします。

- 上記の最初の方法でリストにアクセスした場合は、関連するインスタンスの横にある [表示（View）]（👁） をクリックし、次に、[設定済み修復（Configured Remediations）] セクションで、編集する修復の横にある表示アイコンを再度クリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、編集する修復の横にある [表示（View）]（👁） をクリックします。

ステップ 3 Nmap 修復の作成 （2623 ページ）の説明に従って、必要に応じて変更を加えます。

ステップ 4 変更を保存する場合は[保存（Save）]をクリックし、保存せずに終了する場合は[完了（Done）]をクリックします。

ステップ 5 必要に応じて、その横にある [削除（Delete）]（） をクリックして修復を削除します。

オンデマンド Nmap スキャンの実行

オンデマンド Nmap スキャンは、いつでも必要なときに起動できます。スキャンする IP アドレスとポートを入力するか、既存のスキャン ターゲットを選択することで、オンデマンド スキャンのターゲットを指定できます。

Nmap によって提供されるサーバーやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。

始める前に

- 必要に応じて、Nmap スキャン ターゲットを追加します。Nmap スキャン ターゲットの追加 （2621 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 スキャンの実行時に使用する Nmap 修復の横にある **[スキャン（Scan）]**（） をクリックします。

ステップ 3 必要に応じて、保存済みのスキャン ターゲットを使用してスキャンする場合は、[保存済ターゲット（Saved Targets）] ドロップダウンリストからターゲットを選択して、[ロード（Load）]をクリックします。

ステップ 4 [IP 範囲（IP Range(s)）] フィールドで、スキャンするホストの IP アドレスを指定するかロードされたリストを変更します。

（注）

- IPv4 アドレスのホストの場合は、複数の IP アドレスをカンマで区切って指定するか、CIDR 表記を使用できます。感嘆符（!）を前に挿入して IP アドレスを否定することもできます。
- IPv6 アドレスのホストの場合は、厳密な IP アドレスを使用します。インターフェイスの範囲は入力できません。

ステップ 5 [Ports] フィールドで、スキャンするポートを指定するか、ロードされたリストを変更します。

ポート番号、カンマで区切ったポートのリスト、ハイフンで区切ったポート番号の範囲を入力できます。

ステップ 6 [今すぐスキャン（Scan Now）] をクリックします。

次のタスク

- 必要に応じて、タスクのステータスをモニターします。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Viewing Task Messages*」を参照してください。

Nmap スキャンの結果

進行中の Nmap スキャンをモニタし、Firepower システムによって実行されたスキャンの結果あるいは Firepower システム外部で行われたスキャンの結果をインポートして、スキャン結果を表示および分析することができます。

ローカル Nmap モジュールを使用して作成したスキャン結果を、レンダリングされたページとしてポップアップ ウィンドウで表示できます。Nmap 結果ファイルを raw XML 形式でダウンロードすることもできます。

Nmapによって検出されたオペレーティングシステムやサーバの情報を、ホストプロファイルやネットワークマップ内で参照することもできます。ホストのスキャンが生成するサーバー情報がフィルタ除去されているかクローズ状態のポートのサーバーに関する情報の場合、または、スキャンが収集した情報がオペレーティングシステム情報やサーバーのセクションに含めることができない情報の場合、それらの結果は、ホスト プロファイルの [Nmap スキャン結果（Nmap Scan Results）] セクションに含めることができます。

Nmap スキャン結果の表示

Nmap スキャンが完了したら、スキャン結果のテーブルを表示できます。

ユーザーは検索する情報に応じて結果のビューを操作することができます。スキャン結果にアクセスすると表示されるページは、使用するワークフローに応じて異なります。定義済みのワークフローを使用できます。このワークフローにはスキャン結果のテーブル ビューが含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

http://insecure.org で使用可能な Nmap バージョン 1.01 DTD を使用して Nmap の結果をダウンロードして表示することができます。

スキャン結果をクリアすることもできます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 ツールバーで、[スキャン結果（Scan Results）] をクリックします。

ステップ 3 次の選択肢があります。

- Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Event Time Constraints*」の説明に従って、時間範囲を調整します。
- カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。
- スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示するには、スキャン ジョブの横にある [表示（View）] をクリックします。
- テキスト エディタで raw XML コードを表示できるようにスキャン結果ファイルのコピーを保存するには、スキャン ジョブの横の [ダウンロード（Download）] をクリックします。
- スキャン結果をソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- 表示される列を制約するには、非表示にする列の見出しにある[閉じる（Close）]（×）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント
  他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ワークフローの次のページにドリルダウンするには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Using Drill-Down Pages*」を参照してください。
- スキャン インスタンスや修復を設定するには、ツールバーの [スキャナ（Scanners）] をクリックしてください（Nmap スキャンの管理 （2618 ページ） を参照）。
- ワークフローページ内およびワークフローページ間で移動するには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Workflow Page Navigation Tools*」を参照してください。
- その他のイベント ビューに移動して関連するイベントを表示するには、[ジャンプ（Jump to）] ドロップダウン リストから、表示するイベント ビューの名前を選択します。
- スキャン結果を検索するには、該当するフィールドに検索条件を入力します。

関連トピック

Nmap スキャン結果のフィールド （2628 ページ）

Nmap スキャン結果のフィールド

Nmap スキャンを実行すると、Firewall Management Center でデータベース内のスキャン結果が収集されます。次の表に、表示および検索できるスキャン結果テーブルのフィールドを示します。

表 *201* : スキャン結果のフィールド

フィールド	説明
Start Time	この結果を作成したスキャンの開始日時。
終了時間（End Time）	この結果を作成したスキャンの終了日時。
ターゲット（Target）	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）。
Scan Type	この結果を作成したスキャンのタイプを示す、`Nmap` またはサードパーティのスキャナ名。
スキャン モード（Scan Mode）	この結果を作成したスキャンのモード： • [オンデマンド（On Demand）]：オン デマンドで実行されたスキャンからの結果。 • [インポート済み（Imported）]：別のシステムでスキャンされてFirewall Management Centerにインポートされた結果。 • [スケジュール済み（Scheduled）]：スケジュール済みタスクとして実行されたスキャンからの結果。
結果	スキャンの結果。
ドメイン	スキャン ターゲットのドメイン。このフィールドは、マルチドメイン展開の場合にのみ存在します。

Nmap スキャン結果のインポート

システムの外部で実行されたNmapスキャンによって作成されたXML結果ファイルをインポートできます。以前にシステムからダウンロードしたXML結果ファイルもインポートできます。Nmap スキャン結果をインポートする場合、結果ファイルは XML 形式で、Nmap バージョン 1.01 DTD に準拠している必要があります。Nmap結果の作成と Nmap DTD の詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内に存在している必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[スキャナ（Scanners）]**を選択します。

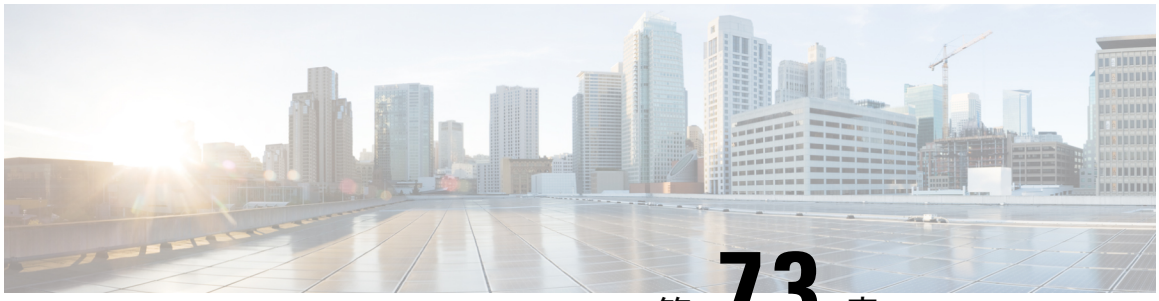
ステップ 2 ツールバーで、[結果のインポート（Import Results）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、結果ファイルに移動します。

ステップ 4 [インポートの結果（Import Results）] ページに戻ったら、[インポート（Import）] をクリックして結果をインポートします。

ホスト アイデンティティ ソースの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ホスト入力データ機能に対するセキュリティの改善	6.5	任意（Any）	TLS 1.2 が Firewall Management Center とホスト入力クライアント間の通信に使用されるようになりました。トピックホスト入力クライアントの設定（2606ページ）をこの情報について更新しました。



第 73 章

アプリケーションの検出

次のトピックでは、Firepower システム アプリケーション検出について説明します。

- 概要：アプリケーション検出 （2631 ページ）
- アプリケーション検出の要件と前提条件 （2639 ページ）
- カスタム アプリケーション ディテクタ （2639 ページ）
- ディテクタ詳細情報の表示またはダウンロード （2650 ページ）
- ディテクタ リストのソート （2651 ページ）
- ディテクタ リストのフィルタリング （2651 ページ）
- 他のディテクタ ページへの移動 （2653 ページ）
- ディテクタのアクティブおよび非アクティブの設定 （2653 ページ）
- カスタム アプリケーション ディテクタの編集 （2654 ページ）
- ディテクタの削除 （2655 ページ）

概要：アプリケーション検出

Firepower システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーションを制御するために不可欠です。

システムによって検出されるアプリケーションには以下の 3 種類があります。

- HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル
- Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント
- HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの *Web* アプリケーション

システムは、ディテクタに指定されている特性に従って、ネットワーク トラフィック内のアプリケーションを識別します。たとえば、システムはパケット ヘッダーに含まれる ASCII パターンによってアプリケーションを確認できます。加えて、Secure Socket Layer（SSL）プロトコル

ディテクタは、セキュアなセッションからの情報を使用して、セッションからアプリケーションを識別します。

Firepower システムのアプリケーション ディテクタには以下の 2 つのソースがあります。

- システム提供ディテクタ。Web アプリケーション、クライアント、およびアプリケーション プロトコルを検出します。

  アプリケーション（およびオペレーティング システム）に対して使用できるシステム提供ディテクタは、インストールされている Firepower システムのバージョンと VDB のバージョンによって異なります。リリース ノートとアドバイザリに、新しいディテクタと更新されたディテクタに関する情報が記載されています。また、プロフェッショナル サービスが作成した個別のディテクタをインポートすることもできます。

- カスタム アプリケーション プロトコル ディテクタ。Web アプリケーション、クライアント、アプリケーションプロトコルを検出するためにユーザーが作成するディテクタです。

また、暗黙的アプリケーション プロトコル検出を通してアプリケーション プロトコルを検出することもできます。これは、クライアントの検出に基づいてアプリケーションプロトコルの存在を推測するものです。

ネットワーク検出ポリシーで定義されているように、システムはモニタ対象ネットワーク内のホスト上で動作しているアプリケーションプロトコルだけを識別します。たとえば、モニタされていないリモート サイト上の FTP サーバに内部ホストがアクセスする場合、システムはアプリケーション プロトコルを FTP として識別しません。一方、モニタされているホスト上の FTP サーバにリモートまたは内部ホストがアクセスする場合、システムはアプリケーションプロトコルを肯定的に識別できます。

モニタ対象ホストが非モニタ対象サーバに接続するために使用するクライアントをシステムで識別できる場合、システムはクライアントの対応するアプリケーションプロトコルを識別することができますが、そのプロトコルをネットワーク マップに追加することはしません。アプリケーション検出が発生するためには、クライアントセッションにサーバからの応答が含まれている必要があることに注意してください。

システムは、検出した各アプリケーションの特徴を把握します（アプリケーションの特性（1734 ページ）を参照）。システムはこれらの特徴を使用して、アプリケーション フィルタと呼ばれるアプリケーションのグループを作成します。アプリケーション フィルタは、アクセス制御するため、およびレポートとダッシュボード ウィジェットで使用する検索結果とデータを制限するために使用されます。

また、エクスポートした NetFlow レコード、Nmap のアクティブ スキャン、ホスト入力機能を使用してアプリケーション ディテクタ データを補完することもできます。

関連トピック

アプリケーション制御の設定のベストプラクティス （1732 ページ）
アプリケーション ディテクタの基本 （2633 ページ）

アプリケーション ディテクタの基本

システムは、アプリケーションディテクタを使用して、ネットワーク上で一般的に使用されるアプリケーションを識別します。[ディテクタ（Detectors）] ページ（**[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]**）を使用してディテクタ リストを表示し、検出機能をカスタマイズします。

ディテクタまたはその状態（アクティブ/非アクティブ）を変更できるかどうかは、そのタイプによって異なります。システムは、アクティブなディテクタのみを使用して、アプリケーション トラフィックを分析します。

（注） シスコが提供するディテクタは、システムおよびVDBのアップデートによって変更される可能性があります。更新されたディテクタに関する情報については、リリースノートおよびアドバイザリを参照してください。

（注） Firepowerアプリケーションの識別のために、ポートは意図的にリストされていません。シスコのアプリケーションのいずれについても、アプリケーションの関連ポートは報告されません。これは、ほとんどのアプリケーションはポートに依存しないためです。シスコのプラットフォームの検出機能では、ネットワークのどのポートで実行されているサービスでも識別できます。

シスコが提供する内部ディテクタ

内部ディテクタは、クライアント、Webアプリケーション、およびアプリケーション プロトコルのトラフィック用の特別なディテクタ カテゴリです。内部ディテクタはシステム アップデートによって配信され、常にオンになっています。

アプリケーションがクライアント関連のアクティビティを検出するように設計された内部ディテクタと照合する場合で、特定のクライアントディテクタがない場合は、汎用クライアントが報告される場合があります。

シスコが提供するクライアント ディテクタ

クライアントディテクタは、クライアントトラフィックを検出し、VDBまたはシステム アップデートを介して配信されるか、またはCisco Professionalサービスによってインポート用に提供されます。クライアントディテクタを有効または無効にすることができます。インポートしたクライアント ディテクタのみエクスポートできます。

シスコが提供する Web アプリケーション ディテクタ

*Web*アプリケーションディテクタは、HTTPトラフィック ペイロード内のWebアプリケーションを検出し、VDB またはシステム アップデートを介して配信されます。Web アプリケーション ディテクタは常にオンになっています。

シスコが提供するアプリケーション プロトコル（ポート）ディテクタ

ポートベースのアプリケーション プロトコル ディテクタは、ウェルノウン ポートを使用してネットワーク トラフィックを識別します。これらはVDBまたはシステム アップデートを介して配信されるか、またはCisco Professionalサービスによってインポート用に提供されます。アプリケーション プロトコル ディテクタを有効または無効にしたり、カスタム ディテクタの基礎として使用するためにディテクタ定義を表示することができます。

シスコが提供するアプリケーション プロトコル（**Firepower**）ディテクタ

Firepower ベースのアプリケーション プロトコル ディテクタは、Firepowerアプリケーション フィンガープリントを使用してネットワーク トラフィックを分析し、VDB またはシステム アップデートを介して配信されます。アプリケーション プロトコル ディテクタを有効または無効にすることができます。

カスタム アプリケーション ディテクタ

カスタムアプリケーションディテクタはパターンベースです。クライアント、Webアプリケーション、またはアプリケーションプロトコルのトラフィックからのパケット内のパターンを検出します。インポートされたカスタム ディテクタを完全に制御できます。

Web インターフェイスでのアプリケーション プロトコルの識別

次の表に、検出されたアプリケーションプロトコルの識別方法の概略を示します。

表 *202 :* システムのアプリケーションプロトコルの識別

ID	説明
アプリケーション プロトコル名	Firewall Management Center は、次のアプリケーション プロトコルの場合に、名前でアプリケーション プロトコルを識別します。 • システムによって肯定的に識別された • NetFlowデータを使用して識別され、`/etc/sf/services`にポートとアプリケーション プロトコルの関連付けが存在する • ホスト入力機能を使用して手動で識別された • Nmap または別のアクティブな発生源によって識別された

ID	説明
pending	Firewall Management Center は、システムが肯定的と否定的のどちらでもアプリケーションを識別できない場合に、アプリケーション プロトコルを pending として識別します。 多くの場合、システムが保留中のアプリケーションを識別するには、より多くの接続データを収集して分析する必要があります。 [アプリケーションの詳細（Application Details）] および [サーバ（Servers）] テーブルやホスト プロファイルで pending ステータスが表示されるのは、特定のアプリケーション プロトコル トラフィック（検出されたクライアントまたは Web アプリケーション トラフィックから推論されたトラフィック以外）が検出されたアプリケーション プロトコルだけです。
unknown	Firewall Management Center は、以下の場合にアプリケーションプロトコルを unknown として識別します。 • アプリケーションがシステムのいずれのディテクタとも一致しない。 • アプリケーションプロトコルが NetFlow データを使用して識別されたが、/etc/sf/services にポートとアプリケーションプロトコルの関連付けが存在しない。 • Snort がセッションを閉じたが、デバイスにまだセッションが残っている。この場合、トラフィックはファイアウォールを通過できますが、アプリケーションは検出されません。
空白	使用可能なすべての検出データが検証されましたが、アプリケーション プロトコルが識別されませんでした。[アプリケーションの詳細（Application Details）] および [サーバー（Servers）] テーブルとホスト プロファイルでは、アプリケーション プロトコルが検出されなかった非 HTTP 汎用クライアント トラフィックに対して、アプリケーション プロトコルが空白として表示されます。

クライアント検出からの暗黙的アプリケーション プロトコル検出

非監視対象サーバにアクセスするために監視対象ホストが使用しているクライアントをシステムが識別できる場合、Firewall Management Center はその接続でクライアントに対応するアプリケーションプロトコルが使用されていると推測します（システムは監視対象ネットワーク上のアプリケーションだけを追跡するため、通常、接続ログには監視対象ホストが非監視対象サーバにアクセスしている接続に関するアプリケーションプロトコル情報が含まれていません）。

暗黙的アプリケーション プロトコル検出と呼ばれるこのプロセスの結果は次のようになります。

- システムはこれらのサーバの New TCP Port イベントまたは New UDP Port イベントを生成しないため、サーバが [サーバ（Servers）] テーブルに表示されません。加えて、これらの

アプリケーションプロトコルの検出を基準にして、検出イベントアラートまたは相関ルールをトリガーすることはできません。

- アプリケーション プロトコルはホストに関連付けられないため、ホスト プロファイルの詳細を表示したり、サーバ ID を設定したり、トラフィック プロファイルまたは相関ルールに関するホストプロファイル資格内の情報を使用したりできません。加えて、システムはこの種の検出に基づいて脆弱性とホストを関連付けません。

ただし、アプリケーションプロトコル情報が接続内に存在するかどうかに対する相関イベントをトリガーできます。また、接続ログ内のアプリケーションプロトコル情報を使用して、接続トラッカーとトラフィック プロファイルを作成できます。

ホスト制限と検出イベント ロギング

システムがクライアント、サーバ、または Web アプリケーションを検出すると、関連するホストがすでにクライアント、サーバ、または Web アプリケーションの最大数に達していなければ、検出イベントが生成されます。

ホスト プロファイルには、ホストごとに最大 16 のクライアント、100 のサーバ、および 100 の Web アプリケーションが表示されます。

クライアント、サーバ、または Web アプリケーションの検出によって異なるアクションはこの制限の影響を受けないことに注意してください。たとえば、サーバー上でトリガーするように設定されたアクセス コントロール ルールでは、引き続き、接続イベントが記録されます。

アプリケーション検出に関する特別な考慮事項

SFTP

SFTP トラフィックを検出するためには、同じルールが SSH も検出する必要があります。

Squid

システムは、次のいずれかの場合に Squid サーバ トラフィックを肯定的に識別します。

- モニタ対象ネットワーク上のホストからプロキシ認証が有効になっている Squid サーバへの接続をシステムが検出した場合
- モニタ対象ネットワーク上の Squid プロキシ サーバからターゲット システム（つまり、クライアントが情報または別のリソースを要求する宛先サーバ）への接続をシステムが検出した場合

ただし、システムは次の場合に Squid サービス トラフィックを識別できません。

- 監視対象ネットワーク上のホストが、プロキシ認証が無効になっている Squid サーバに接続している場合
- Squid プロキシ サーバが HTTP 応答から Via: ヘッダー フィールドを除去するように設定されている場合

SSL アプリケーション検出

システムは、Secure Socket Layer（SSL）セッションからのセッション情報を使用してセッション内のアプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションを識別するアプリケーション ディテクタを備えています。

システムは暗号化された接続を検出すると、その接続を汎用 HTTPS 接続として、または、該当する場合には SMTPS などのより特殊なセキュア プロトコルとしてマークします。システムは SSL セッションを検出すると、そのセッションに対する接続イベント内の **Client** フィールドに `SSL client` を追加します。セッションの Web アプリケーションが識別されると、システムでトラフィックの検出イベントが生成されます。

SSL アプリケーション トラフィックの場合は、管理対象デバイスも、サーバ証明書から一般名を検出して SSL ホスト パターンからのクライアントまたは Web アプリケーションと照合できます。システムが特定のクライアントを識別すると、`SSL client` をそのクライアントの名前に置き換えます。

SSL アプリケーション トラフィックは暗号化されるため、システムは暗号化されたストリーム内のアプリケーション データではなく、証明書内の情報しか識別に使用できません。そのため、SSL ホスト パターンではアプリケーションを制作した会社しか識別できない場合があり、同じ会社が作成した SSL アプリケーションは識別情報が同じ可能性があります。

HTTPS セッションが HTTP セッション内から起動される場合などは、管理対象デバイスがクライアント側のパケット内のクライアント証明書からサーバ名を検出します。

SSL アプリケーション識別を有効にするには、応答側のトラフィックを監視するアクセス コントロール ルールを作成する必要があります。このようなルールには、SSL アプリケーションに関するアプリケーション条件または SSL 証明書からの URL を使用した URL 条件を含める必要があります。ネットワーク検出では、応答側の IP アドレスがネットワーク上に存在しなくても、ネットワーク検出ポリシーでモニタできます。アクセス コントロール ポリシーの設定によって、トラフィックが識別されるかどうかが決まります。SSL アプリケーションの検出を識別するには、アプリケーション ディテクタ リストで、または、アプリケーション条件をアクセス コントロール ルールに追加するときに、`SSL protocol` タグでフィルタ処理します。

参照先 Web アプリケーション

Web サーバがトラフィックを他の Web サイト（通常は、アドバタイズメント サーバ）に参照する場合があります。ネットワーク上で発生するトラフィック参照のコンテキストをわかりやすくするために、システムは、参照セッションに対するイベント内の [Web アプリケーション（Web Application）] フィールドにトラフィックを参照した Web アプリケーションを列挙します。VDB に既知の照会先サイトのリストが含まれています。システムがこのようなサイトのいずれかからのトラフィックを検出すると、照会元サイトがそのトラフィックに対するイベントと一緒に保存されます。たとえば、Facebook 経由でアクセスされるアドバタイズメントが実際は Advertising.com 上でホストされている場合は、検出された Advertising.com トラフィックが Facebook Web アプリケーションに関連付けられます。また、システムは、Web サイトで他のサイトへの単リンクが提供されている場合などは、HTTP トラフィック内の参照元 URL を検出することもできます。この場合、参照元 URL は [HTTP 参照元（HTTP Referrer）] イベント フィールドに表示されます。

イベントでは、参照元アプリケーションが存在する場合に、それがトラフィックの Web アプリケーションとして列挙されますが、URL は参照先サイトの URL です。上の例では、トラフィックに対する接続イベントの Web アプリケーションは Facebook ですが、URL は Advertising.com です。参照元 Web アプリケーションが検出されない場合、ホストが自身を参照している場合、または参照がチェインしている場合は、参照先アプリケーションが Web アプリケーションとして表示される場合もあります。ダッシュボードでは、Web アプリケーションの接続カウントとバイト カウントに、Web アプリケーションが参照先のトラフィックに関連付けられたセッションが含まれます。

照会先トラフィックに対して明示的に機能するルールを作成する場合は、照会元アプリケーションではなく、照会先アプリケーションに関する条件を追加する必要があることに注意してください。Facebook から参照される Advertising.com トラフィックをブロックするには、Advertising.com アプリケーションのアクセス コントロール ルールにアプリケーション条件を追加します。

Snort 3 でのアプリケーション検出

（注） Snort 3 は、すべてのトラフィックを監視するために AppID を必要とする他の構成が AC ポリシーに存在しない場合、ネットワーク検出ポリシーフィルタで定義されている特定のネットワークサブネットでのみ AppID インスペクションを有効にするという点で、Snort 2 と同等になりました。

Snort 3 では、デフォルトですべてのネットワークに対してアプリケーション検出が常に有効になっています。アプリケーション検出を無効にするには、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]** を選択し、ポリシーの編集をクリックし、アプリケーション ルールを削除します。

ステップ 2 **[ポリシー（Policies）]** > **[SSL]** を選択し、[削除（Delete）] をクリックして SSL ポリシーを削除します。

ステップ 3 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択し、[削除（Delete）] をクリックしてネットワーク検出ポリシーを削除します。

ステップ 4 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]** を選択し、編集するポリシーの [編集（Edit）]（ ） をクリックします。次に **[セキュリティインテリジェンス（Security Intelligence）]** > **[URL（URLs）]** タブを選択して、URL の許可リストまたはブロックリストを削除します。

ステップ 5 デフォルトの DNS ルールは削除できないため、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[DNS]** を選択し、編集をクリックして、有効になっているボックスをオフにし、DNS ポリシーを無効にします。

ステップ 6 アクセス コントロール ポリシーの [詳細（Advanced）] 設定で、[Threat Intelligence Directorを有効にする（Enable Threat Intelligence Director）] および [DNSトラフィックへのレピュテーション適用を有効にする（Enable reputation enforcement on DNS traffic）] オプションを無効にします。

ステップ 7 アクセス コントロール ポリシーを保存して展開します。

アプリケーション検出の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 検出管理者（Discovery Admin）

カスタム アプリケーション ディテクタ

ネットワーク上でカスタムアプリケーションを使用する場合、アプリケーションの識別に必要な情報をシステムに提供するカスタム Web アプリケーション、クライアント、またはアプリケーションプロトコルディテクタを作成します。アプリケーションディテクタの種類は、[プロトコル（Protocol）]、[タイプ（Type）]、および [検出方向（Direction）] フィールドで選択した内容によって決まります。

システムがサーバ トラフィックでアプリケーション プロトコルの検出および識別を開始するように、クライアントセッションにサーバからの応答パケットを含める必要があります。UDP トラフィックの場合、応答パケットの送信元がサーバとして指定されることに注意してください。

すでに別の Firewall Management Center にディテクタを作成している場合、そのディテクタをエクスポートして、この Firewall Management Center にインポートすることができます。その後、必要に応じてインポートしたディテクタを編集できます。カスタム ディテクタおよび Cisco Professional サービスが提供するディテクタをエクスポートおよびインポートすることができます。ただし、シスコが提供するその他の種類のディテクタをエクスポートおよびインポートすることは**できません**。

カスタムアプリケーションディテクタおよびユーザー定義アプリケーション フィールド

次のフィールドを使用して、カスタム アプリケーション ディテクタおよびユーザー定義アプリケーションを設定できます。

カスタム アプリケーション ディテクタ フィールド：概要

基本および高度なカスタム アプリケーション ディテクタを設定するには、次のフィールドを使用します。

アプリケーション プロトコル（Application Protocol）

検出するアプリケーションプロトコル。これには、システムが提供するアプリケーションまたはユーザー定義のアプリケーションを指定できます。

アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグを使用してアプリケーション プロトコルを選択するか、作成する必要があります。

説明

アプリケーション ディテクタの説明。

[名前（Name）]

アプリケーション ディテクタの名前。

ディテクタ タイプ（Detector Type）

ディテクタのタイプ（[基本（Basic）] または [高度（Advanced）]）。基本的なアプリケーションディテクタは、一連のフィールドとして Web インターフェイスで作成されます。高度なアプリケーション ディテクタは、外部で作成され、カスタム .lua ファイルとしてアップロードされます。

カスタムアプリケーションディテクタ（Custom Application Detector）フィールド：検出パターン

基本的なカスタム アプリケーション ディテクタの検出パターンを設定するには、次のフィールドを使用します。

方向（Direction）

ディテクタが検出するトラフィックの送信元。[クライアント（Client）] または [サーバー（Server）]。

オフセット（Offset）

システムがパターンの検索を開始する必要がある、パケット ペイロードの先頭からのパケットの場所（バイト単位）。

パケット ペイロードは 0 バイトから始まるため、パケット ペイロードの先頭から数えたバイト数から 1 を減算することでオフセットを計算します。たとえば、パケットの 5 桁目

のビットパターンを検索するには、[オフセット（Offset）]フィールドに「4」と入力します。

パターン

パターン文字列は、選択した [タイプ（Type）] に関連付けられます。

ポート

ディテクタが検出するトラフィックのポート。

プロトコル

検出するプロトコル。選択するプロトコルによって、[タイプ（Type）]フィールドが表示されるか [URL（URL）] フィールドが表示されるかが決まります。

プロトコル（および、場合によっては、[タイプ（Type）]フィールドと [方向（Direction）] フィールドの後続の選択）によって、作成するアプリケーションディテクタのタイプ（Web アプリケーション、クライアント、またはアプリケーションプロトコル）が決まります。

ディテクタ タイプ（**Detector Type**）	プロトコル	タイプ（**Type**）または 方向（**Direction**）
Web アプリケーション（Web Application）	HTTP	[タイプ（Type）] は [コンテンツ タイプ（Content Type）] または [URL（URL）] です。
	RTMP	任意（Any）
	SSL	任意（Any）
クライアント	HTTP	[タイプ（Type）] は [ユーザー エージェント（User Agent）] です。
	SIP	任意（Any）
	TCP または UDP	[方向（Direction）] は [クライアント（Client）] です。
アプリケーション プロトコル（Application Protocol）	TCP または UDP	[方向（Direction）] は [サーバー（Server）] です。

タイプ（Type）

入力したパターン文字列のタイプ。表示されるオプションは、選択した [プロトコル（Protocol）] によって決まります。プロトコルとして [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりに [URL（URL）] フィールドが表示されます。

（注） [タイプ（Type）] として [ユーザー エージェント（User Agent）] を選択すると、システムはアプリケーションの [タグ（Tag）] を **User-Agent Exclusion** に自動的に設定します。

タイプの選択	文字列特性
Ascii	文字列は ASCII でエンコードされます。
Common Name	文字列は、サーバー応答メッセージ内の commonName フィールドの値です。
コンテンツ タイプ（Content Type）	文字列は、サーバー応答ヘッダー内のコンテンツ タイプ フィールドの値です。
16 進数	文字列は、16 進表記です。
組織	文字列は、サーバー応答メッセージ内の organizationName フィールドの値です。
SIP サーバー	文字列は、メッセージ ヘッダー内の From フィールドの値です。
SSL ホスト（SSL Host）	文字列は、ClientHello メッセージ内の server_name フィールドの値です。
URL	文字列は URL です。 （注） ディテクタは、ユーザーが入力する文字列が URL の完全なセクションであると想定します。たとえば、**cisco.com** と入力した場合、**www.cisco.com/support** や **www.cisco.com** と一致しますが、**www.wearecisco.com** とは一致しません。
ユーザー エージェント（User Agent）	文字列は、GET リクエスト ヘッダー内の user-agent フィールドの値です。これは SIP プロトコルにも使用可能であり、文字列が SIP メッセージ ヘッダー内の User-Agent フィールドの値であることを示します。

URL

RTMP パケットの C2 メッセージ内の swfURL フィールドの完全な URL または URL のセクション。[プロトコル（Protocol）] として [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりにこのフィールドが表示されます。

（注） ディテクタは、ユーザーが入力する文字列が URL の完全なセクションであると想定します。たとえば、**cisco.com** と入力した場合、**www.cisco.com/support** や **www.cisco.com** と一致しますが、**www.wearecisco.com** とは一致しません。

ユーザー定義のアプリケーション フィールド

基本および高度なカスタム アプリケーション ディテクタでユーザー定義のアプリケーションを設定するには、次のフィールドを使用します。

ビジネスとの関連性（Business Relevance）

アプリケーションが娯楽ではなく組織のビジネス活動のコンテキストで使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

カテゴリ

アプリケーションの最も基本的な機能を表す一般的な分類。

説明

アプリケーションの説明。

[名前（Name）]

アプリケーションの名前。

リスク（Risk）

アプリケーションが組織のセキュリティ ポリシーに対抗する目的で使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）] または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

タグ（Tags）

アプリケーションに関する追加情報を提供する 1 つ以上の事前定義されたタグ。アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグをアプリケーションに追加する必要があります。

カスタム アプリケーション ディテクタの設定

基本または高度なカスタム アプリケーション ディテクタを設定できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]** を選択します。

ステップ 2 [カスタム ディテクタの作成（Create Custom Detector）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 アプリケーション ドロップダウン リストから [アプリケーションプロトコル（Application Protocol）] を選択します。次の選択肢があります。

- 既存のアプリケーションプロトコルのディテクタを作成する場合（たとえば、非標準ポートで特定のアプリケーション プロトコルを検出する場合）、ドロップダウン リストからアプリケーション プロトコルを選択します。
- ユーザー定義アプリケーションのディテクタを作成する場合は、ユーザー定義アプリケーションを作成する （2645 ページ）に示されている手順に従います。

ステップ 5 [ディテクタタイプ（Detector Type）] として [基本（Basic）] または [高度（Advanced）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 [検出パターン（Detection Patterns）]、[検出基準（Detection Criteria）]、または [暗号化された可視性エンジンのプロセス割り当て（Encrypted Visibility Engine Process Assignments）] を設定します。

- 基本ディテクタを設定する場合は、基本ディテクタでの検出パターンの指定 （2646ページ）の説明に従って、プリセットした [検出パターン（Detection Patterns）] を指定します。
- 高度なディテクタを設定する場合は、高度なディテクタでの検出条件の指定 （2647ページ）の説明に従って、カスタム [検出基準（Detection Criteria）] を指定します。
- 暗号化された可視性エンジン（EVE）検出器を設定している場合は、この章の「*EVE* のプロセス割り当ての指定」で説明されているように、カスタム EVE プロセス割り当てを指定します。

注意
高度なカスタムディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

ステップ 8 必要に応じて、カスタムアプリケーションプロトコルディテクタのテスト （2649 ページ）の説明に従って、[パケット キャプチャ（Packet Captures）] を使用して新しいディテクタをテストします。

ステップ 9 [保存（Save）] をクリックします。

（注）

アクセス コントロール ルールにアプリケーションを含めると、ディテクタは自動的にアクティブにされ、使用中は非アクティブにできません。

次のタスク

- ディテクタのアクティブおよび非アクティブの設定（2653ページ）の説明に従ってディテクタをアクティブにします。

関連トピック

カスタム アプリケーション ディテクタおよびユーザー定義アプリケーション フィールド（2640 ページ）

ユーザー定義アプリケーションを作成する

ここで作成するアプリケーション、カテゴリ、およびタグは、アクセス コントロール ルールやアプリケーション フィルタ オブジェクト マネージャで使用できます。

注意 ユーザー定義アプリケーションを作成すると、展開プロセスを経由することなく、ただちにSnort プロセスが再起動します。Snort プロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作（165 ページ）を参照してください。

始める前に

- カスタム アプリケーション ディテクタの設定（2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [カスタムのアプリケーションディテクタを作成する（Create A Custom Application Detector）] ダイアログボックスで、[アプリケーション（Application）]フィールドの横にある[追加（Add）]（＋）をクリックします。

ステップ 2 [名前（Name）] を入力します。

ステップ 3 [説明（Description）] を入力します。

ステップ 4 [ビジネスとの関連性（Business Relevance）] を選択します。

ステップ 5 [リスク（Risk）] を選択します。

ステップ 6 [カテゴリ（Categories）] の横にある [追加（Add）] をクリックしてカテゴリを追加し、新しいカテゴリの名前を入力するか、または [カテゴリ（Categories）] ドロップダウン リストから既存のカテゴリを選択します。

ステップ 7 （オプション）タグの横にある **[追加（Add）]** をクリックして、新しいタグを入力するか、**[タグ（Tags）]** ドロップダウンリストで既存のタグを選択します。

ステップ 8 [OK] をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

カスタム アプリケーション ディテクタおよびユーザー定義アプリケーション フィールド（2640 ページ）

基本ディテクタでの検出パターンの指定

アプリケーション プロトコルのパケット ヘッダーで特定のパターン文字列を検索するよう、カスタム アプリケーション プロトコル ディテクタを設定できます。また、複数のパターンを検索するようにディテクタを設定することもできます。この場合は、アプリケーションプロトコルのトラフィックは、アプリケーションプロトコルを確実に識別するため、ディテクタのすべてのパターンとマッチングさせる必要があります。

アプリケーション プロトコル ディテクタは、オフセットを使用して ASCII または 16 進数のパターンを検索できます。

始める前に

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページの [検出パターン（Detection Patterns）] セクションで、[追加（Add）] をクリックします。

ステップ 2 [アプリケーション（Application）] ドロップダウンリストからプロトコルタイプを選択します。

ステップ 3 [タイプ（Type）] ドロップダウンリストからパターンタイプを選択します。

ステップ 4 指定した [タイプ（Type）] に一致する [パターン（Pattern）] 文字列を入力します。

ステップ 5 オプションで、[オフセット（Offset）] を入力します（バイト単位）。

ステップ 6 オプションで、使用するポートに基づいてアプリケーションプロトコルのトラフィックを指定するには、1 から 65535 までのポートを [ポート（Port(s)）] フィールドに入力します。複数のポートを使用する場合は、カンマで区切ります。

ステップ 7 [方向（Direction）] : [クライアント（Client）] または [サーバー（Server）] をクリックします。

ステップ 8 [OK] をクリックします。

ヒント

パターンを削除する場合は、削除するパターンの横にある [削除（Delete）]（🗑）をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

高度なディテクタでの検出条件の指定 （2647 ページ）

高度なディテクタでの検出条件の指定

⚠

注意 高度なカスタムディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

⚠

注意 信頼できないソースから .lua ファイルをアップロードしないでください。

カスタム .lua ファイルには、カスタム アプリケーションのディテクタ設定を含めます。カスタム .lua ファイルを作成するには、lua プログラミング言語に関する高度な知識とシスコの C-lua API に関する経験が求められます。以下を使用して、.lua ファイルを準備することを強くお勧めします。

- lua プログラミング言語に関するサードパーティの説明書と参考資料
- オープン ソース ディテクタ開発者ガイド： https://www.snort.org/downloads
- OpenAppID Snort コミュニティ リソース： http://blog.snort.org/search/label/openappid

（注） システムは、システム コールまたはファイル I/O を参照する .lua ファイルをサポートしていません。

始める前に

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。
- 該当する .lua ファイルをダウンロードし、内容を調べることによって、有効な .lua ファイルを作成する準備を進めます。ディテクタ ファイルのダウンロードの詳細については、ディテクタ詳細情報の表示またはダウンロード （2650 ページ）を参照してください。
- カスタム アプリケーションのディテクタ設定を含む有効な .lua ファイルを作成します。

手順

ステップ 1 高度なカスタム アプリケーション ディテクタの [ディテクタの作成（Create Detector）] ページにある [検出条件（Detection Criteria）] セクションで、[追加（Add）] をクリックします。

ステップ 2 [参照...（Browse...）] をクリックして、**`.lua`** ファイルに移動し、アップロードします。

ステップ 3 [OK] をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

基本ディテクタでの検出パターンの指定 （2646 ページ）

EVE のプロセス割り当ての指定

暗号化された可視性エンジン（EVE）で検出されたプロセスを新しいアプリケーションか既存のアプリケーションにマッピングするように、独自のカスタム アプリケーション ディテクタを設定できます。

始める前に

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページの [暗号化された可視性エンジンのプロセス割り当て（Encrypted Visibility Engine Process Assignments）] セクションで、[追加（Add）] をクリックします。

ステップ 2 [プロセス名（Process Name）] と [最小プロセス確実性（Minimum Process Confidence）] の値を入力します。

（注）
[プロセス名（Process Name）] フィールドにテキストを入力できますが、このフィールドでは大文字と小文字が区別されます。この値は、EVE で検出された正確なプロセス名と一致している必要があります。[最小プロセス確実性（Minimum Process Confidence）] には、0 ～ 100 までの任意の数値を指定できます。ここで指定するのは、接続イベントの [暗号化された可視性プロセスの確実性スコア（ncrypted Visibility Process Confidence Score）] フィールドに表示される数値です。

[暗号化された可視性プロセスの確実性スコア（Encrypted Visibility Process Confidence Score）] フィールドの詳細については、『Cisco Firepower Management Center Administration Guide』の「*Connection and Security Intelligence Event Fields*」セクションを参照してください。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 [アプリケーションディテクタリスト（Application Detector listing）] ページで、作成したディテクタをアクティブ化します。詳細については、ディテクタのアクティブおよび非アクティブの設定（2653ページ）を参照してください。ディテクタをアクティブにすると、Firewall Management Center に登録されているすべての FTD にディテクタファイルがプッシュされます。

次のタスク

- カスタム アプリケーション ディテクタの設定（2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

カスタム アプリケーション プロトコル ディテクタのテスト

検出するアプリケーションプロトコルからのトラフィックを持つパケットが格納されたパケット キャプチャ（pcap）ファイルが存在する場合、その pcap ファイルに対してカスタム アプリケーション プロトコル ディテクタをテストできます。シスコでは、不要なトラフィックのない単純でクリーンな pcap ファイルを使用することをお勧めします。

pcap ファイルは 256 KB 以下でなければなりません。それより大きい pcap ファイルに対してディテクタのテストを試行すると、Firewall Management Center は自動的にファイルを切り捨

て、不完全なファイルをテストします。ディテクタをテストするためにファイルを使用する前に、pcap の未解決のチェックサムを修正する必要があります。

始める前に

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタを設定します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページの [パケット キャプチャ（Packet Captures）] セクションで、[追加（Add）] をクリックします。

ステップ 2 ポップアップ ウィンドウで pcap ファイルを参照し、[OK] をクリックします。

ステップ 3 pcap ファイルの内容に対してディテクタをテストするには、pcap ファイルの横にある評価アイコンをクリックします。メッセージに、テストが成功したかどうかが示されます。

ステップ 4 必要に応じて手順 1 ～ 3 を繰り返し、その他の pcap ファイルに対してディテクタをテストします。

ヒント

pcap ファイルを削除するには、削除するファイルの横にある [削除（Delete）]（🗑）をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2643 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

ディテクタ詳細情報の表示またはダウンロード

ディテクタ リストを使用して、アプリケーション ディテクタの詳細を表示（すべてのディテクタ）したり、ディテクタの詳細をダウンロード（カスタム アプリケーション ディテクタのみ）したりできます。

手順

ステップ 1 アプリケーション ディテクタの詳細を表示するには、次のいずれかを実行します。

- 関連する VDB バージョンについては、https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html の『*Cisco Firepower Application Detector Reference*』[英語] を参照してください。
- a. **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]** を選択します。

  b. リストをフィルタ処理して、特定のディテクタを検索します。

  c. **情報**（ ） をクリックします。

ステップ 2 カスタム アプリケーション ディテクタのディテクタ詳細をダウンロードするには、[ダウンロード（download）]（ ） をクリックします。

コントロールが淡色表示されている場合、設定が先祖ドメインに属しているか、またはユーザが必要な権限を持っていません。

ディテクタ リストのソート

[ディテクタ（Detectors）] ページには、デフォルトで名前のアルファベット順にディテクタがリストされます。列見出しの横にある上または下矢印は、ページがその列でその方向にソートされていることを示します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]** を選択します。

ステップ 2 該当する列見出しをクリックします。

ディテクタ リストのフィルタリング

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]** を選択します。

ステップ 2 ディテクタ リストのフィルタ グループ （2652 ページ）に記載されているフィルタ グループの 1 つを展開し、フィルタの横にあるチェックボックスを選択します。グループ内のすべてのフィルタを選択するには、グループ名を右クリックし、[すべて選択（Check All）] を選択します。

ステップ 3 あるフィルタを削除するには、[フィルタ（Filters）] フィールドにあるフィルタの名前の**削除**（×）をクリックするか、フィルタリストでフィルタを無効にします。グループ内のすべてのフィルタを削除するには、グループ名を右クリックし、[すべて選択解除（Uncheck All）] を選択します。

ステップ 4 すべてのフィルタを削除するには、検出機能に適用されるフィルタ リストの横の [すべてクリア（Clear all）] をクリックします。

ディテクタ リストのフィルタ グループ

複数のフィルタ グループを別個にまたは組み合わせて使用し、ディテクタのリストをフィルタリングすることができます。

名前（Name）

ユーザが入力した文字列を含む名前または説明でディテクタを検索します。文字列には任意の英数字または特殊文字を含めることができます。

カスタム フィルタ（Custom Filter）

オブジェクト管理ページで作成したカスタム アプリケーション フィルタに一致するディテクタを検索します。

作成者（Author）

ディテクタを作成したユーザに照らしてディテクタを検索します。次によってディテクタをフィルタリングできます。

- カスタム ディテクタを作成またはインポートした個々のユーザ
- Cisco。これは、個別にインポートされたアドオン ディテクタを除く、シスコが提供するすべてのディテクタを表します（ディテクタをインポートした場合、そのユーザはそのディテクタの作成者になります）。
- 任意のユーザ（Any User）。これは、によって提供されたのではないすべてのディテクタを表します。

状態（State）

状態（つまり、アクティブまたは非アクティブ）に照らしてディテクタを検索します。

タイプ

アプリケーションディテクタの基本（2633ページ）に示すように、ディテクタ タイプに従ってディテクタを検索します。

プロトコル

ディテクタが検査するトラフィック プロトコルに照らしてディテクタを検索します。

カテゴリ（Category）

検出するアプリケーションに割り当てられたカテゴリに照らしてディテクタを検索します。

タグ

検出するアプリケーションに割り当てられたタグに照らしてディテクタを検索します。

リスク（Risk）

検出するアプリケーションに割り当てられたリスク（Very High、High、Medium、Low、Very Low）を基準にディテクタを検索します。

ビジネスとの関連性（Business Relevance）

検出するアプリケーションに割り当てられたビジネスとの関連性（[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、[非常に低い（Very Low）]）に照らしてディテクタを検索します。

他のディテクタ ページへの移動

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]** を選択します。

ステップ 2 次のページを表示するには、[右矢印（right arrow）]（ > ）をクリックします。

ステップ 3 前のページを表示するには、[左矢印（Left Arrow）]（ < ）をクリックします。

ステップ 4 別のページを表示するには、ページ番号を入力して、Enter キーを押します。

ステップ 5 最後のページに移動するには、[右端矢印（right end arrow）]（ >| ）をクリックします。

ステップ 6 最初のページに移動するには、[左端矢印（Left End Arrow）]（ |< ）をクリックします。

ディテクタのアクティブおよび非アクティブの設定

ネットワーク トラフィックを分析するためにディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。

システムの検出機能を補完するために、ポートごとに複数のアプリケーションディテクタをアクティブにすることができます。

ポリシーのアクセス コントロール ルールにアプリケーションを含め、そのポリシーを導入するときに、そのアプリケーションに対してアクティブなディテクタがない場合、1つ以上のディテクタが自動的にアクティブになります。同様に、導入されているポリシーのアプリケーションが使用されているときに、そのアプリケーションのアクティブなディテクタをすべて非アクティブにしようとしても、ディテクタを非アクティブにすることはできません。

ヒント パフォーマンスを向上させるために、使用する予定のないアプリケーションプロトコル、クライアント、または Web アプリケーションのディテクタはすべて非アクティブにします。

注意 システムまたはカスタムのアプリケーション ディテクタをアクティブ化/非アクティブ化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細は Snort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーションディテクタ（Application Detectors）]** を選択します。

ステップ 2 アクティブまたは非アクティブにするディテクタの横にあるスライダをクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

（注）
一部のアプリケーションディテクタはその他のディテクタによって必要とされることに注意してください。そのようなディテクタのいずれかを非アクティブにすると、それに依存するディテクタも無効となることを示す警告が表示されます。

カスタム アプリケーション ディテクタの編集

カスタム アプリケーション ディテクタを変更するには、次の手順を使用します。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーションディテクタ（Application Detectors）]** を選択します。

ステップ 2 変更するディテクタの横にある[編集（Edit）]（）をクリックします。代わりに[表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 カスタムアプリケーションディテクタの設定 （2643 ページ）の説明に従って、ディテクタを変更します。

ステップ 4 ディテクタの状態に応じて、次の保存オプションがあります。

- 非アクティブなディテクタを保存するには、[保存（Save）] をクリックします。
- 非アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。
- アクティブなディテクタを保存してすぐに使用を開始するには、[保存して再アクティブ化（Save and Reactivate）] をクリックします。

  注意
  カスタム アプリケーション ディテクタを保存して再びアクティブ化すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snortプロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

- アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。

ディテクタの削除

カスタムディテクタおよびCisco Professionalサービスが提供する個別にインポートされたアドオンディテクタを削除することができます。その他のCiscoが提供するディテクタを削除することはできませんが、その多くを非アクティブにすることはできます。

（注） ディテクタが展開されたポリシーで使用されている間は、そのディテクタを削除できません。

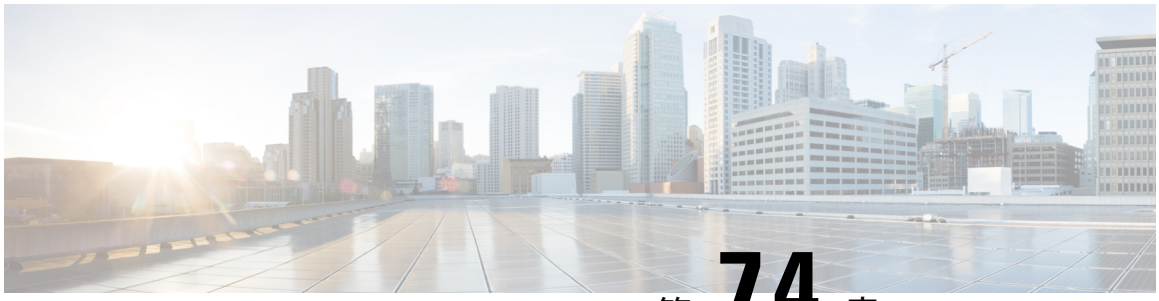
注意 アクティブ化されたカスタム アプリケーション ディテクタを削除すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snortプロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーションディテクタ（Application Detectors）]** を選択します。

ステップ 2 削除するディテクタの横にある [削除（Delete）]（） をクリックします。 代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 **[OK]** をクリックします。



第 74 章

ネットワーク検出ポリシー

以下のトピックでは、ネットワーク検出ポリシーを作成、設定、管理する方法について説明します。

- 概要：ネットワーク検出ポリシー （2657 ページ）
- ネットワーク検出ポリシーの要件と前提条件 （2658 ページ）
- ネットワーク検出のカスタマイズ （2658 ページ）
- ネットワーク検出ルール （2660 ページ）
- 高度なネットワーク検出オプションの設定 （2671 ページ）
- ネットワーク検出戦略のトラブルシューティング （2681 ページ）

概要：ネットワーク検出ポリシー

Firewall Management Center 上のネットワーク検出ポリシーは、システムが組織のネットワークアセットに関するデータを収集する方法と、どのネットワークセグメントとポートをモニタ対象とするかを制御します。

システムがモニターしてトラフィック内のネットワークデータに基づいて検出データを生成するネットワークとポート、およびポリシーを展開するゾーンは、ポリシー内の検出ルールで指定します。ルール内では、ホスト、アプリケーション、権限のないユーザを検出するかどうかを設定できます。検出からネットワークとゾーンを除外するルールを作成できます。NetFlow エクスポータからのデータの検出を設定して、ネットワーク上でユーザデータが検出されるトラフィックのプロトコルを制限できます。

ネットワーク検出ポリシーに用意されている単一のデフォルトルールは、すべてのモニタ対象トラフィックからアプリケーションを検出するように設定されています。このルールが除外するネットワーク、ゾーン、ポートはなく、ホストとユーザの検出も設定されていません。また、このルールは NetFlow エクスポータをモニタするように設定されてはいません。このポリシーは、管理対象デバイスが Firewall Management Center に登録されると、デフォルトでそのデバイスに導入されます。ホストまたはユーザデータの収集を開始するには、検出ルールを追加または変更して、ポリシーをデバイスに再展開する必要があります。

ネットワーク検出の範囲を調整する場合は、追加の検出ルールを作成して、デフォルトルールを変更または削除できます。

管理対象デバイスごとのアクセス コントロール ポリシーは、そのデバイスに許可されたトラフィック、つまり、ネットワーク検出を使用してモニタ可能なトラフィックを定義することに注意してください。アクセスコントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションのアクティビティに関するトラフィックを検査できなくなります。たとえば、アクセスコントロールポリシーでソーシャルネットワーキングアプリケーションへのアクセスをブロックすると、システムはそれらのアプリケーションに関する検出データを一切提供できなくなります。

検出ルールでトラフィック ベースのユーザ検出を有効にすると、一連のアプリケーション プロトコル全体のトラフィック内のユーザ ログイン アクティビティを通して権限のないユーザを検出できます。必要に応じて、すべてのルールにわたって特定のプロトコル内の検出を無効にできます。一部のプロトコルを無効にすると、Firewall Management Center モデルに関連付けられたユーザ制限に達するのを防ぐのに役立ち、他のプロトコルからのユーザに使用可能なユーザ カウントを確保できます。

詳細ネットワーク検出設定を使用すれば、記録するデータの種類、検出データの保存方法、アクティブにする侵害の兆候（IOC）ルール、影響評価に使用する脆弱性マッピング、送信元からの検出データが競合していた場合の対処を管理できます。また、ホスト入力の送信元やNetFlow エクスポータをモニター対象として追加することもできます。

ネットワーク検出ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

リーフ

ユーザの役割

- 管理者
- 検出管理者（Discovery Admin）

ネットワーク検出のカスタマイズ

Firepower システムによって収集されるネットワーク トラフィックに関する情報は、この情報を関連付けて最も脆弱で最も重要なネットワークのホストを識別することができる場合に、最もその価値を発揮します。

たとえば、ネットワーク上に SuSE Linux のカスタマイズ バージョンを実行している複数のデバイスがある場合、システムはそのオペレーティング システムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに

SuSE Linux に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行する他のホストを識別するために使用できるカスタム フィンガープリントを、ホストのいずれか 1 台に対して作成することができます。フィンガープリントに SuSE Linux の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

また、ホストの入力機能を使用して、ホスト データをサードパーティ システムからネットワーク マップに直接入力することもできます。ただし、サードパーティのオペレーティング システムやアプリケーション データは、脆弱性情報に自動的にマッピングされません。脆弱性を確認し、サードパーティのオペレーティング システム、サーバ、アプリケーション プロトコル データを使用してホストの影響の関連付けを実行する場合、サードパーティ システムからのベンダーとバージョンの情報を、脆弱性データベース（VDB）にリストされているベンダーとバージョンにマッピングする必要はあります。また、ホストの入力データを継続的に維持する必要がある場合もあります。アプリケーション データを Firepower システムのベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムがネットワーク上のホストで実行されているアプリケーション プロトコルを識別できない場合は、システムがポートまたはパターンに基づいてアプリケーションを識別できるようにする、ユーザ定義のアプリケーション プロトコル ディテクタを作成できます。また、特定のアプリケーション ディテクタをインポートしたり、アクティブ/非アクティブにしたりすることによって、Firepower システムのアプリケーション検出機能をカスタマイズすることができます。

さらに、Nmap アクティブ スキャナのスキャン結果を使用してオペレーティング システムやアプリケーション データの検出を置き換えたり、サードパーティの脆弱性で脆弱性リストを拡張したりすることもできます。システムは複数のソースからのデータを照合して、アプリケーションの ID を判別できます。

ネットワーク検出ポリシーの設定

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 ポリシーの次のコンポーネントを設定します。

- 検出ルール：ネットワーク検出ルールの設定 （2661 ページ）を参照してください。
- ユーザのトラフィックベースの検出：トラフィックに基づくユーザー検出の設定（2670 ページ）を参照してください。
- 高度なネットワーク検出オプション：高度なネットワーク検出オプションの設定（2671 ページ）を参照してください。

- カスタム オペレーティング システム定義（フィンガープリント）：クライアント用のカスタムフィンガープリントの作成（2591 ページ）およびサーバー用のカスタムフィンガープリントの作成 （2594 ページ）を参照してください。

ネットワーク検出ルール

ネットワーク検出ルールを使用すれば、ネットワーク マップに対して検出される情報を調整し、必要な特定のデータだけを含めるようにすることができます。ネットワーク検出ポリシー内のルールは順番に評価されます。モニタリング基準が重複したルールを作成できますが、その場合はシステム パフォーマンスに影響する可能性があります。

モニタリングからホストまたはネットワークを除外すると、そのホストまたはネットワークがネットワーク マップに表示されず、それに対するイベントが報告されません。ただし、ローカル IP のホスト検出ルールが無効になっている場合、検出エンジンインスタンスは既存のホストデータを使用せずに各フローから新たにデータを構築するため、より高い処理負荷の影響を受けます。

モニタリングからロードバランサ（またはロードバランサ上の特定のポート）と NAT デバイスを除外することを推奨します。これらのデバイスは紛らわしいイベントを過剰に生成するため、データベースがいっぱいになったり、Firewall Management Center が過負荷になったりする可能性があります。たとえば、モニター対象 NAT デバイスが短期間にオペレーティング システムの複数の更新を表示する場合があります。ロードバランサと NAT デバイスの IP アドレスがわかっている場合は、モニタリングからそれらを除外できます。

ヒント システムは、ネットワーク トラフィックを検査することにより、複数のロード バランサと NAT デバイスを識別できます。

加えて、カスタム サーバ フィンガープリントを作成する必要がある場合は、フィンガープリントを行っているホストとの通信に使用されている IP アドレスをモニタリングから一時的に除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。フィンガープリントを作成したら、その IP アドレスをモニタするようにポリシーを設定し直すことができます。

シスコでは、NetFlow エクスポータと管理対象デバイスを使用して、同じネットワークセグメントをモニター**しない**ことも推奨しています。重複しないルールを使用してネットワーク検出ポリシーを設定するのが理想です。管理対象デバイスによって生成された重複接続ログはシステムによって破棄されます。ただし、管理対象デバイスと NetFlow エクスポータの両方で検出された接続に関する重複接続ログを破棄することは**できません**。

ネットワーク検出ルールの設定

検出ルールを設定し、ニーズに合わせてホスト データとアプリケーション データの検出を調整できます。

ヒント　ほとんどの場合、RFC 1918 のアドレスに検出を制限することを推奨します。

始める前に

- ネットワークデータを検出するトラフィックの接続を記録していることを確認します。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「*Best Practices for Connection Logging*」を参照してください。
- エクスポートされた NetFlow レコードを収集する場合は、NetFlow エクスポータのネットワーク検出ポリシーへの追加（2677 ページ）の説明に従って NetFlow エクスポータを追加します。
- 検出パフォーマンス グラフを表示するには、検出ルールでホスト、ユーザー、およびアプリケーションを有効にする必要があります。これは、システム パフォーマンスに影響を与える可能性があることに注意してください。

手順

ステップ 1　**[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2　[ルールの追加（Add Rule）] をクリックします。

ステップ 3　アクションと検出されるアセット（2662 ページ）の説明に従って、ルールの [アクション（Action）] を設定します。

ステップ 4　オプションの検出パラメータを設定します。

- ルール アクションを特定のネットワークに制限します。モニター対象ネットワークの制限（2663 ページ）を参照してください。
- ルール アクションを特定のゾーン内のトラフィックに制限します。ネットワーク検出ルールのゾーンの設定（2667 ページ）を参照してください。
- ポートをモニターリングから除外します。ネットワーク検出ルールでのポート除外（2666 ページ）を参照してください。
- NetFlow データ検出のルールの設定します。NetFlow データ検出のルールの設定（2664 ページ）を参照してください。

ステップ 5　[保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

アクションと検出されるアセット

検出ルールを設定する場合は、ルールのアクションを選択する必要があります。アクションの効果は、管理対象デバイスとNetFlowエクスポータのどちらからデータを検出するルールを使用しているかによって異なります。

次の表に、これら2つのシナリオで指定されたアクション設定を使用したルールで検出されるアセットの説明を示します。

表 *203 :* 検出ルールのアクション

操作	オプション	管理対象デバイス	NetFlow エクスポータ
除外（Exclude）	--	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。
Discover	ホスト（Hosts）	検出イベントに基づいて、ネットワークマップにホストを追加します。（任意。ユーザ検出が有効になっていない場合は必須）。	NetFlow レコードに基づいて、ネットワーク マップにホストを追加し、接続をログに記録します。（必須）
Discover	アプリケーション	アプリケーション検出に基づいて、ネットワーク マップにアプリケーションを追加します。アプリケーションも検出しないルールでは、ホストまたはユーザを検出できないことに注意してください。（必須）	NetFlow レコードと `/etc/sf/services` 内のポートとアプリケーションプロトコルの関連付けに基づいて、ネットワーク マップにアプリケーションプロトコルを追加します。（オプション）
Discover	ユーザー	ネットワーク検出ポリシーで設定されたユーザープロトコルに関するトラフィック ベースの検出に基づいてユーザーをユーザー テーブルに追加し、ユーザー アクティビティをログに記録します。（オプション）	適用対象外
NetFlow接続のロギング（Log NetFlow Connections）	--	適用対象外	NetFlow 接続のみをログに記録します。ホストまたはアプリケーションは検出しません。

ルールを使用して管理対象デバイスのトラフィックをモニタする場合は、アプリケーション ロギングが必要です。ルールを使用してユーザをモニタする場合は、ホスト ロギングが必要で

す。ルールを使用して、エクスポートされたNetFlowレコードをモニタする場合は、ユーザをログに記録するように設定することはできず、アプリケーション ロギングは任意です。

（注） ネットワーク検出ポリシーの[アクション（Action）]の設定に基づいて、エクスポートされたNetFlowレコードで接続が検出されます。アクセス コントロール ポリシーの設定に基づいて、管理対象デバイス ラフィックで接続が検出されます。

モニター対象ネットワーク

検出ルールは、モニタ対象アセットの検出を、指定されたネットワーク上のホストとの間のトラフィックだけを対象にして行います。検出ルールでは、指定されたネットワーク内の1つ以上のIPアドレスが割り当てられた接続に対して検出が行われ、モニタ対象ネットワーク内のIPアドレスに対してのみイベントが生成されます。デフォルトの検出ルールでは、モニタされているすべてのトラフィックのアプリケーションを検出します（すべてのIPv4トラフィックについては`0.0.0.0/0`、すべてのIPv6トラフィックについては`::/0`）。

NetFlow検出を処理し、接続データだけを記録するルールを設定すると、システムは、指定のネットワークの接続元と接続先のIPアドレスを記録します。ネットワーク検出ルールがNetFlowネットワーク接続を記録する唯一の方法を提供することに注意してください。

また、ネットワーク オブジェクトまたはオブジェクト グループを使用してモニター対象ネットワークを指定することもできます。

モニター対象ネットワークの制限

すべての検出ルールに1つ以上のネットワークを含める必要があります。

手順

ステップ1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択します。

ステップ2 [ルールの追加（Add Rule）]をクリックします。

ステップ3 [ネットワーク（Networks）]をクリックします（表示されていない場合）。

ステップ4 （オプション）[使用可能なネットワーク（Available Networks）]リストにネットワークオブジェクトを追加します。詳細については、「ディスカバリ ルール設定時にネットワーク オブジェクトを作成する （2665ページ）」を参照してください。

ネットワーク検出ポリシーで使用されるネットワーク オブジェクトを変更した場合、その変更は設定の変更を展開するまで反映されません。

ステップ5 ネットワークを指定します。

- [使用可能なネットワーク（Available Networks）]リストからネットワークを選択します。ネットワークがすぐにリストに表示されない場合は、**リロード**（）をクリックします。

- [使用可能なネットワーク（Available Networks）] ラベルの下にあるテキスト ボックスに IP アドレスを入力します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

NetFlow データ検出のルールの設定

システムは、NetFlow エクスポータからのデータを使用して、接続および検出イベントを生成し、ネットワークマップにホストとアプリケーションのデータを追加できます。

検出ルール内で NetFlow エクスポータを選択する場合、ルールは指定されたネットワークの NetFlow データの検出に制限されます。NetFlow デバイスを選択すると使用可能なルール アクションが変更されるため、モニターする NetFlow デバイスを選択してからルール動作の他の側面を設定します。NetFlow エクスポータをモニターするためのポートの除外を設定することはできません。

始める前に

- NetFlow-enabled デバイスをネットワーク検出ポリシーに追加します。NetFlow エクスポータのネットワーク検出ポリシーへの追加 （2677 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [NetFlow デバイス（NetFlow Device）] を選択します。

ステップ 4 [NetFlowデバイス（NetFlow Device）] ドロップダウンリストから、モニターする NetFlow エクスポータの IP アドレスを選択します。

ステップ 5 システムの管理対象デバイスで収集する NetFlow データのタイプを指定します。

- 接続のみ：[アクション（Action）] ドロップダウン リストから `Log NetFlow Connections` を選択します。
- ホスト、アプリケーション、および接続：[アクション（Action）] ドロップダウン リストから `Discover` を選択します。[ホスト（Hosts）]チェックボックスが自動的にオンになり、接続データの収集が有効になります。オプションで、[アプリケーション]チェックボックスをオンにして、アプリケーション データを収集できます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ディスカバリ ルール設定時にネットワーク オブジェクトを作成する

新規ネットワーク オブジェクトを再使用可能なネットワーク オブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なネットワークのリストにそれらのオブジェクトを追加できます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [ネットワーク（Networks）] で、[ルールの追加（Add Rule）] をクリックします。

ステップ 3 [使用可能なネットワーク（Available Networks）] の横にある [追加（Add）] (＋) をクリックします。

ステップ 4 ネットワーク オブジェクトの作成（1351 ページ）の説明に従って、ネットワーク オブジェクトを作成します。

ステップ 5 ネットワーク検出ルールの設定（2661 ページ）の説明に従って、ネットワーク検出ルールの追加を完了します。

ポート除外

モニタリングからホストを除外できるのと同様に、モニタリングから特定のポートを除外できます。次に例を示します。

- ロードバランサは短期間に同じポート上の複数のアプリケーションを報告する可能性があります。モニタリングからそのポートを除外する（Web ファームを処理するロード バランサ上のポート 80 を除外するなど）ようにネットワーク検出ルールを設定できます。
- 組織で特定の範囲のポートを使用するカスタム クライアントを使用しているとします。このクライアントからのトラフィックが紛らわしいイベントを過剰に生成する場合は、モニタリングからそれらのポートを除外できます。同様に、DNS トラフィックをモニタしないように設定することもできます。この場合は、検出ポリシーがポート 53 をモニタしないように、ルールを設定します。

除外するポートを追加するときには、[利用可能なポート（Available Ports）] リストから再利用可能なポート オブジェクトを選択するのか、送信元または宛先除外リストにポートを直接追加するのか、新しい再利用可能なポートを作成してからそれを除外リストに移動するのかを決定できます。

（注） NetFlow データの検出を処理するルールでポートを除外することはできません。

ネットワーク検出ルールでのポート除外

NetFlow データ検出を処理するルールにあるポートを除外することはできません。

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ポート除外（Port Exclusions）] をクリックします。

ステップ 4 必要に応じて、ディスカバリ ルール設定時にポート オブジェクトを作成する （2666ページ）で説明されているように、使用可能なポート リストにポート オブジェクトを追加します。

ステップ 5 次のいずれかの方法を使用して、モニターリング対象から特定の送信元ポートを除外します。

- [使用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[送信元に追加（Add to Source）] をクリックします。
- ポート オブジェクトを追加せずに特定の送信元ポートからのトラフィックを除外するには、[選択済の送信元ポート リスト（Selected Source Ports）] で、[プロトコル（Protocol）] を選択し、[ポート（Port）] 番号（1 から 65535 の数値）を入力して、[追加（Add）] をクリックします。

ステップ 6 次のいずれかの方法を使用して、モニターリング対象から特定の宛先ポートを除外します。

- [使用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[宛先に追加（Add to Destination）] をクリックします。
- ポート オブジェクトを追加せずに特定の宛先ポートからのトラフィックを除外するには、[選択済の宛先ポート リスト（Selected Destination Ports）] で、[プロトコル（Protocol）] を選択し、[ポート（Port）] 番号を入力して、[追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ディスカバリ ルール設定時にポート オブジェクトを作成する

新規ポートオブジェクトを、システム内の任意の場所で使用できる再使用可能なポートオブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なポートのリストにそれらのオブジェクトを追加できます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。
ステップ 2 [ネットワーク（Networks）] で、[ルールの追加（Add Rule）] をクリックします。
ステップ 3 [ポート除外（Port Exclusions）] をクリックします。
ステップ 4 [利用可能なポート（Available Ports）] リストにポートを追加するには、[追加（Add）] (+) をクリックします。
ステップ 5 **名前**を入力します。
ステップ 6 [プロトコル（Protocol）] フィールドで、除外するトラフィックのプロトコルを指定します。
ステップ 7 [ポート（Port）] フィールドに、モニターリングから除外するポートを入力します。

単一のポート、ダッシュ（-）を使用したポートの範囲、またはポートとポート範囲のカンマ区切りのリストを指定できます。許容されるポート値は 1 ～ 65535 です。

ステップ 8 [保存（Save）] をクリックします。
ステップ 9 ポートがすぐにリストに表示されない場合は、[更新（Refresh）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ネットワーク検出ルールのゾーン

パフォーマンスを向上させるために、ルール内の監視対象ネットワークに物理的に接続されている管理対象デバイス上のセンシング インターフェイスがルール内のゾーンに含まれるように、検出ルールを設定することができます。

残念ながら、ネットワーク設定の変更は通知されないことがあります。ネットワーク管理者が通知せずにルーティングやホストの変更によりネットワーク設定を変更した場合、正しいネットワーク検出ポリシー設定を完全に把握するのが難しくなります。管理対象デバイス上のセンシングインターフェイスがどのようにネットワークに物理的に接続されているかが不明な場合は、ゾーンの設定はデフォルト値のままにしておいてください。このデフォルト値によって、システムは展開環境内のすべてのゾーンに検出ルールを展開します（ゾーンが除外されない場合、システムではすべてのゾーンに検出ポリシーを展開します。）。

ネットワーク検出ルールのゾーンの設定

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。
ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ゾーン（Zones）] をクリックします。

ステップ 4 [使用可能なゾーン（Available Zones）] リストでゾーンを選択します。

ステップ 5 [保存（Save）] をクリックして、変更内容を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

トラフィック ベース検出のアイデンティティ ソース

トラフィックベースの検出は、システムでサポートされている唯一の権限のないアイデンティティソースです。トラフィック ベース検出を設定すると、管理対象デバイスは、指定したネットワークでのLDAP、AIM、POP3、IMAP、Oracle、SIP（VoIP）、FTP、HTTP、MDNS、SMTPのログインを検出します。トラフィック ベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティ ソースとは異なり、トラフィック ベースの検出はネットワーク検出ポリシーで設定します。トラフィックに基づくユーザー検出の設定（2670 ページ）を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。
- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。
- トラフィック ベースの検出では SMTP ロギングを制限することができません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。システムが SMTP ログインを検出しても、一致する電子メール アドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログイン アクティビティのユーザー アクティビティ タイプは [失敗したユーザー ログイン（Failed User Login）] です。

（注） システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得（Capture Failed Login Attempts）] を有効にする必要があります。

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザ アクティビティとして記録するために Firewall Management Centerに送信します。

- ログインで識別されたユーザー名。
- ログインの時刻。
- ログインに関係する IP アドレス。このアドレスは、ユーザーのホスト（LDAP、POP3、IMAP、および AIM ログインの場合）、サーバー（HTTP、MDNS、FTP、SMTP および Oracle ログインの場合）、またはセッション発信元（SIP ログインの場合）の IP アドレスになります。
- ユーザーの電子メールアドレス（POP3、IMAP、および SMTP ログインの場合）。
- ログインを検出したデバイスの名前。

ユーザがすでに検出されている場合、Firewall Management Centerはそのユーザのログイン履歴を更新します。Firewall Management Center は POP3 および IMAP ログイン内の電子メール アドレスを使用して LDAP ユーザに関連付ける場合があることに注意してください。これは、Firewall Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メール アドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Firewall Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。これは、それらのログイン イベントには Firewall Management Center が他のログイン タイプに関連付けることができるデータが含まれていないためです。

Firewall Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録**しません**。

- そのログインタイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザーデータベースに電子メールアドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザーが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

トラフィック ベースの検出戦略

ユーザーアクティビティを検出するプロトコルを制限して、検出するユーザーの総数を削減することにより、ほぼ完全なユーザー情報を提供していると思われるユーザーに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Firewall Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Firewall Management Centerは、これらのユーザーとその他のユーザー タイプを関連付けることができません。

トラフィックに基づくユーザー検出の設定

ネットワーク検出ルールでトラフィック ベースのユーザー検出を有効にすると、ホスト検出が自動で有効になります。トラフィック ベースの検出の詳細については、トラフィック ベース検出のアイデンティティ ソース （2668 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [ユーザー（Users）] をクリックします。

ステップ 3 [編集（Edit）]（ ） をクリックします。

ステップ 4 ログインを検出するプロトコルのチェックボックスをオンにするか、ログインを検出しないプロトコルのチェックボックスをオフにして、[失敗したログイン試行のキャプチャ（Capture Failed Login Attempts）] を有効にするかどうかを選択します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザー検出を有効/無効にすると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （165 ページ）を参照してください。

- ネットワーク検出ルールの設定 （2661 ページ）の説明に従って、ユーザーを検出するようにネットワーク検出ルールを設定します。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

高度なネットワーク検出オプションの設定

ネットワーク検出ポリシーの [詳細（Advanced）] を使用すれば、検出するイベント、検出データの保存期間と更新頻度、影響相関に使用する脆弱性マッピング、およびオペレーティングシステム ID とサーバー ID の競合の解決方法に関するポリシー全体の設定を構成できます。加えて、ホスト入力ソースと NetFlow エクスポータを追加して、他のソースからのデータのインポートを許可できます。

（注） 検出イベントとユーザー活動イベントのデータベースイベント制限はシステム構成で設定されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 変更する設定の隣にある[編集（Edit）]（）または[追加（Add）] ()をクリックします。

- [データ ストレージ設定（Data Storage Settings）]：ネットワーク検出データ ストレージの設定 （2679 ページ）の説明に従って、設定を更新します。
- [イベント ロギング設定（Event Logging Settings）]：ネットワーク検出イベント ロギングの設定 （2679 ページ）の説明に従って、設定を更新します。
- [全般設定（General Settings）]：ネットワーク検出の一般設定を行う （2672 ページ）の説明に従って、設定を更新します。
- [ID 競合設定（Identity Conflict Settings）]：ネットワーク検出アイデンティティ競合の解決の設定 （2674 ページ）の説明に従って、設定を更新します。

- [侵害の兆候設定（General Settings）]：侵害の兆候ルールの有効化（2676ページ）の説明に従って、設定を更新します。
- [NetFlow エクスポータ（NetFlow Exporters）]：NetFlow エクスポータのネットワーク検出ポリシーへの追加（2677 ページ）の説明に従って、設定を更新します。
- [OS およびサーバーの ID ソース（OS and Server Identity Sources）]：ネットワーク検出 OS およびサーバー アイデンティティ ソースの追加（2680ページ）の説明に従って、設定を更新します。
- [影響評価に使用する脆弱性（Vulnerabilities to use for Impact Assessment）]：ネットワーク検出の脆弱性影響評価の有効化（2675 ページ）の説明に従って、設定を更新します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開（172 ページ）を参照してください。

ネットワーク検出の一般設定

一般設定は、システムがネットワーク マップを更新する頻度と、検出中にサーババナーをキャプチャするかどうかを制御します。

[バナーのキャプチャ（Capture Banners）]

サーバー ベンダーとバージョン（「バナー」）をアドバタイズするネットワーク トラフィックからの見出し情報をシステムで保存させる場合、このチェックボックスをオンにします。この情報は、収集された情報に追加のコンテキストを提供できます。サーバ詳細にアクセスすることによって、ホストに関して収集されたサーバ バナーにアクセスできます。

[アップデート間隔（Update Interval）]

システムが情報を更新する時間間隔（ホストの IP アドレスのいずれかが最後に検出された時点、アプリケーションが使用された時点、アプリケーションのヒット数など）。デフォルト設定は 3600 秒（1 時間）です。

更新タイムアウトの時間間隔を短く設定すると、より正確な情報がホスト画面に表示されますが、より多くのネットワーク イベントが生成されることに注意してください。

ネットワーク検出の一般設定を行う

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [全般設定（General Settings）] の横にある[編集（Edit）]（）をクリックします。
ステップ 4 ネットワーク検出の一般設定 （2672 ページ）の説明に従って設定を更新します。
ステップ 5 [保存（Save）] をクリックして、全般設定を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ネットワーク検出アイデンティティ競合の設定

システムは、オペレーティング システムとサーバのフィンガープリントをトラフィック内のパターンに照合することで、どのオペレーティング システムおよびアプリケーションがホストで実行されているかを判別します。最も信頼できるオペレーティング システムとサーバの ID 情報を提供するために、システムは複数のソースからのフィンガープリント情報を照合します。

システムは、すべてのパッシブ データを使用して、オペレーティング システム ID を抽出し、信頼値を割り当てます。

デフォルトでは、ID 競合が存在しなければ、スキャナまたはサード パーティ アプリケーションによって追加された ID データで、Firepower System によって検出された ID データが上書きされます。[アイデンティティ ソース（Identity Sources）] 設定を使用して、スキャナとサードパーティ アプリケーションのフィンガープリント ソースをプライオリティでランク付けできます。システムはソースごとに 1 つずつの ID を保持しますが、プライオリティが最も高いサードパーティ アプリケーションまたはスキャナ ソースからのデータのみが最新の ID として使用されます。ただし、プライオリティに関係なく、ユーザ入力データによって、スキャナまたはサードパーティ アプリケーションのデータが上書きされることに注意してください。

ID 競合は、[アイデンティティ ソース（Identity Sources）] 設定に列挙されたアクティブ スキャナ ソースまたはサードパーティ アプリケーション ソースと Firepower システム ユーザのどちらかから取得された既存の ID と競合する ID をシステムが検出した場合に発生します。デフォルトでは、ID 競合は自動的に解決されないため、ホスト プロファイルを通して、または、ホストをスキャンし直すか新しい ID データを追加し直してパッシブ ID を上書きすることにより、解決する必要があります。ただし、パッシブ ID またはアクティブな ID のいずれかを維持することで、競合を自動的に解決するようにシステムを設定できます。

[ID 競合イベントを生成する（Generate Identity Conflict Event）]

ID 競合が発生したときにシステムがイベントを生成するかどうかを指定します。

[自動的に競合を解決する（Automatically Resolve Conflicts）]

[自動的に競合を解決する（Automatically Resolve Conflicts）] ドロップダウン リストから、次のいずれかを選択します。

- ID 競合の手動での競合解決を強制する場合は、[無効（Disabled）]

- ID 競合が発生したときにシステムがパッシブ フィンガープリントを使用するようにする場合は、[アイデンティティ（Identity）]
- ID 競合が発生したときにシステムが優先度が最も高いアクティブなソースの現在の ID を使用するようにする場合は、[キープアクティブ（Keep Active）]

ネットワーク検出アイデンティティ競合の解決の設定

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [ID競合設定（Identity Conflict Settings）] の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 ネットワーク検出アイデンティティ競合の設定（2673 ページ）の説明に従って、[ID競合設定の編集（Edit Identity Conflict Settings）] ポップアップ ウィンドウの設定を更新します。

ステップ 5 [保存（Save）] をクリックして、ID 競合設定を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ネットワーク検出の脆弱性の影響の評価オプション

システムで侵入イベントとの影響相関を実行する方法を設定できます。有効な選択肢は次のとおりです。

- システム ベースの脆弱性情報を使用して影響相関を実行する場合は、[ネットワーク検出の脆弱性マッピングを使用（Use Network Discovery Vulnerability Mappings）] チェックボックスをオンにします。
- サードパーティの脆弱性参照を使用して影響相関を実行する場合は、[サードパーティの脆弱性マッピングを使用（Use Third-Party Vulnerability Mappings）] チェックボックスをオンにします。詳細については、*Firepower* システムホスト入力 *API* ガイドを参照してください。

チェックボックスのどちらかまたは両方を選択できます。システムが侵入イベントを生成し、選択された脆弱性マッピング セット内の脆弱性のあるサーバまたはオペレーティング システムがそのイベントに関係するホストに含まれている場合、侵入イベントは脆弱（レベル1：赤）影響アイコンでマークされます。ベンダーまたはバージョン情報のないサーバの場合は、Firewall Management Center 構成で脆弱性マッピングを有効にする必要があることに注意してください。

両方のチェックボックスをオフにした場合は、侵入イベントが脆弱（レベル 1：赤）影響アイコンでマークされません。

関連トピック

サードパーティの脆弱性のマッピング （2602 ページ）

ネットワーク検出の脆弱性影響評価の有効化

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [影響評価を使用するための脆弱性（Vulnerabilities to use for Impact Assessment）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 4 ネットワーク検出の脆弱性の影響の評価オプション （2674 ページ）説明に従って、[脆弱性設定の編集（Edit Vulnerability Settings）] ポップアップ ウィンドウで設定を更新します。

ステップ 5 [保存（Save）] をクリックして、脆弱性設定を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

侵害の兆候

システムでは、ネットワーク検出ポリシー内の IOC ルールを使用して悪意のある手段によって侵害されている可能性があるホストが特定されます。ホストがこれらのシステム提供のルールで指定されている条件を満たしている場合、そのホストはシステムによって侵害の兆候（IOC）でタグ付けされます。関連のルールは *IOC* ルールと呼ばれます。各 IOC ルールは 1 種類の IOC タグに対応しています。*IOC* タグは可能性のある侵害の性質を指定します。

次のうちいずれかの事態が発生すると、関与しているホストおよびユーザに Firewall Management Center がタグを付けます。

- システムは、侵入、接続、セキュリティ インテリジェンス、およびファイルまたはマルウェアイベントを使用してモニタ対象のネットワークとそのトラフィックについて集められたデータを関連付け、潜在的な IOC が発生したと判断します。
- Firewall Management Center は AMP クラウドを経由して Secure Endpoint の展開から IOC データをインポートすることができます。このデータがホスト自体の活動（個別のプログラムによってまたはプログラム上で実行されるアクションなど）を検査するため、ネットワーク専用データでは理解するのが難しい可能性がある脅威に対する理解が促されます。便宜上、Firewall Management Center はシスコが開発した新しい IOC タグを AMP クラウドから自動的に取得します。

この機能を設定するには、侵害の兆候ルールの有効化 （2676 ページ）を参照してください。

また、ホストのIOCデータに対する相関ルールと、IOCでタグ付けされたホストから成るコンプライアンス allow リストも記述することができます。

タグ付けされた IOC の調査や操作を行うには、Cisco Secure Firewall Management Center アドミニストレーション ガイド参照してください。

侵害の兆候ルールの有効化

システムで侵害の兆候（IOC）を検出してタグを付けるには、まず、ネットワーク検出ポリシーで 1 つ以上の IOC ルールを有効化する必要があります。IOC ルールのそれぞれが IOC タグの 1 つのタイプに対応します。すべての IOC ルールはシスコが事前定義しています。オリジナルルールを作成することはできません。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストが絶対に監視対象ネットワーク上に出現しない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。

ヒント　個別のホストまたはその関連ユーザーの IOC ルールを無効にするには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Discovery Events」の章を参照してください。

始める前に

IOC ルールはシステムの他のコンポーネントと、Secure Endpoint によって提供されるデータに基づいてトリガーされるため、これらのコンポーネントは正しくライセンス付与されていて、IOC タグを設定できるようにIOCルールに合わせて構成されている必要があります。侵入検知および防御（IPS）および Advanced Malware Protection（AMP）など、有効にする予定の IOC ルールに関連付けられているシステムの機能を有効にします。IOCルールの関連機能が有効になっていないと、関連データが収集されず、ルールをトリガーできません。

手順

ステップ 1　**[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2　[詳細設定（Advanced）] をクリックします。

ステップ 3　[侵害の兆候設定（Indications of Compromise Settings）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 4　IOC 機能全体のオンとオフを切り替えるには、[IOC の有効化（Enable IOC）] の横にあるスライダをクリックします。

ステップ 5　個別の IOC ルールをグローバルに有効または無効にするには、ルールの [有効（Enabled）] 列のスライダをクリックします。

ステップ 6　[保存（Save）] をクリックして IOC ルール設定を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

NetFlow エクスポータのネットワーク検出ポリシーへの追加

この手順に従って、NetFlowエクスポータを追加します。検出ルールで現在使用中のエクスポータは削除できないことに注意してください。

始める前に

- 「NetFlow データを使用するための要件 （2581 ページ）」で前提条件を確認します。
- 「NetFlow データ （2580 ページ）」でNetFlow エクスポータを設定します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [NetFlow デバイス（NetFlow Devices）] の横にある [追加（Add）] (＋) をクリックします。

ステップ 4 エクスポータの [IPアドレス（IP Address）] を入力します。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

- 「ネットワーク検出ルールの設定 （2661 ページ）」でNetFlow トラフィックをモニタリングするネットワーク検出ルールを設定します。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ネットワーク検出のデータ ストレージ設定

ディスカバリのデータ ストレージ設定では、ホスト制限とタイムアウトの設定が行われます。

ホスト制限の到達時（When Host Limit Reached）

Secure Firewall Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。ホスト制限に到達した後に新しいホストを検出すると、[ホスト制限の到達時（When Host Limit Reached）] オプションが制御を行います。次の操作を実行できます。

ホストをドロップ（Drop hosts）

システムは、長期間非アクティブになっているホストをドロップして、新しいホストを追加します。これがデフォルトの設定です。

新しいホストを挿入しない（Don't insert new hosts）

システムは、新たに検出されたホストを追跡しません。システムが新しいホストを追跡するのは、管理者がドメインのホスト制限を増加させた後などに、ホストカウントが制限を下回る場合、ネットワークマップからホストを手動で削除する場合、またはホストが非アクティブであることからタイムアウトと見なされる場合のみです。

表 *204 :* マルチテナンシーによるホスト制限への到達

設定	ドメインのホスト制限の有無	ドメインのホスト制限に到達した場合	先祖ドメインのホスト制限に到達した場合
ホストをドロップ	Yes	制限付きドメインの最も古いホストをドロップします。	ホストをドロップするように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。 ドロップされるホストがなければ、ホストの追加は行われません。
	×	適用対象外	ホストをドロップし、一般プールを共有するように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。
新しいホストを挿入しない	YesまたはNo	ホストの追加は行われません。	ホストの追加は行われません。

ホスト タイムアウト（Host Timeout）

システムが、非アクティブであるという理由でネットワークマップからホストを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。ホスト IP アドレスと MAC アドレスは個別にタイムアウトすることができますが、関連するアドレスのすべてがタイムアウトするまで、ホストはネットワーク マップから削除されません。

ホストの早期タイムアウトを避けるために、ホストのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

サーバ タイムアウト（Server timeout）

システムが、非アクティブであるという理由でネットワークマップからサーバを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。

サーバの早期タイムアウトを避けるために、サービスのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

クライアント アプリケーションのタイムアウト（Client Application Timeout）

システムが、非アクティブであるという理由でネットワーク マップからクライアントを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。

クライアントのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

関連トピック

ホスト制限（Host Limit） （2444 ページ）

ネットワーク検出データ ストレージの設定

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [ネットワーク検出のデータストレージ設定（Network Discovery Data Storage Settings）] の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 ネットワーク検出のデータ ストレージ設定（2677ページ）の説明に従って、[データ ストレージ設定（Data Storage Settings）] ダイアログの設定を更新します。

ステップ 5 [保存（Save）] をクリックして、データ ストレージ設定を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ネットワーク検出イベント ロギングの設定

イベントロギング設定は、検出イベントとホスト入力イベントを記録するかどうかを制御します。イベントを記録しない場合は、イベント ビューで検索することも、相関ルールをトリガーするために使用することもできません。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [イベントロギング設定（Event Logging Settings）] の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Discovery Events*」の章の説明に従って、データベースに記録する検出イベントタイプとホスト入力イベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 5 [保存（Save）] をクリックして、イベント ロギング設定を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ネットワーク検出 OS およびサーバー アイデンティティ ソースの追加

ネットワーク検出ポリシーの [詳細（Advanced）] で、新しいアクティブソースを追加し、また、既存の送信元の優先度やタイムアウトの設定を変更できます。

このページにスキャナを追加しても、Nmap スキャナ用の完全な統合機能は追加されませんが、インポートされたサードパーティ アプリケーションまたはスキャン結果の統合が可能になります。

サードパーティ アプリケーションまたはスキャナからデータをインポートする場合は、ソースからの脆弱性がネットワークで検出された脆弱性にマップされていることを確認してください。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]** を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [OSとサーバーIDソース（OS and Server Identity Sources）] の横にある [編集（Edit）]（✎） をクリックします。

ステップ 4 新しいソースを追加するには、[ソースの追加（Add Sources）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 ドロップダウン リストからインプット ソースの [タイプ（Type）] を選択します。

- AddScanResult機能を使用してスキャン結果をインポートする場合は、[スキャナ（Scanner）] を選択します。
- スキャン結果をインポートしない場合は、[アプリケーション（Application）] を選択します。

ステップ 7 このソースによるネットワーク マップへの ID の追加からその ID の削除までの期間を指定するには、[タイムアウト（Timeout）] ドロップダウンリストから、[時間（Hours）]、[日（Days）]、または [週（Weeks）] を選択し、該当する期間を入力します。

ステップ 8 必要に応じて、以下を行います。

- ソースを昇格させて、オペレーティング システム ID とアプリケーション ID よりもリストでは下にあるソースを優先的に使用するには、そのソースを選択して上矢印をクリックします。
- ソースを降格させて、リストで上にあるソースから提供される ID が存在しない場合にのみオペレーティング システム ID とアプリケーション ID を使用するには、そのソースを選択して下矢印をクリックします。
- ソースを削除するには、ソースの横にある [削除（Delete）]（） をクリックします。

ステップ 9 [保存（Save）] をクリックして、ID ソース設定を保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

サードパーティの脆弱性のマッピング （2602 ページ）

ネットワーク検出戦略のトラブルシューティング

システムのデフォルトの検出機能に変更を加える前に、実装すべきソリューションを決定できるように、どのホストが正しく識別されていないかと、その原因を分析してください。

管理対象デバイスは正しく配置されていますか

ロードバランサ、プロキシ サーバ、NAT デバイスなどのネットワーク デバイスが、識別されないホストまたは誤って識別されたホストと管理対象デバイスとの間に存在する場合は、カスタム フィンガープリントを使用するのではなく、誤って識別されたホストのより近くに管理対象デバイスを配置します。このシナリオでは、カスタム フィンガープリントの使用は推奨しません。

識別されないオペレーティング システムに一意の TCP スタックがありますか

システムがホストを誤って識別した場合、カスタム フィンガープリントを作成してアクティブにするか、検出（ディスカバリ）データの代わりに Nmap またはホストの入力データを使用するかを決定するために、ホストが誤って識別された理由を調べる必要があります。

注意 ホストの誤認が発生した場合は、カスタム フィンガープリントを作成する前にサポート担当者にお問い合わせください。

ホストがデフォルトではシステムに検出されないオペレーティング システムを実行していて、識別用の TCP スタックの特性を既存の検出されているオペレーティング システムと共有していない場合、カスタム フィンガープリントを作成する必要があります。

たとえば、システムで識別できない一意のTCPスタックを保持するLinuxのカスタマイズバージョンが存在する場合、継続的に自分でデータを更新する必要のあるスキャン結果またはサードパーティのデータを使用するのではなく、システムがそのホストを識別してそのホストを監視し続けることができるカスタム フィンガープリントを作成する方が便利です。

オープン ソースのLinuxディストリビューションの多くで同じカーネルを使用しているため、システムではLinuxのカーネル名を使用してそれらを識別することに注意してください。Red Hat Linux システム用のカスタム フィンガープリントを作成する場合、同じフィンガープリントが複数のLinuxディストリビューションに一致するために、その他のオペレーティング システム（Debian Linux、Mandrake Linux、Knoppix など）が Red Hat Linux として識別されることがあります。

フィンガープリントをすべての状況で使用するのが適切なわけではありません。たとえば、ホストのTCPスタックに変更が加えられ、別のオペレーティング システムと類似する(または同じ)ものになることがあります。たとえば、Apple Mac OS X ホストのフィンガープリントがLinux 2.4 ホストと同じになるように変更されると、システムはホストを Mac OS X ではなくLinux 2.4 として識別します。この Mac OS X ホストのカスタム フィンガープリントを作成すると、すべての正規の Linux 2.4 ホストが Mac OS X ホストとして誤認される場合があります。この場合、Nmap が正しくホストを識別するならば、そのホストに対して定期的な Nmap スキャンをスケジュールできます。

ホスト入力を使用して、サードパーティ製のシステムからデータをインポートする場合、サーバおよびアプリケーション プロトコルを説明するためにサードパーティが使用するベンダー、製品、およびバージョンの文字列を、それらの製品の Cisco の定義にマッピングする必要があります。アプリケーション データを Firepower システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたはWebアプリケーションの影響評価には使用されないことに注意してください。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現在の ID を判別することがあります。

Nmap データの場合、定期的な Nmap スキャンをスケジュールできます。ホスト入力データの場合、インポート用の Perl スクリプトまたはコマンド ライン ユーティリティを定期的に実行できます。ただし、アクティブのスキャン データとホスト入力データは、検出（ディスカバリ）データの頻度で更新されないことがあるので注意してください。

Firepower システムがすべてのアプリケーションを識別できますか

ホストがシステムによって正しく識別されるものの、識別されないアプリケーションがホストにある場合、ユーザ定義のディテクタを作成して、アプリケーションを識別するために役立つポートおよびパターン マッチング情報をシステムに提供することができます。

脆弱性を修正するパッチを適用しましたか

システムがホストを正しく識別するものの、適用した修正が反映されない場合、ホスト入力機能を使用してパッチ情報をインポートすることができます。パッチ情報をインポートする場合、修正名をデータベース内の修正にマッピングする必要があります。

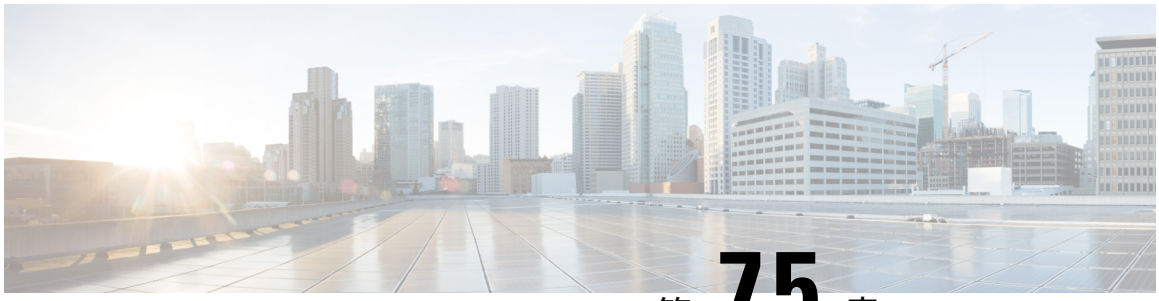
サードパーティ製の脆弱性を追跡しますか

影響の関連付け（相関）に使用したいサードパーティ製システムからの脆弱性情報がある場合、サーバおよびアプリケーションプロトコル用のサードパーティの脆弱性IDをCiscoのデータベース内の脆弱性IDにマッピングしてから、ホスト入力機能を使用してそれらの脆弱性をインポートすることができます。ホスト入力機能の使用の詳細については、『*Firepower* システムホスト入力 *API* ガイド』を参照してください。アプリケーション データをFirepowerシステムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたはWebアプリケーションの影響評価には使用されないことに注意してください。

第 XIII 部

FlexConfig ポリシー

• FlexConfig ポリシー （2687 ページ）



第 75 章

FlexConfig ポリシー

ここでは、FlexConfig ポリシーの設定および展開方法について説明します。

- FlexConfig ポリシーの概要 （2687 ページ）
- FlexConfig ポリシーの要件と前提条件 （2711 ページ）
- FlexConfig の注意事項と制約事項 （2712 ページ）
- FlexConfig ポリシーによるデバイス設定のカスタマイズ （2712 ページ）
- FlexConfig の例 （2729 ページ）
- FlexConfig ポリシーの移行 （2737 ページ）
- FlexConfig の履歴 （2739 ページ）

FlexConfig ポリシーの概要

FlexConfig ポリシーは FlexConfig オブジェクトの番号付きリストのコンテナです。各オブジェクトは、定義する一連の Apache Velocity のスクリプト言語コマンド、ASA ソフトウェアの設定コマンド、および変数に影響を与えます。各 FlexConfig オブジェクトの内容は、基本的に、割り当てられたデバイスに展開する一連の ASA コマンドを生成するプログラムです。このコマンド シーケンスは、その後、Firewall Threat Defense デバイスで関連機能を設定します。

Firewall Threat Defense では、ASA 設定コマンドを使用して、すべての機能ではなく一部の機能を実装します。Firewall Threat Defense 設定コマンドの一意のセットはありません。代わりに、FlexConfig のポイントは、Firewall Management Center ポリシーおよび設定を介して直接まだサポートされていない機能を設定できることです。

注意 シスコでは、ASA に精通している上級ユーザーが自身の責任で行う場合にのみ FlexConfig ポリシーを使用することを**強く**お勧めします。禁止されていないコマンドはすべて、設定できます。FlexConfig ポリシーによって機能を有効にすると、他の設定された機能により意図しない結果を引き起こす可能性があります。

設定した FlexConfig ポリシーに関するサポートについては、Cisco Technical Assistance Center にお問い合わせください。Cisco Technical Assistance Center は、顧客に代わってカスタム設定を設計したり、作成したりしません。シスコは、その他の Firepower システムの機能との正しい動作または相互運用性を保証しません。FlexConfig 機能は廃止になる可能性があります。完全に保証された機能のサポートについては、Firewall Management Center サポートを待つ必要があります。判別できない場合は、FlexConfig ポリシーを使用しないでください。

FlexConfig ポリシーの推奨される使用法

FlexConfig ポリシーには、推奨される使用法が主に 2 つあります。

- ASA から Firewall Threat Defense に変換し、Firewall Management Center で直接サポートされない互換機能を使用している（および引き続き使用する必要がある）場合。この場合、ASA で **show running-config** コマンドを使用してその互換機能の設定を確認し、その機能を実装する FlexConfig オブジェクトを作成します。オブジェクトの導入設定（1 回/毎回、前に付加/後ろに付加）をいろいろと試して、正しい設定になるようにします。2 つのデバイスで、**show running-config** の出力を比較して確認します。
- Firewall Threat Defense を使用しているものの、構成が必要な設定または機能がある場合（たとえば、Cisco Technical Assistance Center から、発生している特定の問題を解決するための具体的な設定を指示された場合）。複雑な機能については、ラボデバイスを使用して FlexConfig をテストし、期待する動作を得られることを確認します。

システムには、テスト対象の設定を表す一連の定義済み FlexConfig オブジェクトが含まれています。これらのオブジェクトのなかに必要な機能を表すものがない場合は、まず、標準ポリシーで同等の機能を設定できるかどうかを判断します。たとえば、アクセス コントロール ポリシーには侵入検知および防御、HTTP およびその他のタイプのプロトコル インスペクション、URL フィルタリング、アプリケーション フィルタリング、アクセス制御が含まれており、ASA はこれらの要素を別個の機能を使用して実装します。多くの機能は CLI コマンドを使用して設定されていないので、**show running-config** の出力にすべてのポリシーが表示されるわけではありません。

（注） 常に、ASA と Firewall Threat Defense との間の重複は 1 対 1 であるわけではないことに注意してください。ASA の設定を Firewall Threat Defense デバイス上で完全に再現しようとしないでください。FlexConfig を使用して設定した機能は慎重にテストする必要があります。

FlexConfig オブジェクトの CLI コマンド

Firewall Threat Defense では一部の機能の設定に ASA コンフィギュレーション コマンドを使用します。ASA のすべての機能に Firewall Threat Defense との互換性があるわけではありませんが、Firewall Threat Defense で使用はできるが Firewall Management Center ポリシーでは設定できない機能があります。こうした機能を設定するには、FlexConfig オブジェクトを使って必要な CLI を指定します。

FlexConfig を使って手動で機能を設定する場合、ユーザは自身の責任において正しいコマンド シンタックスを理解し、実装してください。FlexConfig ポリシーは CLI コマンド シンタックスの検証は行いません。正しいシンタックスと CLI コマンドの設定に関する詳細については、ASA ドキュメンテーションを参照してください。

- 『ASA CLI Configuration Guides』では機能を設定する方法について説明しています。ガイドはこちらからご覧ください。 https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- 『ASA Command References』ではコマンド名ごとにその他の情報が記載されています。リファレンスはこちらからご覧ください。 https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

ここでは、設定コマンドについて詳しく説明します。

ASA ソフトウェア バージョンと現在の CLI 設定の決定

システムでは、いくつかの機能の設定に ASA ソフトウェア コマンドを使用するため、Firewall Threat Defense デバイスで実行されているソフトウェアで使用される現在の ASA バージョンを決定する必要があります。このバージョン番号は、機能を設定する手順について利用する ASA CLI 設定ガイドを示します。また、CLI ベースの現在の設定をチェックし、実装する ASA 設定と比較する必要もあります。

ASA 設定は Firewall Threat Defense 設定とは大きく異なることを覚えておいてください。多数の Firewall Threat Defense ポリシーは CLI の外で設定されるため、コマンドを見て設定を確認することはできません。ASA と Firewall Threat Defense の設定の間に 1 対 1 の対応を作成しようとはしないでください。

この情報を表示するには、デバイスの管理インターフェイスへの SSH 接続を確立し、次のコマンドを発行します。

- **show version system** また、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号を検索します。（Secure Firewall Management Center CLI ツールを使用してコマンドを発行する場合は、**system** キーワードを省略します。）
- **show running-config** ：現在の CLI 設定を表示します。
- **show running-config all** ：現在の CLI 設定にすべてのデフォルト コマンドを含めます。

また、次の手順を使用して、Firewall Management Center 内からこれらのコマンドを発行することもできます。

手順

ステップ 1 **[システム（System）] > [ヘルス（Health）] > [モニター（Monitor）]** を選択します。

ステップ 2 FlexConfig ポリシーの対象となるデバイスの名前をクリックします。

目的のデバイスを表示するために、[ステータス（Status）] テーブルの [カウント（Count）] カラムにある開く/閉じるの矢印をクリックする必要がある場合があります。

ステップ 3 [システムとトラブルシューティングの詳細を表示（View System and Troubleshoot Details）] をクリックします。

ステップ 4 [詳細なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 5 [脅威防御 CLI（Threat Defense CLI）] をクリックします。

ステップ 6 [デバイス（Device）] を選択し、次にコマンドとして **show** を選択し、パラメータとして **version** を入力するか、他のコマンドの 1 つを入力します。

ステップ 7 [実行（Execute）] をクリックします。

version を入力した場合、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号の出力を検索します。

後で実行する分析のために、出力を選択して Ctrl + C を押し、テキスト ファイルに貼り付けることができます。

禁止された CLI コマンド

FlexConfig の目的は、Firewall Management Center を使用している Firewall Threat Defense デバイスで設定できない ASA デバイスで使用可能な機能を設定することです。

したがって、Firewall Management Center に同等の機能がある ASA 機能は設定することができません。次の表に、これらの禁止されたコマンド領域のいくつかを示します。

また、一部の **clear** コマンドは管理対象ポリシーと重複しており、管理対象ポリシーの設定の一部を削除する可能性があるため禁止されています。

FlexConfig オブジェクト エディタでは、禁止されたコマンドをオブジェクトに含めることはできません。

禁止された CLI コマンド	説明
AAA	設定がブロックされます。
AAA-Server	設定がブロックされます。

禁止された CLI コマンド	説明
Access-list	高度 ACL、拡張 ACL、および標準 ACL がブロックされます。Ethertype ACL は許可されます。 テンプレート内のオブジェクト マネージャで定義されている標準および拡張 ACL オブジェクトを変数として使用することができます。
ARP Inspection	設定がブロックされます。
As-path Object	設定がブロックされます。
Banner	設定がブロックされます。
BGP	設定がブロックされます。
Clock	設定がブロックされます。
Community-list Object	設定がブロックされます。
コピー（Copy）	設定がブロックされます。
削除（Delete）	設定がブロックされます。
DHCP	設定がブロックされます。
パスワードを有効にする（Enable Password）	設定がブロックされます。
削除（Erase）	設定がブロックされます。
Fragment Setting	**fragment reassembly** を除きブロックされます。
Fsck	設定がブロックされます。
HTTP	設定がブロックされます。
ICMP	設定がブロックされます。
インターフェイス（Interface）	**nameif**、**mode**、**shutdown**、**ip address**、および **mac-address** コマンドのみがブロックされます。
Multicast Routing	設定がブロックされます。
NAT	設定がブロックされます。
Network Object/Object-group	FlexConfig オブジェクトでの Network オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているネットワーク オブジェクトとグループを変数として使用することができます。

禁止された CLI コマンド	説明
NTP	設定がブロックされます。
OSPF/OSPFv3	設定がブロックされます。
ポケットベル	設定がブロックされます。
パスワードの暗号化	設定がブロックされます。
Policy-list Object	設定がブロックされます。
Prefix-list Object	設定がブロックされます。
リロード（Reload）	リロードはスケジュールできません。システムは、システムを再起動するために**reload**コマンドを使用せず、**reboot**コマンドを使用します。
RIP	設定がブロックされます。
Route-Map Object	FlexConfig オブジェクトでの Route-map オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているルートマップ オブジェクトを変数として使用することができます。
Service Object/Object-group	FlexConfig オブジェクトでの Service オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているポート オブジェクトを変数として使用することができます。
SNMP	設定がブロックされます。
SSH	設定がブロックされます。
Static Route	設定がブロックされます。
Syslog	設定がブロックされます。
Time Synchronization	設定がブロックされます。
Timeout	設定がブロックされます。
VPN	設定がブロックされます。

テンプレート スクリプト

スクリプト言語を使用して、FlexConfig オブジェクト内部での処理を制御できます。スクリプト言語命令は、Apache Velocity 1.3.1 テンプレート エンジンでサポートされているコマンドの

サブセットです。Velocity テンプレート エンジンは、ループ、if/else ステートメント、および変数をサポートする Java ベースのスクリプト言語です。

スクリプト言語の使用方法についての詳細は、『*Velocity Developer Guide*』（http://velocity.apache.org/engine/devel/developer-guide.html）を参照してください。

FlexConfig 変数

コマンドまたは処理手順の一部がスタティック情報ではなくランタイム情報に依存する場合は、FlexConfig オブジェクトに変数を使用できます。展開時に、変数は変数のタイプに基づいてデバイスのその他の設定から取得された文字列に置き換えられます。

- ポリシー オブジェクト変数は、Firewall Management Center で定義されているオブジェクトから取得された文字列に置き換えられます。
- システム変数は、デバイス自体やデバイスに設定されたポリシーから取得した情報に置き換えられます。
- プロセス変数は、スクリプト コマンドの処理時に、ポリシー オブジェクトまたはシステム変数の内容とともにロードされます。たとえば、ループで、ポリシーオブジェクトまたはシステム変数から 1 つの値をプロセス変数に反復してロードし、プロセス変数を使用して、コマンド文字列を形成するか、その他のアクションを実行します。これらのプロセス変数は、FlexConfig オブジェクト内の [変数（Variables）] リストに表示されません。また、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用してこれらを追加しません。
- 秘密キー変数は、FlexConfig オブジェクト内の変数に定義された単一の文字列に置き換えられます。

変数は、$ 文字で始まりますが、@ で始まる秘密キーを除きます。たとえば、$ifname は次のコマンドのポリシー オブジェクト変数で、@keyname は秘密キーです。

```
interface $ifname
key @keyname
```

（注） ポリシー オブジェクトまたはシステム変数を初めて挿入する場合は、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用して挿入する必要があります。このアクションによって、FlexConfig オブジェクト エディタの下部にある [変数（Variables）] リストに変数が追加されます。ただし、システム変数を使用する場合でも、後続の使用では変数文字列を入力する必要があります。オブジェクトまたはシステム変数の割り当てがないプロセス変数を追加する場合は、[挿入（Insert）] メニューを使用しないでください。秘密キーを追加する場合は、常に [挿入（Insert）] メニューを使用します。秘密キーの変数は [変数（Variables）] リストに表示されません。

変数が単一の文字列、文字列のリスト、または値のテーブルのいずれとして解決されるかは、変数に割り当てるポリシー オブジェクトまたはシステム変数のタイプによって決まります（秘

密キーは、常に、単一の文字列として解決されます）。変数を適切に処理するには、何が返されるかを理解する必要があります。

次の各トピックでは、変数のさまざまなタイプとその処理方法について説明します。

変数の処理方法

ランタイムで、変数は単一の文字列、同じタイプの文字列のリスト、異なるタイプの文字列のリスト、あるいは名前付き値の表として解決することができます。また、複数の値に解決される変数の長さは一定、不定のどちらにすることもできます。変数を正しく処理するためには、何が返されるかを理解する必要があります。

返される値には、主に次の可能性があります。

単一値変数

変数が常に単一の文字列に解決される場合、FlexConfig スクリプトを変更せずに、その変数をそのまま使用できます。

たとえば、定義済みのテキスト変数 tcpMssBytes は常に単一の値（数値でなければなりません）に解決されます。**Sysopt_basic** FlexConfig は if/then/else 構造を使用して、別の単一値テキスト変数 tcpMssMinimum に基づきセグメントの最大サイズを設定します。

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

この例では、FlexConfig オブジェクト エディタで [挿入（Insert）] メニューを使用して最初の $tcpMssBytes の使用を追加しますが、#else 行には直接この変数を入力します。

秘密鍵の変数は、特殊なタイプの単一値変数です。秘密鍵では、変数を繰り返し使用する場合でも常に [挿入（Insert）] メニューを使用して変数を追加します。これらの変数は、FlexConfig オブジェクト内の [変数（Variables）] リストに表示されません。

（注） ネットワーク オブジェクトのポリシー オブジェクト変数も、IP アドレスの単一の指定（ホスト アドレス、ネットワーク アドレス、アドレス範囲のいずれか）になります。ただしこの場合、ASA コマンドには特定のアドレス タイプが必要であるため、期待されるアドレスのタイプを把握している必要があります。たとえば、コマンドにホストアドレスが必要な場合、ネットワーク アドレスを含むオブジェクトを指すネットワーク オブジェクト変数を使用すると、導入時にエラーが発生します。

同じタイプの複数の値を持つ変数

ポリシーオブジェクトおよびシステム変数のなかには、同じタイプの複数の値に解決されるものがあります。たとえば、ネットワーク オブジェクト グループを指すオブジェクト変数は、

そのグループ内の IP アドレスのリストに解決されます。同様に、システム変数 $SYS_FW_INTERFACE_NAME_LIST は、インターフェイス名のリストに解決されます。

同じタイプの複数の値に対応するテキスト オブジェクトを作成することもできます。たとえば、定義済みのテキストオブジェクト enableInspectProtocolList には複数のプロトコル名を含めることができます。

同じタイプの項目のリストに解決される複数の値を持つ変数は、長さが不定であることはよくあります。たとえば、ユーザは随時インターフェイスを設定または設定解除できるので、デバイス上にある名前付きインターフェイスの数を前もって知ることはできません。

そのため、同じタイプの複数の値を持つ変数を処理するには、通常はループを使用します。たとえば、定義済みの FlexConfig **Default_Inspection_Protocol_Enable** では、#foreach ループを使用して enableInspectProtocolList オブジェクトの各値を処理します。

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

この例では、スクリプトが各値を順に $protocol 変数に代入し、その結果を ASA の **inspect** コマンドで使用して、そのプロトコルに対してインスペクションエンジンを有効にします。この場合、変数名として単純に $protocol と入力します。オブジェクトやシステム値を変数に代入するわけではないので、[挿入（Insert）] メニューを使用して変数を追加することはしません。ただし、$enableInspectProtocolList を追加する場合は、[挿入（Insert）] メニューを使用する必要があります。

システムは $enableInspectProtocolList 内の値がなくなるまで、#foreach と #end の間にあるコードをループ処理します。

タイプが異なる複数の値を持つ変数

それぞれの値が異なる目的を果たす、複数の値を持つテキストオブジェクトを作成できます。たとえば、定義済みの **netflow_Destination** テキスト オブジェクトに、インターフェイス名、宛先 IP アドレス、UDP ポート番号という 3 つの値がこの順で設定されているとします。

このように定義するオブジェクトは、既定の数の値を持たなければなりません。そうでないと、処理するのが難しくなります。

このようなオブジェクトを処理するには、get メソッドを使用します。オブジェクト名の末尾に **.get(*n*)** と入力し、*n* をそのオブジェクトのインデックスで置き換えます。テキスト オブジェクトは値を 1 からリストしますが、インデックスは 0 からカウントします。

たとえば、Netflow_Add_Destination オブジェクトは次の行を使用して、netflow_Destination に含まれる 3 つの値を ASA の **flow-export** コマンドに追加します。

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

この例では、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用して $netflow_Destination の最初の使用を追加してから、**.get(0)** を追加します。ただし、**$netflow_Destination.get(1)** および **$netflow_Destination.get(2)** の変数は直接入力して指定する必要があります。

値のテーブルに解決される、複数の値を持つ変数

システム変数のなかには、値のテーブルを返すものがあります。そのような変数に該当するのは、たとえば $SYS_FTD_ROUTED_INTF_MAP_LIST のように、MAP が名前に含まれる変数です。ルーテッド インターフェイス マップは、以下のようなデータを返します（わかりやすくするために改行が追加されています）。

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

上記の例では、4 つのインターフェイスに関する情報が返されています。インターフェイスごとに、名前付き値のテーブルが含まれています。たとえば、intf_hardwarare_id はインターフェイス ハードウェアの名前プロパティであり、GigabitEthernet0/0 などの文字列として返されます。

このような変数は、通常は長さが不定であるため、値を処理するにはループ処理を使用する必要があります。また、取得対象の値を示すために、変数名にプロパティ名も追加する必要があります。

たとえば、IS-IS 構成では、インターフェイス コンフィギュレーション モードで、論理名を持つインターフェイスに ASA の **isis** コマンドを追加する必要があります。ただし、このモードを開始する際は、インターフェイスのハードウェア名を使用します。したがって、論理名を持つインターフェイスを識別してから、それらのインターフェイスだけをそれぞれのハードウェア名を使用して設定する必要があります。ISIS_Interface_Configuration の定義済み FlexConfig は、そのために、ループ内にネストされた if/then 構造を使用します。以下のコードを見るとわかるように、#foreach スクリプト コマンドで各インターフェイス マップを $intf 変数に読み込んだ後、#if ステートメントでマップ（$intf.intf_logical_name）から intf_logical_name の値を取得し、その値が isisIntfList 定義済みテキスト変数で定義されているリストに含まれている場合は、intf_hardwarare_id の値（$intf.intf_hardwarare_id）を使用してインターフェイス コマンドを入力します。IS-IS を設定するインターフェイスの名前を追加する場合は、isisIntfList 変数を編集する必要があります。

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

変数がデバイスに関して返す内容を表示する方法

変数が何を返すかを評価する簡単な方法は、変数の注釈付きリストを処理するだけの簡単な FlexConfig オブジェクトを作成することです。次に、作成したオブジェクトを FlexConfig ポリシーに割り当て、ポリシーをデバイスに割り当てます。ポリシーを保存してから、そのデバイスの設定のプレビューをプレビューします。解決された値がプレビューに表示されます。プレビューのテキストを選択し、Ctrl キーを押した状態で C キーを押し、出力を分析用にテキストファイルに貼り付けることができます。

（注） ただし、FlexConfig には有効な設定コマンドが一切含まれていないため、FlexConfig をデバイスに展開しないでください。展開すると展開エラーが生じます。プレビューの取得後、FlexConfig ポリシーから FlexConfig オブジェクトを削除し、ポリシーを保存します。

たとえば、次の FlexConfig オブジェクトを作成することができます。

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

このオブジェクトのプレビューは以下のように表示されます（明確にするために改行が追加されています）。

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###
```

```
###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, diagnostic]
```

FlexConfig ポリシー オブジェクト変数

ポリシー オブジェクト変数は、オブジェクト マネージャで設定されている特定のポリシー オブジェクトに関連付けられます。FlexConfigオブジェクトにポリシー オブジェクト変数を挿入する場合、変数に名前を付け、これに関連付けられているオブジェクトを選択します。

関連付けられているオブジェクトと完全に同じ名前を変数に付けても、変数自体は、関連付けられたオブジェクトと同じではありません。FlexConfig で初めてスクリプトに変数を追加し、オブジェクトとの関連付けを確立するには、FlexConfig オブジェクト エディタの **[挿入（Insert）]** > **[ポリシー オブジェクトの挿入（Insert Policy Object）]** > ***[オブジェクト タイプ（Object Type）]*** メニューを使用する必要があります。単に $ 記号に続けてオブジェクト名を入力しても、ポリシー オブジェクト変数は作成されません。

以下のタイプのオブジェクトを指す変数を作成できます。各変数に適切なタイプのオブジェクトを作成するようにしてください。オブジェクトを作成するには、**[オブジェクト（Objects）]**> **[オブジェクト管理（Object Management）]** に移動します。

- テキスト オブジェクト（Text Objects）：テキスト文字列の場合。これには、IP アドレス、番号や、インターフェイス、ゾーン名などの自由形式のテキストが含まれます。コンテンツ テーブルから **[FlexConfig]** > **[テキスト オブジェクト（Text Object）]** を選択し、[テキスト オブジェクトの追加（Add Text Object）] をクリックします。単一の値または複数の値を含むようにこれらのオブジェクトを設定できます。これらのオブジェクトは柔軟性が高く、FlexConfig オブジェクト内で使用するよう特別に構築されています。詳細については、FlexConfig テキスト オブジェクトの設定 （2720 ページ）を参照してください。
- ネットワーク（Network）：IP アドレスの場合。ネットワーク オブジェクトまたはグループを使用できます。コンテンツ テーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** または [グループの追加（Add Group）] を選択します。グループ オブジェクトを使用すると、変数によりグループ内の各 IP アドレス指定のリストが返されます。アドレスは、オブジェクトの内容に応じて、ホスト、ネットワーク、またはアドレス範囲にできます。ネットワーク（1349 ページ）を参照してください。
- セキュリティ ゾーン（Security Zones）：セキュリティ ゾーンまたはインターフェイス グループ内のインターフェイスの場合。コンテンツ テーブルから [インターフェイス（Interface）] を選択し、**[追加（Add）]** > **[セキュリティ ゾーン（Security Zones）]** または [インターフェイス グループ（Interface Group）] を選択します。セキュリティ ゾーン変数では、設定中のデバイスのゾーンまたはグループ内のインターフェイスのリストが返されます。インターフェイス（Interface） （1346 ページ）を参照してください。
- 標準 ACL オブジェクト（Standard ACL Object）：標準アクセス コントロール リストの場合。標準 ACL 変数では、標準 ACL オブジェクトの名前が返されます。コンテンツ テーブルから **[アクセス リスト（Access List）]** > **[標準（Standard）]** を選択し、[標準アクセス リスト オブジェクトの追加（Add Standard Access List Object）] をクリックします。アクセスリスト （1319 ページ）を参照してください。
- 拡張 ACL オブジェクト（Extended ACL Object）：拡張アクセス コントロール リストの場合。拡張 ACL 変数では、拡張 ACL オブジェクトの名前が返されます。コンテンツ テーブルから **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択し、[拡張アクセス リスト オブジェクトの追加（Add Extended Access List Object）] をクリックします。アクセスリスト （1319 ページ）を参照してください。
- ルート マップ（Route Map）：ルート マップ オブジェクトの場合。ルート マップ変数では、ルート マップ オブジェクトの名前が返されます。コンテンツ テーブルから [ルート マップ（Route Map）] を選択し、[ルート マップの追加（Add Route Map）] をクリックします。「ルート マップ （1380 ページ）」を参照してください。

FlexConfig システム変数

システム変数は、デバイス自体やデバイスに設定されたポリシーから取得した情報に置き換えられます。

FlexConfig オブジェクト エディタの **[挿入（Insert）]** > **[システム変数の挿入（Insert System Variable）]** > ***[変数名]*** メニューを使用して、最初の変数を FlexConfig のスクリプトに追加し、

システム変数とのアソシエーションを確立します。単に$記号に続けてシステム変数名を入力しても、FlexConfig オブジェクトのコンテキストでのシステム変数は作成されません。

次の表に、使用可能なシステム変数の説明を示します。変数を使用する前に、通常、その変数に何が返されるかを確認します。変数がデバイスに関して返す内容を表示する方法（2697ページ）を参照してください。

名前	説明
SYS_FW_OS_MODE	デバイスのオペレーティング システム モード。値はROUTEDまたは TRANSPARENT です。
SYS_FW_OS_MULTIPLICITY	デバイスがシングル コンテキスト モードまたはマルチ コンテキスト モードのいずれで動作するか。値は、SINGLE、MULTI、または NOT_APPLICABLE です。
SYS_FW_MANAGEMENT_IP	デバイスの管理 IP アドレス。
SYS_FW_HOST_NAME	デバイスのホスト名。
SYS_FTD_INTF_POLICY_MAP	キーがインターフェイス名で、値がポリシーマップのマップ。この変数は、デバイスにインターフェイスベースのサービス ポリシーが定義されていない場合、値を返しません。
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	インスペクションが有効になっているプロトコルのリスト。
SYS_FTD_ROUTED_INTF_MAP_LIST	デバイスのルーテッド インターフェイス マップのリスト。各マップには、ルーテッド インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_SWITCHED_INTF_MAP_LIST	デバイスのスイッチド インターフェイス マップのリスト。各マップには、スイッチド インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_INLINE_INTF_MAP_LIST	デバイスのインライン インターフェイス マップのリスト。各マップには、インライン セット インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_PASSIVE_INTF_MAP_LIST	デバイスのパッシブ インターフェイス マップのリスト。各マップには、パッシブ インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_INTF_BVI_MAP_LIST	デバイスのブリッジ仮想インターフェイスマップのリスト。各マップには、BVI 構成に関連する一連の名前付き値が含まれます。
SYS_FW_INTERFACE_HARDWARE_ID_LIST	GigabitEthernet0/0など、デバイスのインターフェイスのハードウェア名のリスト。
SYS_FW_INTERFACE_NAME_LIST	内部など、デバイスのインターフェイスの論理名のリスト。

名前	説明
SYS_FW_INLINE_INTERFACE_NAME_LIST	パッシブまたは ERSPAN パッシブとして設定されたインターフェイスの論理名のリスト。
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	すべてのルーテッド インターフェイスなど、インライン セットの一部ではないインターフェイスの論理名のリスト。

定義済みの FlexConfig オブジェクト

定義済みの FlexConfig オブジェクトは、選択機能に検証済みの設定を提供します。Firewall Management Center を使用して設定できない機能を設定する必要がある場合は、これらのオブジェクトを使用します。

次の表に、使用可能なオブジェクトを示します。関連するテキスト オブジェクトをメモしてください。定義済みの FlexConfig オブジェクトの動作をカスタマイズするには、これらのテキスト オブジェクトを編集する必要があります。テキスト オブジェクトにより、ネットワークおよびデバイスで必要な IP アドレスとその他の属性を使用して、設定をカスタマイズできます。

定義済みの FlexConfig オブジェクトを変更する必要がある場合は、オブジェクトをコピーしてそれを変更し、新しい名前で保存します。定義済みの FlexConfig オブジェクトを直接編集することはできません。

FlexConfig を使用して、他の ASA ベースの機能を設定できますが、これらの機能の設定は検証されていません。ASA 機能が Firewall Management Center ポリシーで設定できる機能と重複している場合は、FlexConfig を使用して設定しないでください。

たとえば、Snort 検査には HTTP プロトコルが含まれるため、ASA スタイルの HTTP 検査を有効にしないでください。（実際に、enableInspectProtocolList オブジェクトに **http** を追加することはできません。この場合、デバイスを誤って設定することが回避されます）。代わりに、必要に応じて、アプリケーションまたは URL フィルタリングを実行するアクセス コントロール ポリシーを設定し、HTTP 検査要件を実装します。

表 *205* : 定義済みの *FlexConfig* オブジェクト

FlexConfig オブジェクト名	説明	関連するテキストオブジェクト
Default_Inspection_Protocol_Disable	global_policy デフォルト ポリシー マップのプロトコルを無効にします。	disableInspectProtocolList
Default_Inspection_Protocol_Enable	global_policy デフォルト ポリシー マップのプロトコルを有効にします。	enableInspectProtocolList
Inspect_IPv6_Configure	global_policy ポリシー マップで IPv6 検査を設定し、IPv6 ヘッダー コンテンツに基づいてトラフィックを記録およびドロップします。	IPv6RoutingHeaderDropLogList、IPv6RoutingHeaderLogList、IPv6RoutingHeaderDropList。

FlexConfig オブジェクト名	説明	関連するテキストオブジェクト
Inspect_IPv6_UnConfigure	IPv6 検査をクリアおよび無効にします。	—
ISIS_Configure	IS-IS ルーティングのグローバル パラメータを設定します。	isIsNet、isIsAddressFamily、isISType
ISIS_Interface_Configuration	インターフェイス レベルの IS-IS 設定。	isIsAddressFamily、IsIsIntfList また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します
ISIS_Unconfigure	デバイスの IS-IS ルータ設定をクリアします。	—
ISIS_Unconfigure_All	デバイスから IS-IS ルータ設定をクリアします（デバイスインターフェイスの IS-IS ルータ割り当てなど）。	—
Netflow_Add_Destination	NetFlow エクスポートの宛先を作成し、設定します。	Netflow_Destinations、netflow_Event_Types
Netflow_Clear_Parameters	NetFlow エクスポートのグローバルデフォルト設定を復元します。	—
Netflow_Delete_Destination	NetFlow エクスポートの宛先を削除します。	Netflow_Destinations、netflow_Event_Types
Netflow_Set_Parameters	NetFlow エクスポートのグローバルパラメータを設定します。	netflow_Parameters
NGFW_TCP_NORMALIZATION	デフォルトTCP正規化設定を変更します。	—
Policy_Based_Routing	この設定例を使用するには、コピーしてインターフェイス名を変更し、r-map-object テキストオブジェクトを使用してオブジェクト マネージャでルート マップ オブジェクトを特定します。	—
Policy_Based_Routing_Clear	デバイスからポリシーベース ルーティング設定をクリアします。	—
Sysopt_AAA_radius	RADIUS アカウンティング応答内の認証キーを無視します。	—
Sysopt_AAA_radius_negate	Sysopt_AAA_radius設定を拒否します。	—

FlexConfig オブジェクト名	説明	関連するテキストオブジェクト
Sysopt_basic	sysopt 待機時間、TCP パケットの最大セグメントサイズ、詳細トラフィック統計情報を設定します。	tcpMssMinimum、tcpMssBytes
Sysopt_basic_negate	sysopt_basic 詳細トラフィック統計情報、待機時間、TCP 最大セグメントサイズをクリアします。	—
Sysopt_clear_all	デバイスからすべての sysopt 設定をクリアします。	—
Sysopt_noproxyarp	noproxy arp CLI を設定します。	システム変数 SYS_FW_NON_INLINE_INTF_NAME_LIST を使用します
Sysopt_noproxyarp_negate	Sysopt_noproxyarp 設定をクリアします。	システム変数 SYS_FW_NON_INLINE_INTF_NAME_LIST を使用します
Sysopt_Preserve_Vpn_Flow	syopt 保存 VPN フローを設定します。	—
Sysopt_Preserve_Vpn_Flow_negate	Sysopt_Preserve_Vpn_Flow 設定をクリアします。	—
Sysopt_Reclassify_Vpn	sysopt 再分類 vpn を設定します。	—
Sysopt_Reclassify_Vpn_Negate	sysopt 再分類 vpn を拒否します。	—
Threat_Detection_Clear	脅威検出 TCP 代行受信設定をクリアします。	—
Threat_Detection_Configure	TCP 代行受信によって代行受信される攻撃の脅威検出統計情報を設定します。	threat_detection_statistics
Wccp_Configure	このテンプレートは WCCP を設定する例を提供します。	isServiceIdentifier、serviceIdentifier、wccpPassword
Wccp_Configure_Clear	WCCP 設定をクリアします。	—

廃止された FlexConfig オブジェクト

次の表に、GUI でネイティブに設定できるようになった機能を設定するオブジェクトを示します。できるだけ早くこれらのオブジェクトの使用を中止してください。

表 *206 :* 廃止された定義済みの *FlexConfig* オブジェクト

廃止されたバージョン	FlexConfig オブジェクト	説明	現在の設定場所
7.3	DHCPv6_Prefix_Delegation_Configure	IPv6 プレフィックス委任の 1 つの外部インターフェイス（プレフィックス委任クライアント）と 1 つの内部インターフェイス（委任されたプレフィックスの受信者）を設定します。このテンプレートを使用するには、テンプレートをコピーして変数を変更します。 関連するテキストオブジェクト：pdoutside、pdinside また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します	インターフェイス IPv6 の設定。
7.3	DHCPv6_Prefix_Delegation_UnConfigure	DHCPv6 プレフィックス委任設定を削除します。	インターフェイス IPv6 の設定。
6.3	Default_DNS_Configure	デフォルト DNS グループを設定します。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバーを定義します。 関連するテキストオブジェクト：defaultDNSNameServerList, defaultDNSParameters	プラットフォームの設定。
6.3	DNS_Configure	デフォルト以外の DNS サーバーグループの DNS サーバーを設定します。グループの名前を変更するには、オブジェクトをコピーします。	オブジェクトマネージャの **DNS サーバーグループ**。
6.3	DNS_UnConfigure	Default_DNS_Configure と DNS_Configure で実行される DNS サーバーの構成を削除します。DNS_Configure を変更した場合に DNS サーバー グループ名を変更するには、オブジェクトをコピーします。	オブジェクトマネージャの **DNS サーバーグループ**。

廃止されたバージョン	FlexConfig オブジェクト	説明	現在の設定場所
7.2	Eigrp_Configure	EIGRP ルーティングのネクストホップ、自動集約、ルータ ID、eigrp スタブを設定します。 関連するテキストオブジェクト：eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary	すべての EIGRP オブジェクトについては、EIGRP（1205 ページ）を参照してください。 システムでは、アップグレード後に展開できますが、EIGRP 構成をやり直すように警告されます。このプロセスを支援するために、コマンドライン移行ツールが用意されています。
7.2	Eigrp_Interface_Configure	EIGRP インターフェイス認証モード、認証キー、Hello インターバル、ホールド時間、スプリット ホライズンを設定します。 関連するテキストオブジェクト：eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します	
7.2	Eigrp_Unconfigure	デバイスから自律システムの EIGRP 設定をクリアします。	
7.2	Eigrp_Unconfigure_all	すべての EIGRP 設定をクリアします。	
6.3	TCP_Embryonic_Conn_Limit	初期接続制限を設定して SYN フラッド サービス妨害（DoS）攻撃から保護します。 関連するテキストオブジェクト：tcp_conn_misc、tcp_conn_limit	サービスポリシー。
6.3	TCP_Embryonic_Conn_Timeout	初期接続タイムアウトを設定して SYN フラッド サービス妨害（DoS）攻撃から保護します。 関連するテキストオブジェクト：tcp_conn_misc、tcp_conn_timeout	サービスポリシー。

廃止されたバージョン	FlexConfig オブジェクト	説明	現在の設定場所
7.2	VxLAN_Clear_Nve	デバイスから VxLAN_Configure_Port_And_Nve が使用される場合、NVE 1 設定を削除します。	すべての VXLAN オブジェクトについては、VXLAN インターフェイスの設定（697 ページ）を参照してください。 以前のバージョンで FlexConfig を使用して VXLAN インターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN 設定をやり直す場合は、FlexConfig 設定を削除します。
7.2	VxLAN_Clear_Nve_Only	展開時にインターフェイスで設定された NVE 設定をクリアします。	
7.2	VxLAN_Configure_Port_And_Nve	VLAN ポートと NVE 1 を設定します。 関連するテキストオブジェクト：vxlan_Port_And_Nve	
7.2	VxLAN_Make_Nve_Only	NVE のみのインターフェイスを設定します。 関連するテキストオブジェクト：vxlan_Nve_Only また、システム変数 SYS_FTD_ROUTED_MAP_LIST と SYS_FTD_SWITCHED_INTF_MAP_LIST を使用します	
7.2	VxLAN_Make_Vni	VNI インターフェイスを作成します。これを展開した後、VNI インターフェイスを正しく検出するには、デバイスの登録を解除して、再登録する必要があります。 関連するテキストオブジェクト：vxlan_Vni	

定義済みのテキスト オブジェクト

複数の定義済みのテキスト オブジェクトがあります。これらのオブジェクトは、定義済みの FlexConfig オブジェクトで使用される変数に関連付けられています。ほとんどの場合、関連付けられた FlexConfig オブジェクトを使用するにはこれらのオブジェクトを編集して値を追加する必要があります。そうしない場合、展開中にエラーが表示されます。これらのオブジェクトの一部にはデフォルト値が含まれていますが、その他は空となっています。

テキスト オブジェクトの編集の詳細については、FlexConfigテキスト オブジェクトの設定 （2720 ページ）を参照してください。

名前	説明	関連する FlexConfig オブジェクト
defaultDNSNameServerList (非推奨メソッド.)	デフォルト DNS グループで設定する DNS サーバの IP アドレス。 バージョン 6.3 以降では、Threat Defenseプラットフォーム設定ポリシーでデータインターフェイスの DNS を設定します。	Default_DNS_Configure
defaultDNSParameters (非推奨メソッド.)	デフォルト DNS サーバー グループの DNS動作を制御するパラメータ。オブジェクトには、再試行、タイムアウト、有効期限エントリ タイマー、ポール タイマー、ドメイン名の個別のエントリが順番に含まれています。 バージョン 6.3 以降では、Threat Defenseプラットフォーム設定ポリシーでデータインターフェイスの DNS を設定します。	Default_DNS_Configure
disableInspectProtocolList	デフォルト ポリシー マップ（global_policy）のプロトコルを無効にします。	Disable_Default_Inspection_Protocol
dnsNameServerList	ユーザー定義の DNS グループで設定する DNS サーバーの IP アドレス。	DNS_Configure
dnsParameters	デフォルト以外の DNS サーバー グループの DNS動作を制御するパラメータ。オブジェクトには、再試行、タイムアウト、ドメイン名、ドメイン名、ネーム サーバー インターフェイスの個別のエントリが順番に含まれています。	DNS_Configure

名前	説明	関連する FlexConfig オブジェクト
enableInspectProtocolList	デフォルト ポリシー マップ（global_policy）のプロトコルを有効にします。検査が Snort 検査と競合するプロトコルを追加することはできません。	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	ユーザーが拒否する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査でドロップをログに記録せずにドロップされます。	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	ユーザーが拒否し、ログに記録する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査でドロップされ、ドロップに関する syslog メッセージが送信されます。	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	許可するが、ログに記録する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査で許可されますが、ヘッダーの存在に関する syslog メッセージが送信されます。	Inspect_IPv6_Configure
isIsAddressFamily	IPv4 または IPv6 アドレス ファミリ。	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	論理インターフェイス名のリスト。	ISIS_Interface_Configuration
isIsISType	IS タイプ（level-1、level-2-only、または level-1-2）。	ISIS_Configure
isIsNet	ネットワーク エンティティ。	ISIS_Configure
isServiceIdentifier	false の場合は、標準 **web-cache** サービス識別子を使用します。	Wccp_Configure
netflow_Destination	1 つの NetFlow エクスポート宛先のインターフェイス、接続先、および UDP ポート番号を定義します。	Netflow_Add_Destination

名前	説明	関連する FlexConfig オブジェクト
netflow_Event_Types	エクスポートされる宛先のイベントのタイプを **all**、**flow-create**、**flow-defined**、**flow-teardown**、**flow-update** のいずれかのサブセットとして定義します。	Netflow_Add_Destination
netflow_Parameters	NetFlow エクスポートのグローバル設定を指定します。アクティブ更新間隔（フロー更新イベント間の分数）、遅延（フロー作成遅延（秒単位）。デフォルトの 0 ではコマンドは表示されません）、およびテンプレートタイムアウト レート（分単位）。	Netflow_Set_Parameters
PrefixDelegationInside	DHCPv6 プレフィックス委任の内部インターフェイスを設定します。オブジェクトには、インターフェイス名、IPv6 サフィックスとプレフィックス長、およびプレフィックスプール名の複数のエントリが順番に含まれています。	なし、ただし DHCPv6_Prefix_Delegation_Configure のコピーとともに使用できます。
PrefixDelegationOutside	外部 DHCPv6 プレフィックス委任クライアントを設定します。オブジェクトには、インターフェイス名と IPv6 プレフィックス長の複数のエントリが順番に含まれています。	なし、ただし DHCPv6_Prefix_Delegation_Configure のコピーとともに使用できます。
serviceIdentifier	ダイナミック WCCP サービス ID 番号。	Wccp_Configure
tcp_conn_limit (非推奨メソッド.)	TCP 初期接続制限を設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能をThreat Defense サービス ポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Limit

名前	説明	関連する FlexConfig オブジェクト
tcp_conn_misc (非推奨メソッド.)	TCP 初期接続設定を設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能を Threat Defense サービスポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Limit、TCP_Embryonic_Conn_Timeout
tcp_conn_timeout (非推奨メソッド.)	TCP 初期接続タイムアウトを設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能を Threat Defense サービスポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Timeout
tcpMssBytes	最大セグメント サイズ（バイト単位）。	Sysopt_basic
tcpMssMinimum	このフラグが true の場合にのみ設定される最大セグメントサイズ（MSS）を設定するかどうかをチェックします。	Sysopt_basic
threat_detection_statistics	TCP 代行受信の脅威検出統計情報に使用されるパラメータ。	Threat_Detection_Configure
vxlan_Nve_Only	インターフェイスで NVE-only を設定するためのパラメータ： • インターフェイスの論理名 • IPv4 アドレス（ルーテッド インターフェイスではオプション） • IPv4 ネットマスク（ルーテッドインターフェイスではオプション）	VxLAN_Make_Nve_Only

名前	説明	関連する FlexConfig オブジェクト
vxlan_Port_And_Nve	VXLAN のポートおよびNVE を設定するために使用されるパラメータ： • vxlan ポート • 送信元インターフェイス（論理名） • タイプ（ピアまたは mcast） • ピアとなる IP アドレスまたは default-mcast-group	VxLAN_Configure_Port_And_Nve
vxlan_Vni	VNI を作成するために使用されるパラメータ： • インターフェイス番号（1 ～ 10000） • segment-id（1 ～ 16777215） • nameif（インターフェイスの論理名） • タイプ（ルーテッドまたはトランスペアレント） • IP アドレス（ルーテッドモードのデバイスの場合に使用）またはブリッジグループ番号（トランスペアレントモードのデバイスの場合に使用） • ネットマスク（デバイスがルーテッドモードの場合）または未使用	VxLAN_Make_Vni
wccpPassword	WCCP パスワード。	Wccp_Configure

FlexConfig ポリシーの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

FlexConfig の注意事項と制約事項

- FlexConfig ポリシーに誤りがあると、システムは失敗した FlexConfig を含む展開の試行に含まれるすべての変更をロールバックします。展開の失敗が原因でロールバックに設定のクリアが含まれるため、ネットワークに悪影響を及ぼす可能性があります。営業時間外の FlexConfig の変更を含む、展開のタイミングを検討します。また、FlexConfig の変更だけが含まれるように展開を分離し、その他のポリシーの更新が行われないようにします。
- VxLAN_Make_VNI オブジェクトを使用する場合は、クラスタまたはハイ アベイラビリティ ペアを形成する前に、同じ FlexConfig をクラスタまたはハイ アベイラビリティ ペアのすべてのユニットに展開する必要があります。管理センターでは、クラスタまたはハイアベイラビリティペアを形成する前に、すべてのデバイスでVXLANインターフェイスを照合する必要があります。
- SIPインスペクションなどの接続に適用されるサービスを設定する場合は、デバイスのCLIに移動し、**clear conn** コマンドを入力して接続をクリアします。接続が再構築されると、新しい設定がセッションに適用されます。

FlexConfig ポリシーによるデバイス設定のカスタマイズ

FlexConfigポリシーを使用して、Firewall Threat Defenseデバイスの設定をカスタマイズします。

FlexConfig を使用する前に、Firewall Management Center のその他の機能を使用して、必要なすべてのポリシーと設定を設定してみます。FlexConfig は、Firewall Threat Defense との互換性があるが、他の方法では Firewall Management Center で設定できない ASA ベースの機能を設定するための最終手段です。

次に、FlexConfig ポリシーを設定し、導入するためのエンドツーエンドの手順を示します。

手順

ステップ 1 設定する CLI コマンド シーケンスを特定します。

ASA デバイスに機能する設定がある場合は、**show running-config** を使用して必要なコマンドのシーケンスを取得します。必要に応じてインターフェイス名、IPアドレスなどの項目を調整します。

新しい機能の場合は、ラボの設定で ASA デバイスに実装して、コマンド シーケンスが適切であることを確認することをお勧めします。

詳細は、次のトピックを参照してください。

- FlexConfig ポリシーの推奨される使用法 （2688 ページ）
- FlexConfig オブジェクトの CLI コマンド （2689 ページ）

ステップ 2 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツテーブルから **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]** を選択します。

事前定義済みFlexConfigオブジェクトを確認して、必要なコマンドを生成できるかどうかを判断します。**表示**（🔍） をクリックして、オブジェクトの内容を表示します。既存のオブジェクトが必要なオブジェクトに近い場合は、最初にオブジェクトをコピーして、そのコピーを編集します。定義済みの FlexConfig オブジェクト （2701 ページ）を参照してください。

また、オブジェクトの確認によって、FlexConfig オブジェクトの構造、コマンド構文、および予測されるシーケンシングを把握できます。

（注）
使用するオブジェクトを見つけた場合は、オブジェクトの下の [変数（Variables）] リストを直接またはコピーして確認します。SYS で始まるすべて大文字の変数名（システム変数）を除くすべての変数名を記録します。これらの変数は、特にデフォルト値のカラムでオブジェクトに値がないことが示されている場合に、編集またはオーバーライドの定義が必要になる可能性があるテキスト オブジェクトです。

ステップ 3 独自のFlexConfigオブジェクトを作成する必要がある場合は、必要な変数を特定し、関連オブジェクトを作成します。

導入する必要があるCLIには、時間の経過とともに調整する必要があるIPアドレス、インターフェイス名、ポート番号、およびその他のパラメータが含まれている場合があります。これらは、必要な値が含まれているオブジェクトを指す変数に隔離することをお勧めします。また、設定の一部であるが、時間の経過とともに変化する可能性がある文字列の変数が必要な場合があります。

さらに、ポリシーを割り当てる各デバイスに異なる値が必要かどうかを特定します。たとえば、3 つのデバイスの機能を設定し、これらのデバイスそれぞれに指定されたコマンドで異なるインターフェイス名または IP アドレスの指定が必要になる場合があります。各デバイスのオブジェクトをカスタマイズする必要がある場合は、オブジェクトを作成するときにオーバーライドを有効にして、デバイスごとのオーバーライド値を定義します。

変数のさまざまなタイプおよび必要に応じた関連オブジェクトの設定方法については、次のトピックを参照してください。

- FlexConfig 変数 （2693 ページ）
- FlexConfig ポリシー オブジェクト変数 （2698 ページ）
- FlexConfig システム変数 （2699 ページ）
- FlexConfig テキスト オブジェクトの設定 （2720 ページ）

ステップ 4 事前定義済み FlexConfig オブジェクトを使用する場合は、変数として使用されるテキスト オブジェクトを編集します。

FlexConfig テキスト オブジェクトの設定 （2720 ページ）を参照してください。

ステップ 5 （必要な場合）FlexConfig オブジェクトの設定 （2714 ページ）。

事前定義済みオブジェクトが機能しない場合にのみ、オブジェクトを作成する必要があります。

ステップ 6 FlexConfig ポリシーの設定 （2722 ページ）。

ステップ 7 FlexConfig ポリシーのターゲット デバイスの設定 （2723 ページ）。

ポリシーを作成するときに、デバイスにポリシーを割り当てることもできます。ポリシーをプレビューするには、そのポリシーに 1 つ以上のデバイスが割り当てられている必要があります。

ステップ 8 FlexConfig ポリシーのプレビュー （2724 ページ）。

ポリシーをプレビューする前に変更を保存する必要があります。

生成されたコマンドが目的のものであること、およびすべての変数が正しく解決されていることを確認します。

ステップ 9 メニューバーで、**[展開（Deploy）] > [展開（Deployment）]** を選択します。

ステップ 10 ポリシーに割り当てられたデバイスを選択して [展開（Deploy）] をクリックします。

展開が完了するまで待機します。

ステップ 11 展開された構成の確認 （2725 ページ）。

ステップ 12 （必要な場合）FlexConfig を使用した設定済み機能の削除 （2727 ページ）。

他のタイプのポリシーとは異なり、単にデバイスから FlexConfig を割り当て解除しても関連設定は削除されません。FlexConfig で生成された設定を削除するには、指示された手順に従う必要があります。

現在製品によって直接サポートされているために機能を削除する場合は、FlexConfig から管理対象機能への変換 （2728 ページ）も参照してください。

FlexConfig オブジェクトの設定

FlexConfig オブジェクトを使用して、デバイスに展開する設定を定義します。各 FlexConfig ポリシーは、FlexConfig オブジェクトのリストで構成されるため、オブジェクトは基本的に Apache Velocity スクリプト コマンド、ASA ソフトウェア コンフィギュレーション コマンド、および変数で構成されるコード モジュールです。

直接使用できる事前定義済みの FlexConfig オブジェクトがいくつかあります。これらを編集する必要がある場合は、コピーすることができます。また、独自のオブジェクトをはじめから作成することもできます。FlexConfig オブジェクトの内容の範囲は、単一の簡単なコマンド文字

列から、変数およびスクリプトコマンドを使用してデバイスまたは展開ごとに内容が異なるコマンドを展開する複雑な CLI コマンド構造におよびます。

また、FlexConfig ポリシーを定義するときに、FlexConfig ポリシー オブジェクトを作成できます。

始める前に

次の点を考慮してください。

- FlexConfig オブジェクトはデバイスに展開されるコマンドに変換されます。これらのコマンドは、グローバルコンフィギュレーションモードですでに発行されています。したがって **enable** コマンドと **configure terminal** コマンドを FlexConfig オブジェクトの一部として含めないでください。
- 必要な変数のタイプを特定し、必要なポリシーオブジェクトを作成します。FlexConfig オブジェクトの編集時に変数のオブジェクトを作成することはできません。
- コマンドがデバイスの VPN またはアクセス コントロール設定とまったく競合していないことを確認します。
- インターフェイスのコマンド セットが複数ある場合は、最後のコマンド セットだけが展開されます。したがって、開始コマンドと終了コマンドを使用してインターフェイスを設定しないことを推奨します。インターフェイスを設定する例として、事前定義済み FlexConfig オブジェクトの ISIS_Interface_Configuration を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクトタイプのリストから **[FlexConfig]** > **[FlexConfig オブジェクト（FlexConfig Object）]** を選択します。

ステップ 3 次のいずれかを実行します。

- [FlexConfig オブジェクトの追加（Add FlexConfig Object）] をクリックして、新しいオブジェクトを作成します。
- [編集（Edit）]（ ） をクリックして、既存のオブジェクトを編集します。
- **表示**（ ） をクリックして、事前定義済みオブジェクトの内容を表示します。
- 事前定義済みオブジェクトを編集するには、**クローン**（ ） をクリックして、同じ内容の新しいオブジェクトを作成します。

ステップ 4 **名前**を入力し、オプションでオブジェクトの説明を入力します。

ステップ 5 オブジェクト本体領域に、必要な設定を生成するためのコマンドと命令を入力します。

オブジェクトの内容は、有効な ASA ソフトウェアのコマンド シーケンスを生成する一連のスクリプト コマンドおよびコンフィギュレーション コマンドです。Firewall Threat Defense デバイスでは、ASA ソフトウェア コマンドを使用して一部の機能を設定します。スクリプト コマンドおよびコンフィギュレーション コマンドの詳細については、次を参照してください。

- テンプレート スクリプト （2692 ページ）
- FlexConfig オブジェクトの CLI コマンド （2689 ページ）

変数を使用して、ランタイムにのみ通知される情報やデバイスごとに異なる情報を指定できます。プロセス変数に入力しますが、[挿入（Insert）] メニューを使用して、ポリシーオブジェクトまたはシステム変数に関連付けられているか、秘密キーである変数を追加する必要があります。変数の詳細については、FlexConfig 変数 （2693 ページ）を参照してください。

- システム変数を挿入するには、**[挿入（Insert）] > [システム変数の挿入（Insert System Variable）] > [変数名]** を選択します。これらの変数の詳細については、FlexConfig システム変数 （2699 ページ）を参照してください。
- ポリシー オブジェクトの変数を挿入するには、**[挿入（Insert）] > [ポリシー オブジェクトの挿入（Insert Policy Object）] > [オブジェクト タイプ]** を選択し、適切なオブジェクトのタイプを選択します。次に、変数に名前を付け（関連付けられたポリシー オブジェクトと同じ名前にすることができます）、変数に関連付けるオブジェクトを選択し、[保存（Save）] をクリックします。これらのタイプの詳細については、FlexConfig ポリシー オブジェクト変数（2698 ページ）を参照してください。手順の詳細については、FlexConfig オブジェクトへのポリシーオブジェクト変数の追加 （2718 ページ）を参照してください。
- 秘密キーの変数を挿入するには、**[挿入（Insert）] > [秘密キー（Secret Key）]** を選択し、変数名と値を定義します。手順の詳細については、秘密キーの設定 （2719 ページ）を参照してください。

（注）
[挿入（Insert）] メニューを使用して、新しいポリシー オブジェクトまたはシステム変数を作成する必要があります。ただし、その変数を後で使用するために、$ を含めて入力する必要があります。これは、システム変数にも当てはまります。システム変数を初めて使用する場合は、[挿入（Insert）] メニューから追加します。次に、後で使用するために入力します。1 つのシステム変数に [挿入（Insert）] メニューを複数回使用すると、システム変数が [変数（Variables）] リストに複数回追加され、FlexConfig が有効ではなくなるため、変更を保存できなくなります。プロセス変数（ポリシー オブジェクトやシステム変数に関連付けられていない）の場合は、変数を入力します。秘密キーを追加する場合は、常に [挿入（Insert）] メニューを使用します。秘密キーの変数は [変数（Variables）] リストに表示されません。

ステップ 6 展開の頻度およびタイプを選択します。

- [展開（Deployment）]：オブジェクトにコマンドを [1 回（Once）] または [毎回（Everytime）] 展開することを指定します。適切なオプションを選択する唯一の方法は、展開の結果をテストする方法です。

  最初に [毎回（Everytime）] を選択します。次に、FlexConfig ポリシーにオブジェクトをアタッチして、設定を展開します。展開に成功したら、FlexConfig ポリシーに戻り、FlexConfig

ポリシーのプレビュー（2724ページ）の説明に従って、割り当てられたいずれかのデバイスの設定をプレビューします。`###CLI generated from managed features ###` のラベルが付いたセクションに、オブジェクト内のコマンドの clear または negate コマンドが含まれていて、`###Flex-config Appended CLI ###` セクションに機能を再設定するためのコマンドが含まれている場合、[毎回（Everytime）] が適切なオプションであることがわかります。

negate コマンドが表示されていない場合でも、デバイス設定に少し変更を加えて、別の展開を実行します。展開が正常に完了したら、展開トランスクリプトを確認できます（展開された構成の確認（2725ページ）を参照）。（コマンドがすでに設定されている場合でも）コマンドがエラーなく再発行されているのを確認できたら、[毎回（Everytime）] のままにします。

システムがオブジェクト内のコマンドを最初に取り消してから再発行しない場合、または展開の結果に、コマンドに固有のエラーがある場合にのみ [1回（Once）] に変更します。場合によっては、設定済みのコマンドの発行を許可されないことがありますが、それは例外的です。

追加のヒント：

- FlexConfig オブジェクトが、ネットワーク オブジェクトや ACL オブジェクトなどのシステム管理対象オブジェクトを指している場合は、[毎回（Everytime）] を選択します。そうしないと、オブジェクトに対する更新が展開されない可能性があります。
- オブジェクトで行う操作が設定のクリアだけの場合は、[1回（Once）] を使用します。そして、次の展開後に FlexConfig ポリシーからオブジェクトを削除します。

- [タイプ（Type）]：次のいずれかを選択します。
  - [後に付加（Append）]：（デフォルト）。オブジェクトのコマンドは、Firewall Management Center ポリシーから生成された設定の最後に配置されます。管理対象オブジェクトから生成されたオブジェクトを指すポリシーオブジェクトの変数を使用する場合は、[後に付加（Append）] を使用する必要があります。その他のポリシー向けに生成されたコマンドがオブジェクトで指定されているものと重複する場合は、このオプションを選択してコマンドが上書きされないようにする必要があります。これは最も安全なオプションです。
  - [前に付加（Prepend）]：オブジェクトのコマンドは、Firewall Management Center ポリシーから生成された設定の最初に配置されます。通常、設定をクリアまたは除外するコマンドに [前に付加（Prepend）] を使用します。

ステップ 7 （オプション）オブジェクト本体の上にある **検証**（） をクリックして、スクリプトの整合性を確認します。

[保存（Save）] をクリックするたびに、オブジェクトが検証されます。無効なオブジェクトを保存することはできません。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

FlexConfig オブジェクトへのポリシーオブジェクト変数の追加

FlexConfig ポリシー オブジェクトに、ポリシー オブジェクトの他のタイプと関連付けられた変数を挿入できます。FlexConfig をデバイスに展開すると、これらの変数は関連づけられたオブジェクトの名前やコンテンツに合わせて変換されます。

FlexConfig オブジェクトで初めてポリシー オブジェクト変数を使うときは、次の手順に従ってください。オブジェクトを再度参照する必要が生じたら、（$マークを含めて）変数を入力します。変数の使用方法を理解するには、変数の処理方法（2694 ページ）を参照してください。

始める前に

FlexConfig オブジェクトの設定の詳細については、FlexConfig オブジェクトの設定 （2714 ページ） を参照してください。

手順

ステップ 1 FlexConfig ポリシーオブジェクトの編集中に、[挿入（Insert）]>[ポリシーオブジェクトの挿入（Insert Policy Object）]>[オブジェクトのタイプ（Object Type）] から、適切なタイプのオブジェクトを選択します。

ステップ 2 変数の名前を入力し、任意で説明を入力します。

名前は、FlexConfig オブジェクトのコンテキストの中で一意なものである必要があります。スペースを含めることはできません。変数に関連付けるオブジェクトと同一の名前を使用できます。

ステップ 3 変数と関連付けるオブジェクトを選択し、[追加（Add）] をクリックしてこれを [選択済みオブジェクト（Selected Object）] リストに移動します。

変数には、1 つのみのオブジェクトを関連付けることができます。

（注）
テキストオブジェクトには、必要に応じて前もって定義されたオブジェクトを選択できます。しかし、これらオブジェクトの多くにはデフォルト値はありません。オブジェクトの更新では、必須の値を直接与えるか、ないしは FlexConfig オブジェクトを展開するデバイスのオーバーライドとして与える必要があります。これらのオブジェクトを更新せずに FlexConfig の展開を試行しても、多くの場合展開のエラーにつながります。

ステップ 4 [保存（Save）] をクリックします。

変数は、FlexConfig オブジェクトエディタの下の変数リストに表示されます。

秘密キーの設定

秘密キーは、パスワードなどの、内容をマスクする単一文字列の変数です。機密情報の拡散を防ぐため、これらの変数にはシステムによって特別な処理が行われます。

秘密キー変数は FlexConfig オブジェクトの変数リストに表示されません。

FlexConfig オブジェクトで秘密キー変数を作成、挿入、および管理するには、次の手順を使用します。他のタイプ変数とは異なり、所定の秘密キー変数を挿入する必要があるたびに **Insert** コマンドを使用できます。処理については、これらの変数は単一値のテキストオブジェクト変数と同様に機能します。単一値変数 （2694 ページ）を参照してください。

（注） 秘密キー変数で定義されたデータは、FlexConfig ポリシーのプレビュー時を除き、ユーザーからマスクされます。また、FlexConfig ポリシーをエクスポートする場合、すべての秘密キー変数の内容が消去されます。ポリシーをインポートする場合、各秘密キー変数を手動で編集してデータを入力する必要があります。

始める前に

FlexConfig オブジェクトの設定の詳細については、FlexConfig オブジェクトの設定 （2714 ページ）を参照してください。

手順

ステップ 1 FlexConfig ポリシー オブジェクトを編集する際には、**[挿入（Insert）]** > **[秘密キー（Secret Key）]** を選択します。

ステップ 2 [秘密キーの挿入（Insert Secret Key）] ダイアログボックスで、次のいずれかの手順を実行します。

- 新しいキーを作成するには、[秘密キーの追加（Add Secret Key）] をクリックし、次の情報を入力して [追加（Add）] をクリックします。
  - [秘密キー名（Secret Key Name）]：変数の名前。この名前は、前に @ が付けられて FlexConfig オブジェクトに表示されます。
  - [パスワード（Password）]、[パスワードの確認（Confirm Password）]：入力と同時に、アスタリスクでマスクされる秘密の文字列です。
- FlexConfig オブジェクトに秘密キー変数を挿入するには、変数のチェックボックスをオンにします。
- 秘密キー変数の値を編集するには、変数の [編集（Edit）]（ ） をクリックします。変更を加えて、[追加（Add）] をクリックします。
- 秘密キー変数を削除するには、変数の [削除（Delete）]（ ） をクリックします。

ステップ 3 [保存（Save）] をクリックします。

FlexConfig テキスト オブジェクトの設定

ポリシー オブジェクト変数の対象として FlexConfig オブジェクトでテキスト オブジェクトを使用します。変数を使用して、ランタイムにのみ通知される情報やデバイスごとに異なる情報を指定できます。展開中に、テキスト オブジェクトを指す変数はテキスト オブジェクトの内容に置き換えられます。

テキスト オブジェクトには自由形式の文字列が含まれます。キーワード、インターフェイス名、番号、IP アドレスなどにすることも可能です。内容は、FlexConfig スクリプト内の情報の使用方法によって異なります。

テキスト オブジェクトを作成または編集する前に、必要な内容を特定します。これにはオブジェクトの処理方法が含まれます。これを決めることで、1 つの文字列オブジェクトまたは複数の文字列オブジェクトのいずれを作成するかを決定するのに役立ちます。次のトピックを参照してください。

- FlexConfig 変数 （2693 ページ）
- 変数の処理方法 （2694 ページ）

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクト タイプのリストから **[FlexConfig]** > **[テキスト オブジェクト（Text Object）]** を選択します。

ステップ 3 次のいずれかを実行します。

- [テキスト オブジェクトの追加（Add Text Object）] をクリックして、新しいオブジェクトを作成します。
- [編集（Edit）]（✎） をクリックして、既存のオブジェクトを編集します。事前定義済み FlexConfigオブジェクトを使用する場合に必要となる、事前定義済みテキスト オブジェクトを編集できます。

ステップ 4 **名前**を入力し、オプションでオブジェクトの説明を入力します。

ステップ 5 （新しいオブジェクトのみ）ドロップダウン リストから**変数タイプ**を選択します。

- [単一（Single）]：オブジェクトに単一のテキスト文字列を含める必要がある場合。
- [複数（Multiple）]：オブジェクトにテキスト文字列のリストを含める必要がある場合。

オブジェクトの保存後は変数タイプを変更できません。

ステップ 6 変数タイプが [複数（Multiple）] の場合は、上下矢印を使用して [カウント（Count）] を指定します。

数を変更すると、オブジェクトの行が追加されたり、削除されたりします。

ステップ 7 オブジェクトに内容を追加します。

変数番号の横のテキスト ボックスをクリックして値を入力するか、テキスト オブジェクトを使用する FlexConfig オブジェクトを割り当てられる各デバイスに対してデバイスの上書きを設定できます。両方行うこともできますが、この場合、ベース オブジェクトで設定した値は、指定したデバイスの上書きが存在しない場合にデフォルト値として機能します。

事前定義済みオブジェクトの編集時には、デバイスの上書きを使用することをお勧めします。これは、別の FlexConfig ポリシーでオブジェクトを使用する必要がある他のユーザー用に、デフォルトが残るようにするためです。実行するアプローチは、組織の要件に応じて異なります。

ヒント
一部の事前定義済みオブジェクトには、各値が特定の目的を提供する複数の値が必要です。オブジェクトの予測される値を特定するために、説明テキストを注意深く読みます。手順では、base 値を変更する代わりに上書きを使用する必要があることが指定される場合があります。enableInspectProtocolList の場合は、インスペクションに Snort インスペクションとの互換性がないプロトコルを入力できません。

デバイスの上書きを使用する場合は、次の手順を実行します。

a) [オーバーライドを許可（Allow Override）] チェックボックスにマークを付けます。
b) [オーバーライド（Overrides）] を展開し（必要な場合）、[追加（Add）] をクリックします。

   上書きがデバイスにすでにある場合は、上書きの編集アイコンをクリックして変更します。

c) [オブジェクトのオーバーライドの追加（Add Object Override）] ダイアログボックスの [ターゲット（Targets）] で、値を定義するデバイスを選択し、[追加（Add）] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。
d) [オーバーライド（Overrides）] をクリックし、必要に応じて [カウント（Count）] を調整し、変数フィールドをクリックして、デバイスの値を入力します。
e) [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （172 ページ）を参照してください。

FlexConfig ポリシーの設定

FlexConfig ポリシーには、FlexConfig オブジェクトの 2 つの順序のリストが含まれています。1 つは先頭に追加されたリスト、もう 1 つは末尾に追加されたリストです。先頭に追加/末尾に追加の説明については、FlexConfig オブジェクトの設定 （2714 ページ）を参照してください。

FlexConfig ポリシーは、複数のデバイスに割り当てることができる共有ポリシーです。

手順

ステップ 1 **[デバイス（Devices）] > [FlexConfig]** を選択します。

ステップ 2 次のいずれかを実行します。

- [新しいポリシー（New Policy）] をクリックして、新しい FlexConfig ポリシーを作成します。名前を入力するプロンプトが表示されます。必要に応じて、[使用可能なデバイス（Available Devices）] リストでデバイスを選択し、[ポリシーに追加（Add to Policy）] をクリックしてデバイスを割り当てます。[保存（Save）] をクリックします。
- [編集（Edit）]（） をクリックして、既存のポリシーを編集します。名前や説明を編集モードでクリックして変更できます。
- [コピー（Copy）]（） をクリックして、同じ内容の新しいポリシーを作成します。名前を入力するプロンプトが表示されます。デバイス割り当てはコピーに保持されません。
- 削除アイコンをクリックして、不要になったポリシーを削除します。

ステップ 3 ポリシーに必要な FlexConfig オブジェクトを [使用可能な FlexConfig（Available FlexConfig）] リストから選択し、[>] をクリックしてポリシーに追加します。

オブジェクトは FlexConfig オブジェクトで指定した展開タイプに基づいて、先頭に追加されたリストまたは末尾に追加されたリストに自動的に追加されます。

選択したオブジェクトを削除するには、オブジェクトの横にある [削除（Delete）]（） をクリックします。

ステップ 4 選択したオブジェクトごとに、オブジェクトの横にある **表示**（） をクリックして、オブジェクトで使用されている変数を特定します。

SYS で始まるシステム変数を除き、変数に関連付けられているオブジェクトが空でないことを確認する必要があります。空白または間に何もない角カッコは、空のオブジェクトを示します。ポリシーを展開する前に、これらのオブジェクトを編集する必要があります。

（注）
オブジェクトのオーバーライドを使用する場合、これらの値はこのビューに表示されません。したがって、空のデフォルト値は、必ずしもオブジェクトが必要な値で更新されていないことを意味するわけではありません。設定をプレビューすると、変数が所定のデバイスに対して正しく解決されるかどうかが示されます。「FlexConfig ポリシーのプレビュー （2724 ページ）」を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- ポリシーのターゲット デバイスを設定します。FlexConfig ポリシーのターゲット デバイスの設定 （2723 ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

FlexConfig ポリシーのターゲット デバイスの設定

FlexConfig ポリシーを作成するときに、ポリシーを使用するデバイスを選択できます。その後、次の説明に従って、ポリシーに対するデバイスの割り当てを変更できます。

（注） 通常、デバイスからポリシーの割り当てを解除すると、次回の展開時に、システムは関連付けられた設定を自動的に削除します。ただし、FlexConfig オブジェクトはカスタマイズされたコマンドを展開するためのスクリプトであるため、単にデバイスから FlexConfig ポリシーの割り当てを解除しても、FlexConfig オブジェクトによって設定されたコマンドは削除されません。FlexConfig によって生成されたコマンドをデバイスの構成から削除することが目的の場合は、FlexConfig を使用した設定済み機能の削除 （2727 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、FlexConfig ポリシーを編集します。

ステップ 2 [ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 3 [ターゲットデバイス（Targeted Devices）] で、ターゲットリストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。ポリシーは、デバイス、高可用性ペア、およびクラスタを構成するデバイスに割り当てることができます。
- 削除：1 つのデバイスの横にある [削除（Delete）]（ ） をクリックするか、複数のデバイスを選択して、右クリックしてから [選択項目の削除（Delete Selection）] を選択します。

ステップ 4 [OK] をクリックして選択内容を保存します。

ステップ 5 [保存（Save）] をクリックして、FlexConfig ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

FlexConfig ポリシーのプレビュー

FlexConfig ポリシーをプレビューして、FlexConfig オブジェクトが、どのように CLI コマンドに変換されるかを確認します。プレビューには、FlexConfig オブジェクトで使用されるスクリプトおよび変数から、選択したデバイスに応じて生成されるコマンドが示されます。変数はデバイスの設定に基づいて解決されるため、展開される内容を明確に理解できます。

プレビューを使用すると、FlexConfig オブジェクトの潜在的な問題が見つかります。期待される結果がプレビューに示されるまで、オブジェクトを修正します。

設定は、デバイスごとに個別にプレビューする必要があります。これは、変数がデバイス設定に基づいてさまざまに解決される可能性があるためです。

手順

ステップ 1 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、FlexConfig ポリシーを編集します。

ステップ 2 未確定の変更がある場合は、[保存（Save）] をクリックします。

プレビューには、最後に保存したバージョンのポリシーに含まれる FlexConfig オブジェクトの結果のみが示されます。新しく追加したオブジェクトのプレビューを確認するには、ポリシーを保存する必要があります。

ステップ 3 [設定のプレビュー（Preview Config）] をクリックします。

ステップ 4 [デバイスの選択（Select Device）] ドロップダウンリストからデバイスを選択します。

システムは、デバイスからの情報と設定済みのポリシーを取得して、次回のデバイスへの展開時に生成する CLI コマンドを決定します。出力を選択してから Ctrl + C を押すことで、その出力をクリップボードにコピーできます。この出力は、詳細な分析のためにテキストファイルに貼り付けることができます。

プレビューには、次のセクションが含まれています。

- Flex-config により前に付加される CLI（Flex-config Prepended CLI）：FlexConfig によって生成されるコマンドであり、設定の前に付加されます。
- 管理対象の機能から生成された CLI（CLI generated from managed features）：Firewall Management Center で設定されたポリシーに応じて生成されるコマンドです。コマンドは、デバイスへの最後の正常な展開後の新規ポリシーまたは変更されたポリシーに対して生成されます。これらのコマンドは、割り当て済みのポリシーを実装するために必要なすべてのコマンドを表しているわけではありません。このセクション内のコマンドは、FlexConfig オブジェクトから生成されたものではありません。
- Flex-config により後に付加される CLI（Flex-config Appended CLI）：FlexConfig によって生成されるコマンドであり、設定の後に付加されます。

ステップ 5 [閉じる（Close）] ボタンをクリックして、プレビュー ダイアログを閉じます。

展開された構成の確認

デバイスにFlexConfigポリシーを展開した後、展開が成功したこと、およびこの構成が期待どおりのものであることを確認します。また、デバイスが期待どおりに機能していることを確認します。

手順

ステップ1 展開が成功したことを確認するには、次の手順を実行します。

a) メニューバーの [通知（Notifications）] をクリックします。このアイコンは、[展開（Deploy）] と [システム（System）] の間にある、名前のないアイコンです。

アイコンは、次のいずれかで、エラーがあると番号が付くことがあります。

- **（警告がないことを示す）**：警告とエラーはいずれもシステム上に存在していないことを示します。
- **（1 つ以上の警告があることを示す）**：1 つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
- **（1 つ以上のエラーがあることを示す）**：1 つ以上のエラーと任意の数の警告がシステム上に存在することを示します。

b) [展開（Deployment）] で、展開が成功したことを確認します。

c) 詳細な情報、特に失敗した展開の詳細を表示するには、[履歴の表示（Show History）] をクリックします。

d) 左側の列にあるジョブのリストで展開ジョブを選択します。

ジョブは新しい順に表示され、リストの一番上に最新のジョブが表示されます。

e) 右側の列にあるデバイスの [トランスクリプト（Transcript）] 列でダウンロードアイコンをクリックします。

展開トランスクリプトには、デバイスに送信されたコマンドおよびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、FlexConfig から送信したコマンドを含む、エラーを示すメッセージを探します。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注）
管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

たとえば、次のシーケンスは、論理名が outside の GigabitEthernet0/0 を設定するコマンドを Firewall Management Center が送信したことを示しています。デバイスは、自動的にセキュリティレベルを 0 に設定したことを応答しました。Firewall Threat Defense がセキュリティレベルを使用することはありません。FlexConfig に関連したメッセージは、トランスクリプトの [CLI 適用（CLI Apply）] セクションにあります。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

ステップ 2 展開された構成に必要なコマンドが含まれていることを確認します。

これは、デバイスの管理 IP アドレスへの SSH 接続を確立することで行うことができます。**show running-config** コマンドを使用して、設定を表示します。

または、Secure Firewall Management Center 内で CLI ツールを使用します。

a) >**[ヘルス（Health）]**>**[モニター（Monitor）]** を選択し、デバイスの名前をクリックします。

ステータス テーブルの [カウント（Count）] 列で開く/閉じる矢印をクリックしてデバイスを表示することが必要になる場合があります。

b) [詳細なトラブルシューティング（Advanced Troubleshooting）] をクリックします。
c) [脅威防御 CLI（Threat Defense CLI）] をクリックします。
d) コマンドとして [show] を選択し、パラメータとして「**running-config**」と入力します。
e) [実行（Execute）] をクリックします。

実行中の構成がテキスト ボックスに表示されます。構成を選択し、Ctrl キーを押した状態で C キーを押して、後で分析できるようにテキスト ファイルに貼り付けることができます。

ステップ 3 デバイスが期待どおりに機能していることを確認します。

機能に関連する **show** コマンドを使用して、詳細情報と統計情報を表示します。たとえば、追加のプロトコル インスペクションを有効にした場合、**show service-policy** コマンドを使用すると、この情報が提供されます。使用する正確なコマンドは機能に依存し、機能の設定方法を学習するときに使用した ASA 構成ガイドおよびコマンド リファレンスに記載されています。

統計情報を表示するコマンドで数（ヒット数、接続数など）が変更されていないことが示された場合、構成は有効であっても意味がないことがあります。トラフィックが、統計情報に表示されるはずのデバイスを通過していることがわかっている場合は、構成に欠如しているものを確認します。たとえば、トラフィックは、機能が適用される前に NAT またはアクセス ルールによってドロップまたは変更される場合があります。

SSH セッションまたは Firewall Management Center CLI ツールから **show** コマンドを使用できます。

ただし、使用する必要がある **show** コマンドを Firewall Threat Defense CLI 内で直接使用できない場合は、デバイスへのSSH接続を確立してコマンドを使用する必要があります。CLIから、次のコマンド シーケンスを入力して、診断 CLI 内で特権 EXEC モードに切り替えます。ここから、これらのサポートされない **show** コマンドを入力できます。

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

FlexConfig を使用した設定済み機能の削除

FlexConfig を使用して設定した一連の設定コマンドの削除が必要な場合は、その設定を手動で削除する必要があります。デバイスから FlexConfig ポリシーの割り当てを解除しても、すべての設定が削除されないことがあります。

手動で設定を削除するには、新しい FlexConfig オブジェクトを作成して、設定コマンドを消去または無効化します。

始める前に

オブジェクトによって生成された設定の一部またはすべてを手動で削除する必要があるかどうかを確認するには、次の手順を実行します。

1. FlexConfig ポリシーのプレビュー（2724 ページ）の説明に従い、設定のプレビューを調べます。FlexConfig オブジェクト内のすべてのコマンドを削除するための clear または negate コマンドが `###CLI generated from managed features ###` セクションに含まれている場合は、FlexConfig ポリシーから単純にオブジェクトを削除し、保存して再展開できます。
2. FlexConfig ポリシーからオブジェクトを削除し、変更を保存して、もう一度設定をプレビューします。`###CLI generated from managed features ###` セクションにまだ必要な clear または negate コマンドが含まれていない場合は、次の手順を実行して、手動で設定を削除する必要があります。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択して、FlexConfig オブジェクトを作成することで、設定コマンドを消去または取り消します。

機能に構成時の設定をすべて削除できる **clear** コマンドがある場合は、そのコマンドを使用します。たとえば、事前定義されている ISIS_Unconfigure_All オブジェクトには、次に示すように、すべての ISIS 関連の設定コマンドを削除する 1 つのコマンドが含まれています。

```
clear configure router isis
```

その機能に **clear** コマンドが存在しない場合は、削除する各コマンドの **no** 形式を使用する必要があります。たとえば、事前定義されている Sysopt_basic_negate オブジェクトは、事前定義されている Sysopt_basic オブジェクトで設定したコマンドを削除します。

```
no sysopt traffic detailed-statistics

no sysopt connection timewait
```

通常、設定を削除する FlexConfig オブジェクトを前に追加された、1 回のみ展開されるオブジェクトとして設定します。

ステップ 2 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、新しい FlexConfig ポリシーを作成するか、既存のポリシーを編集します。

設定コマンドを展開する FlexConfig ポリシーを保持する場合は、コマンドの取り消し専用の新しいポリシーを作成して、そのポリシーにデバイスを割り当てます。その後で、新しい FlexConfig オブジェクトをポリシーに追加します。

すべてのデバイスから完全に FlexConfig 設定オブジェクトを削除する場合は、既存の FlexConfig ポリシーから該当するコマンドを削除して、それらのコマンドを設定を取り消すオブジェクトで置き換えます。

ステップ 3 [保存（Save）] をクリックして、FlexConfig ポリシーを保存します。

ステップ 4 [設定のプレビュー（Preview Config）] をクリックして、消去および取り消しコマンドが適切に生成されていることを確認します。

ステップ 5 メニューバーの **[展開（Deploy）]** > **[展開（Deployment）]** を選択し、デバイスを選択して [展開（Deploy）] をクリックします。

展開が完了するまで待機します。

ステップ 6 コマンドが削除されたことを確認します。

デバイスの実行コンフィギュレーションを表示して、コマンドが削除されていることを確認します。詳細については、展開された構成の確認 （2725 ページ）を参照してください。

ステップ 7 FlexConfig ポリシーの編集中に、[ポリシーの割り当て（Policy Assignments）] をクリックして、デバイスを削除します。必要に応じて、ポリシーから FlexConfig オブジェクトを削除します。

FlexConfig ポリシーは単に不要な設定コマンドを削除するものであるため、削除の完了後にデバイスに割り当てたポリシーを保持する必要はありません。

ただし、FlexConfig ポリシーにデバイスで設定する必要のあるオプションが残っている場合は、そのポリシーから取り消しオブジェクトを削除します。これらは不要です。

FlexConfig から管理対象機能への変換

ソフトウェアリリースごとに、管理対象機能、つまり FlexConfig の外部で制御されるポリシーを介して直接設定する機能が製品に追加されます。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。ご使用の構成は自動的に変換されません。アップグレード後は、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作

成したりすることはできません。ソフトウェアのアップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。

FlexConfig を使用して設定した機能が管理対象機能としてサポートされるようになったら、FlexConfig の使用から管理対象機能の使用に変換する必要があります。ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。GUI と FlexConfig の両方で機能を設定することはサポートされていません。

（注） 移行する機能設定が移行ツールでサポートされている場合は、この手順の代わりに移行ツールを使用してください。

手順

ステップ 1 FlexConfig を使用した設定済み機能の削除 （2727 ページ）で説明されているように、FlexConfig を削除します。

ステップ 2 新しくサポートされた管理対象機能の設定を構成します。

リリースノートには、そのリリースの新機能のリストがあります。

FlexConfig の例

次に、FlexConfig の使用例をいくつか示します。

高精度時間プロトコルの設定方法（ISA 3000）

高精度時間プロトコル（PTP）は、パケットベース ネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。それらのデバイスクロックは、一般的に精度と安定性が異なります。このプロトコルは、産業用のネットワーク化された測定およびコントロールシステム向けに設計されており、必要な帯域幅は最小限で、処理オーバーヘッドが少ないため、分散システムでの使用に最適です。

PTP システムは、PTP デバイスと非 PTP デバイスの組み合わせで構成される分散ネットワークシステムです。PTP デバイスには、オーディナリクロック、境界クロック、およびトランスペアレントクロックが含まれます。非 PTP デバイスには、ネットワークスイッチ、ルータ、およびその他のインフラストラクチャ デバイスが含まれます。

Firewall Threat Defense デバイスは、トランスペアレントクロックとして設定できます。Firewall Threat Defense デバイスは、自身のクロックを PTP クロックと同期しません。Firewall Threat Defense デバイスは、PTP クロックで定義されている PTP のデフォルトプロファイルを使用します。

PTPデバイスを設定するときは、連携させるデバイスのドメイン番号を定義します。したがって、複数のPTPドメインを設定した後、1つの特定のドメインにPTPクロックを使用するように各非PTPデバイスを設定できます。

始める前に

デバイスが使用するPTPクロックに設定されているドメイン番号を確認します。この例では、PTPドメイン番号が10であることを前提としています。また、システムがドメイン内のPTPクロックに到達できるインターフェイスを決定します。

以下に、PTPの設定に関するガイドラインを示します。

- この機能は、Cisco ISA 3000アプライアンスでのみ使用できます。
- Cisco PTPは、マルチキャストPTPメッセージのみサポートしています。
- PTPはIPv4ネットワークでのみ使用でき、IPv6ネットワークでは使用できません。
- PTP設定は、スタンドアロンかブリッジ グループ メンバーかを問わず、物理イーサネット データ インターフェイスでサポートされます。管理インターフェイス、サブインターフェイス、EtherChannel、ブリッジ仮想インターフェイス（BVI）、またはその他の仮想インターフェイスではサポートされません。
- VLANサブインターフェイスでのPTPフローは、適切なPTP設定が親インターフェイス上に存在する場合にサポートされます。
- PTPパケットが確実にデバイスを通過できるようにする必要があります。PTPトラフィックはUDP宛先ポート319と320、および宛先IPアドレス224.0.1.129によって識別されます。そのため、このトラフィックを許可するアクセス コントロール ルールはすべて動作します。
- ルーテッド ファイアウォール モードでは、PTPマルチキャストグループのマルチキャストルーティングを有効にする必要があります。さらに、PTPをイネーブルにしたインターフェイスがブリッジグループに含まれ**ていない**場合は、IGMPマルチキャスト グループ224.0.1.129に参加するようにインターフェイスを設定する必要があります。物理インターフェイスがブリッジグループメンバーである場合、IGMPマルチキャストグループに参加するように設定しないでください。

手順

ステップ1 （ルーテッド モードのみ）マルチキャスト ルーティングを有効にし、インターフェイスのIGMPグループを設定します。

ルーテッド モードでは、マルチキャスト ルーティングを有効にする必要があります。また、スタンドアロンの物理インターフェイス、つまりブリッジ グループ メンバー以外のインターフェイスについても、224.0.1.129 IGMPグループに参加するようにインターフェイスを設定する必要があります。IGMPグループに参加するようにブリッジグループ メンバーを設定することはできませんが、ブリッジグループ メンバーのPTP設定はIGMP参加なしでも動作します。

PTP を設定するデバイスごとに次の手順を実行します。

（注）
各デバイス（GigabitEthernet1/1 など）の各 PTP クロック側インターフェイスのハードウェア名を書き留めます。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスを編集します。
b) [ルーティング（Routing）] をクリックします。
c) [マルチキャストルーティング（Multicast Routing）] > [IGMP] を選択します。
d) [マルチキャスト ルーティングの有効化（Enable Multicast Routing）] チェックボックスをオンにします。
e) [参加グループ（Join Group）] をクリックします。
f) [追加（Add）] をクリックし、[IGMP参加グループパラメータの追加（Add IGMP Join Group parameters）] ダイアログボックスで、次のオプションを設定して [OK] をクリックします。

- [インターフェイス（Interface）]：PTP クロック側スタンドアロン インターフェイスを選択します。
- [参加グループ（Join Group）]：新しいネットワークオブジェクトを追加するには、[+] をクリックします。アドレス 224.0.1.129 のホスト オブジェクトを作成します。追加インターフェイスを設定する場合は、このオブジェクトを選択するだけです。（ネットワーク オブジェクトの作成 （1351 ページ） を参照。）

デバイス上の PTP クロック側スタンドアロン インターフェイスごとにこの手順を繰り返します。

g) [ルーティング（Routing）] ページで [保存（Save）] をクリックします。

ステップ 2 FlexConfig オブジェクトを作成して、インターフェイス上で PTP をグローバルに有効にします。

次の手順では、設定しているすべてのデバイスで PTP クロック側インターフェイスが同じであると仮定しています。異なるデバイスで異なるインターフェイスを使用している場合は、組み合わせごとに個別のオブジェクトを作成する必要があります。たとえば、デバイス A および B で GigabitEthernet1/1、デバイス C と D で GigabitEthernet1/2、デバイス E と F で GigabitEthernet1/1 と 1/2 の両方を使用する場合は、3 つの個別の FlexConfig オブジェクトと、その後に 3 つの FlexConfig ポリシーをそれぞれ作成する必要があります（次の手順で説明）。

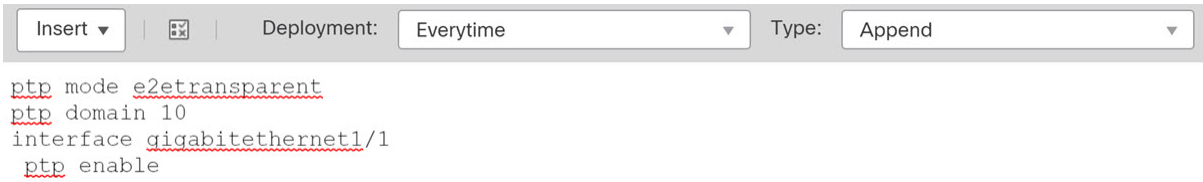
a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) コンテンツのテーブルから **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]** を選択します。
c) [FlexConfigオブジェクトの追加（Add FlexConfig Object）] をクリックし、次のプロパティを設定して、[保存（Save）] をクリックします。

- [名前（Name）]：オブジェクト名。たとえば、Enable_PTP などです。
- [展開（Deployment）]：[毎回（Everytime）] を選択します。この設定をすべての展開に送信し、設定されたままにする必要があります。

- [タイプ（Type）]：デフォルトの [後に付加（Append）] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。このため、インターフェイス設定に加えられた他の変更はこれらのコマンドの前に設定されます。
- [オブジェクト本文（Object body）]：オブジェクト本文で、PTP をグローバルに設定するために必要なコマンドを各 PTP クロック側インターフェイスで入力します。たとえば、PTP ドメイン 10 のグローバル設定と GigabitEthernet1/1 のインターフェイス設定に必要なコマンドは次のとおりです。

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

オブジェクト本文は、次のようになります。



ステップ 3 FlexConfig ポリシーを作成し、デバイスに割り当てます。

PTP クロック側インターフェイスのさまざまな組み合わせに対して複数の FlexConfig オブジェクトを作成した場合、オブジェクトごとに個別の FlexConfig ポリシーを作成し、設定する必要があるインターフェイスに基づいてそれらのポリシーを正しいデバイスに割り当てる必要があります。デバイスのグループごとに次の手順を繰り返します。

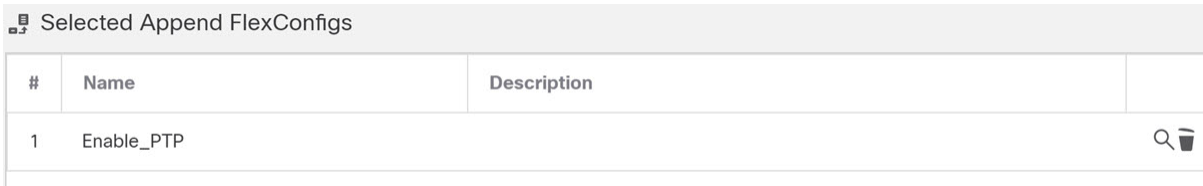
a) **[デバイス（Devices）] > [FlexConfig]** を選択します。

b) [新しいポリシー（New Policy）] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

c) コンテンツのテーブルの [ユーザー定義（User Defined）] フォルダ内にある PTP FlexConfig オブジェクトを選択し、[>] をクリックしてポリシーに割り当てます。

オブジェクトが [選択済み追加FlexConfig（Selected Append FlexConfigs）] リストに追加されます。



d) [保存（Save）] をクリックします。
e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存（Save）] の下にある **[ポリシー割り当て（Policy Assignment）]** リンクをクリックし、ここで割り当てを行います。
f) [設定のプレビュー（Preview Config）] をクリックし、[プレビュー（Preview）] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定CLIのプレビューが生成されます。PTP FlexConfigオブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。PTP コマンドの場合、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

ステップ 4 変更を展開します。

FlexConfig ポリシーをデバイスに割り当てたため、展開に関する警告が常に表示されます。これはFlexConfigの使用方法に関する注意です。[続行（Proceed）] をクリックし、展開を続行します。

展開が完了したら、展開の履歴を確認し、展開のトランスクリプトを表示できます。これは展開に失敗した場合に特に役立ちます。展開された構成の確認（2725ページ） を参照してください。

ステップ 5 各デバイスで PTP 設定を確認します。

SSH またはコンソール セッションから各デバイスにかけて PTP の設定を確認します。

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
```

```
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 4
 PTP version: 2
 Port state: Disabled
```

停電時の自動ハードウェアバイパスの設定方法（ISA 3000）

ハードウェア バイパスを有効にして、停電時でもトラフィックがインターフェイス ペア間を通過できるようにできます。サポートされているインターフェイスペアは銅線インターフェイスの GigabitEthernet 1/1 と 1/2、および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルを保有している場合は、銅線イーサネット ペア（GigabitEthernet 1/1 と 1/2）でのみハードウェア バイパスがサポートされます。

ハードウェア バイパスがアクティブの場合、トラフィックはレイヤ 1 でそれらのインターフェイス ペア間を通過します。Firewall Threat Defense CLI には、インターフェイスがダウンしていることが表示されます。ファイアウォール機能はないため、トラフィックのデバイス通過を許可することのリスクを理解している必要があります。

CLI コンソールまたは SSH セッションで、**show hardware-bypass** コマンドを使用して動作ステータスをモニターします。

始める前に

ハードウェア バイパスを機能させるための前提条件：

- インターフェイス ペアは同じブリッジ グループに配置する必要があります。
- インターフェイスはスイッチのアクセス ポートに接続する必要があります。トランク ポートには接続しないでください。

デバイスに割り当てられたアクセス コントロール ポリシーに付加された Threat Defense サービス ポリシーを使用して、TCP シーケンス番号のランダム化をグローバルに無効にすることをお勧めします。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号（ISN）が乱数に書き換えられます。ハードウェア バイパスがアクティブになると、ISA 3000 はデータ パスには入らず、シーケンス番号は変換されません。受信側のクライアントが予期しないシーケンス番号を受信すると接続がドロップされるため、TCP セッションを再確立する必要があります。TCP シーケンス番号のランダム化が無効になっている場合でも、スイッチオーバー中に一時的にダウンするリンクがあるため、一部の TCP 接続は再確立する必要があります。

手順

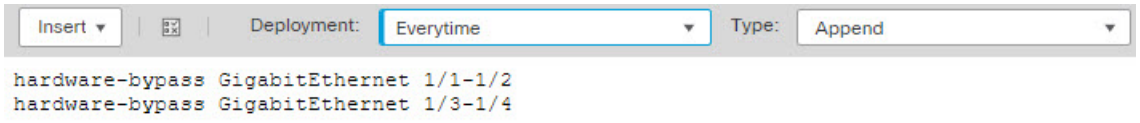
ステップ 1 自動バイパスを有効にする FlexConfig オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から**[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]**を選択します。
c) [FlexConfigオブジェクトの追加（Add FlexConfig Object）] をクリックし、次のプロパティを設定して、[保存（Save）] をクリックします。

- [名前（Name）]：オブジェクト名。たとえば、Enable_HW-Bypass です。
- [展開（Deployment）]：[毎回（Everytime）] を選択します。この設定をすべての展開に送信し、設定されたままにする必要があります。
- [タイプ（Type）]：デフォルトの [後に付加（Append）] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
- [オブジェクト本文（Object body）]：オブジェクト本文に、自動ハードウェアバイパスを有効にするために必要なコマンドを入力します。たとえば、可能な両方のインターフェイスペアに必要なコマンドは次のとおりです。

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

オブジェクト本文は、次のようになります。



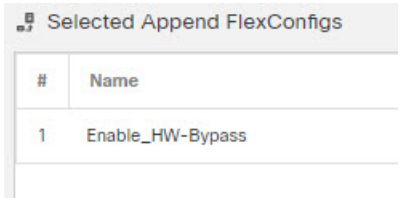
ステップ 2 FlexConfig ポリシーを作成し、デバイスに割り当てます。

a) **[デバイス（Devices）]** > **[FlexConfig]** を選択します。
b) [新しいポリシー（New Policy）] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

c) 目次の [ユーザー定義（User Defined）] フォルダ内にあるハードウェアバイパス FlexConfig オブジェクトを選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加FlexConfig（Selected Append FlexConfigs）] リストに追加されます。



d) **[保存（Save）]** をクリックします。

e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存（Save）] の下にある **[ポリシー割り当て（Policy Assignment）]** リンクをクリックし、ここで割り当てを行います。

f) [設定のプレビュー（Preview Config）] をクリックし、[プレビュー（Preview）] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。ハードウェアバイパス FlexConfig オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。ハードウェア バイパス コマンドの場合、次のような出力が表示されます。

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

ステップ 3 変更を展開します。

FlexConfig ポリシーをデバイスに割り当てたため、展開に関する警告が常に表示されます。これは FlexConfig の使用方法に関する注意です。[続行（Proceed）] をクリックし、展開を続行します。

展開が完了したら、展開の履歴を確認し、展開のトランスクリプトを表示できます。これは展開に失敗した場合に特に役立ちます。展開された構成の確認（2725 ページ） を参照してください。

次のタスク

ハードウェアバイパスを手動で呼び出したり、手動でオフにしたりする場合は、次の 2 つの FlexConfig オブジェクトを作成する必要があります。

- 手動でバイパスを開始するもの。これには、両方のペアに対してバイパスを呼び出すかどうかに応じて、次のコマンドのいずれかまたは両方が含まれます。

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

- 手動でバイパスをオフにするもの。次のコマンドのいずれかまたは両方が含まれます。

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

次に、いずれかのオブジェクトを FlexConfig ポリシーに追加し、変更を展開して、バイパスをオンまたはオフにする必要があります。また、展開後に FlexConfig ポリシーからオブジェクトをすぐに削除する必要もあります。バイパスを手動で呼び出す場合は、プロセスを繰り返して再度オフにする必要があります。したがって、この手動による方法を使用するには、FlexConfig ポリシーと追加の展開を頻繁かつ慎重に編集する必要があります。

FlexConfig ポリシーの移行

注目 FlexConfig ポリシーの移行に関するこの項は、ECMP、VXLAN、および EIGRP ポリシーの移行のみを対象としています。

以前のバージョンの Firewall Management Center では、ECMP、VXLAN、および EIGRP ポリシーは FlexConfig オブジェクトとポリシーを使用して設定していましたが、Management Center の UI でそれらのポリシーを直接設定できるようになりました。Management Center を以前のバージョンからアップグレードする場合、FlexConfig の設定は保持されます。ただし、UI からポリシーを管理するには、対応する**[デバイスの設定（Device（Edit））]** > **[ルーティング（Routing）]**ページで設定をやり直し、FlexConfig から設定を削除する必要があります。UI でのポリシーの作成を自動化するために、Firewall Management Centerにはポリシーを FlexConfig から UI に移行するオプションがあります。ただし、移行されたポリシーは FlexConfig から削除されません。移行後の手順については、ステップ 7 （2738 ページ）を参照してください。

始める前に

- 展開された FlexConfig ポリシーが最新であることを確認します。移行オプションは、少なくとも 1 つのデバイスでポリシーが最新の場合にのみ使用できます。古いポリシーを持つデバイスについては、移行は行われません。
- ポリシーが FlexConfig と Management Center の両方で設定されている場合：
  - ポリシーが **[デバイスの編集（Device (Edit)）]** > **[ルーティング（Routing）]** ですでに設定されている場合、移行は開始されません。
  - 展開中に、Management Center にエラーメッセージが表示されます。EIGRP 移行エラーメッセージの例：*EIGRP is configured through FlexConfig object and also under Device Listing ->Routing EIGRP for the device. Maintain the EIGRP configuration in either Routing EIGRP or FlexConfig.*（EIGRP は FlexConfig オブジェクトを使用して設定します。デバイスの [デバイスリスト（Device Listing）] -> [EIGRP のルーティング（Routing EIGRP）] で設定することもできます。EIGRP 設定のメンテナンスは、[EIGRP のルーティング（Routing EIGRP）] または FlexConfig で行ってください）
- ポリシーで使用されるネットワークオブジェクトが Management Center に存在する場合は、移行中にそのオブジェクトが再利用されます。移行中に IP アドレス設定に一致するネットワークオブジェクトがない場合、*bb* にタイムスタンプと整数が付加された新しいネットワークオブジェクトが作成されます。たとえば、***bb_<timestamp>_<integer>*** のようになります。このようなネットワークオブジェクトが複数ある場合、名前の整数変数は 1 ずつ増分されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[FlexConfig]** を選択し、移行する FlexConfig ポリシーに対して [編集（Edit）]（✎） をクリックします。

ステップ 2 [設定の移行（Migrate Config）] をクリックします。

（注）
移行が開始されると、[設定の移行（Migrate Config）] オプションと FlexConfig の [編集（Edit）] オプションの両方が使用できなくなります。

次の場合、[設定の移行（Migrate Config）] オプションは使用できません。

- 移行する FlexConfig CLI に該当するものが存在しない。
- FlexConfig ポリシーが、どの FlexConfig オブジェクトにも関連付けられていない。
- FlexConfig ポリシーに関連付けられたデバイスが存在しない。

ステップ 3 [Flex設定の移行（Migrate Flex Configuration）] ダイアログボックスで、設定の移行先のデバイスを選択し、[Ok] をクリックします。

移行の進捗状況はタスク通知として表示されます。移行が完了したら、[詳細の表示（View Details）] リンクをクリックして、移行レポート（PDF 形式）をダウンロードします。

ステップ 4 ポリシーの変更を表示するには、**[システム（System）]** > **[モニタリング（Monitoring）]** > **[監査（Audit）]** を選択し、[Flex Config の移行（Flex Config Migration）] メッセージをクリックします。

ステップ 5 FlexConfig 移行レポートを表示するには、**[システム（System）]** > **[モニタリング（Monitoring）]** > **[監査（Audit）]** を選択し、[Flex Configの移行（Flex Config Migration）] メッセージをクリックします。完全な移行レポートを表示するには、[レポート（Report）] アイコンをクリックします。

ステップ 6 対応する **[デバイスの編集（Device (Edit)）]** > **[ルーティング（Routing）]** ページで、移行された設定を確認します。

ステップ 7 デバイスの FlexConfig から特定のポリシー設定を削除するには、Management Center で次の手順を実行します。

a) デバイスで移行された FlexConfig ポリシーを識別します。
b) コピーオプションを使用して、FlexConfig ポリシーの複製を作成します。
c) 複製された FlexConfig ポリシーから対応する CLI オブジェクトを削除します。
d) 複製された FlexConfig ポリシーにデバイスを関連付けます。

ステップ 8 設定を保存して展開します。

FlexConfig の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
移行ツールのサポート。	7.3.0	いずれか	Flex で構成された ECMP、VXLAN、および EIGRP ポリシーを Management Center に移行するサポートが導入されました。 新規/変更された画面：**[デバイス（Devices）]** > **[FlexConfig]** > **[FlexConfigの移行（Migrate FlexConfig）]**
FlexConfig での BFD 設定の削除。	7.3.0	いずれか	Management Center ユーザーインターフェイスで BFD ポリシーを直接設定するためのサポートが導入され、BFD ポリシーを設定するための FlexConfig サポートは削除されました。
プライオリティキューの削除。	7.2.5	7.2.5	Threat Defense でプライオリティキューを設定するためのサポートが削除されました。
FlexConfig での EIGRP 設定の削除。	7.2.0	いずれか	Management Center ユーザーインターフェイスで EIGRP を直接設定するためのサポートが導入され、EIGRP ポリシーを設定するための FlexConfig サポートは削除されました。
PBR 設定の削除。	7.1.0	7.1.0	FMC ユーザーインターフェイスで PBR を直接設定するためのサポートが導入され、FTD 7.1 以降の PBR を設定するための FlexConfig サポートは削除されました。 新規/変更されたコマンド：**policy-route route-map***routemap-object-name*。
FlexConfig での ECMP ゾーン作成サポートの削除。	7.1.0	いずれか	FMC ユーザーインターフェイスで ECMP ゾーンを直接設定するためのサポートが導入され、EIGRP ゾーンを設定するための FlexConfig サポートは削除されました。
ISA 3000 デバイスの高精度時間プロトコル（PTP）の設定。	6.5.0	いずれか	FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。 FlexConfig オブジェクトに、**ptp**（インターフェイス モード）コマンド、グローバル コマンド **ptp mode e2etransparent**、**ptp domain** を追加できるようになりました。 新規/変更されたコマンド：**show ptp**。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
委任された FlexConfig オブジェクト。	6.3.0	いずれか	FlexConfig を使用して設定した以前のリリースの一部の機能が、FMC で直接サポートされるようになりました。この FlexConfig オブジェクトを使用している場合は削除し、新しいオブジェクトを使用するように設定を変換する必要があります。次に、非推奨の FlexConfig オブジェクトおよびテキスト オブジェクトを示します。 • defaultDNSNameServerList および defaultDNSParameters テキスト オブジェクトを含む **Default_DNS_Configure**。プラットフォーム設定ポリシーで、データ インターフェイスの DNS を設定してください。 • **TCP_Embryonic_Conn_Limit**、tcp_conn_misc and tcp_conn_limit テキスト オブジェクト。これらの機能は、FTD サービスポリシーで設定します。ポリシーは、デバイスに割り当てられているアクセス制御ポリシーの [詳細（Advanced）] タブで確認できます。 • **TCP_Embryonic_Conn_Timeout**、tcp_conn_misc および tcp_conn_timeout テキスト オブジェクト。FTD サービスポリシーでこれらの機能を設定します。

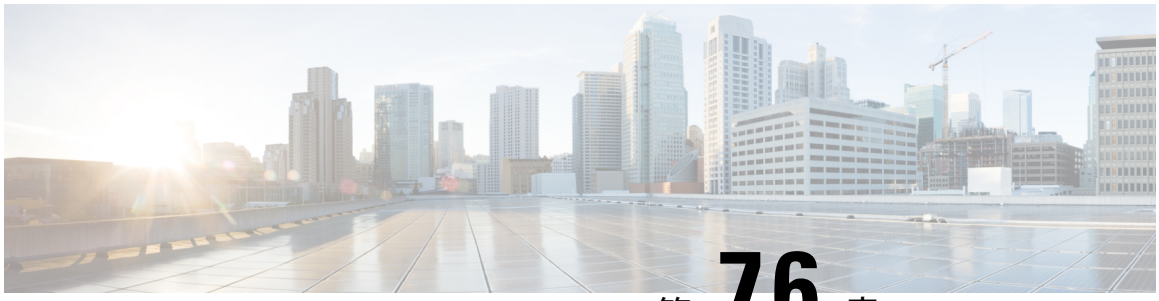
機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
FlexConfig の更新。	6.2.1	いずれか	政府による認定要件に従って、パスワード、システム提供またはユーザ定義の FlexConfig オブジェクトの共有キーなどの機密情報はすべて、秘密キー変数を使用してマスクする必要があります。FMC をバージョン 6.2.1 以降に更新すると、FlexConfig オブジェクト内のすべての機密情報が秘密鍵の変数形式に変換されます。 さらに、次の新しい FlexConfig テンプレートが追加されます。 • **Default_DNS_Configure** テンプレートでは、デフォルトの DNS グループを使用できます。これはデータインターフェイスを介して名前を解決するコマンドまたは機能のホスト名を解決するために使用されます。 • **TCP 初期接続制限およびタイムアウト設定**テンプレートでは、SYN フラッド DoS 攻撃から保護するように初期接続制限/タイムアウト CLI を設定できます。 • **脅威検出の設定およびクリア**テンプレートでは、TCP 代行受信によって傍受された攻撃の脅威検出統計情報を設定できます。 • **IPV6 ルータ ヘッダーの検査**テンプレートでは、さまざまなタイプの特定のヘッダーを選択的に許可またはブロックするように IPV6 検査ヘッダーを設定できます（RH タイプ 2、モバイルの許可など）。 • **DHCPv6 プレフィックス委任**テンプレートでは、IPv6 プレフィックス委任に対して 1 つの外部インターフェイス（プレフィックス委任クライアント）と 1 つの内部インターフェイス（委任されたプレフィックスの受信者）を設定します。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
FlexConfig。	6.2.0	いずれか	FlexConfig 機能では、FMC を使用して ASA CLI テンプレートベースの機能を FTD デバイスに展開できます。この機能を使用すると、FTD デバイスで現在使用できない最も重要な ASA 機能の一部を有効にできます。この機能は、ポリシー内で連携するテンプレートとオブジェクトとして構造化されています。デフォルトのテンプレートは Cisco TAC で公式にサポートされています。 新規/変更された画面： • **[デバイス（Devices）] > [FlexConfig]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfigオブジェクト（FlexConfig Objects）]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [テキストオブジェクト（Text Object）]**

第 XIV 部

高度なネットワーク分析と前処理

- ネットワーク分析ポリシーと侵入ポリシーに対するアクセスコントロールの詳細設定 （2745 ページ）
- ネットワーク分析ポリシーの開始 （2755 ページ）
- アプリケーション層プリプロセッサ （2767 ページ）
- SCADA プリプロセッサ （2851 ページ）
- トランスポート層およびネットワーク層のプリプロセッサ （2865 ページ）
- 特定の脅威の検出 （2909 ページ）
- アダプティブ プロファイル （2933 ページ）



第 76 章

ネットワーク分析ポリシーと侵入ポリシーに対するアクセス コントロールの詳細設定

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシー用の高度な設定を行う手順を示します。

- ネットワーク分析および侵入ポリシーのアクセス コントロールの詳細設定について （2745 ページ）
- ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定の要件と前提条件 （2745 ページ）
- トラフィック識別の前に通過するパケットのインスペクション （2746 ページ）
- ネットワーク分析プロファイルの詳細設定 （2748 ページ）

ネットワーク分析および侵入ポリシーのアクセス コントロールの詳細設定について

アクセス コントロール ポリシーにおける詳細設定の多くは、設定のために特定の専門知識を要する侵入検知設定と予防設定を制御します。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

トラフィック識別の前に通過するパケットのインスペクション

URL フィルタリング、アプリケーション検出、レート制限、インテリジェントアプリケーションバイパスなどの一部の機能では、接続を確立するとともに、システムが、トラフィックを識別して、そのトラフィックを処理するアクセスコントロールルール（存在する場合）を決定するために、いくつかのパケットを通過させる必要があります。

これらのパケットを検査し、宛先に到達することを防止し、イベントを生成するために、アクセス コントロール ポリシーを明示的に設定する必要があります。トラフィック識別の前に通過するパケットを処理するためのポリシーの指定 （2747 ページ）を参照してください。

システムが接続を処理する必要があるアクセスコントロールルールまたはデフォルトアクションを識別するとすぐに、接続内の残りのパケットが適宜処理され検査されます。

トラフィック識別の前に通過するパケットを処理するためのベストプラクティス

- アクセス コントロール ポリシーに指定されたデフォルトのアクションは、これらのパケットには適用されません。
- 代わりに、以下のガイドラインを使用して、アクセス コントロール ポリシーの詳細設定で [アクセス コントロール ルールが決定される前に使用される侵入ポリシー（Intrusion Policy used before Access Control rule is determined）] の値を選択します。
  - システムによって作成された侵入ポリシーまたはカスタム侵入ポリシーを選択できます。たとえば、[バランスのとれたセキュリティと接続（Balanced Security and Connectivity）] を選択できます。
  - パフォーマンス上の理由から、特別な理由がないかぎり、この設定はアクセス コントロール ポリシーに設定されているデフォルトのアクションと一致している必要があります。

- システムが侵入インスペクションを実行しない場合（たとえば、検出専用の導入において）は、[アクティブなルールなし（No Rules Active）] を選択します。システムはこれらの初期パケットのインスペクションを行わず、これらのパケットの通過が許可されます。
- デフォルトでは、この設定は、デフォルトの変数セットを使用します。これが目的に適していることを確認してください。詳細については、変数セット （1406ページ）を参照してください。
- 最初に一致したネットワーク分析ルールに関連付けられているネットワーク分析ポリシーが、選択されたポリシーに対してトラフィックを前処理します。ネットワーク分析ルールがない場合、あるいはどのルールも一致しない場合は、デフォルトのネットワーク分析ポリシーが使用されます。

トラフィック識別の前に通過するパケットを処理するためのポリシーの指定

（注） この設定は、デフォルト侵入ポリシーと呼ばれることもあります。（これは、アクセス コントロール ポリシーのデフォルトアクションとは異なります。）

始める前に

これらの設定のベストプラクティスを確認します。トラフィック識別の前に通過するパケットを処理するためのベストプラクティス （2746 ページ） を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [アクセス制御ルールが決定される前に使用されている侵入ポリシー（ntrusion Policy used before Access Control rule is determined）] ドロップダウン リストから、侵入ポリシーを選択します。

ユーザーが作成したポリシーを選択した場合は、[編集（Edit）]（） をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 3 必要に応じて、[侵入ポリシーの変数セット（Intrusion Policy Variable Set）] ドロップダウン リストから別の変数セットを選択します。変数セットの横にある [編集（Edit）]（） を選択して、変数セットを作成および編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

変数セット （1406 ページ）

ネットワーク分析プロファイルの詳細設定

ネットワーク分析ポリシーは、特に侵入の試みの前兆となるかもしれない異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックをデコードおよび前処理する方法を制御します。トラフィックの前処理は、セキュリティインテリジェンスの照合およびトラフィックの復号の後、侵入ポリシーによるパケットインスペクションの前に行われます。デフォルトでは、システム提供の [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーが、デフォルト ネットワーク分析ポリシーです。

ヒント システムによって提供される [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです。複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます

これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するために使用できます

システムがトラフィックを前処理するときに、パケットはルール番号の上位から下位の順序でネットワーク分析ルールに照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

デフォルトのネットワーク分析ポリシーの設定

システムによって作成されたポリシーまたはユーザーが作成したポリシーを選択できます。

（注） プリプロセッサを無効にしているが、システムは有効になっている侵入ルールまたはプリプロセッサルールと照合して前処理されたパケットを評価する必要がある場合、システムはプリプロセッサを自動的に有効にして使用します。しかし、ネットワーク分析ポリシーWebインターフェイスでは無効のままです。前処理の調整、特に複数のカスタムネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理および侵入インスペクションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる**必要があります**。

手順

ステップ 1 アクセスコントロールポリシーエディタで、[詳細設定（Advanced）]をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）]セクションの横にある[編集（Edit）]（✎）をクリックします。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）]ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。

ユーザーが作成したポリシーを選択した場合は、[編集（Edit）]（✎）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）]をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

カスタム ポリシーの制限 （1992 ページ）

ネットワーク分析ルール

アクセスコントロールポリシーの詳細設定で、ネットワーク分析ルールを使用してネットワーク トラフィックへの前処理設定を調整できます。

ネットワーク分析ルールには1から番号が付けられます。システムがトラフィックを前処理するときに、パケットはルール番号の昇順で上から順にネットワーク分析ルールに照合され、すべてのルールの条件が一致する最初のルールに従ってトラフィックが前処理されます。

ルールには、ゾーン、ネットワーク、VLANタグの条件を追加できます。ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、ネットワーク条件を持つがゾーン条件を持たないルールは、その入力または出力インターフェイスに関係なく、送信元または宛先 IP アドレスに基づいてトラフィックを評価します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

ネットワーク分析ポリシールール条件

ルール条件を使用すると、ネットワーク分析ポリシーを微調整して、制御するユーザーとネットワークを対象にできます。詳細については、次の項を参照してください。

関連トピック

セキュリティゾーンルール条件 （1877 ページ）
ネットワークルール条件 （816 ページ）
VLAN タグルール条件 （1792 ページ）

セキュリティゾーンルール条件

セキュリティゾーンはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することで、トラフィックフローを管理、分類、および復号しやすくします。

セキュリティゾーンは、トラフィックをその送信元と宛先のセキュリティゾーンで制御または復号します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ヒント　ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

ネットワークルール条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注）　アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

VLAN タグルール条件

（注）　アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

- 他のすべてのモデルの Firewall Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

ネットワーク分析ルールの設定

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ヒント
[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックし、既存のカスタム ネットワーク分析ポリシーを表示および編集します。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 追加する条件をクリックして、ルールの条件を設定します。

ステップ 5 [ネットワーク分析（Network Analysis）] をクリックし、このルールに一致するトラフィックの前処理に使用する [ネットワーク分析ポリシー（Network Analysis Policy）] を選択します。

[編集（Edit）]（）をクリックして、新しいウィンドウでカスタムポリシーを編集します。システムによって提供されたポリシーは編集できません。

ステップ 6 **[追加（Add）]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ネットワーク分析ルールの管理

ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは1つのポリシーにのみ属します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[侵入ポリシーおよびネットワーク分析ポリシー（Intrusion and Network Analysis Policies）] セクションの横にある[編集（Edit）]（）をクリックします。

代わりに[表示（View）]（）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 カスタム ルールを編集します。次の選択肢があります。

- ルールの条件を編集する、またはルールによって呼び出されるネットワーク分析ポリシーを変更するには、ルールの横にある[編集（Edit）]（）をクリックします。
- ルールの評価順序を変更するには、ルールをクリックして正しい位置にドラッグします。複数のルールを選択するには、Shift キーおよび Ctrl キーを使用します。
- ルールを削除するには、ルールの横にある[削除（Delete）]（）をクリックします。

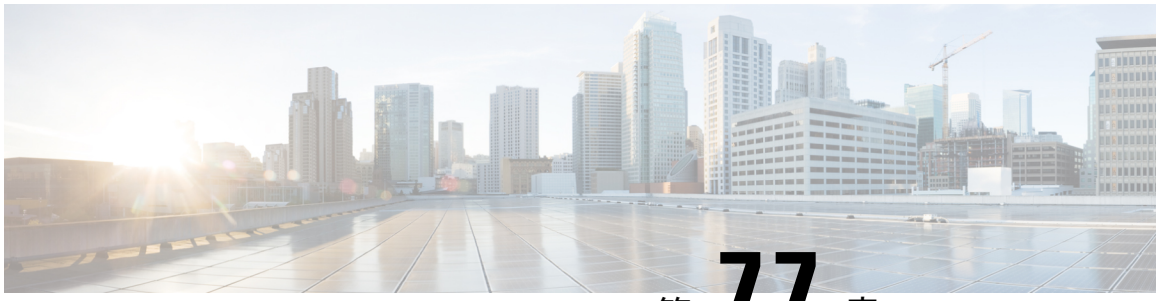
ヒント
ルールを右クリックするとコンテキストメニューが表示され、新しいネットワーク分析ルールの切り取り、コピー、貼り付け、編集、削除、および追加を実行できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。



第 77 章

ネットワーク分析ポリシーの開始

ここでは、ネットワーク分析ポリシーの使用を開始する方法について説明します。

- ネットワーク分析ポリシーの基本 （2755 ページ）
- ネットワーク分析ポリシーのライセンス要件 （2756 ページ）
- ネットワーク分析ポリシーの要件と前提条件 （2756 ページ）
- ネットワーク分析ポリシーの管理 （2756 ページ）

ネットワーク分析ポリシーの基本

ネットワーク分析ポリシーは、多数のトラフィックの前処理オプションを制御し、アクセス コントロール ポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、セキュリティ インテリジェンスによる照合や SSL 復号の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは Balanced Security and Connectivity ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。便宜を図るため、システムによっていくつかの変更不可能なネットワーク分析ポリシーが提供されます。これらのポリシーは、Talos インテリジェンス グループによってセキュリティおよび接続の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、カスタム ネットワーク分析ポリシーを作成することもできます。

ヒント システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。ネットワーク分析ポリシーと侵入ポリシーが連動してトラフィックを検査します。

複数のカスタムネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることにより、特定のセキュリティ ゾーン、ネットワーク、VLAN 用に前処理オプションを調整できます。

ネットワーク分析ポリシーのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

ネットワーク分析ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

ネットワーク分析ポリシーの管理

手順

ステップ 1 **[**ポリシー（**Policies**）**]** > **[**アクセス制御（**Access Control**）**]** 見出し > **[**アクセス制御（**Access Control**）**]** を選択してから **[**ネットワーク分析ポリシー（**Network Analysis Policy**）**]** をクリックするか、 **[**ポリシー（**Policies**）**]** > **[**アクセス制御（**Access Control**）**]** 見出し > **[**侵入（**Intrusion**）**]** を選択してから **[**ネットワーク分析ポリシー（**Network Analysis Policies**）**]**をクリックします。

（注）

カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 ネットワーク分析ポリシーを管理します。

- [比較（Compare）]：**[ポリシーの比較（Compare Policies）]** をクリックします（「ポリシーの比較」を参照）。
- 作成：新しいネットワーク分析ポリシーを作成する場合は、[ポリシーの作成（Create Policy）] をクリックします。

  ネットワーク分析ポリシーの 2 つのバージョン（[Snort 2 バージョン（Snort 2 Version）]と [Snort 3 バージョン（Snort 3 Version）]）が作成されます。
- 削除：ネットワーク分析ポリシーを削除する場合は、[削除（Delete）]（） をクリックして、ポリシーの削除を確認します。アクセスコントロールポリシーが参照しているネットワーク分析ポリシーは削除できません。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- [展開（Deploy）]：**[展開（Deploy）]** > **[展開（Deployment）]** をクリックします（設定変更の展開 （172 ページ） を参照）。
- 編集：既存のネットワーク分析ポリシーを編集する場合は、[編集（Edit）]（） をクリックして、ネットワーク分析ポリシーの設定とキャッシュされた変更（2761 ページ）で説明する手順を実行します。

  代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- レポート：**[レポート（Report）]**（） をクリックします（現在のポリシーレポートの生成 （192 ページ） を参照）。

ネットワーク分析ポリシーの作成

既存のすべてのネットワーク分析ポリシーは、対応する Snort 2 バージョンでも Snort 3 バージョンでも Firewall Management Center で使用できます。新しいネットワーク分析ポリシーを作成すると、Snort 2 バージョンと Snort 3 バージョンの両方で作成されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** > **[ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] に入力します。

ステップ 4 使用可能な選択肢から [検査モード（Inspection Mode）] を選択します。

- [検出（Detection）]
- [防御（Prevention）]

ステップ 5 [ベースポリシー（Base Policy）] を選択し、[保存（Save）] をクリックします。

（注）
Snort 3 および SSL 復号または TLS サーバーアイデンティティを使用している場合は、**防止**モードでネットワーク分析ポリシー（NAP）を構成します。

新しいネットワーク分析ポリシーが、対応する Snort 2 バージョンと Snort 3 バージョンで作成されます。

ネットワーク分析ポリシーの変更

ネットワーク分析ポリシーを変更して、名前、説明、またはベースポリシーを変更できます。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）] > [ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 名前、説明、検査モード、またはベースポリシーを変更するには、[編集（Edit）] をクリックします。

（注）
ネットワーク分析ポリシーの名前、説明、ベースポリシー、および検査モードを編集すると、編集内容は Snort 2 と Snort 3 の両方のバージョンに適用されます。特定のバージョンの検査モードを変更する場合は、それぞれのバージョンのネットワーク分析ポリシーページから変更できます。

ステップ 3 [保存（Save）] をクリックします。

Snort 2 の場合のカスタムネットワーク分析ポリシーの作成

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、インライン モードを選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ネットワーク分析ポリシーのインライン モードでは、プリプロセッサでトラフィックを変更（正規化）したりドロップしたりして、攻撃者が検出を回避する可能性を最小限にすることができます。パッシブな展開では、インライン モードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。

関連トピック

基本レイヤ （2181 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更 （2764 ページ）
カスタム ネットワーク分析ポリシーの作成 （2759 ページ）
ネットワーク分析ポリシーの編集 （2761 ページ）

カスタム ネットワーク分析ポリシーの作成

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policies）]** をクリックします。

（注）
カスタム ユーザー ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るかどうか尋ねられたときに [キャンセル（Cancel）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [基本ポリシー（Base Policy）] で最初の基本ポリシーを選択します。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

注目
カスタム NAP の設定中に、[ベースポリシー（Base Policy）] として [最大検出（Maximum Detection）] を選択すると、パフォーマンスが低下する可能性があります。実稼働環境に導入する前に、この設定を確認してテストすることを推奨します。

ステップ 6 プリプロセッサがインライン導入でのトラフィックに影響するようにする場合は、[インライン モード（Inline Mode）] を有効化します。

ステップ 7 ポリシーを作成するには：

- 新しいポリシーを作成して [ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るには、[ポリシーの作成（Create Policy）] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度なネットワーク分析ポリシーエディタでそれを開いて編集するには、[ポリシーの作成と編集（Create and Edit Policy）] をクリックします。

Snort 2 のネットワーク分析ポリシー管理

[ネットワーク分析ポリシー（Network Analysis Policy）] ページ（または **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします）で、現在のカスタム ネットワーク分析ポリシーを次の情報とともに確認できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザー
- プリプロセッサがトラフィックに影響を与えることを許可する [Inline Mode] 設定が有効になっているかどうか
- どのアクセス コントロール ポリシーとデバイスが、ネットワーク分析ポリシーを使用してトラフィックを前処理しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これら 2 つのネットワーク分析ポリシーは、基本ポリシーとして「Balanced Security and Connectivity」ネットワーク分析ポリシーを使用します。両者の唯一の相違点はインライン モードの設定です。インライン ポリシーではプリプロセッサによるトラフィックの影響が有効化され、パッシブ ポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

ただし、システムのユーザーアカウントの権限が侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。

関連トピック

カスタム ネットワーク分析ポリシーの作成 （2759 ページ）
ネットワーク分析ポリシーの編集 （2761 ページ）

ネットワーク分析ポリシーの設定とキャッシュされた変更

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要があることに留意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

システムは、ユーザごとに1つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。

関連トピック

ポリシーがトラフィックで侵入を検査する方法 （1981 ページ）
カスタム ポリシーの制限 （1992 ページ）

ネットワーク分析ポリシーの編集

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policies）]** をクリックします。

（注）
カスタム ユーザー ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 設定するネットワーク分析ポリシーの横にある[編集（Edit）]（✎）をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ネットワーク分析ポリシーを編集します。

- 基本ポリシーの変更：基本ポリシーを変更するには、[ポリシー情報（Policy Information）] ページの [基本ポリシー（Base Policy）] ドロップダウンリストから、基本ポリシーを選択します。
- ポリシー階層の管理：ポリシー階層を管理するには、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。
- プリプロセッサの変更：プリプロセッサの設定有効または無効にするか、あるいは編集するには、ナビゲーション パネルで [設定（Settings）] をクリックします。
- トラフィックの変更：プリプロセッサがトラフィックを変更またはドロップできるようにするには、[ポリシー情報（Policy Information）] ページで [インライン モード（Inline Mode）] チェックボックスをオンにします。
- 設定の表示：基本ポリシーの設定を表示するには、[ポリシー情報（Policy Information）] ページで [基本ポリシーの管理（Manage Base Policy）] をクリックします。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- プリプロセッサでイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、プリプロセッサのルールを有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

基本レイヤ （2181 ページ）
基本ポリシーの変更 （2183 ページ）
Snort 2 のネットワーク分析ポリシーでのプリプロセッサの構成 （2762 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更 （2764 ページ）
レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

Snort 2 のネットワーク分析ポリシーでのプリプロセッサの構成

プリプロセッサは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックの詳細な検査に備えます。プリプロセッサは、ユーザが設定したプリプロセッサ オプションをパケットがトリガーしたときに、プリプロセッサイベントを生成できます。デフォルトで有

効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。

（注） 多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、VLAN にグローバルに適用されることに注意してください。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

また、侵入ポリシーでは ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することにも注意してください。

関連トピック

DCE/RPC プリプロセッサ （2768 ページ）
DNP3 プリプロセッサ （2855 ページ）
DNS プリプロセッサ （2782 ページ）
FTP/Telnet デコーダ （2787 ページ）
GTP プリプロセッサ （2824 ページ）
HTTP Inspect プリプロセッサ （2796 ページ）
IMAP プリプロセッサ （2826 ページ）
インライン正規化プリプロセッサ （2872 ページ）
IP 最適化プリプロセッサ （2881 ページ）
Modbus プリプロセッサ （2852 ページ）
パケット デコーダ （2887 ページ）
POP プリプロセッサ （2829 ページ）
機密データ検出の基本 （2203 ページ）
SIP プリプロセッサ （2818 ページ）
SMTP プリプロセッサ （2833 ページ）
SSH プリプロセッサ （2840 ページ）
SSL プリプロセッサ （2845 ページ）
Sun RPC プリプロセッサ （2815 ページ）
TCP ストリームの前処理 （2892 ページ）
UDP ストリームの前処理 （2906 ページ）
カスタム ポリシーの制限 （1992 ページ）

インライン導入でのプリプロセッサによるトラフィックの変更

インライン導入（つまり、ルーテッド インターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、あるいはインライン インターフェイスのペアを使用して関連する設定をデバイスに展開する導入）では、一部のプリプロセッサがトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルールエンジンで分析されるようにパケットを準備します。ユーザは、プリプロセッサの [これらの TCP オプションを許可（Allow These TCP Options）] と [回復不能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）] オプションを使用して、特定のパケットをブロックすることもできます。
- システムは無効なチェックサムを持つパケットをドロップできます。
- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。

ネットワーク分析ポリシーに設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効にして正しく設定するとともに、管理対象デバイスをインラインで正しく展開する必要があります。最後に、ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定を有効にする必要があります。

ネットワーク分析ポリシーの注記におけるプリプロセッサの設定

ネットワーク分析ポリシーのナビゲーション パネルで [設定（Settings）] を選択すると、ポリシーによりタイプ別のプリプロセッサがリストされます。[設定（Settings）]ページで、ネットワーク分析ポリシーのプリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。

プリプロセッサを設定するには、それを有効にする必要があります。プリプロセッサを有効にすると、そのプリプロセッサに関する設定ページへのサブリンクがナビゲーションパネル内の [設定（Settings）] リンクの下に表示され、この設定ページへの [編集（Edit）] リンクが [設定（Settings）] ページのプリプロセッサの横に表示されます。

ヒント プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサ設定ページで[デフォルトに戻す（Revert to Defaults）] をクリックします。プロンプトが表示されたら、復元することを確認します。

プリプロセッサを無効にすると、サブリンクと [編集（Edit）] リンクは表示されなくなりますが、設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをある方法で最初に復号または前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

実際にトラフィックを変更せずに、設定がインライン展開でどのように機能するかを評価する場合は、インライン モードを無効にできます。タップ モードでのパッシブ展開またはインラ

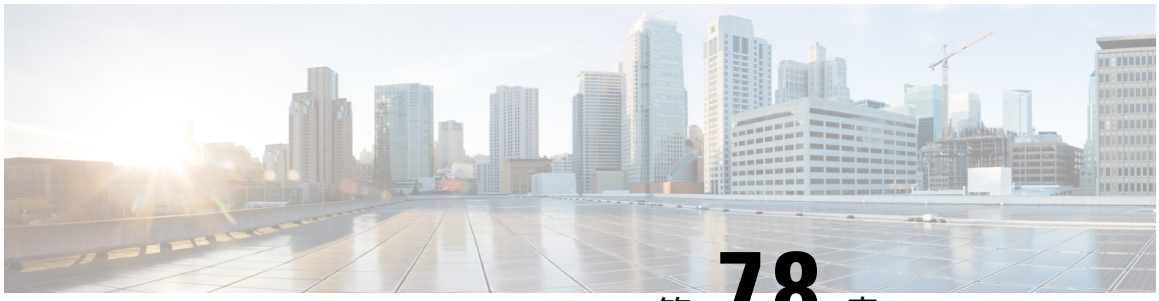
イン展開では、インラインモード設定に関係なくシステムがトラフィックに影響を及ぼすことはありません。

（注） インラインモードを無効にすることで、侵入イベントのパフォーマンス統計グラフに影響を及ぼす可能性があります。インライン展開でインライン モードが有効の場合、侵入イベントパフォーマンス ページ（**[概要（Overview）]** > **[概要（Summary）]** > **[侵入イベントパフォーマンス（Intrusion Event Performance）]**）には、正規化し、ブロックされたパケットを示すグラフが表示されます。インラインモードが無効の場合、またはパッシブ展開である場合、多くのグラフによりシステムが正規化するか、またはドロップするトラフィックに関するデータが表示されます。

（注） インライン展開では、インラインモードを有効にし、[TCPペイロードの正規化（Normalize TCP Payload）] オプションを有効にしたままインライン正規化プリプロセッサを設定することを推奨します。パッシブ展開では、adaptive profile updatesを使用することを推奨します。

関連トピック

トランスポート/ネットワーク プリプロセッサの詳細設定 （2866 ページ）
チェックサム検証 （2870 ページ）
インライン正規化プリプロセッサ （2872 ページ）



第 78 章

アプリケーション層プリプロセッサ

次のトピックでは、アプリケーション層プリプロセッサおよびその設定方法について説明します。

- アプリケーション層のプリプロセッサの概要 （2767 ページ）
- アプリケーション層プリプロセッサのライセンス要件 （2768 ページ）
- アプリケーション層プリプロセッサの要件と前提条件 （2768 ページ）
- DCE/RPC プリプロセッサ （2768 ページ）
- DNS プリプロセッサ （2782 ページ）
- FTP/Telnet デコーダ （2787 ページ）
- HTTP Inspect プリプロセッサ （2796 ページ）
- Sun RPC プリプロセッサ （2815 ページ）
- SIP プリプロセッサ （2818 ページ）
- GTP プリプロセッサ （2824 ページ）
- IMAP プリプロセッサ （2826 ページ）
- POP プリプロセッサ （2829 ページ）
- SMTP プリプロセッサ （2833 ページ）
- SSH プリプロセッサ （2840 ページ）
- SSL プリプロセッサ （2845 ページ）

アプリケーション層のプリプロセッサの概要

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

アプリケーション層プロトコルにより、同一データをさまざまな方法で表すことができます。Firepowerシステムは、特定タイプのパケットデータを侵入ルールエンジンが分析可能なフォーマットに正規化する、アプリケーション層プロトコルデコーダを提供しています。アプリケーション層プロトコル エンコードを正規化することにより、ルール エンジンでさまざまなデー

タ形式のパケットに同じコンテンツ関連ルールを効果的に適用し、有意な結果を得ることができます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

ほとんどの場合、侵入ルールで関連するプリプロセッサルールが有効になっていないと、プリプロセッサはイベントを生成しません。

アプリケーション層プリプロセッサのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

アプリケーション層プリプロセッサの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

DCE/RPC プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP および UDP 経由で転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block（SMB）プロトコルまたは Samba でさらにカプセル化されることがあります。Samba は、Windows や UNIX/Linux 系のオペレーティング システムから構成される混合環境でプロセス間通信に使用されるオープンソースの SMB 実装です。また、ネットワーク上の Windows IIS Web サーバーでは IIS RPC over HTTP が使用されることがあります。IIS RPC over HTTP は、プロキシ TCP により伝送される DCE/RPC トラフィックに、ファイアウォールを介して分散通信を提供します。

DCE/RPC プリプロセッサ オプションとその機能の説明には、Microsoft による DCE/RPC の実装である MSRPC が含まれることに注意してください。SMB のオプションと機能についての説明は、SMB と Samba の両方に当てはまります。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバー（ネットワーク上の Windows または Samba が稼働している任意のホスト）を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバー応答でも発生することがあります。DCE/RPC プリプロセッサは、TCP、UDP、および SMB トランスポートでカプセル化された DCE/RPC 要求と応答を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP により伝送される DCE/RPC も含まれます。プリプロセッサは DCE/RPC データ ストリームを分析し、DCE/RPC トラフィックにおける異常な動作と回避技術を検出します。また、SMB データ ストリームを分析し、異常な SMB 動作と回避技術を検出します。

IP 最適化プリプロセッサによる IP 最適化および TCP ストリーム プリプロセッサによる TCP ストリームの再構成に加えて、DCE/RPC プリプロセッサは、SMB のセグメント化解除と DCE/RPC の最適化も行います。

最後に、DCE/RPC プリプロセッサはルール エンジンで処理できるように DCE/RPC トラフィックを正規化します。

コネクションレス型およびコネクション型 DCE/RPC トラフィック

DCE/RPC メッセージは、2 種類の DCE/RPC Protocol Data Unit（PDU）の 1 つに準拠します。

コネクション型 DCE/RPC PDU プロトコル

DCE/RPC プリプロセッサは、TCP、SMB、および RPC over HTTP トランスポートでコネクション型 DCE/RPC を検出します。

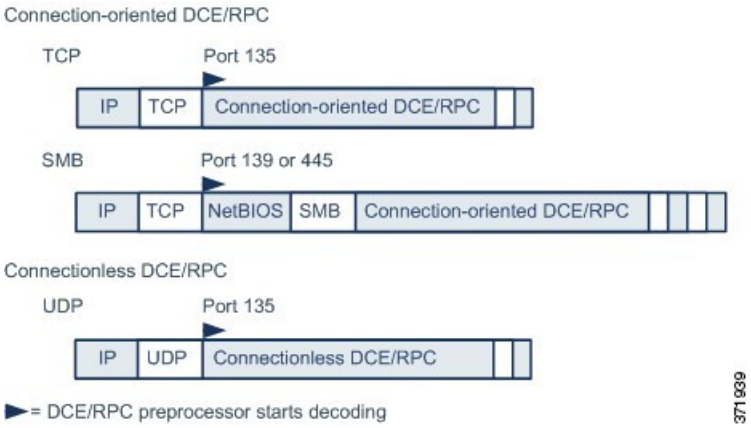
コネクションレス型 DCE/RPC PDU プロトコル

DCE/RPC プリプロセッサは、UDP トランスポートでコネクションレス型 DCE/RPC を検出します。

この 2 つの DCE/RPC PDU プロトコルには、それぞれ固有の見出しとデータ特性があります。たとえば、コネクション型 DCE/RPC のヘッダーの長さは通常は 24 バイトですが、コネクションレス型 DCE/RPC のヘッダーの長さは 80 バイト（固定）です。また、フラグメント化コネクションレス型 DCE/RPC のフラグメントの正しい順序は、コネクションレス型トランスポートでは処理できないため、代わりに、コネクションレス型 DCE/RPC ヘッダーの値によって維持する必要があります。これとは対照的に、コネクション型 DCE/RPC の正しいフラグメント順

序はトランスポート プロトコルによって維持されます。DCE/RPC プリプロセッサは、これらや他のプロトコル固有の特性を使用して、両方のプロトコルで異常やその他の回避技術をモニターし、トラフィックをデコードおよび復号してからルール エンジンに渡します。

次の図は、DCE/RPC プリプロセッサが各種トランスポートの DCE/RPC トラフィックの処理を開始するポイントを示します。



この図の次の点に注意してください。

- ウェルノウン TCP または UDP ポート 135 は、TCP および UDP トランスポートの DCE/RPC トラフィックを特定します。
- この図には RPC over HTTP は含まれていません。

  RPC over HTTP の場合、コネクション型 DCE/RPC は、図に示すように、HTTP を介した初期設定シーケンスの後、TCP 経由で直接伝送されます。
- DCE/RPC プリプロセッサは通常、NetBIOS セッション サービス用のウェルノウン TCP ポート 139 か、同様に実装されたウェルノウン Windows ポート 445 で SMB トラフィックを受信します。

  SMB には DCE/RPC 伝送以外にも多数の機能があるため、プリプロセッサは SMB トラフィックが DCE/RPC トラフィックを伝送しているかどうかをまず検査します。伝送していない場合は処理を停止し、伝送している場合は処理を続行します。
- IP によりすべての DCE/RPC トランスポートがカプセル化されます。
- TCP は、すべてのコネクション型 DCE/RPC を伝送します。
- UDP はコネクションレス型 DCE/RPC を伝送します。

DCE/RPC ターゲット ベース ポリシー

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初

のフラグメントの opnum（操作番号）ヘッダー フィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの opnum フィールドを使用します。

Windows と Samba の SMB の実装にも、大きな違いがあります。たとえば、Windows は名前付きパイプの操作時に SMB OPEN および READ コマンドを認識しますが、Samba はこれらのコマンドを認識しません。

DCE/RPC プリプロセッサを有効にすると、デフォルトのターゲットベース ポリシーが自動的に有効になります。必要に応じて、異なる Windows や Samba バージョンを実行する他のホストを対象としたターゲット ベース ポリシーを追加できます。デフォルトのターゲットベース ポリシーは、別のターゲットベース ポリシーに含まれていないホストに適用されます。

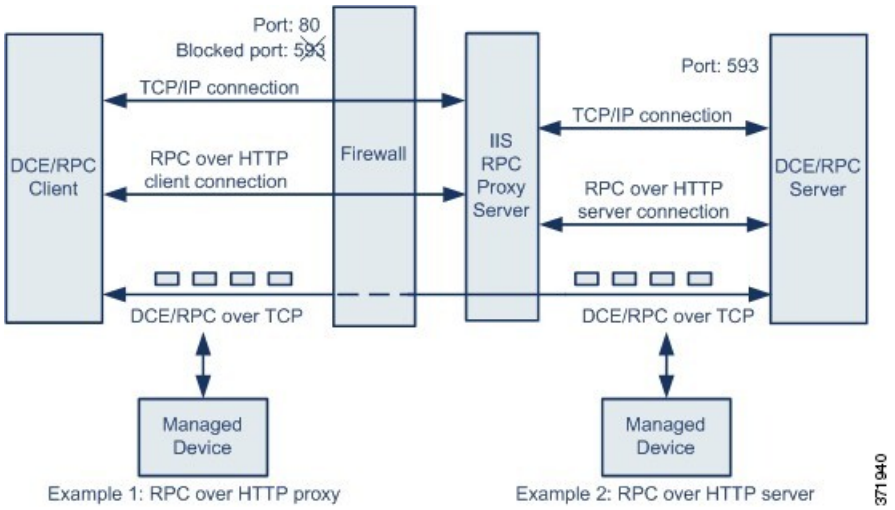
各ターゲットベースのポリシーでは次の設定が可能です。

- 1 つ以上のトランスポートを有効にし、それぞれについて検出ポートを指定します。
- 自動検出ポートを有効にして指定します。
- 指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそのことを検出するように、プリプロセッサを設定します。
- SMB トラフィックでファイルを検出し、検出されたファイルで指定されたバイト数を検査するように、プリプロセッサを設定します。
- SMB プロトコルの知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB AndX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定します。

DCE/RPC プリプロセッサで SMB トラフィック ファイル検出を有効にするほかに、オプションでこれらのファイルをキャプチャしてブロックするか、またはダイナミック分析のために Cisco AMP クラウドに送信するように、ファイル ポリシーを設定できます。そのポリシー内で、[アクション（Action）] として [ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] を選択し、[アプリケーション プロトコル（Application Protocol）] として [任意（Any）] または [NetBIOS-ssn (SMB)] を選択して、ファイル ルールを作成する必要があります。

RPC over HTTP トランスポート

Microsoft RPC over HTTP では、次の図に示すように、DCE/RPC トラフィックをトンネリングして、ファイアウォールを通過させることができます。DCE/RPC プリプロセッサは Microsoft RPC over HTTP バージョン 1 を検出します。



Microsoft IIS プロキシ サーバと DCE/RPC サーバは、同じホストまたは別々のホストにインストールできます。いずれの場合でも、個別のプロキシ オプションとサーバ オプションがあります。この図の次の点に注意してください。

- DCE/RPC サーバはポート 593 で DCE/RPC クライアント トラフィックをモニタしますが、ファイアウォールはこのポート 593 をブロックします。

  通常、ファイアウォールではデフォルトでポート 593 がブロックされます。

- RPC over HTTP は、ファイアウォールによって許可される可能性が高いウェルノウン HTTP ポート 80 を使用して、HTTP 経由で DCE/RPC を伝送します。

- 例 1 のように、DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間のトラフィックをモニタする場合は、[RPC over HTTP プロキシ（RPC over HTTP proxy）] オプションを選択します。

- 例 2 のように、Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上にあり、デバイスが 2 つのサーバ間のトラフィックをモニタしている場合は、[RPC over HTTP サーバ（RPC over HTTP server）] オプションを選択します。

- RPC over HTTP により DCE/RPC クライアントとサーバー間でのプロキシ セットアップが完了した後、トラフィックは TCP を経由したコネクション型 DCE/RPC だけで構成されます。

DCE/RPC グローバル オプション

グローバル DCE/RPC プリプロセッサ オプションは、プリプロセッサの機能を制御します。[到達したメモリ容量（Memory Cap Reached）] および [SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] オプション以外のオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

最大フラグメント サイズ（Maximum Fragment Size）

[最適化の有効化（Enable Defragmentation）] が選択されている場合、DCE/RPC フラグメントの許容最大長を指定します。これよりも大きなフラグメントの場合、プリプロセッサは処理のためにフラグメントの一部を切り捨て、指定のサイズにしてから最適化を行いますが、実際のパケットは変更されません。空白フィールドの場合、このオプションは無効になります。

[最大フラグメント サイズ（Maximum Fragment Size）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

リアセンブリしきい値（Reassembly Threshold）

[最適化の有効化（Enable Defragmentation）] が選択されている場合、0 を指定するとこのオプションは無効になります。あるいは、フラグメント化された DCE/RPC の最小バイト数を、該当する場合は、再構成されたパケットをルールエンジンに送信する前にキューに入れるセグメント化 SMB のバイト数を指定します。低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このオプションを有効にする場合は、パフォーマンスの影響をテストしておく必要があります。

[リアセンブリしきい値（Reassembly Threshold）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

最適化の有効化（Enable Defragmentation）

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。無効にすると、プリプロセッサは引き続き異常を検出して DCE/RPC データをルール エンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このオプションには、DCE/RPC トラフィックを最適化しないという柔軟性がありますが、ほとんどの DCE/RPC エクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試みが行われます。このオプションを無効にすると、ほとんどの既知のエクスプロイトがバイパスされ、検出漏れが大量に発生します。

到達したメモリ容量（Memory Cap Reached）

プリプロセッサに割り当てられた最大メモリ制限に達したか、またはこの制限を超過したことを検出します。最大メモリ制限に達したか、またはこの制限を超過した場合、プリプロセッサはメモリ キャップ イベントを引き起こしたセッションに関連付けられているすべての保留データを解放し、セッションのそれ以降の部分を無視します。

ルール 133:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）

SMB `Session Setup AndX` 要求および応答に指定されている Windows または Samba のバージョンを検出します。検出されたバージョンが、[ポリシー（Policy）] 設定オプションで設定されている Windows または Samba のバージョンと異なる場合、そのセッションに限り、検出されたバージョンが設定バージョンをオーバーライドします。

たとえば、[ポリシー（Policy）] に Windows XP を設定した場合に、プリプロセッサが Windows Vista を検出すると、プリプロセッサはそのセッションでは Windows Vista ポリシーを使用します。その他の設定は引き続き有効です。

DCE/RPC トランスポートが SMB ではない場合は（トランスポートが TCP または UDP の場合）、バージョンを検出できず、ポリシーを自動的に設定できません。

このオプションを有効にするには、ドロップダウン リストで次のいずれかを選択します。

- サーバ/クライアント トラフィックでポリシー タイプを検査するには、[クライアント（Client）] を選択します。
- クライアント/サーバ トラフィックでポリシー タイプを検査するには、[サーバ（Server）] を選択します。
- サーバ/クライアント トラフィックとクライアント/サーバ トラフィックの両方でポリシー タイプを検査するには、[両方（Both）] を選択します。

レガシー SMB 検査モード（Legacy SMB Inspection Mode）

[レガシーSMB検査モード（Legacy SMB Inspection Mode）] が有効な場合、システムは SMB バージョン 1 トラフィックにのみ SMB 侵入ルールを適用し、トランスポートとして SMB バージョン 1 を使用して DCE/RPC 侵入ルールを DCE/RPC トラフィックに適用します。このオプションが無効な場合、システムは SMB バージョン 1、2、および 3 を使用してトラフィックに SMB 侵入ルールを適用しますが、SMB バージョン 1 のみ、トランスポートとして SMB を使用して DCE/RPC 侵入ルールを DCE/RPC トラフィックに適用します。

関連トピック

基本コンテンツおよび protected_content キーワードの引数 （2074 ページ）
概要：byte_jump および byte_test キーワード

DCE/RPC ターゲットベース ポリシー オプション

各ターゲットベース ポリシーでは、TCP、UDP、SMB、および RPC over HTTP トランスポートのうち1つ以上を有効にできます。トランスポートを有効にする場合は、1つ以上の検出ポート（DCE/RPC トラフィックを伝送することがわかっているポート）を指定する必要があります。

シスコでは、デフォルトの検出ポート（ウェルノウンポートまたは各プロトコルで一般に使用されているポート）を使用することを推奨しています。検出ポートを追加するのは、デフォルト以外のポートで DCE/RPC トラフィックを検出した場合だけです。

Windows のターゲットベース ポリシーでは、ネットワークのトラフィックに一致するように、1 つ以上の任意のトランスポートのポートを任意の組み合わせで指定できます。しかし、Samba のターゲットベース ポリシーでは SMB トランスポートのポートだけを指定できます。

（注） 少なくとも 1 つのトランスポートが有効になっている DCE/RPC ターゲットベース ポリシーを追加した場合を除き、デフォルトのターゲットベースポリシーでは少なくとも 1 つの DCE/RPC トランスポートを有効にする必要があります。たとえば、すべての DCE/RPC 実装に対してホストを指定し、未指定のホストにはデフォルトのターゲットベース ポリシーを展開したくない場合があります。そのような場合は、デフォルトのターゲットベース ポリシーのトランスポートを有効化しないようにします。

（オプション）自動検出ポートを有効にして指定できます。プリプロセッサは、自動検出ポートとして指定されたポートを最初にテストして、そのポートが DCE/RPC トラフィックを伝送しているかどうかを判別し、DCE/RPC トラフィックを検出した場合にのみ処理を続行します。

自動検出ポートを有効にする場合は、エフェメラル ポート範囲全体に対応するよう、自動検出ポートが 1024 から 65535 の範囲に設定されていることを確認してください。

自動検出は、トランスポート検出ポートによって識別されていないポートでのみ発生する点にも注意してください。

[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] オプションまたは [SMB 自動検出ポート（SMB Auto-Detect Ports）] オプションで自動検出ポートを有効にしたり指定したりすることはほとんどありません。これは、指定されているデフォルト検出ポートを除き、どちらの場合もトラフィックが発生することはほとんどなく、その見込みも少ないためです。

各ターゲットベース ポリシーでは、次に示すさまざまなオプションを指定できます。以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Networks

DCE/RPC ターゲットベース サーバー ポリシーを展開するホストの IP アドレス。また、ターゲットベース ポリシーを追加する場合は、[ターゲットの追加（Add Target）] ポップアップ ウィンドウの [サーバー アドレス（Server Address）] フィールドに指定した名前。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを設定できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべて を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Policy

モニター対象ネットワーク セグメントのターゲット ホストが使用する Windows または Samba DCE/RPC の実装。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。

SMB の無効な共有（SMB Invalid Shares）

指定した共有リソースへの接続が試行されると、プリプロセッサが検出する 1 つ以上の SMB 共有リソースを識別します。複数の共有をカンマで区切って指定できます。また必要に応じて、共有を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。次に例を示します。

```
"C$", D$, "admin", private
```

[SMB ポート（SMB Ports）] が有効に設定されている場合、プリプロセッサは SMB トラフィックで無効な共有を検出します。

ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることに注意してください。たとえば、ドライブ C は C$ または "C$" として指定します。

SMB の無効な共有を検出するには、[SMB ポート（SMB Ports）] か、[SMB 自動検出ポート（SMB Auto-Detect Ports）] を有効にする必要があることにも注意してください。

ルール 133:26 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

SMB 最大 AndX チェーン（SMB Maximum AndX Chain）

連結された SMB AndX コマンドの許容最大数です。通常、多数の連結 AndX コマンドは異常な動作を表し、場合によっては回避試行を示している可能性があります。連結コマンドを許可しない場合は 1 を指定し、連結コマンドの数の検出を無効にするには 0 を指定します。

プリプロセッサは最初に連結コマンドの数をカウントし、関連する SMB プリプロセッサ ルールが有効であり、連結コマンドの数が設定されている値と等しいかそれ以上の場合にはイベントを生成することに注意してください。その後、処理が続行されます。

注意 SMB プロトコルに詳しいユーザーだけが [SMB AndX の最大チェーン（SMB Maximum AndX Chains）] オプションのデフォルト設定を変更するようにしてください。

ルール 133:20 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

RPC プロキシ トラフィックのみ（RPC proxy traffic only）

[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] が有効である場合、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであるか、または他の Web サーバー トラフィックを含んでいる可能性があるかどうかを示します。たとえば、ポート 80 はプロキシ トラフィックとその他の Web サーバー トラフィックの両方を伝送する可能性があります。

このオプションが無効になっている場合は、プロキシ トラフィックとその他の Web サーバー トラフィックの両方が想定されます。たとえばサーバーが専用プロキシ サーバーである場合などに、このオプションを有効にします。有効にすると、プリプロセッサはトラフィックを調べて DCE/RPC を伝送しているかどうかを判別し、伝送していない場合はそのトラフィックを無視し、伝送している場合は処理を続行します。このオプションを有効にすることで機能が追加されるのは、[RPC over HTTP Proxy Ports] チェック ボックスも有効にされている場合だけであることに注意してください。

RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバーの間に配置されている場合に、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

有効である場合、DCE/RPC トラフィックが確認されるポートを追加できますが、Web サーバーは一般に DCE/RPC トラフィックとその他のトラフィックの両方にデフォルト ポートを使用するため、この操作が必要になることはあまりありません。有効である場合、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] は有効にしませんが、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであり、その他の Web サーバー トラフィックを含んでいない場合は、[RPC プロキシ トラフィックのみ（RPC Proxy Traffic Only）] を有効にします。

（注） このオプションを選択することがあるとすれば、きわめて稀なケースです。

RPC over HTTP サーバー ポート（RPC over HTTP Server Ports）

Microsoft IIS RPC プロキシ サーバーと DCE/RPC サーバーが異なるホスト上に配置されており、デバイスがこの 2 つのサーバー間のトラフィックをモニターしている場合、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

一般に、このオプションを有効にするときは、ネットワーク上のプロキシ Web サーバーに注意を払わない場合でも、1025 ～ 65535 のポート範囲で [RPC over HTTP サーバー自動検出ポート（RPC over HTTP Server Auto-Detect Ports）] も有効にする必要があります。場合によっては RPC over HTTP サーバー ポートを再設定することがあり、その際には再設定したサーバー ポートをこのオプションのポート リストに追加する必要があることに注意してください。

TCP Ports

指定の各ポートでの TCP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 から 65535 までのポート範囲で [TCP Auto-Detect Ports] も有効にする必要もあります。

UDP Ports

指定の各ポートでの UDP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 から 65535 までのポート範囲で [UDP Auto-Detect Ports] も有効にする必要があります。

SMB Ports

指定の各ポートでの SMB の DCE/RPC トラフィックの検出を有効にします。

デフォルトの検出ポートを使用した SMB トラフィックが発生することがあります。他のポートはほとんどありません。通常はデフォルト設定を使用してください。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、ターゲット ポリシーに対して設定されているポリシータイプをセッションごとに自動的にオーバーライドできます。

RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバーの間に配置されている場合に、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

有効である場合は、エフェメラルポート範囲全体をカバーするため、一般にポート範囲として 1025 から 65535 を指定します。

RPC over HTTP サーバー自動検出ポート（RPC over HTTP Server Auto-Detect Ports）

Microsoft IIS RPC プロキシ サーバーおよび DCE/RPC サーバーが異なるホスト上に配置されており、デバイスがこの 2 つのサーバー間のトラフィックをモニターしている場合、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

TCP 自動検出ポート（TCP Auto-Detect Ports）

指定のポートで TCP の DCE/RPC トラフィックの自動検出を有効にします。

UDP Auto-Detect Ports

指定の各ポートで UDP の DCE/RPC トラフィックの自動検出を有効にします。

SMB Auto-Detect Ports

SMB の DCE/RPC トラフィックの検出を有効にします。

（注） このオプションを選択することがあるとすれば、きわめて稀なケースです。

SMB ファイル インスペクション（SMB File Inspection）

ファイル検出のための SMB トラフィックのインスペクションを有効にします。次の選択肢があります。

- ファイル インスペクションを無効にするには、[Off] を選択します。
- SMB でファイルデータを検査するが、DCE/RPC トラフィックは検査しない場合は、[Only] を選択します。このオプションを選択すると、ファイルと DCE/RPC トラフィックの両方を検査する場合よりもパフォーマンスが向上する可能性があります。
- SMB でファイルと DCE/RPC トラフィックの両方を検査するには、[On] を選択します。このオプションを選択すると、パフォーマンスに影響する可能性があります。

SMB トラフィックでの次のファイルについてのインスペクションはサポートされていません。

- 1 つの TCP または SMB セッションで同時に転送されたファイル
- 複数の TCP または SMB セッションにわたって転送されたファイル
- メッセージ署名のネゴシエート時など、非連続データを使用して転送されたファイル
- 同一オフセットに異なるデータが含まれており、データがオーバーラップしている転送ファイル
- リモート クライアントがファイル サーバーに保存し、そのクライアントで編集用に開かれたファイル

SMB File Inspection Depth

[SMB File Inspection] が [Only] または [On] に設定されている場合に、SMB トラフィックでファイルが検出された時に検査されるデータのバイト数です。次のいずれかを指定します。

- 正の値
- `0`：ファイル全体を検査する場合
- `-1`：ファイル インスペクションを無効にする場合

アクセス コントロール ポリシーの [詳細（Advanced）] タブの [ファイルおよびマルウェアの設定（File and Malware Settings）] セクションで定義された値以下になるように、このフィールドに値を入力します。[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] で定義されている値よりも大きい値をこのオプ

ションに設定すると、アクセス コントロール ポリシーの設定が、有効な最大値として使用されます。

[SMB ファイル インスペクション（SMB File Inspection）] が [オフ（Off）] に設定されている場合、このフィールドは無効になります。

トラフィックに関連する DCE/RPC ルール

ほとんどの DCE/RPC プリプロセッサ ルールでは、SMB、コネクション型 DCE/RPC、またはコネクションレス型 DCE/RPC のトラフィックで検出される異常や検知回避技術に対してトリガーします。トラフィック タイプ別に有効にできるルールを次の表に示します。

表 *207*: トラフィックに関連する *DCE/RPC* ルール

トラフィック	プリプロセッサ ルール GID:SID
SMB	133:2 ～ 133:26、133:48 ～ 133:59
コネクション型 DCE/RPC	133:27 ～ 133:39
コネクションレス型 DCE/RPC の検出	133:40 ～ 133:43

DCE/RPC プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

DCE/RPC プリプロセッサを設定するには、プリプロセッサの機能を制御するグローバル オプションを変更するか、IP アドレスと稼働している Windows または Samba のバージョンによってネットワーク上の DCE/RPC サーバーを識別する 1 つ以上のターゲットベース サーバー ポリシーを指定します。ターゲットベース ポリシー構成では、トランスポート プロトコルの有効化、DCE/RPC トラフィックをホストに伝送するポートの指定、およびその他のサーバー固有オプションの設定も行います。

始める前に

- カスタム ターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、および VLAN のサブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2748 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DCE/RPC の構成（DCE/RPC Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [DCE/RPCの構成（DCE/RPC Configuration）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 [グローバル設定（Global Settings）] セクションのオプションを変更します。DCE/RPC グローバル オプション （2772 ページ）を参照してください。

ステップ 8 次の選択肢があります。

- サーバープロファイルの追加：[サーバー（Servers）] の横にある[追加（Add）]()をクリックします。1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。
- サーバープロファイルの削除：ポリシーの横にある[削除（Delete）]（）をクリックします。
- サーバープロファイルの編集：[サーバー（Servers）]の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。DCE/RPC ターゲットベース ポリシー オプション （2774 ページ）を参照してください。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、DCE/RPC プリプロセッサ ルール（GID 132 または 133）を有効にします。詳細については、侵入ルール状態の設定 （2032 ページ）、DCE/RPC グローバル オプション （2772 ページ）、DCE/RPC ターゲットベース ポリシー オプション （2774 ページ）、およびトラフィックに関連する DCE/RPC ルール （2780 ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション （2286 ページ）
DCE/RPC キーワード （2131 ページ）
レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

DNS プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

DNS プリプロセッサは、DNS ネーム サーバー応答を検査し、次に示す特定のエクスプロイトがあるかどうかを確認します。

- RData テキスト フィールドに対するオーバーフローの試行
- 古い DNS リソース レコード タイプ
- 試験的な DNS リソース レコード タイプ

最も一般的なタイプの DNS ネーム サーバ応答には、応答を求めたクエリ内のドメイン名に対応する 1 つ以上の IP アドレスが示されています。その他のタイプのサーバ応答には、たとえば、電子メール メッセージの宛先や、元のクエリの対象のサーバからは取得できない情報を提供できるネーム サーバの位置などが記述されています。

DNS 応答には以下の構成要素があります。

- メッセージ ヘッダー
- 1 つ以上の要求が含まれる [質問（Question）] セクション
- [質問（Question）] セクションの要求に応答する 3 つのセクション
  - 応答
  - 権限（Authority）

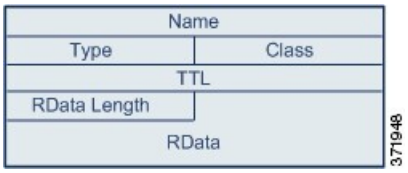
- その他の情報（Additional Information）

この 3 セクションの応答には、ネーム サーバーに保持されているリソース レコード（RR）の情報が反映されます。次の表で、これらの 3 つのセクションについて説明します。

表 *208 : DNS* ネーム サーバ *RR* 応答

セクション	内容	例
応答	クエリに対する特定の回答を提供する 1 つ以上のリソース レコード（オプション）	ドメイン名に対応する IP アドレス
権限	権威ネーム サーバを指し示す 1 つ以上のリソース レコード（オプション）	応答の権威ネーム サーバーの名前
その他の情報	[応答（Answer）] セクションに関連する追加情報を提供する 1 つ以上のリソース レコード（オプション）	クエリ対象の別のサーバの IP アドレス

さまざまなタイプのリソース レコードがありますが、これらはすべて一貫して次の構造を保っています。



理論上、すべてのタイプのリソース レコードを、ネーム サーバ応答メッセージの [応答（Answer）]、[権威（Authority）]、または [追加情報（Additional Information）] セクションで使用できます。DNS プリプロセッサは、検出されたエクスプロイトについて、3 つの各応答セクションのすべてのリソース レコードを検査します。

[タイプ（Type）] および [RData] リソース レコード フィールドは、DNS プリプロセッサでは特に重要です。[タイプ（Type）] フィールドは、リソース レコードのタイプを示します。[RData]（リソース データ）フィールドは、応答の内容を示します。[RData] フィールドのサイズと内容は、リソース レコードのタイプによって異なります。

DNS メッセージは通常、UDP トランスポート プロトコルを使用しますが、信頼性のある配信を必要とするメッセージ タイプである場合や、メッセージ サイズが UDP で処理可能なサイズを超えている場合は、TCP を使用します。DNS プリプロセッサは、UDP および TCP の両方のトラフィックで DNS サーバ応答を検査します。

DNS プリプロセッサは、ミッドストリームで検出された TCP セッションを検査せず、ドロップされたパケットが原因でセッションの状態が失われるとインスペクションを終了します。

DNS プリプロセッサ オプション

ポート

このフィールドは、送信元ポート、または DNS プリプロセッサが DNS サーバー応答をモニターする必要があるポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

DNS プリプロセッサ用に設定する一般的なポートは、ウェルノウン ポート 53 です。これは、DNS ネーム サーバーが UDP および TCP の両方で DNS メッセージに使用するポートです。

RData テキスト フィールドでのオーバーフローの試行の検出

リソース レコード タイプが TXT（テキスト）の場合、RData フィールドは可変長の ASCII テキスト フィールドになります。

このオプションを選択した場合は、MITRE の Current Vulnerabilities and Exposures データベースの CVE-2006-3441 エントリで指定した特定の脆弱性を検出します。これは、Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1 および Service Pack 2、Windows Server 2003 Service Pack 1 の既知の脆弱性です。攻撃者はこの脆弱性を悪用して、[RData] テキスト フィールドの長さの誤算を引き起こし、結果としてバッファ オーバーフローを発生させるよう悪意をもって作られたネーム サーバー応答をホストに送信するか受信させることで、ホストを完全に制御できます。

アップグレードによってこの脆弱性が修正されていないオペレーティング システムが稼働しているホストがネットワーク内に含まれている可能性がある場合は、このオプションを有効にする必要があります。

ルール 131:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定 （2032 ページ） を参照してください。

古い DNS RR タイプの検知

RFC 1035 ではさまざまなリソース レコード タイプが古いタイプとして指定されています。これらは古いレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコードタイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の古いリソース レコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *209 :* 古い *DNS* リソース レコード タイプ

RR タイプ	コード	説明
3	MD	メールの宛先

RR タイプ	コード	説明
4	MF	メールのフォワーダ

ルール 131:1 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

試験的な DNS RR タイプの検出

RFC 1035 ではさまざまなリソース レコード タイプが試験的なタイプとして指定されています。これらは試験的なレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコードタイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の試験的なレコードタイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *210*：試験的な *DNS* リソース レコード タイプ

RR タイプ	コード	説明
7	MB	メールボックスのドメイン名
8	MG	メール グループ メンバー
9	MR	メール リネーム ドメイン名
10	NUL	空白のリソース レコード

ルール 131:2 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

DNS プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DNS の構成（DNS Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [DNSの構成（DNS Configuration）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 DNS プリプロセッサ オプション （2784 ページ）で説明されている設定を変更します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、DNS プリプロセッサルール（GID 131）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」および「DNS プリプロセッサ オプション （2784 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

侵入ポリシーとネットワーク分析ポリシーのレイヤ （2179 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

FTP/Telnet デコーダ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

FTP/Telnet デコーダは FTP および Telnet データ ストリームを分析して、ルール エンジンによる処理の前に FTP および Telnet コマンドを正規化します。

グローバル FTP および Telnet オプション

FTP/Telnet デコーダがパケットのステートフル インスペクションまたはステートレス インスペクションを実行するかどうか、デコーダが暗号化 FTP または Telnet セッションを検出するかどうか、およびデコーダが暗号化データの検出後にデータ ストリームの検査を続行するかどうかを決定するグローバル オプションを設定できます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、FTP/Telnetデコーダは状態を保存し、各パケットにセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

FTP データ転送を検査するには、このオプションを選択する必要があります。

暗号化トラフィックの検出（Detect Encrypted Traffic）

暗号化 Tenet および FTP セッションを検出します。

ルール 125:7 と 126:2 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定 （2032ページ） を参照してください。

暗号化データの検査を続行（Continue to Inspect Encrypted Data）

プリプロセッサに対し、データ ストリームの暗号化後もデータ ストリームの検査を続行し、最終的に処理できるデコードされたデータを検索するように指示します。

Telnet オプション

FTP/Telnet デコーダによる Telnet コマンドの正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を設定できます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

ポート

Telnet トラフィックを正規化するポートを示します。通常、Telnet は TCP ポート 23 に接続します。インターフェイスで、複数のポートをカンマで区切って指定します。

⚠

注意 暗号化トラフィック（SSL）はデコードできないので、ポート 22（SSH）を追加すると、予想外の結果が生じる可能性があります。

正規化（Normalize）

指定のポートへの Telnet トラフィックを正規化します。

異常検知（Detect Anomalies）

対応する SE（サブネゴシエーション終了）がない Telnet SB（サブネゴシエーション開始）の検出を有効にします。

Telnetがサポートするサブネゴシエーションは、SB（サブネゴシエーション開始）で開始し、SE（サブネゴシエーション終了）で終了していなければなりません。しかし、一部の Telnet サーバ実装では、対応する SE のない SB が無視されます。これは、回避事例につながるおそれのある異常な動作です。FTP はコントロール接続で Telnet プロトコルを使用するため、FTP もこの動作の影響を受けます。

ルール 126:3 を有効にすることでイベントを生成でき、インライン展開では、この異常が Telnet トラフィックで検出される場合に違反パケットをドロップできます。FTP コマンドチャネルで検出される場合はルール 125:9 を有効にできます。侵入ルール状態の設定（2032 ページ）を参照してください。

Are You There 攻撃のしきい値（Are You There Attack Threshold Number）

連続する AYT コマンドの数が指定のしきい値を超えた場合にそのことを検出します。Cisco は、AYT しきい値としてデフォルト値以下の値を設定することを推奨します。

ルール 126:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

サーバーレベルの FTP オプション

複数の FTP サーバーでデコード オプションを設定できます。作成する各サーバー プロファイルには、トラフィックをモニターするサーバーのサーバー IP アドレスとポートが含まれます。検証する FTP コマンドと、特定のサーバーで無視する FTP コマンドを指定し、コマンドの最大パラメータ長を設定できます。また、デコーダが特定のコマンドで検証する特定のコマンド構文を設定し、代替最大コマンド パラメータ長を設定することもできます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

Networks

FTP サーバーの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

単一IPアドレスまたはアドレスブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。設定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべてを表すアドレス表記（0.0.0.0/0 または ::/0）を使用することはできません。

Ports

管理対象デバイスがトラフィックをモニターするFTPサーバーのポートを指定するには、このオプションを使用します。インターフェイスで、複数のポートをカンマで区切って指定します。ポート 21 は FTP トラフィック用のウェルノウン ポートです。

File Get コマンド（File Get Commands）

サーバーからクライアントにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

⚠

注意 サポートからの指示がない限り、[File Get コマンド（File Get Commands）] フィールドを変更しないでください。

File Put コマンド（File Put Commands）

クライアントからサーバーにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

⚠

注意 サポートからの指示がない限り、[File Put コマンド（File Put Commands）] フィールドを変更しないでください。

追加 FTP コマンド（Additional FTP Commands）

デコーダが検出するコマンドを追加で指定するには、この行を使用します。複数のコマンドを追加する場合は、コマンドをスペースで区切ってください。

追加できるコマンドには、XPWD、XCWD、XCUP、XMKD、XRMD があります。これらのコマンドの詳細については、RFC 775（Network Working Group によるディレクトリに基づく FTP コマンドの仕様）を参照してください。

デフォルト最大パラメータ長（Default Max Parameter Length）

代替最大パラメータ長が設定されていないコマンドの最大パラメータ長を検出するには、このオプションを使用します。代替最大パラメータ長は、必要な数だけ追加できます。

ルール 125:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

代替最大パラメータ長（Alternate Max Parameter Length）

異なる最大パラメータ長を検出するコマンドを指定し、それらのコマンドの最大パラメータ長を指定するには、このオプションを使用します。[Add] をクリックして行を追加し、特定のコマンドで検出する異なる最大パラメータ長を指定します。

Check Commands for String Format Attacks

指定されたコマンドでフォーマット文字列攻撃を検査するには、このオプションを使用します。

ルール 125:5 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

コマンドの妥当性（Command Validity）

特定のコマンドの有効な形式を入力するには、このオプションを使用します。[追加（Add）] をクリックして、コマンド検証行を追加します。

ルール 125:2 と 125:4 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

FTP 転送を無視（Ignore FTP Transfers）

データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして FTP データ転送のパフォーマンスを改善するには、このオプションを使用します。

（注） データ転送を検査するには、グローバル FTP/Telnet オプション [ステートフル インスペクション（Stateful Inspection）] を選択する必要があります。

FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[Detect Telnet Escape Codes within FTP Commands] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP サーバーによる Telnet 消去コマンドの処理方法と一致する必要があります。一般に、新しい FTP サーバーは Telnet 消去コマンドを無視しますが、ほとんどの古いサーバーは Telnet 消去コマンドを処理する点に注意してください。

トラブルシューティング オプション：FTP コマンドの検証設定のログを記録（Troubleshooting Options：Log FTP Command Validation Configuration）

トラブルシューティングについてサポートに問い合わせた際に、サーバー用にリストされている FTP コマンドごとに設定情報を出力するように、システムを設定することを指示される場合があります。

⚠

注意 サポートからの指示がない限り [FTP コマンドの検証設定のログを記録（Log FTP Command Validation Configuration）] を有効にしないでください。

FTP コマンドの検証ステートメント

FTP コマンドに対する検証ステートメントを設定するときには、複数の代替パラメータをスペースで区切って指定できます。2 つのパラメータ間にバイナリ OR 関係を作成するには、検証ステートメントでこの 2 つのパラメータをパイプ文字（|）で区切って指定します。パラメータを大カッコ（[]）で囲むと、これらのパラメータがオプションであることを示します。パラメータを中カッコ（{}）で囲むと、これらのパラメータが必須であることを示します。

FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントを作成できます。

FTP コマンド パラメータ検証ステートメントに使用できるパラメータを次の表に示します。

表 *211 : FTP* コマンド パラメータ

使用するパラメータ	実行される検証
`int`	示されるパラメータが整数である必要があります。

使用するパラメータ	実行される検証
`number`	示されるパラメータが 1 ～ 255 の範囲内の整数である必要があります。
`char` _chars	示されるパラメータが単一文字であり、かつ _chars 引数に指定した文字の 1 つである必要があります。 たとえば、検証引数 `char` SBC を使用して `MODE` のコマンド検証を定義すると、`MODE` コマンドのパラメータが、文字 `S`（Stream モードを示す）、文字 `B`（Block モードを示す）、または文字 `C`（Compressed モードを示す）を含んでいるかどうかが検証されます。
`date` _datefmt	_datefmt に `#` が含まれている場合、示されるパラメータは数値である必要があります。 _datefmt に `C` が含まれている場合、示されるパラメータは文字である必要があります。 _datefmt にリテラル文字列が含まれている場合、示されるパラメータはリテラル文字列に一致している必要があります。
`string`	示されるパラメータが文字列である必要があります。
`host_port`	示されるパラメータは、RFC 959（Network Working Group による File Transfer Protocol 仕様）で定義されている有効なホスト ポート指定子である必要があります。

上記の表の構文を必要に応じて組み合わせることにより、トラフィックを検証する必要がある各 FTP コマンドを正しく検証するパラメータ検証ステートメントを作成できます。

（注） TYPE コマンドに複合式を含める場合は、式をスペースで囲んでください。また、式内の各オペランドをスペースで囲んでください。たとえば、`char A|B` ではなく `char A | B` と入力します。

関連トピック

サーバーレベルの FTP オプション （2788 ページ）
FTP コマンドの検証ステートメント （2791 ページ）

クライアントレベルの FTP オプション

カスタム FTP クライアント プロファイルを設定するには、これらのオプションを使用します。オプション記述にプリプロセッサ ルールが含まれない場合、そのオプションはプリプロセッサ ルールに関連付けられません。

ネットワーク

FTP クライアントの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべてを表すアドレス表記（0.0.0.0/0 または ::/0）を使用することはできません。

最大応答長（Max Response Length）

このオプションを使用して、クライアントが受け入れる FTP コマンドに許可される最大応答長を指定します。これにより、基本的なバッファ オーバーフローを検出できます。

ルール 125:6 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

FTP バウンス試行の検出（Detect FTP Bounce Attempts）

FTP バウンス攻撃を検出するには、このオプションを使用します。

ルール 125:8 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

FTP バウンスの許可（Allow FTP Bounce to）

FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとそれらのホスト上のポートのリストを設定するには、このオプションを使用します。

FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP クライアン

トによる Telnet 消去コマンドの処理方法に一致している必要があります。一般に、新しい FTP クライアントは Telnet 消去コマンドを無視しますが、ほとんどの古いクライアントは Telnet 消去コマンドを処理する点に注意してください。

FTP/Telnet デコーダの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

クライアントからのFTPトラフィックをモニターするように、FTPクライアントのクライアント プロファイルを設定できます。

始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2748 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policies）]** をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [FTPとTelnetの構成（FTP and Telnet Configuration）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 7 グローバル FTP および Telnet オプション （2787 ページ）の説明に従って、[グローバル設定（Global Settings）] セクションのオプションを設定します。

ステップ 8 Telnet オプション （2787 ページ）の説明に従って、[Telnet の設定（Telnet Settings）] セクションのオプションを設定します。

ステップ 9 FTP サーバー プロファイルを管理します。

- サーバープロファイルの追加：[FTPサーバー（FTP Server）] の横にある[追加（Add）] (＋)をクリックします。クライアントの 1 つ以上の IP アドレスを [サーバアドレス（Server Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。
- サーバー プロファイルの編集：[FTP サーバー（FTP Server）] の下にあるカスタム プロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。サーバーレベルの FTP オプション （2788 ページ）を参照してください。
- サーバープロファイルの削除：プロファイルの横にある[削除（Delete）]（🗑）をクリックします。

ステップ 10 FTP クライアント プロファイルを管理します。

- クライアントプロファイルの追加：[FTPクライアント（FTP Client）] の横にある[追加（Add）] (＋)をクリックします。クライアントの 1 つ以上の IP アドレスを [クライアントアドレス（Client Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。
- クライアントプロファイルの編集：[FTP クライアント（FTP Client）] の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] ページ エリアの設定を変更できます。クライアントレベルの FTP オプション （2792 ページ）を参照してください。
- クライアントプロファイルの削除：カスタムプロファイルの横にある[削除（Delete）]（🗑）をクリックします。

ステップ 11 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、FTP および telnet プリプロセッサ ルール（GID 125 および 126）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

HTTP Inspect プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

HTTP Inspect プリプロセッサは、次の処理を行います。

- ネットワーク上の Web サーバーに送信される HTTP 要求と Web サーバーから受信する HTTP 応答をデコードおよび正規化する。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバーに送信されたメッセージを URI、非 cookie ヘッダー、cookie ヘッダー、メソッド、メッセージ本文の各コンポーネントに分ける。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバーから受信したメッセージをステータス コード、ステータス メッセージ、非 set-cookie ヘッダー、cookie ヘッダー、応答本文の各コンポーネントに分ける。
- URI エンコード攻撃の可能性を検出する。
- 正規化データを追加ルール処理に使用できるようにする。
- JavaScript などの悪意のあるスクリプトによる攻撃を検出して防止する。

HTTP トラフィックはさまざまな形式でエンコードされている可能性があり、このことが、ルールによる適切な検査の実施を困難にしています。HTTP Inspect は 14 種類のエンコードをデコードし、HTTP トラフィックが最良のインスペクションを受けられるようにします。

HTTP Inspect のオプションは、グローバルに設定するか、1 つのサーバーで設定するか、またはサーバー リストに対して設定することができます。

プリプロセッサ エンジンは HTTP の正規化をステートレスに実行することに注意してください。つまり、パケット単位で HTTP 文字列を正規化し、TCP ストリーム プリプロセッサにより再構成された HTTP 文字列のみを処理できます。

fast_blocking

Snort バージョン 2.9.16.0 以降、HTTP Inspect プリプロセッサのグローバル設定オプションである fast_blocking オプションが導入されました。このオプションを使用すると、データがクリアされる前に HTTP データを検査できます。これにより、早期に IPS ルールを評価することができ、ブロックルールが適用されます。データのクリア後に接続がブロックされるのではなく、可能な限り早くブロックされます。この設定は、インライン正規化が有効になっている場合にのみ有効です。

fast_blocking オプションを有効にするには、基本ポリシーとして [最大検出（Maximum Detection）] を指定したネットワーク分析ポリシーを使用する必要があります。

グローバル HTTP 正規化オプション

HTTP Inspect プリプロセッサのグローバル HTTP オプションは、プリプロセッサの機能を制御します。Web サーバ ポートとして指定されていないポートが HTTP トラフィックを受信する場合の HTTP 正規化を有効または無効にするには、このオプションを使用します。

次の点に注意してください。

- [無制限の圧縮解除（Unlimited Decompression）] を有効にすると、変更のコミット時に [圧縮データの最大深さ（Maximum Compressed Data Depth）] および [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] オプションが自動的に 65535 に設定されます。
- 最大値は、[圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] の値が異なる場合に使用されます。
  - デフォルトのネットワーク分析ポリシー
  - 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

異常な HTTP サーバの検出（Detect Anomalous HTTP Servers）

Web サーバー ポートとして指定されていないポートに送信された HTTP トラフィックまたはこのポートで受信した HTTP トラフィックを検出します。

（注） このオプションをオンにする場合は、[HTTP 設定（HTTP Configuration）] ページで、HTTP トラフィックを受信するすべてのポートがサーバプロファイルにリストされていることを確認してください。確認せずにこのオプションと関連するプリプロセッサ ルールを有効にすると、サーバーとの間の通常のトラフィックによってイベントが生成されます。デフォルトのサーバープロファイルには、HTTP トラフィックに一般に使用されるすべてのポートが含まれていますが、このプロファイルを変更した場合は、イベントの生成を防ぐために別のプロファイルにそれらのポートを追加する必要があります。

ルール 120:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

HTTP プロキシ サーバーの検出（Detect HTTP Proxy Servers）

[HTTP プロキシの使用を許可（Allow HTTP Proxy Use）] オプションで定義されていないプロキシ サーバーを使用する HTTP トラフィックを検出します。

ルール 119:17 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

圧縮データの最大深さ（Maximum Compressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、圧縮解除する圧縮データの最大サイズを設定します。

圧縮解除データの最大深さ（Maximum Decompressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、正規化された圧縮データの最大サイズを設定します。

サーバーレベルの HTTP 正規化オプション

サーバーレベルのオプションは、モニター対象サーバーごとに設定するか、すべてのサーバーに対してグローバルに設定するか、またはサーバーリストに対して設定することができます。また、事前定義のサーバープロファイルを使用してこれらのオプションを設定するか、またはご使用の環境のニーズに合わせて個別に設定することができます。これらのオプション、またはこれらのオプションを設定するデフォルトプロファイルの 1 つを使用して、トラフィックを

正規化する HTTP サーバー ポート、正規化するサーバー応答ペイロードの量、および正規化するエンコードのタイプを指定します。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

Networks

1 つ以上のサーバーの IP アドレスを指定するには、このオプションを使用します。1 つの IP アドレスまたはアドレスブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

デフォルト プロファイルを含めてプロファイルの合計数は最大 255 ですが、さらに、HTTP サーバー リストに最大 496 文字（約 26 エントリ）を含めることができ、すべてのサーバー プロファイルに対して合計 256 のアドレス エントリを指定できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`すべて` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Ports

プリプロセッサ エンジンが HTTP トラフィックを正規化するポート。ポート番号が複数ある場合は、カンマで区切ります。

サイズ超過のディレクトリ長（Oversize Dir Length）

指定された値よりも長い URL ディレクトリを検出します。

指定された長さよりも長い URL の要求をプロセッサが検出した場合にイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 119:15 を有効にします。

クライアント フローの深さ（Client Flow Depth）

[Ports] で定義されているクライアント側 HTTP トラフィックで、ルールにより検査される raw HTTP パケットのバイト数（見出しとペイロード データを含む）を指定します。ルール内の HTTP コンテンツ ルール オプションによって要求メッセージの特定の部分が検査される場合は、[クライアント フローの深さ（Client Flow Depth）] は適用されません。

次のいずれかを指定します。

- 正の値によって、最初のパケットで指定のバイト数が検査されます。最初のパケットのバイト数が指定のバイト数よりも少ない場合は、パケット全体が検査されます。指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることに注意してください。

また、値 300 を指定すると、通常は、多くのクライアント要求ヘッダーの終わりにある大きな HTTP Cookie のインスペクションが排除されることにも注意してください。

- 0 を指定すると、すべてのクライアント側トラフィックが検査されます。これにはセッション内の複数のパケットが含まれ、必要な場合にはバイトの上限を超えることもあります。この値はパフォーマンスに影響する可能性があることに注意してください。
- -1 を指定すると、クライアント側のすべてのトラフィックが無視されます。

サーバー フローの深さ（Server Flow Depth）

[Ports] で指定されたサーバー側 HTTP トラフィックで、ルールにより検査される raw HTTP パケットのバイト数を指定します。[Inspect HTTP Responses] が無効である場合は raw 見出しとペイロードが検査され、[Inspect HTTP Response] が有効である場合は、raw 応答ボディのみが検査されます。

Server Flow Depth は、[Ports] で定義されているサーバー側 HTTP トラフィックで、ルールにより検査されるセッション内の raw サーバー応答データのバイト数を指定します。このオプションを使用して、HTTP サーバー応答データのインスペクションのレベルとパフォーマンスのバランスを調整できます。ルール内の HTTP コンテンツ オプションによって要求メッセージの特定の部分が検査される場合は、Server Flow Depth は適用されません。

クライアント フローの深さ（Client Flow Depth）とは異なり、サーバー フローの深さ（Server Flow Depth）では、ルールが検査するバイト数を、HTTP 要求パケットごとではなく、HTTP 応答ごとのバイト数として指定します。

次のいずれかの値を指定できます。

- 正の値：

  [HTTP 応答の検査（Inspect HTTP Responses）] が**有効**である場合、raw HTTP 応答ボディのみが検査され、raw HTTP ヘッダーは検査されません。また、[圧縮データの検査（Inspect Compressed Data）] が有効である場合は、圧縮解除データも検査されます。

  [Inspect HTTP Responses] が**無効**である場合、raw パケット 見出しとペイロードが検査されます。

  セッションの応答バイト数が指定の値よりも少ない場合は、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）すべての応答パケットが完全に検査されます。セッションの応答バイト数が指定の値よりも多い場合、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）指定のバイト数だけが検査されます。

  Flow Depth の値が小さい場合、[Ports] で定義されているサーバー側トラフィックを対象とするルールで、検出漏れが発生する可能性があります。これらのルールのほとんどは HTTP 見出しまたはコンテンツ（これは多くの場合非見出しデータの先頭の約 100 バイト内にあります）を対象とします。通常見出しの長さは 300 バイト未満ですが、見出しサイズは異なることがあります。

  指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることにも注意してください。

- 0 を指定すると、[Port] で定義されているすべての HTTP サーバー側トラフィックでパケット全体が検査されます。これにはセッションでの 65535 バイトよりも大きな応答データも含まれます。

  この値はパフォーマンスに影響する可能性があることに注意してください。

- -1：

  [Inspect HTTP Responses] が**有効**な場合、raw HTTP 見出しだけが検査され、raw HTTP 応答ボディは検査されません。

  [Inspect HTTP Responses] が**無効**である場合、[Ports] で定義されているすべてのサーバー側トラフィックは無視されます。

Maximum Header Length

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合は、HTTP 要求、および HTTP 応答で、指定されている最大バイト数よりも長いヘッダー フィールドを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:19 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

最大ヘッダー数（Maximum Number of Headers）

HTTP 要求でヘッダー数がこの設定を超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:20 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

最大スペース数（Maximum Number of Spaces）

折りたたみ行のスペースの数が HTTP 要求のこの設定と等しいか、超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:26 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

HTTP クライアント ボディの抽出の深さ（HTTP Client Body Extraction Depth）

HTTP クライアント要求のメッセージ ボディから抽出するバイト数を指定します。侵入ルールを使用して抽出データを検査するには、`content` または `protected_content` キーワードを [HTTP クライアント ボディ（HTTP Client Body）] オプションと共に選択します。

クライアント ボディを無視するには、-1 を指定します。クライアント ボディ全体を抽出するには、0 を指定します。抽出対象のバイト数を指定すると、システム パフォーマンスが向上す

ることがある点に注意してください。また、侵入ルールで[HTTP クライアント ボディ（HTTP Client Body）] オプションが機能するためには、0 か 0 より大きい値を指定する必要があることに注意してください。

小さいチャンク サイズ（Small Chunk Size）

チャンクが小さいとみなされるサイズの最大バイト数を指定します。正の値を指定します。値 0 を指定すると、異常な小さなセグメントの連続の検出が無効になります。詳細については、[Consecutive Small Chunks] オプションを参照してください。

Consecutive Small Chunks

チャンク転送エンコードを使用するクライアント トラフィックまたはサーバー トラフィックで異常に大量であるとみなされる、連続する小さなチャンクの数を指定します。[Small Chunk Size] オプションは、小さなチャンクの最大サイズを指定します。

たとえば、10 バイト以下のチャンクが 5 つ連続していることを検出するには、[小さいチャンク サイズ（Small Chunk Size）] に 10 を設定し、[連続する小さいチャンク（Consecutive Small Chunks）] に 5 を設定します。

大量の小さなチャンクが検出される場合に イベントを生成し、インライン展開では、違反パケットをドロップします。するには、クライアント トラフィックの場合はプリプロセッサ ルール 119:27 を有効にし、サーバー トラフィックの場合はルール 120:7 を有効にします。[小さいチャンク サイズ（Small Chunk Size）] が有効であり、このオプションが 0 または 1 に設定されている場合にこれらのルールを有効にすると、指定されたサイズ以下のすべてのチャンクでイベントがトリガーとして使用されます。

HTTP メソッド（HTTP Methods）

システムがトラフィックで検出すると予期される、GET および POST 以外の HTTP 要求メソッドを指定します。複数の値はカンマで区切ります。

侵入ルールでは、HTTP メソッドのコンテンツを検索するために、`content` または `protected_content` キーワードが **HTTP Method** 引数と共に使用されます。GET、POST、およびこのオプションで設定されているメソッド以外のメソッドがトラフィックで検出される場合にイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 119:31 を有効にします。侵入ルール状態の設定 （2032 ページ）を参照してください。

No Alerts

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

（注） このオプションは、HTTP の標準テキスト ルールと共有するオブジェクト ルールを無効にしません。

HTTP ヘッダーの正規化（Normalize HTTP Headers）

[Inspect HTTP Responses] が有効である場合は、要求見出しと応答見出しで非 cookie データの正規化が有効になります。[Inspect HTTP Responses] が有効**ではない**場合は、要求見出しと応答見出しで cookie を含む HTTP 見出し全体の正規化が有効になります。

Inspect HTTP Cookies

HTTP 要求見出しからの cookie の抽出を有効にします。また、[Inspect HTTP Responses] が有効である場合は、応答見出しの set-cookie データの抽出も有効になります。cookie の抽出が不要な場合は、このオプションを無効にするとパフォーマンスが向上します。

`Cookie:` および `Set-Cookie:` の見出し名、見出し行の先頭のスペース、および見出し行の末尾の `CRLF` は、cookie の一部ではなく見出しの一部として検査されます。

Normalize Cookies in HTTP headers

HTTP 要求見出しの cookie の正規化を有効にします。[Inspect HTTP Responses] が有効である場合は、応答見出しで set-cookie データの正規化が有効になります。このオプションを選択する前に、[Inspect HTTP Cookies] を選択する必要があります。

Allow HTTP Proxy Use

モニター対象 Web サーバーを HTTP プロキシとして使用できるようにします。このオプションは、HTTP 要求のインスペクションでのみ使用されます。

Inspect URI Only

正規化された HTTP 要求パケットの URI 部分のみを検査します。

Inspect HTTP Responses

HTTP 応答の拡張インスペクションが有効になり、プリプロセッサは、HTTP 要求メッセージのデコードと正規化の他に、ルールエンジンによるインスペクションのために応答フィールドを抽出します。このオプションを有効にすると、応答ヘッダー、ボディ、ステータスコードなどがシステムにより抽出されます。また [HTTP Cookie の検査（Inspect HTTP Cookies）] が有効な場合は、set-cookie データも抽出されます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 120:2 と 120:3 を次のように有効にします。

表 *212 : HTTP* 応答ルールのインスペクション

ルール	以下の場合にトリガーする
120:2	無効な HTTP 応答のステータス コードが発生します。
120:3	HTTP応答にはコンテンツ長または転送エンコーディングは含まれません。

UTF エンコードの UTF-8 への正規化（Normalize UTF Encodings to UTF-8）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合、HTTP 応答で UTF-16LE、UTF-16BE、UTF-32LE、および UTF32-BE エンコードが検出され、UTF-8 に正規化されます。

UTF 標準化が失敗した場合にイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 102:4 を有効にします。

圧縮データの検査（Inspect Compressed Data）

[Inspect HTTP Responses] が有効である場合、HTTP 応答ボディでの gzip および deflate 互換圧縮データの圧縮解除と、正規化された圧縮解除データのインスペクションが有効になります。システムは、チャンク HTTP 応答データと非チャンク HTTP 応答データを検査します。システムは、必要に応じて複数のパケットにわたり圧縮解除データをパケット単位で検査します。つまり、システムが異なるパケットの圧縮解除データをインスペクションのために結合させることはありません。[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバー フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 120:6 と120:24 を次のように有効にします。

表 *213 :* 圧縮された *HTTP* 応答ルールのインスペクション

ルール	以下の場合にトリガーする
120:6	圧縮された HTTP 応答の圧縮が失敗しました。
120:24	圧縮された HTTP 応答の部分的な圧縮が失敗しました。

無制限の圧縮解除（Unlimited Decompression）

[Inspect Compressed Data]（および任意で、[Decompress SWF File (LZMA)]、[Decompress SWF File (Deflate)]、または [Decompress PDF File (Deflate)]）が有効な場合、複数のパケットにわたって [Maximum Decompressed Data Depth] がオーバーライドされます。つまり、このオプションにより、複数のパケットにわたる無制限の圧縮解除が有効になります。このオプションを有効にしても、単一パケット内での [圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] には影響しないことに注意してください。また、このオプションを有効にすると、変更のコミット時に、[圧縮データの最大深さ（Maximum Compressed Data Depth）] と [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] が 65535 に設定されることにも注意してください。

Javascript の正規化（Normalize Javascript）

[Inspect HTTP Responses] が有効な場合、HTTP 応答ボディ内での Javascript の検出と正規化を有効にします。プリプロセッサは unescape 関数や decodeURI 関数、String.fromCharCode メソッドなどの難読化 Javascript データを正規化します。プリプロセッサは、unescap、decodeURI、および decodeURIComponent 関数内の次のエンコードを正規化します。

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

プリプロセッサは連続するスペースを検出し、1 つのスペースに正規化します。このオプションが有効である場合、設定フィールドでは、難読化 Javascript データで許容する連続スペースの最大数を指定できます。入力できる値は、1 ～ 65535 です。値 0 を指定すると、このフィールドに関連付けられているプリプロセッサ ルール（120:10）が有効かどうかに関係なく、イベントの生成が無効になります。

プリプロセッサは、Javascript の正符号（+）演算子も正規化し、この演算子を使用して文字列を連結します。

`file_data` 侵入ルール キーワードを使用して、正規化された Javascript データに対し侵入ルールを指し示すことができます。

イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、次に示すように、ルール 120:9、120:10、および 120:11 を有効にします。

表 *214 : [Javascript* の正規化（*Normalize Javascript*）*]* オプションのルール（*Normalize Javascript Option Rules*）

ルール	以下の場合にトリガーする
120:9	プリプロセッサ内の難読化レベルが 2 以上である。
120:10	Javascript 難読化データで連続するスペースの数が、許容される連続スペースの最大数として設定された値以上である。
120:11	エスケープされたデータまたはエンコードされたデータに、複数のエンコード タイプが含まれている。

SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））および SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、これらのオプションは、HTTP 要求の HTTP 応答ボディ内にあるファイルの圧縮部分を圧縮解除します。

（注） HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

- [SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））] は、Adobe ShockWave Flash（.swf）ファイルの LZMA 互換の圧縮部分を圧縮解除します。
- [SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））] は、Adobe ShockWave Flash（.swf）ファイルの deflate 互換の圧縮部分を圧縮解除します。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバー フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file_data 侵入ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:12 および 120:13 を有効にします。

表 *215 : [SWF* ファイルの圧縮解除（*Decompress SWF File***）*]* オプションのルール**

ルール	以下の場合にトリガーする
120:12	deflate ファイルの圧縮解除に失敗
120:13	LZMA ファイルの圧縮解除に失敗

PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、[PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate）] は、HTTP 要求の HTTP 応答ボディ内にある Portable Document Format（.pdf）ファイルの deflate 互換の圧縮部分を圧縮解除します。システムは、/FlateDecode ストリーム フィルタが付いた PDF ファイルだけを圧縮解除できます。他のフィルタ（/FlateDecode /FlateDecode など）はサポートしていません。

（注） HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバー フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file_data 侵入ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:14、120:15、120:16、および 120:17 を有効にします。

表 *216 : [PDF* ファイルの圧縮解除（*Deflate*）（*Decompress PDF File*（*Deflate*））*]* オプションのルール（*Decompress PDF File (Deflate) Option Rules*）

ルール	以下の場合にトリガーする
120:14	ファイルの圧縮解除に失敗
120:15	圧縮タイプがサポート対象外のタイプであるため、ファイルの圧縮解除に失敗
120:16	PDF ストリーム フィルタがサポート対象外のフィルタであるため、ファイルの圧縮解除に失敗
120:17	ファイルの解析に失敗

元のクライアント IP アドレスの抽出（Extract Original Client IP Address）

侵入検査中の、元のクライアント IP アドレスの調査を有効にします。システムは元のクライアント IP アドレスを、X-Forwarded-For（XFF）、True-Client-IP、または [XFF ヘッダーの優先順位（XFF Header Priority）] オプションで定義したカスタム HTTP ヘッダーから抽出します。侵入イベント テーブルで、抽出された元のクライアント IP アドレスを表示できます。

イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。するには、ルール 119:23、119:29、および 119:30 を有効にします。

XFF ヘッダーの優先順位（XFF Header Priority）

HTTP 要求に複数のヘッダーが存在する場合は、システムが元のクライアント IP ヘッダーを処理する順序を指定します。デフォルトでは、システムはまず X-Forwarded-For（XFF）ヘッダーを、次に True-Client-IP ヘッダーを調査します。追加したら、各ヘッダー タイプの横にある上下矢印アイコンを使用して、優先順位を調整します。

このオプションでは、抽出と評価のために、XFF または True-Client-IP 以外の元のクライアント IP ヘッダーを指定できます。[Add] をクリックして、カスタム ヘッダー名をプライオリティ リストに追加します。システムは、XFF または True-Client-IP ヘッダーと同じ構文を使用するカスタム ヘッダーのみをサポートします。

このオプションを設定する場合は、以下の点に留意してください。

- アクセス コントロールと侵入検査の両方で、システムは元のクライアント IP アドレス ヘッダーを評価するときにこの優先順位を使用します。
- 元のクライアント IP ヘッダーが複数ある場合、システムは優先順位が最も高いヘッダーのみを処理します。
- XFF ヘッダーには、要求が渡されたときに経由したプロキシ サーバーを表す、IP アドレスのリストが含まれています。スプーフィングを防止するために、システムはリスト内の

最後の IP アドレス（つまり、信頼されるプロキシにより追加されたアドレス）を、元のクライアント IP アドレスとして使用します。

URI のログ（Log URI）

raw URI が存在する場合に、HTTP 要求パケットから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこの URI を関連付けます。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP URI] 列に、抽出された URI の先頭 50 文字を表示できます。パケット ビューでは、URI 全体（最大 2048 バイト）を表示できます。

ホスト名のログ（Log Hostname）

ホスト名が存在する場合に、HTTP 要求の Host 見出しから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこのホスト名を関連付けます。複数の Host 見出しがある場合は、1 番目の見出しからホスト名を抽出します。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP Hostname] 列に、抽出されたホスト名の先頭 50 文字を表示できます。パケット ビューでは、ホスト名全体（最大 256 バイト）を表示できます。

ルール 119:25 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

有効にすると、このオプションの設定に関係なく、HTTP 要求で複数のホスト ヘッダーが検出された場合、ルール 119:24 がトリガーされます。

プロファイル（Profile）

HTTP トラフィック向けに正規化されたエンコードのタイプを指定します。システムには、ほとんどのサーバーに適用できるデフォルト プロファイル、Apache サーバーと IIS サーバー用のデフォルト プロファイル、およびモニター対象トラフィックのニーズに合わせて調整できるカスタムのデフォルト設定があります。

- すべてのサーバーに対して適切な標準のデフォルト プロファイルを使用するには、[すべて（All）] を選択します。
- システムによって提供される IIS プロファイルを使用するには、[IIS] を選択します。
- システムによって提供される Apache プロファイルを使用するには、[Apache] を選択します。
- 独自のサーバー プロファイルを作成するには、[カスタム（Custom）] を選択します。

サーバーレベルの HTTP 正規化エンコード オプション

HTTP サーバーレベルの [プロファイル（Profile）] オプションを `Custom` に設定すると、HTTP トラフィックに対して正規化されるエンコード タイプを指定できます。また、HTTP のプリプ

ロセッサ ルールを有効にして、異なるエンコード タイプを含むトラフィックに対してイベントを生成できます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

ASCII エンコード

エンコードされた ASCII 文字をデコードし、ルール エンジンが ASCII エンコード URI でイベントを生成するかどうかを指定します。

ルール 119:1 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

UTF-8 エンコード

URI の標準 UTF-8 Unicode シーケンスをデコードします。

ルール 119:6 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

Microsoft %U エンコード

%u とその後に続く 4 文字を使用する IIS %u エンコード スキームをデコードします。この 4 文字は、IIS Unicode コードポイントに関連する 16 進数のエンコード値です。

ヒント　正規のクライアントが %u エンコードを使用することはほとんどないため、シスコは、%u エンコードによってエンコードされている HTTP トラフィックをデコードすることを推奨します。

ルール 119:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

ベア バイト UTF-8 エンコード

ベア バイト エンコードをデコードします。ベア バイト エンコードは、UTF-8 値のデコード時に非 ASCII 文字を有効な値として使用します。

ヒント　ベア バイト エンコードにより、ユーザーは IIS サーバーをエミュレートし、非標準エンコードを正しく解釈することができます。正規のクライアントはこの方法で UTF-8 をエンコードしないため、シスコは、このオプションを有効にすることを推奨します。

ルール 119:4 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

Microsoft IIS エンコード

Unicode コードポイント マッピングを使用してデコードします。

ヒント これは主に攻撃と回避の試行で見られるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:7 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

二重符号化

要求 URI を 2 回通過し、それぞれでデコードを実行するようにすることで、IIS 二重エンコードトラフィックをデコードします。これは通常は攻撃シナリオでのみ検出されるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:2 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

マルチスラッシュ オブファスケーション

1 つの行内の複数のスラッシュを 1 つのスラッシュに正規化します。

ルール 119:8 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

IIS バックスラッシュ オブファスケーション

バックスラッシュをスラッシュに正規化します。

ルール 119:9 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ） を参照してください。

ディレクトリ トラバーサル

ディレクトリ トラバーサルおよび自己参照用ディレクトリを正規化します。一部の Web サイトはディレクトリ トラバーサルを使用してファイルを参照するため、このタイプのトラフィックに対してイベントを生成するために、関連するプリプロセッサルールを有効にすると、誤検出が発生する可能性があります。

ルール 119:10 と 119:11 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

タブ オブファスケーション

スペース区切り記号としてタブを使用する非 RFC 標準を正規化します。Apache やその他の IIS 以外の Web サーバーは、URL の区切り文字としてタブ文字（0x09）を使用します。

（注） このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

ルール 119:12 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

無効な RFC 区切り文字

URI データの改行（\n）を正規化します。

ルール 119:13 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

Webroot ディレクトリ トラバーサル

URL の初期ディレクトリを越えて横断するディレクトリ トラバーサルを検出します。

ルール 119:18 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

タブ区切り（URI）

URI の区切り文字としてタブ文字（0x09）を有効にします。Apache、新しいバージョンの IIS、およびその他の一部の Web サーバーは、URL の区切り文字としてタブ文字を使用します。

（注） このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

非 RFC 文字

対応するフィールドに追加された非 RFC 文字リストが、着信または発信 URI データ内に含まれている場合にそれを検出します。このフィールドを変更する場合は、バイト文字を表す 16

進表記を使用します。このオプションを設定する場合は、値を慎重に設定してください。非常に一般的な文字を使用すると、イベントが大量に発生する可能性があります。

ルール 119:14 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

チャンク形式の最大エンコード サイズ

URI データで異常に大きなチャンク サイズを検出します。

ルール 119:16 と 119:22 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032 ページ）を参照してください。

パイプライン デコードの無効化

パイプライン処理された要求の HTTP デコードを無効にします。このオプションが無効である場合、パイプラインで待機する HTTP 要求には、デコードおよび分析は行われず、汎用パターン マッチングを使用した検査のみが行われるため、パフォーマンスが向上します。

Non-Strict URI 解析

Non-Strict URI 解析を有効にします。このオプションは、「GET /index.html abc xo qr \n」という形式の非標準 URI を受け入れるサーバーのみで使用します。このオプションを使用すると、デコーダは URI が 1 番目のスペースと 2 番目のスペースで囲まれているものと想定します。これは、2 番目のスペースの後に有効な HTTP 識別子がない場合でも同様です。

拡張 ASCII エンコード

HTTP 要求 URI の拡張 ASCII 文字の解析を有効にします。このオプションは、カスタム サーバー プロファイルでのみ使用可能であり、Apache、IIS、またはすべてのサーバー向けに提供されるデフォルト プロファイルでは使用できないことに注意してください。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2078 ページ）

HTTP インスペクト プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致す

るか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2748 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [HTTP の設定（HTTP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [HTTPの設定（HTTP Configuration）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 [グローバル設定（Global Settings）] ページ エリアのオプションを変更します。グローバル HTTP 正規化オプション （2797 ページ）を参照してください。

ステップ 8 次の 3 つの選択肢があります。

- サーバープロファイルの追加：[サーバー（Servers）] セクションの [追加（Add）]（） をクリックします。クライアントの 1 つ以上の IP アドレスを [サーバー アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。リストに入力できる文字数は最大 496 文字、すべてのサーバープロファイルで指定できるアドレス項目の総数は 256、作成できるプロファイルの総数はデフォルト プロファイルを含めて 255 です。
- サーバープロファイルの編集：[サーバー（Servers）] の下で追加したプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。サーバーレベルの HTTP 正規化オプション （2798 ページ）を参照してください。プロファイル値で [カスタム（Custom）] を選択した場合は、サーバーレベルの HTTP 正規化エンコード オプション （2808 ページ）で説明されているエンコーディング オプションを変更することもできます。

- サーバープロファイルの削除：カスタムプロファイルの横にある [削除（Delete）]（）をクリックします。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、HTTP プリプロセッサ ルール（GID 119）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

その他の HTTP 検査プリプロセッサ ルール

特定の設定オプションに関連付けられていない HTTP Inspect プリプロセッサ ルールのイベントを生成するには、次の表の「プリプロセッサ ルール GID：SID」列のルールを有効にできます。

表 *217:* その他の *HTTP* 検査プリプロセッサ ルール

プリプロセッサ ルール GID:SID	以下の場合にトリガーする
119:21	HTTP 要求ヘッダーに複数の `content-length` フィールドがあります。
119:24	HTTP 要求に複数の Host ヘッダーがあります。
119:28	HTTP POST メソッドに `content-length` ヘッダーも chunked に設定された `transfer-encoding` もありません。
119:32	HTTP バージョン 0.9 がトラフィックで検出されました。TCP ストリームの設定も有効にする必要があることに注意してください。
119:33	HTTP URI にエスケープされていないスペースが含まれています。
119:34	TCP 接続に 24 以上のパイプライン処理された HTTP 要求が含まれています。

プリプロセッサ ルール GID:SID	以下の場合にトリガーする
120:5	HTTP 応答トラフィックで UTF-7 エンコードが検出されました。UTF-7 は、SMTP トラフィックなどで 7 ビット パリティが必要な場合にのみ使用してください。
120:8	`content-length` またはチャンク サイズが無効です。
120:18	HTTP サーバー応答はクライアント要求の前に実行されます。
120:19	HTTP 応答に複数のコンテンツ長が含まれています。
120:20	HTTP 応答に複数のコンテンツのエンコーディングが含まれています。
120:25	HTTP 応答に無効なヘッダーの折返しが含まれています。
120:26	HTTP 応答ヘッダーの前に不正な行があります。
120:27	HTTP 応答にヘッダーの末尾が含まれていません。
120:28	無効なチャンク サイズが発生したか、またはチャンク サイズの後に不正な文字が続いています。

Sun RPC プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

リモート プロシージャ コール（RPC）の正規化では、フラグメント化された複数の RPC レコードを取得し、それらを 1 つのレコードに正規化するので、ルール エンジンがそのレコード全体を検査できます。たとえば、攻撃者が RPC `admind` が実行されているポートの検出を試行するとします。一部の UNIX ホストは、RPC `admind` を使用してリモート分散システム タスクを実行します。ホストが弱い認証を実行する場合、悪意のあるユーザーがリモート管理のコントロールを獲得できることがあります。[Snort ID]（SID）575 の標準テキスト ルール（GID：1）では、特定のロケーションでコンテンツを検索して、不適切な `portmap GETPORT` 要求を特定することで、この攻撃を検出します。

Sun RPC プリプロセッサのオプション

ポート

トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。一般的なRPCポートは111および32771です。ネットワークが他のポートにRPCトラフィックを送信する場合は、それらのポートの追加を検討してください。

RPC フラグメント化レコードの検出（Detect fragmented RPC records）

RPC フラグメント化レコードを検出します。

ルール106:1と106:5を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

1パケットの複数レコードの検出（Detect multiple records in one packet）

パケット（または再構成されたパケット）ごとに、複数の RPC 要求を検出します。

ルール106:2を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

1フラグメントを超えるフラグメント化レコード合計の検出（Detect fragmented record sums which exceed one fragment）

現在のパケット長を超える再構成されたフラグメント化レコード長を検出します。

ルール106:3を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

1パケットのサイズを超える単一フラグメント レコードの検出（Detect single fragment records which exceed the size of one packet）

部分的なレコードを検出します。

ルール106:4を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

Sun RPC プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [Sun RPC の構成（Sun RPC Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [Sun RPCの構成（Sun RPC Configuration）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 Sun RPC プリプロセッサのオプション （2816 ページ）で説明されている設定を変更します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、Sun RPC プリプロセッサ ルール（GID 106）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

SIP プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Session Initiation Protocol（SIP）は、インターネット テレフォニー、マルチメディア会議、インスタント メッセージング、オンライン ゲーム、ファイル転送などのクライアント アプリケーションの 1 人以上のユーザに対し、1 つ以上のセッションのコールのセットアップ、変更、およびティアダウンを提供します。各 SIP 要求の *method* フィールドは要求の目的を示し、Request-URI に要求の送信先が指定されます。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。

SIP を使用してコールがセットアップされた後、後続の音声およびビデオによる通信はReal-time Transport Protocol（RTP）により処理されます。セッションのこの部分は、コール チャネル、データ チャネル、または音声/ビデオ データ チャネルと呼ばれることがあります。RTP は、データチャネル パラメータ ネゴシエーション、セッション通知、およびセッションへの招待のために、SIP メッセージ ボディ内で Session Description Protocol（SDP）を使用します。

SIP プリプロセッサは次の処理を実行します。

- SIP 2.0 トラフィックのデコードおよび分析
- SDP データが存在する場合はこのデータを含む SIP ヘッダーとメッセージ ボディを抽出し、抽出したデータを今後のインスペクションのためにルール エンジンに受け渡す
- 次の状態が検出され、対応するプリプロセッサ ルールが有効な場合にイベントを生成する
  - SIP パケット内の異常と既知の脆弱性
  - 順序が間違っているコール シーケンスと無効なコール シーケンス
- コール チャネルの無視（オプション）

プリプロセッサは、SIP メッセージ ボディに組み込まれている SDP メッセージに示されているポートに基づいて RTP チャネルを識別しますが、RTP プロトコル インスペクションを実行しません。

SIP プリプロセッサを使用するときは、次の点に注意してください。

- UDP は通常、SIP でサポートされるメディア セッションを伝送します。UDP ストリームの前処理により、SIP プリプロセッサに対し SIP セッション トラッキングが提供されます。
- SIP ルール キーワードにより、SIP パケット ヘッダーまたはメッセージ ボディを指し示し、検出対象を特定の SIP メソッドまたはステータス コードのパケットに限定できます。

SIP プリプロセッサのオプション

次のオプションでは、1 から 65535 バイトの正の値を指定するか 0 を指定して、関連するルールが有効にされているかどうかにかかわらず、オプションのイベント生成を無効にできます。

- **要求 URI の最大長（Maximum Request URI Length）**
- **コール ID の最大長（Maximum Call ID Length）**
- **要求名の最大長（Maximum Request Name Length）**
- **送信元の最大長（Maximum From Length）**
- **送信先の最大長（Maximum To Length）**
- **経由の最大長（Maximum Via Length）**
- **連絡先の最大長（Maximum Contact Length）**
- **コンテンツの最大長（Maximum Content Length）**

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

ポート

SIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

Methods to Check

検出する SIP メソッドを指定します。次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。メソッド名には英字、数字、下線文字を使用できます。その他の特殊文字は使用できません。複数のメソッドを指定する場合は、カンマで区切ります。

新しい SIP メソッドが今後定義される可能性があるため、設定には、現在定義されていない英字文字列を含めることができます。現在定義されている 21 個のメソッドと追加の 11 個のメソッドを含む、最大 32 個のメソッドがシステムでサポートされます。未定義のメソッドを設定した場合、システムはそれを無視します。

合計 32 個のメソッドには、このオプションに指定するメソッドの他に、侵入ルールで `sip_method` キーワードを使用して指定するメソッドも含まれることに注意してください。

セッション内のダイアログ最大数（Maximum Dialogs within a Session）

ストリームセッション内で許容されるダイアログの最大数を指定します。この数より多くのダイアログが作成されると、ダイアログの数が、指定されている最大数以下になるまで、最も古いダイアログから順に削除されます。1 ～ 4194303 の整数を指定できます。

ルール 140:27 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2032ページ）を参照してください。

要求 URI の最大長（Maximum Request URI Length）

[要求 URI（Request-URI）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:3 が有効である場合、URI が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[要求 URI（Request-URI）] フィールドは、要求の宛先のパスまたはページを示します。

Maximum Call ID Length

[要求または応答のコール ID（request or response Call-ID）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:5 が有効である場合、Call-ID が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[コール ID（Call-ID）] フィールドによって、要求や応答内の SIP セッションが一意に識別されます。

Maximum Request Name Length

要求名で許容される最大バイト数を指定します。要求名は、CSeq トランザクション ID に指定されるメソッドの名前です。ルール 140:7 が有効である場合、リクエスト名が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。

送信元の最大長（Maximum From Length）

要求または応答の [送信元（From）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:9 が有効である場合、[送信元（From）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[送信元（From）] フィールドは、メッセージの発信側を識別します。

Maximum To Length

要求または応答の [送信先（To）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:11 が有効である場合、[送信先（To）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[送信先（To）] フィールドは、メッセージの受信側を識別します。

Maximum Via Length

要求または応答の [経由（Via）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:13 が有効である場合、[経由（Via）] が長いと イベントを生成し、インライン

展開では、違反パケットをドロップします。。[経由（Via）] フィールドには要求がたどるパスが示され、応答の場合は受信者情報が示されます。

Maximum Contact Length

要求または応答の [連絡先（Contact）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:15 が有効である場合、[連絡先（Contact）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[連絡先（Contact）] フィールドには、後続のメッセージについての連絡先を指定する URI が示されます。

Maximum Content Length

要求または応答のメッセージ ボディのコンテンツで許容される最大バイト数を指定します。ルール 140:16 が有効である場合、コンテンツが長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。

音声/ビデオ データ チャネルを無視（Ignore Audio/Video Data Channel）

データ チャネル トラフィックのインスペクションを有効または無効にします。このオプションを有効にすると、プリプロセッサはその他の非データ チャネル SIP トラフィックのインスペクションを続行するので注意してください。

関連トピック

SIP キーワード （2134 ページ）

SIP プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SIP の設定（SIP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [SIPの設定（SIP Configuration）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 SIP プリプロセッサのオプション （2819 ページ）の説明に従ってオプションを変更します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SIP プリプロセッサ ルール（GID 140）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

その他の SIP プリプロセッサ ルール

次の表に示す SIP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の SIP プリプロセッサ ルールと同様に、これらのルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。 する場合は、これらのルールを有効にする必要があります。

表 *218 :* その他の *SIP* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	**以下の場合にトリガーする**
140:1	プリプロセッサがモニターしている SIP セッションの数が、システムで許容される最大数である。
140:2	SIP 要求で [要求 URI（Request URI）] 必須フィールドが空である。

プリプロセッサ ルール GID:SID	以下の場合にトリガーする
140:4	SIP 要求または応答の Call-ID ヘッダー フィールドが空である。
140:6	SIP 要求または応答の CSeq フィールドのシーケンス番号値が、231 未満の 32 ビット符号なし整数ではない。
140:8	SIP 要求または応答の [送信元（From）] 必須フィールドが空である。
140:10	SIP 要求または応答の [送信先（To）] ヘッダー フィールドが空である。
140:12	SIP 要求または応答の [経由（Via）] ヘッダー フィールドが空である。
140:14	SIP 要求または応答で [連絡先（Contact）] 必須フィールドが空である。
140:17	UDP トラフィック内の 1 つの SIP 要求または応答パケットに複数のメッセージが含まれている。SIP の旧バージョンでは複数メッセージがサポートされていますが、SIP 2.0 ではパケットあたり 1 メッセージだけがサポートされていることに注意してください。
140:18	UDP トラフィック内の SIP 要求または応答のメッセージ本文の実際の長さが SIP 要求または応答の [コンテンツ長（Content-Length）] ヘッダー フィールドに指定されている値と一致しない。
140:19	プリプロセッサが SIP 応答の [CSeq] フィールドのメソッド名を認識しない。
140:20	SIP サーバーが、認証済み招待メッセージに対してチャレンジを送信しない。これは InviteReplay 請求攻撃の場合に発生することに注意してください。
140:21	呼び出しが設定される前に、セッション情報が変更される。これは FakeBusy 請求攻撃の場合に発生することに注意してください。
140:22	応答ステータス コードが 3 桁の数字でない。
140:23	[コンテンツ タイプ（Content-Type）] ヘッダー フィールドにコンテンツ タイプが指定されておらず、メッセージ ボディにデータが含まれている。
140:24	SIP バージョンが 1、1.1、2.0 でない。
140:25	SIP 要求で、[CSeq] ヘッダーで指定されたメソッドとメソッド フィールドが一致しない。
140:26	プリプロセッサが SIP 要求のメソッド フィールドに指定されたメソッドを認識しない。

GTP プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）により、GTP コア ネットワークを介した通信が実現します。GTP プリプロセッサは、GTP トラフィックの異常を検出し、コマンド チャネル シグナリング メッセージをインスペクションのためにルール エンジンに転送します。GTP コマンド チャネル トラフィックでエクスプロイトがあるかどうかを検査するには、`gtp_version`、`gtp_type`、および `gtp_info` ルール キーワードを使用します。

1 つの構成オプションで、プリプロセッサが GTP コマンド チャネル メッセージを検査するポートのデフォルト設定を変更できます。

GTP プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次の表に示す GTP プリプロセッサ ルールを有効にする必要があります。

表 *219 : GTP* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
143:1	プリプロセッサが無効なメッセージの長さを検出すると、イベントが生成されます。
143:2	プリプロセッサが無効な情報要素の長さを検出すると、イベントが生成されます。
143:3	プリプロセッサが誤った順序の情報要素を検出すると、イベントが生成されます。

GTP プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

GTP プリプロセッサが GTP コマンド メッセージをモニターするポートを変更するには、次の手順を使用します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [GTP コマンドチャネル構成（GTP Command Channel Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [GTPコマンドチャネル構成（GTP Command Channel Configuration）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 ポート値を入力します。

複数のポートを指定する場合は、カンマで区切ります。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、GTP プリプロセッサ ルール（GID 143）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

IMAP プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Internet Message Application Protocol（IMAP）は、リモート IMAP サーバから電子メールを取得するときに使用されます。IMAP プリプロセッサはサーバー/クライアント IMAP4 トラフィックを検査し、関連するプリプロセッサ ルールが有効な場合は、異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ IMAP4 トラフィックの電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

IMAP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

IMAP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 141:4 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:6 を有効にすると、抽出の失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます（たとえばデータの破損のために抽出が失敗することがあります）。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号する場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:5 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべてのUUエンコードデータをデコードするには、正値を指定するか、0 を指定できます。UU エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:7 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

関連トピック

file_data キーワード （2175 ページ）

IMAP プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択して **[ネットワーク分析ポリシー（Network Analysis Policies）]** をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [IMAP の構成（IMAP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [IMAPの構成（IMAP Configuration）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 IMAP プリプロセッサ オプション （2826 ページ）で説明されている設定を変更します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、IMAP プリプロセッサ ルール（GID 141）を有効にします。侵入ルール状態の設定 （2032 ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

侵入ポリシーとネットワーク分析ポリシーのレイヤ （2179 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

その他の IMAP プリプロセッサ ルール

次の表に示すIMAPプリプロセッサルールは、特定の設定オプションに関連付けられていません。他のIMAPプリプロセッサルールの場合と同様に、これらのルールでイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルールを有効にする必要があります。

表 *220*：その他の *IMAP* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
141:1	プリプロセッサが RFC 3501 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
141:2	プリプロセッサが RFC 3501 に定義されていないサーバ応答を検出すると、イベントが生成されます。
141:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

POP プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Post Office Protocol（POP）は、リモート POP メール サーバから電子メールを取得するときに使用されます。POP プリプロセッサは、サーバーからクライアントへの POP3 トラフィックを検査し、関連付けられているプリプロセッサルールが有効な場合は、異常なトラフィックについてのイベントを生成します。プリプロセッサは、クライアントからサーバーへの POP3 トラフィック内の電子メールの添付ファイルを抽出して復号（デコード）し、添付ファイルデータをルールエンジンに送信することもできます。添付ファイルデータを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

POP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

POP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 142:4 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコード データを無視するには、-1 を指定します。

このオプションが有効であれば、抽出が失敗したときにルール 142:6 を有効にしてイベントを生成し、インライン展開では、違反パケットをドロップします。 できます。抽出は、たとえば、データの破損により失敗することがあります。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号する場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 142:5 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべてのUUエンコードデータをデコードするには、正値を指定するか、0 を指定できます。UU エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 142:7 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）
file_data キーワード （2175 ページ）

POP プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）

カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [POP の構成（POP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [POPの設定（POP Configuration）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 7 POP プリプロセッサ オプション （2830 ページ）で説明されている設定を変更します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、POP プリプロセッサ ルール（GID 142）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

その他の POP プリプロセッサ ルール

次の表に示す POP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の POP プリプロセッサ ルールと同様に、これらのルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。 する場合は、これらのルールを有効にする必要があります。

表 *221 :* その他の *POP* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
142:1	プリプロセッサが RFC 1939 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。

プリプロセッサ ルール GID:SID	説明
142:2	プリプロセッサが RFC 1939 に定義されていないサーバ応答を検出すると、イベントが生成されます。
142:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

SMTP プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

SMTP プリプロセッサはルール エンジンに対し、SMTP コマンドを正規化するように指示します。このプリプロセッサは、クライアントからサーバーへのトラフィック内の電子メールの添付ファイルを抽出して復号（デコード）することもできます。またソフトウェアのバージョンによっては、SMTP トラフィックによりトリガーされた侵入イベントの表示時にコンテキストを提供するために、電子メールのファイル名、アドレス、およびヘッダー データも抽出します。

SMTP プリプロセッサのオプション

正規化を有効または無効にし、SMTP デコーダが検出する異常トラフィックのタイプを制御するオプションを設定できます。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SMTP トラフィックを正規化するポートを指定します。0以上の値を指定できます。複数のポートを指定する場合は、カンマで区切ります。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、SMTPデコーダは状態を保存し、各パケットのセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

Normalize

[すべて（All）] に設定すると、すべてのコマンドが正規化されます。コマンドの後に複数のスペース文字があるかどうかを確認します。

[なし（None）] に設定すると、コマンドは正規化されません。

[Cmds] に設定すると、[カスタム コマンド（Custom Commands）] にリストされているコマンドが正規化されます。

カスタム コマンド（Custom Commands）

[正規化（Normalize）] が [Cmds] に設定されている場合に、リストされているコマンドが正規化されます。

正規化する必要があるコマンドをテキスト ボックスに指定します。コマンドの後に複数のスペース文字があるかどうかを確認します。

スペース文字（ASCII 0x20）とタブ文字（ASCII 0x09）は、正規化の ためにスペース文字としてカウントされます。

Ignore Data

メール データを処理せず、MIME メール 見出し データだけを処理します。

Ignore TLS Data

Transport Layer Security プロトコルで暗号化されたデータを処理しません。

No Alerts

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

Detect Unknown Commands

SMTP トラフィックで不明なコマンドを検出します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:5 を有効にできます。

コマンドラインの最大長（Max Command Line Len）

SMTP コマンドラインがこの値より長い場合にそのことを検出します。コマンドラインの長さを検出しない場合は、0 を指定します。

RFC 2821（Network Working Group による Simple Mail Transfer Protocol 仕様）では、コマンドラインの最大長として 512 が推奨されています。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:1 を有効にできます。

ヘッダー行の最大長（Max Header Line Len）

SMTP データ 見出し行がこの値より長い場合にそのことを検出します。データ ヘッダー行の長さを検出しない場合は、0 を指定します。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:2 および 124:7 を有効にします。

応答行の最大長（Max Response Line Len）

SMTP 応答行がこの値より長い場合にそのことを検出します。応答行の長さを検出しない場合は、0 を指定します。

RFC 2821 では、応答行の最大長として 512 が推奨されています。

ルール 124:3 を有効にすると、このオプションに関して、および [代替のコマンドラインの最大長（Alt Max Command Line Len）] オプション（有効になっている場合）に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

代替のコマンドラインの最大長（Alt Max Command Line Len）

指定のコマンドの SMTP コマンドラインがこの値より長い場合にそのことを検出します。指定したコマンドのコマンドライン長を検出しない場合は、0 を指定します。多数のコマンドに対して、さまざまなデフォルト ライン長が設定されています。

この設定は、指定されたコマンドの [コマンドラインの最大長（Max Command Line Len）] の設定をオーバーライドします。

ルール 124:3 を有効にすると、このオプションに関して、および [応答行の最大長（Max Response Line Len）] オプション（有効になっている場合）に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

無効なコマンド（Invalid Commands）

これらのコマンドがクライアント側から送信された場合にそのことを検出します。

ルール 124:6 を有効にすると、このオプションに関して、および [無効なコマンド（Invalid Commands）] に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

有効なコマンド（Valid Commands）

このリストのコマンドを許可します。

このリストが空の場合でも、プリプロセッサにより許可される有効なコマンドは、ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR です。

（注） RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

ルール 124:4 を有効にすると、このオプションに関して、および [無効なコマンド（Invalid Commands）] オプション（設定済みの場合）に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

データ コマンド（Data Commands）

RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Binary Data Commands

RFC 3030 に基づく BDATA コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Authentication Commands

クライアントおよびサーバー間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Detect xlink2state

X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出します。インライン展開では、システムはこれらのパケットをドロップすることもできます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:8 を有効にできます。

Base64 デコーディングの深さ（Base64 Decoding Depth）

[データを無視（Ignore Data）] が無効である場合、各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。正の値から指定するか0を指定して、すべての Base64 データをデコードします。Base64 データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータをデコードしません。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 124:10 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

このオプションは、廃止されたオプション [MIME デコーディングの有効化（Enable MIME Decoding）] および [MIME デコーディングの最大の深さ（Maximum MIME Decoding Depth）] の代わりに使用されます。廃止されたこれらのオプションは、既存の侵入ポリシーでは後方互換性を維持する目的で引き続きサポートされています。

7-Bit/8-Bit/Binary Decoding Depth

[Ignore Data] が無効である場合、デコードを必要としない各 MIME 電子メール添付ファイルから抽出する最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコード データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータを抽出しません。

Quoted-Printable Decoding Depth

[Ignore Data] が無効である場合、各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。

1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:11 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

[Ignore Data] が無効である場合、各 Unix-to-Unix（UU エンコード）電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:13 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

MIME 添付ファイル名のログ（Log MIME Attachment Names）

MIME Content-Disposition 見出しからの MIME 添付ファイル名の抽出を有効にし、セッションで生成されるすべての侵入イベントをこのファイル名に関連付けます。複数ファイル名がサポートされています。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール添付（Email Attachment）] 列に、イベントに関連付けられているファイル名が表示されます。

受信者アドレスのログ（Log To Addresses）

SMTP RCPT TO コマンドからの受信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの受信者アドレスに関連付けます。複数の受信者がサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール受信者（Email Recipient）] 列に、イベントに関連付けられている受信者が表示されます。

送信者アドレスのログ（Log From Addresses）

SMTP MAIL FROM コマンドからの送信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの送信者アドレスを関連付けます。複数の送信者アドレスがサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール送信者（Email Sender）] 列に、イベントに関連付けられている送信者が表示されます。

ヘッダーのログ（Log Headers）

電子メール 見出しの抽出を有効にします。抽出されるバイト数は、[ヘッダーのログの深さ（Header Log Depth）] に指定されている値によって決まります。

キーワード `content` または `protected_content` を使用して、電子メール ヘッダー データをパターンとして使用する侵入ルールを作成できます。侵入イベント パケット ビューに、抽出された電子メール ヘッダーが表示されます。

ヘッダーのログの深さ（Header Log Depth）

[Log Headers] が有効である場合、抽出する見出しのバイト数を指定します。0 ～ 20480 バイトを指定できます。値 0 を指定すると、[ヘッダーのログ（Log Headers）] が無効になります。

関連トピック

基本コンテンツおよび protected_content キーワードの引数 （2074 ページ）

SMTP デコードの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション ウィンドウで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SMTP の設定（SMTP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [SMTPの設定（SMTP Configuration）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 SMTP プリプロセッサのオプション （2833 ページ）の説明に従ってオプションを変更します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SMTP プリプロセッサ ルール（GID 124）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

SSH プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

SSH プリプロセッサでは、次の攻撃を検出します。

- チャレンジレスポンス バッファ オーバーフロー エクスプロイト
- CRC-32 エクスプロイト
- SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト
- プロトコル不一致
- 不正な SSH メッセージの方向
- バージョン 1 または 2 以外のすべてのバージョン文字列

チャレンジレスポンス バッファ オーバーフロー攻撃と CRC--32 攻撃はいずれもキー交換の後に発生するので、暗号化されています。いずれの攻撃でも、20 KB を超える普通よりも大きなペイロードが認証チャレンジ直後にサーバに送信されます。CRC--32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジレスポンス バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。バージョン文字列は、セッションの開始時に読み取られます。バージョン文字列の違いを除き、この両方の攻撃は同様に扱われます。

SecureCRT SSH エクスプロイトとプロトコル不一致攻撃は、鍵交換前に接続をセキュリティで保護しようとするときに発生します。SecureCRT エクスプロイトでは、非常に長いプロトコル ID 文字列がクライアントに送信され、これが原因でバッファ オーバーフローが発生します。プロトコル不一致は、非 SSH クライアント アプリケーションがセキュア SSH サーバに接続しようとした場合、またはサーバとクライアントのバージョン番号が一致しない場合に発生します。

SSH プリプロセッサは、指定のポートまたはポートのリストでトラフィックを検査するか、または SSH トラフィックを自動的に検出するように設定できます。指定バイト数に達するまでに指定数の暗号化パケットが渡されたか、指定パケット数に達するまでにバイト数が指定最大バイト数を超えるまで、SSH トラフィックの検査が続行されます。最大バイト数を超えた場合は、CRC--32（SSH バージョン 1）攻撃またはチャレンジレスポンス バッファ オーバーフロー（SSH バージョン 2）攻撃が発生したとみなされます。プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

SSH プリプロセッサでは、ブルートフォース攻撃が処理されないことにも注意してください。

SSH プリプロセッサのオプション

次のいずれかが発生すると、プリプロセッサはセッションのトラフィックの検査を停止します。

- この数の暗号化パケットで、サーバーとクライアント間で有効な交換が行われた場合。接続は続行します。
- 検査対象の暗号化パケットの数に達する前に、[サーバー応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）] に達した場合。この場合、攻撃があったものと想定されます。

[Number of Encrypted Packets to Inspect] に達するまでの有効な各サーバー応答により、[Number of Bytes Sent Without Server Response] がリセットされ、パケット カウントが続行します。

次に示す SSH のプリプロセッサの設定例で説明します。

- [サーバー ポート（Server Ports）]：22
- [Autodetect Ports]：off
- [Maximum Length of Protocol Version String]：80
- [Number of Encrypted Packets to Inspect]：25
- [サーバー応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）]：19,600
- 検出オプションはすべて有効です。

この例では、プリプロセッサはポート 22 のトラフィックだけを検査します。つまり自動検出が無効であるため、指定のポートでのみ検査をします。

また、次のいずれかが発生すると、この例のプリプロセッサはトラフィックの検査を停止します。

- クライアントが 25 個の暗号化パケットを送信したが、すべてのパケットのデータ合計が 19,600 バイト以下であった。攻撃はなかったと想定されます。
- クライアントが、25 個の暗号化パケットで 19,600 バイトを超えるデータを送信した。この場合、この例のセッションは SSH バージョン 2 セッションであるため、プリプロセッサはこの攻撃がチャレンジレスポンス バッファ オーバーフロー攻撃であるとみなします。

この例のプリプロセッサは、トラフィックの処理時に以下の状況が発生しているかどうかも検出します。

- 80 バイトより長いバージョン文字列によりトリガーとして使用されるサーバー オーバーフロー（これは SecureCRT エクスプロイトを示します）
- プロトコルの不一致
- 誤った方向に流れるパケット

最後に、プリプロセッサは、バージョン 1 または 2 以外のすべてのバージョン文字列を自動的に検出します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

サーバー ポート（Server Ports）

SSH プリプロセッサがトラフィックを検査する必要があるポートを指定します。

1 つのポートか、複数ポートをカンマで区切ったリストを設定できます。

Autodetect Ports

SSH トラフィックを自動的に検出するようにプリプロセッサを設定します。

このオプションが選択されている場合、プリプロセッサはすべてのトラフィックで SSH バージョン番号を検査します。クライアント パケットにもサーバー パケットにもバージョン番号が含まれていない場合は、処理が停止します。無効である場合、プリプロセッサは [サーバー ポート（Server Ports）] オプションで指定されているトラフィックだけを検査します。

検査する暗号化パケットの最大数（Number of Encrypted Packets to Inspect）

セッションあたりのストリーム再構成された検査対象の暗号化パケットの数を指定します。

このオプションをゼロに設定すると、すべてのトラフィックの通過が許可されます。

検査対象の暗号化パケットの数を減らすと、一部の攻撃が検出されなくなることがあります。検査対象の暗号化パケットの数を増やすと、パフォーマンスに悪影響を及ぼす可能性があります。

Number of Bytes Sent Without Server Response

SSH クライアントが、応答なしでサーバーに送信できる最大バイト数を指定します。この最大バイト数を超えると、チャレンジレスポンス バッファ オーバーフロー攻撃または CRC-32 攻撃が想定されます。

プリプロセッサがチャレンジレスポンス バッファ オーバーフローまたは CRC-32 エクスプロイトを誤検出する場合は、このオプションの値を増やしてください。

Maximum Length of Protocol Version String

サーバーのバージョン文字列の最大許容バイト数を指定します。この値を超えると、SecureCRT エクスプロイトとみなされます。

Detect Challenge-Response Buffer Overflow Attack

チャレンジレスポンス バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:1 を有効にできます。SFTP セッションはルール 128:1 をトリガーする場合があることに注意してください。

SSH1 CRC-32 攻撃の検出（Detect SSH1 CRC-32 Attack）

CRC-32 エクスプロイトの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:2 を有効にできます。

サーバー オーバーフローの検出（Detect Server Overflow）

SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 128:3 を有効にします。

プロトコル不一致の検出（Detect Protocol Mismatch）

プロトコル不一致の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:4 を有効にできます。

正しくないメッセージ方向の検出（Detect Bad Message Direction）

トラフィックのフロー方向が正しくない場合（つまり、推定されるサーバーがクライアント トラフィックを生成したり、クライアントがサーバー トラフィックを生成したりした場合）の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:5 を有効にできます。

特定のペイロードに正しくないペイロード サイズの検出（Detect Payload Size Incorrect for the Given Payload）

SSH パケットに指定された長さが IP ヘッダーに指定されている合計長と矛盾する場合や、メッセージが切り捨てられる場合、つまり完全な SSH ヘッダーを形成できる十分なデータがない場合などの、誤ったペイロード サイズのパケットの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:6 を有効にできます。

正しくないバージョン ストリングの検出（Detect Bad Version String）

有効である場合、プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:7 を有効にできます。

SSH プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSH の構成（SSH Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [SSHの構成（SSH Configuration）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 SSH プリプロセッサのオプション （2841 ページ）の説明に従ってオプションを変更します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、SSH プリプロセッサ ルール（GID 128）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

SSL プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

SSL プリプロセッサでは、SSL インスペクション（検査）を設定できます。SSL インスペクションでは、暗号化トラフィックのブロック、暗号化トラフィックの復号化、またはアクセスコントロール（アクセス制御）によるトラフィックの検査を実行します。SSL インスペクションが設定されているかどうかに関係なく、SSL プリプロセッサでは、トラフィックで検出された SSL ハンドシェイク メッセージも分析し、セッションを暗号化するタイミングを決定します。暗号化トラフィックを識別することにより、システムは暗号化ペイロードの侵入およびファイル インスペクションを停止できます。これによって、誤検出が減少し、パフォーマンスが向上します。

SSL プリプロセッサは、暗号化トラフィックを検査して Heartbleed バグを悪用する試みを検出し、そのような悪用の検出時にイベントを生成することもできます。

セッションが暗号化されると、侵入およびマルウェアに対するトラフィックの検査を一時停止できます。SSL インスペクションを設定した場合、SSL プリプロセッサでは、ユーザがアクセス コントロールによってブロック、復号、または検査を行える暗号化トラフィックも識別します。

SSL プリプロセッサを使用して暗号化トラフィックを復号化するために、ライセンスは必要ありません。マルウェアおよび侵入に対する暗号化ペイロードのインスペクションの停止、Heartbleed バグの悪用の検出など、他のすべての SSL プリプロセッサ機能には保護ライセンスが必要です。

SSL 前処理の仕組み

SSL インスペクションを設定すると、SSL プリプロセッサは暗号化データに対する侵入およびファイル インスペクションを停止して、SSL ポリシーにより暗号化トラフィックを検査します。これにより誤検出を排除できます。SSL プリプロセッサは、SSL ハンドシェイクを検査するときに状態情報を保持し、そのセッションの状態と SSL バージョンの両方を追跡します。

セッションの状態が暗号化されていることをプリプロセッサが検出すると、そのセッションのトラフィックは暗号化されているものとしてシステムによりマークされます。暗号化が確定した場合に暗号化セッションにおけるすべてのパケット処理を停止し、Heartbleed のバグを悪用する試みが検出された場合にイベントを生成するように、システムを設定できます。

パケットごとに、IP ヘッダー、TCP ヘッダー、および TCP ペイロードがトラフィックに含まれており、このトラフィックが SSL 前処理用に指定されているポートで発生することが SSL プリプロセッサにより確認されます。次に示す状況では、対象トラフィックについて、トラフィックが暗号化されているかどうかが判別されます。

- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、サーバとクライアントの両方からの完了メッセージ、および Application レコードが存在するが Alert レコードがない各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、Alert レコードによる応答がない Application レコードが存在する各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、クライアントからの完了メッセージ、および Application レコードが存在するが Alert レコードがないクライアントからの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、Alert レコードによる応答がない Application レコードが存在するクライアントからの 1 つ以上のパケットが、セッションに含まれている。

暗号化トラフィックの処理を停止することを選択する場合、セッションが暗号化されているものとしてマークされると、そのセッションのその後のパケットは無視されます。

また、SSL ハンドシェイク時、プリプロセッサはハートビート要求と応答をモニターします。プリプロセッサは、以下を検出したときにイベントを生成します。

- ペイロード自体よりも大きいペイロード長の値を含むハートビート要求
- [ハートビートの最大長（Max Heartbeat Length）] フィールドに格納されている値よりも大きいハートビート応答

（注） ルール内で SSL 状態またはバージョン情報を使用するには、キーワード `ssl_state` および `ssl_version` をルールに追加します。

関連トピック

SSL キーワード （2125 ページ）

SSL プリプロセッサのオプション

（注） システム付属のネットワーク分析ポリシーは、デフォルトでSSLプリプロセッサを有効にします。暗号化トラフィックがネットワークを通過することを予想している場合、シスコは、カスタム展開で SSL プリプロセッサを無効にしないことを推奨します。

SSL インスペクションを設定しないと、システムは暗号化トラフィックを復号せずに、マルウェアと侵入について暗号化トラフィックの検査を試行します。SSLプリプロセッサを有効にすると、セッションが暗号化されたときにそのことを検出します。SSLプリプロセッサが有効にされると、ルールエンジンがこのプリプロセッサを呼び出し、SSLの状態およびバージョン情報を取得できるようになります。侵入ポリシーでキーワード `ssl_state` および `ssl_version` を使用してルールを有効にする場合は、そのポリシーでSSLプリプロセッサも有効にする必要があります。

ポート

SSLプリプロセッサは、暗号化されたセッションのトラフィックをモニタする必要があるポートを、カンマで区切って指定します。このフィールドで指定されるポートでのみ、暗号化トラフィックが検査されます。

（注） SSLプリプロセッサは、SSLモニタの対象として指定されたポートでSSL以外のトラフィックを検出すると、そのトラフィックをSSLトラフィックとしてデコードすることを試みた後、破損しているものとしてマークします。

暗号化トラフィックの検査を停止する（Stop inspecting encrypted traffic）

セッションが暗号化されているとしてマークされた後、セッションのトラフィックの検査を有効または無効にします。

暗号化されたセッションの検査を無効化しリアセンブルするには、このオプションを有効にします。SSLプリプロセッサによりセッションの状態が維持されるため、セッションのすべてのトラフィックのインスペクションを無効にできます。このオプションが有効になっている場合は、フローが暗号化されていることを確認するためセッションのいくつかのパケットが検証され、その後でディープ インスペクションがバイパスされます。バイパスされたすべてのセッションによって **show snort statistics** コマンドの応答に示される高速転送フローのカウントが増加します。さらに、ディープインスペクションがバイパスされているため、接続イベントのイニシエータとレスポンダのバイト数は正確ではありません。これらは実際のセッションの値よりも少なくなります。これは、Snortによって検査されたパケットのみが含まれており、ディープインスペクションがバイパスされた後のパケットは含まれていないためです。この動作は接続サマリ イベントとウィジェットに表示されるすべてのトラフィックの値に有効です。

システムは、次の両方の場合に、暗号化されたセッションのトラフィックの検査のみを停止します。

- SSL の前処理が有効にされている
- このオプションが選択されている

このオプションをクリアすると、[サーバ側のデータを信頼する（Server side data is trusted）] オプションを変更できません。

サーバ側のデータを信頼する（Server side data is trusted）

[暗号化トラフィックの検査を停止する（Stop inspecting encrypted traffic）] が有効にされてあり、クライアント側のトラフィックにのみ基づいて暗号化されたトラフィックの識別を有効にすると、

ハートビートの最大長（Max Heartbeat Length）

バイト数を指定して、ハートビート バグ悪用の試みに対する SSL ハンドシェイク内のハートビート要求と応答の検査を有効にします。1 ～ 65535 の整数を指定できます。このオプションを無効にする場合は 0 を入力します。

プリプロセッサがハートビート要求を検出し、このペイロード長が実際のペイロード長より大きく、ルール 137:3 が有効にされている場合、または、ルール 137:4 が有効にされている際に、このオプションに設定された値よりハートビート応答のサイズが大きい場合は、プリプロセッサはイベントを生成し、インライン展開では、違反パケットをドロップします。。

SSL プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSL 設定（SSL Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [SSL設定（SSL Configuration）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 SSL プリプロセッサのオプション （2847 ページ） に示されている任意の設定を変更します。

- [ポート（Ports）] フィールドに値を入力します。複数の値を指定する場合は、カンマで区切ります。
- [暗号化トラフィックの検査の停止（Stop inspecting encrypted traffic）] チェックボックスをオンまたはオフにします。
- [暗号化トラフィックの検査の停止（Stop inspecting encrypted traffic）] チェックボックスをオンにした場合は、[サーバー側データは信頼済み（Server side data is trusted）] チェックボックスをオンまたはオフにします。
- [最大ハートビート長（Max Heartbeat Length）] フィールドに値を入力します。

  ヒント
  値 0 を指定すると、このオプションが無効になります。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、SSL プリプロセッサ ルール（GID 137）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

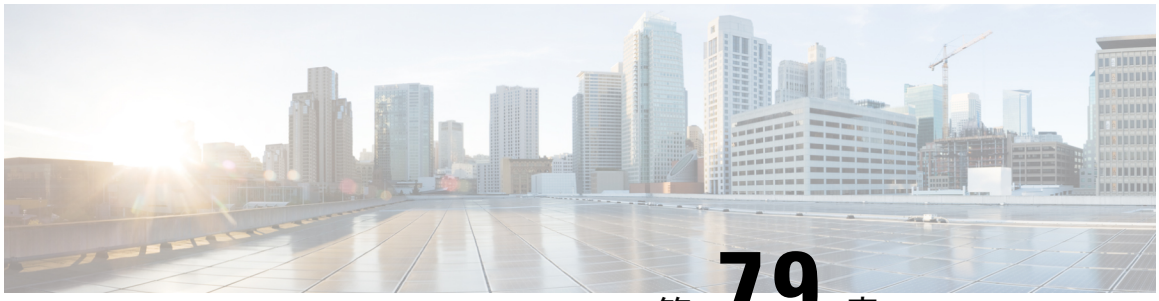
SSL プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、SSL プリプロセッサ ルール（GID 137）を有効にします。

次の表に、有効にできる SSL プリプロセッサ ルールを示します。

表 *222 : SSL* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
137:1	ServerHello メッセージの後の ClientHello メッセージを検出します。これは無効であり、異常な動作とみなされます。
137:2	SSL プリプロセッサ オプション [サーバ側のデータを信頼する（Server side data is trusted）] が無効な場合に、ClientHello メッセージのない ServerHello メッセージを検出します。これは無効であり、異常な動作としてみなされます。
137:3	SSL プリプロセッサ オプション [ハートビートの最大長（Max Heartbeat Length）] にゼロ以外の値が含まれている場合に、ペイロード自体よりも大きいペイロード長の値を含むハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。
137:4	SSL プリプロセッサ オプション [ハートビートの最大長（Max Heartbeat Length）] で指定されているゼロ以外の値よりも大きいハートビート応答を検出します。このようなハートビート応答は、Heartbleed バグを悪用する試みを示しています。



第 79 章

SCADA プリプロセッサ

以下のトピックでは、遠隔監視制御・情報取得（SCADA）プロトコルのプリプロセッサとその設定方法について説明します。

- SCADA プリプロセッサの概要 （2851 ページ）
- SCADA プリプロセッサのライセンス要件 （2852 ページ）
- SCADA プリプロセッサの要件と前提条件 （2852 ページ）
- Modbus プリプロセッサ （2852 ページ）
- DNP3 プリプロセッサ （2855 ページ）
- CIP プリプロセッサ （2857 ページ）
- S7Commplus プリプロセッサ （2862 ページ）

SCADA プリプロセッサの概要

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニター、制御、取得します。Firepower システムは、ネットワーク分析ポリシーの一部として設定できる Modbus、Distributed Network Protocol（DNP3）、Common Industrial Protocol（CIP）、および S7Commplus SCADA プロトコル用のプリプロセッサを提供します。

Modbus、DNP3、CIP、または S7Commplus プリプロセッサが無効になっていて、これらのプリプロセッサのいずれかを必要とする侵入ルールを有効にして展開した場合、システムはプリプロセッサを現在の設定で使用しますが、対応するネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効になったままとなります。

SCADA プリプロセッサのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

SCADA プリプロセッサの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

Modbus プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

関連トピック

SCADA キーワード （2150 ページ）

Modbus プリプロセッサ ポート オプション

ポート

プリプロセッサが Modbus トラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

Modbus プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ネットワークに Modbus 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [Modbus の構成（Modbus Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [Modbusの設定（Modbus Configuration）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 [ポート（Ports）] フィールドに値を入力します。

複数の値を指定する場合は、カンマで区切ります。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、Modbus プリプロセッサ ルール（GID 144）を有効にします。詳細については、「侵入ルール状態の設定 （2032 ページ）」および「Modbus プリプロセッサ ルール （2854 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

Modbus プリプロセッサ ルール

次の表に示す Modbus プリプロセッサ ルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *223 : Modbus* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さと一致していない場合に、イベントが生成されます。 各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

DNP3 プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Distributed Network Protocol（DNP3）は、当初は発電所間で一貫性のある通信を実現する目的で開発された SCADA プロトコルです。DNP3 も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっています。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルール エンジンによる処理のために DNP3 プロトコルをデコードします。ルール エンジンは、DNP3 キーワードを使用して特定のプロトコル フィールドにアクセスします。

関連トピック

DNP3 キーワード （2151 ページ）

DNP3 プリプロセッサ オプション

ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートを指定するか、複数のポートをカンマで区切ったリストを指定できます。

無効な CRC を記録（Log bad CRCs）

DNP3 リンク層フレームに含まれているチェックサムを検証します。無効なチェックサムを含むフレームは無視されます。

ルール 145:1 を有効にすると、無効なチェックサムが検出されたときにイベントを生成し、インライン展開では、違反パケットをドロップします。 できます。

DNP3 プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ネットワークに DNP3 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [DNP3 の構成（DNP3 Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [DNP3の設定（DNP3 Configuration）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 ポートの値を入力します。

複数の値を指定する場合は、カンマで区切ります。

ステップ 8 [不良 CRC の記録（Log bad CRCs）] チェックボックスをオンまたはオフにします。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、DNP3 プリプロセッサ ルール（GID 145）を有効にします。詳細については、侵入ルール状態の設定 （2032ページ）、DNP3プリプロセッサ オプション （2855ページ）、およびDNP3 プリプロセッサ ルール （2857 ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの管理 （2187 ページ）

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

DNP3 プリプロセッサ ルール

次の表に示すDNP3プリプロセッサルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *224 : DNP3* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
145:1	[無効な CRC を記録（Log bad CRC）] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さの DNP3 リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIR フラグを伝送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用する DNP3 リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用する DNP3 要求または応答をプリプロセッサが検出すると、イベントが生成されます。

CIP プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Common Industrial Protocol（CIP）は、産業自動化アプリケーションをサポートするために広く使用されているアプリケーションプロトコルです。EtherNet/IP（ENIP）は、イーサネットベースのネットワークで使用される CIP の実装です。

CIP プリプロセッサは、TCP または UDP で実行される CIP および ENIP トラフィックを検出し、それを侵入ルール エンジンに送信します。カスタム侵入ルールで CIP および ENIP のキー

ワードを使用すると、CIPおよびENIP トラフィックで攻撃を検出できます。「CIPおよびENIP のキーワード」を参照してください。さらに、アクセス コントロール ルールで CIP および ENIP アプリケーションの条件を指定することによって、トラフィックを制御できます。「アプリケーション条件とフィルタの設定 （1795 ページ）」を参照してください。

CIP プリプロセッサのオプション

ポート

CIP および ENIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

（注） リストするデフォルトの CIP 検出ポート 44818 およびその他のポートを、TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）] に追加する必要があります。TCP ストリームのプリプロセス オプション （2895 ページ）およびカスタム ネットワーク分析ポリシーの作成 （2759 ページ）を参照してください。

デフォルトの未接続タイムアウト（秒）

CIP 要求メッセージにプロトコル固有のタイムアウト値が含まれておらず、[TCP 接続あたりの未接続な同時要求の最大数（Maximum number of concurrent unconnected requests per TCP connection）] に達した場合は、このオプションで指定した秒数の間、システムがメッセージの時間を測定します。タイマーが満了すると、他の要求用のスペースを確保するために、メッセージが削除されます。0 ～ 360 の整数を指定できます。0 を指定すると、プロトコル固有のタイムアウト値を持たないすべてのトラフィックは、最初にタイムアウトになります。

TCP 接続あたりの未接続な同時要求の最大数（Maximum number of concurrent unconnected requests per TCP connection）

システムが接続を閉じるまで無応答のままにすることができる同時要求の数。1 ～ 10000 の整数を指定できます。

TCP 接続あたりの CIP 接続の最大数（Maximum number of CIP connections per TCP connection）

システムが TCP 接続ごとに許可する同時 CIP 接続の最大数。1 ～ 10000 の整数を指定できます。

CIP イベント

設計上、セッションごとに1回ずつ、同じアプリケーションがアプリケーションディテクタで検出されてイベント ビューアに表示されます。1 つの CIP セッションでは複数のアプリケーションを別々のパケットに含めることができ、単一のCIPパケットに複数のアプリケーションを格納できます。CIP プリプロセッサは、対応する侵入ルールに従ってすべての CIP と ENIP のトラフィックを処理します。

次の表にイベント ビューに表示される CIP の値を示します。

表 *225 : CIP* イベント フィールドの値

イベント フィールド	表示される値
アプリケーション プロトコル（Application Protocol）	CIP または ENIP
クライアント	CIP クライアントまたは ENIP クライアント
[Webアプリケーション（Web Application）]	次に示す特定のアプリケーションを検出しました。 • トラフィックを許可またはモニターするアクセス制御ルールの場合れた最後のアプリケーション プロトコル。 接続をログに記録するよう設定されたアクセス 制御 ルールが、指定ションのイベントを生成しないことがあります。一方、接続をログれていないアクセス コントロール ルールが、CIP アプリケーションことがあります。 • トラフィックをブロックするアクセス制御ルールの場合、ブロックケーション プロトコル。 アクセス コントロール ルールが CIP アプリケーションのリストをト ビューアに、検出された最初のアプリケーションが表示されます

CIP プリプロセッサ ルール

次の表に示す CIP プリプロセッサ ルールでイベントを生成するには、それらのルールを有効にする必要があります。ルールの有効化については、侵入ルール状態の設定 （2032 ページ）を参照してください。

表 *226 : CIP* プリプロセッサ ルール

GID:SID	ルール メッセージ
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

CIP プリプロセッサの設定のガイドライン

CIP プリプロセッサを設定する際には次の点に注意してください。

- リストするデフォルトの CIP 検出ポート 44818 およびその他の CIP **ポート**を TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）] に追加する必要があります。CIP プリプロセッサのオプション （2858 ページ）、カスタム ネットワーク分析ポリシーの作成 （2759 ページ）、および TCP ストリームのプリプロセス オプション （2895 ページ） を参照してください。
- イベント ビューアには、CIP アプリケーションに対する特別な処理が用意されています。CIP イベント （2858 ページ）を参照してください。
- 侵入防御アクションをアクセス コントロール ポリシーのデフォルトのアクションとして使用することをお勧めします。
- CIP プリプロセッサは、アクセス コントロール ポリシーのデフォルト アクション [アクセス制御：すべてのトラフィックを信頼（Access Control: Trust All Traffic）] をサポートしていません。このアクションを実行すると、侵入ルールとアクセス コントロール ルールで指定された CIP アプリケーションによりトリガーされたトラフィックがドロップされないなど、望ましくない動作が生じる可能性があるためです。
- CIP プリプロセッサは、アクセス コントロール ポリシーのデフォルト アクション [アクセス制御：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をサポートしていません。このアクションを実行すると、ブロックされると想定されない CIP アプリケーションがブロックされるなど、望ましくない動作が生じる可能性があるためです。
- CIP プリプロセッサは、CIP アプリケーションのアプリケーション可視性（ネットワーク検出を含む）をサポートしていません。
- CIP および ENIP アプリケーションを検出し、それらをアクセス コントロール ルールや侵入ルールなどで使用するには、対応するカスタム ネットワーク分析ポリシーで CIP プリプロセッサを手動で有効にする必要があります。カスタム ネットワーク分析ポリシーの作成 （2759 ページ）、「デフォルトのネットワーク分析ポリシーの設定」、および ネットワーク分析ルールの設定 （2752 ページ） を参照してください。
- CIP のプリプロセッサ ルールおよび CIP 侵入ルールをトリガーするトラフィックをドロップするには、対応する侵入ポリシーの [インラインの場合ドロップする（Drop when Inline）] オプションが有効になっていることを確認します。
- アクセス コントロール ルールを使用して CIP または ENIP アプリケーション トラフィックをブロックするには、対応するネットワーク分析ポリシーでインライン正規化プリプロセッサおよびその [インライン モード（Inline Mode）] オプションが有効になっている（デフォルト設定）ことを確認してください。カスタム ネットワーク分析ポリシーの作成 （2759 ページ）、「デフォルトのネットワーク分析ポリシーの設定」、およびインライン導入でのプリプロセッサによるトラフィックの変更 （2764 ページ） を参照してください。

CIP プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

始める前に

- CIP **ポート**としてリストするデフォルトの CIP 検出ポート 44818 およびその他のポートを TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）] に追加する必要があります。CIP プリプロセッサのオプション（2858ページ）、カスタムネットワーク分析ポリシーの作成（2759ページ）、および TCP ストリームのプリプロセス オプション （2895 ページ） を参照してください。
- CIP プリプロセッサの設定のガイドライン （2859 ページ） の内容についてよく理解しておきます。
- CIP プリプロセッサは、Firewall Threat Defense デバイスではサポートされていません。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [CIP 設定（CIP Configuration）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 6 CIP プリプロセッサのオプション （2858 ページ）で説明するオプションを変更できます。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 の場合、CIP 侵入ルールを有効にし、オプションで CIP プリプロセッサルール（GID 148）を有効にします。詳細については、侵入ルール状態の設定 （2032 ページ）、CIP プリプロセッサルール （2859 ページ）、およびCIP イベント （2858 ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

S7Commplus プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

S7Commplus プリプロセッサは、S7Commplus トラフィックを検出します。カスタム侵入ルールで S7Commplus キーワードを使用して、S7Commplus トラフィックの攻撃を検出できます。「S7Commplus キーワード （2155 ページ）」を参照してください。

S7Commplus プリプロセッサの設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

S7Commplus プリプロセッサは、すべての Firewall Threat Defense デバイスでサポートされています。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）

カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [SCADAプリプロセッサ（SCADA Preprocessors）] の下の [S7Commplus設定（S7Commplus Configuration）] が無効になっている場合は、[有効（Enabled）] をクリックします。

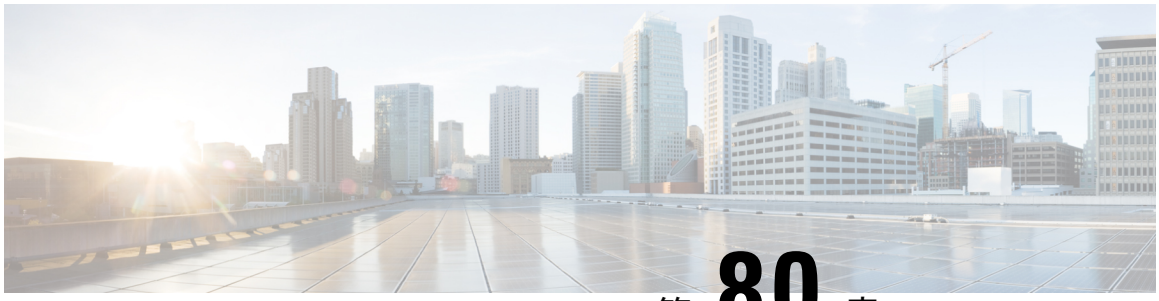
ステップ 6 必要に応じて、[S7Commplusの設定（S7Commplus Configuration）] の横にある [編集（Edit）]（） をクリックし、[s7commplus_ports] を変更して、プリプロセッサが S7Commplus トラフィックを検査するポートを識別します。複数のポートを指定する場合は、カンマで区切ります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、S7Commplus プリプロセッサルール（GID 149）を有効にします。詳細については、「侵入ルール状態の設定（2032 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開（172 ページ）を参照してください。



第 80 章

トランスポート層およびネットワーク層のプリプロセッサ

以下のトピックでは、トランスポート層およびネットワーク層プリプロセッサとそれらの設定方法について説明します。

- トランスポート層およびネットワーク層のプリプロセッサの概要 （2865 ページ）
- トランスポート層およびネットワーク層のプリプロセッサのライセンス要件 （2866ページ）
- トランスポート層およびネットワーク層のプリプロセッサの要件と前提条件 （2866ページ）
- トランスポート/ネットワーク プリプロセッサの詳細設定 （2866 ページ）
- チェックサム検証 （2870 ページ）
- インライン正規化プリプロセッサ （2872 ページ）
- IP 最適化プリプロセッサ （2881 ページ）
- パケット デコーダ （2887 ページ）
- TCP ストリームの前処理 （2892 ページ）
- UDP ストリームの前処理 （2906 ページ）

トランスポート層およびネットワーク層のプリプロセッサの概要

トランスポート層およびネットワーク層のプリプロセッサは、IP フラグメンテーション、チェックサム検証、TCP および UDP セッションの前処理を悪用する攻撃を検出します。パケットがプリプロセッサに送信される前に、パケット デコーダはパケット ヘッダーとペイロードを、プリプロセッサおよび侵入ルールエンジンで簡単に使用できるフォーマットに変換し、パケットヘッダー内でさまざまな変則的動作を検出します。インライン正規化プリプロセッサは、パケットをデコードした後、他のプリプロセッサにパケットを送信する前に、インライン型展開を対象にトラフィックを正規化します。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

トランスポート層およびネットワーク層のプリプロセッサのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

トランスポート層およびネットワーク層のプリプロセッサの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

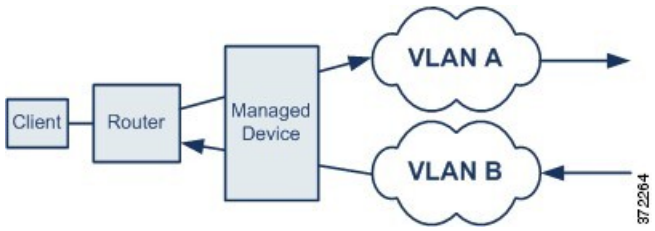
- 管理者
- 侵入管理者

トランスポート/ネットワーク プリプロセッサの詳細設定

トランスポート層とネットワーク層のプリプロセッサの詳細設定は、アクセス コントロール ポリシーが展開されるすべてのネットワーク、ゾーン、VLANにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

無視される **VLAN** ヘッダー

同じ接続で異なる方向に流れるトラフィックの VLAN タグが異なると、トラフィックのリアセンブルやルールの処理に影響を与える場合があります。たとえば、以下の図では、同じ接続のトラフィックを VLAN A で送信し、VLAN B で受信できます。



展開でパケットを正しく処理するため、VLANヘッダーを無視するようにシステムを設定できます。

侵入廃棄ルールでのアクティブ応答

廃棄ルールは、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された侵入ルールまたはプリプロセッサ ルールです。インライン展開では、システムは TCP または UDP 廃棄ルールに応答するために、トリガーしたパケットをドロップし、そのパケットが開始されたセッションをブロックします。

ヒント UDP データ ストリームは一般にセッションという観点では考慮されないため、ストリーム プリプロセッサはカプセル化 IP データグラム ヘッダーの送信元と宛先の IP アドレス フィールドと UDP ヘッダーのポート フィールドを使用してフローの方向を判別し、UDP セッションを識別します。

問題のあるパケットによって TCP または UDP 廃棄ルールがトリガーされた時点で、1 つ以上のアクティブ応答を開始して、より正確かつ明示的に TCP 接続または UDP セッションを閉じるようにシステムを設定することができます。アクティブ応答は、ルーテッド展開およびトランスペアレント展開を含むインライン展開で使用できます。アクティブ応答は、パッシブ展開には適していないか、またはサポートされていません。

アクティブ応答を設定するには、次の手順を実行します。

- TCP または UDP（**resp** キーワードのみ）の侵入ルールを作成または変更します。侵入ルール ヘッダー プロトコル （2049 ページ）を参照してください。
- 侵入ルールに **react** キーワードまたは **resp** キーワードを追加します。アクティブ応答のキーワード （2158 ページ）を参照してください。
- 必要に応じて、TCP 接続の場合は、送信する追加のアクティブ応答の最大数と、アクティブ応答の間に待機する秒数を指定します。トランスポート/ネットワーク プリプロセッサの詳細オプション （2868 ページ）の「**アクティブ応答の最大数（Maximum Active Responses）**」および「**最小応答時間（秒）（Minimum Response Seconds）**」を参照してください。

アクティブ応答は、一致するトラフィックが廃棄ルールをトリガーとして使用したときに、次のように、そのセッションをクローズします。

- **TCP**：トリガーを使用したパケットを廃棄し、クライアントとサーバ両方のトラフィックに TCP リセット（RST）パケットを挿入します。
- **UDP**：セッションの両端に ICMP 到達不能パケットを送信します。

トランスポート/ネットワーク プリプロセッサの詳細オプション

接続の追跡時に VLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）

トラフィックの識別時に VLAN ヘッダーを無視するか、それとも考慮するかを指定します。次のようになります。

- このオプションを選択すると、VLANヘッダーが無視されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出する可能性がある展開済みデバイスに使用します。
- このオプションを無効にすると、VLANヘッダーが考慮されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出しない展開済みデバイスに使用します。

アクティブ応答の最大数（Maximum Active Responses）

TCP接続あたりのアクティブ応答の最大数を指定します。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから [最小応答秒数（Minimum Response Seconds）] を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0 を設定すると、**resp** または **react** ルールによってトリガーされる追加のアクティブ応答が無効になります。侵入廃棄ルールでのアクティブ応答 （2867 ページ）およびアクティブ応答のキーワード （2158 ページ）を参照してください。

トリガーされた **resp** または **react** ルールは、このオプションの設定に関係なく、アクティブ応答を開始することに注意してください。

最小応答時間（秒）（Minimum Response Seconds）

[最大アクティブ応答数（Maximum Active Responses）] に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を指定します。

トラブルシューティングオプション：セッション終了ロギングしきい値（Troubleshooting Options: Session Termination Logging Threshold）

⚠

注意 [セッション終了ロギングしきい値（Session Termination Logging Threshold）] は、サポート担当から指示されない限り変更しないでください。

トラブルシューティングの電話中に、個別の接続が指定したしきい値を超えた場合にメッセージを記録するようにシステムを設定することをサポートから依頼される場合があります。この

オプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従って実行してください。

このオプションは、ログに記録されるメッセージのバイト数を指定します。セッションが終了し、メッセージが指定のバイト数を超えた場合は、ログに記録されます。

（注） 上限は 1 GB ですが、管理対象デバイスでストリーム処理のために割り当てられるメモリの量によっても制限されます。

関連トピック

アクティブ応答のキーワード （2158 ページ）

トランスポート/ネットワーク プリプロセッサの詳細設定の構成

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者である必要があります。

手順

ステップ 1 アクセス制御ポリシーエディタで、変更するポリシーの [編集（Edit）]（✎） をクリックします。

ステップ 2 **[詳細（More）] > [詳細設定（Advanced Settings）]** の順にクリックし、[トランスポート/ネットワークプリプロセッサ設定（Transport/Network Preprocessor Settings）] セクションの横の [編集（Edit）]（✎） をクリックします。

ステップ 3 トラブルシューティング オプション [セッション終了のロギングしきい値（Session Termination Logging Threshold）] を除き、トランスポート/ネットワーク プリプロセッサの詳細オプション（2868 ページ）の説明に従ってオプションを変更します。

注意
[セッション終了のロギングしきい値（Session Termination Logging Threshold）] は、サポートからの指示がない限り変更しないでください。

ステップ 4 [OK] をクリックします。

次のタスク

- 必要に応じて、アクセス コントロール ポリシーの編集（1749ページ）の説明に従ってさらにポリシーを設定します。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

チェックサム検証

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

システムは、あらゆるプロトコル レベルのチェックサムを検証することで、IP、TCP、UDP、およびICMPによる送信データが完全に受信されていることを確認できます。さらに基本的なレベルで、パケットが転送中に改ざんされたり、誤って変更されたりしていないことも確認できます。チェックサムはアルゴリズムを使用して、パケットでのプロトコルの整合性を検証します。システムが終端のホストでパケットに書き込まれた値を計算し、それがチェックサムと同じであれば、そのパケットは変更されていないと見なされます。

チェックサムの検証を無効にすると、ネットワークが侵入攻撃にさらされる危険があります。システムは、チェックサム検証イベントを生成しないことに注意してください。インライン展開では、パケットのチェックサムが正しくない場合、そのパケットをドロップするようにシステムを設定できます。

チェックサム検証オプション

次のオプションは、いずれも、パッシブ展開またはインライン展開で [有効（Enabled）] または [無効（Disabled）] に設定することができます。インライン展開では [ドロップ（Drop）] に設定することもできます。

- **ICMP チェックサム（ICMP Checksums）**
- **IP チェックサム（IP Checksums）**
- **TCP チェックサム（TCP Checksums）**
- **UDP チェックサム（UDP Checksums）**

違反パケットをドロップするには、オプションを [ドロップ（Drop）] に設定するだけでなく、関連付けられているネットワーク分析ポリシーの [インライン モード（Inline Mode）] を有効にし、確実にデバイスがインラインで展開されるようにする必要があります。

パッシブ展開またはタップ モードでのインライン展開で、これらのオプションを [ドロップ（Drop）] に設定することは、[有効（Enabled）] に設定するのと同じです。

注目 [TCP チェックサム（TCP checksums）] で、[無視（Ignore）] オプション（デフォルト）を選択すると、設定された Snort ルールがバイパスまたは無視されます。

すべてのチェックサム検証オプションは、デフォルトで、[有効（Enabled）] になっています。ただし、Firewall Threat Defense ルーテッド トランスペアレント インターフェイスでは、IP

チェックサム検証に失敗したパケットは常にドロップされます。Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスが、パケットを Snort プロセスに渡す前に、正しくないチェックサムを使用して UDP パケットを修正することに注意してください。

関連トピック

インライン導入でのプリプロセッサによるトランスペアレントの変更 （2764 ページ）

チェックサムの確認

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [トランスポート層/ネットワーク層のプロセッサ（Transport/Network Layer Preprocessors）] の下にある [チェックサムの確認（Checksum Verification）] が無効になっている場合、[有効（Enabled）] をクリックします。

ステップ 6 [チェックサムの確認（Checksum Verification）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 チェックサム検証 （2870 ページ） で説明されているオプションを変更します。

（注）
[TCPチェックサム（TCP checksums）] で、[無視（Ignore）] オプション（デフォルト）を選択すると、設定された Snort ルールがバイパスまたは無視されます。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤ管理 （2185 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

インライン正規化プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

インライン正規化プリプロセッサは、インライン展開で攻撃者が検出を免れる可能性を最小限にするために、トラフィックを正規化します。

（注） システムでトラフィックに影響を与えるには、ルーテッド、スイッチド、またはトランスペアレント インターフェイスあるいはインライン インターフェイス ペアを使用して、関連する設定を管理対象デバイスに展開する必要があります。

IPv4、IPv6、ICMPv4、ICMPv6、TCP トラフィックを任意に組み合わせて正規化を指定できます。ほとんどの正規化は、パケット単位で行われ、インライン正規化プリプロセッサによって処理されます。ただし、TCP ストリーム プリプロセッサは、TCP ペイロードの正規化を含む、ほとんどの状態関連パケットおよびストリームの正規化を処理します。

インライン正規化は、パケット デコーダによるデコードの直後に行われます。その後で、別のプリプロセッサによる処理が行われます。正規化は、パケット層の内部から外部への方向で行われます。

インライン正規化プリプロセッサはイベントを生成しません。インライン正規化プリプロセッサの役割は、インライン展開の別のプリプロセッサおよびルールエンジンで使用できるようにパケットを準備することです。また、システムが処理するパケットが、ネットワーク上のホストで受信したパケットと同じであるようにする役割もあります。

（注） インライン展開では、インラインモードを有効にし、[TCPペイロードの正規化（Normalize TCP Payload）] オプションを有効にしたままインライン正規化プリプロセッサを設定することを推奨します。パッシブ展開では、adaptive profile updatesを使用することを推奨します。

関連トピック

インライン導入でのプリプロセッサによるトラフィックの変更 （2764 ページ）
アダプティブ プロファイルについて （2933 ページ）

インライン正規化オプション

最小 TTL（Minimum TTL）

[TTL のリセット（Reset TTL）] がこのオプションに設定する値以上の値に設定されている場合、このオプションは以下を指定します。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 存続可能時間（TTL）（IPv4 Time to Live (TTL)）] フィールドの最小許容値。TTL のパケット値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。
- [Normalize IPv6] が有効にされている場合は、[IPv6 Hop Limit] フィールドの最小許容値。ホップ リミットの値がこの値を下回る場合、[Reset TTL] に設定された値に正規化されます。

このフィールドが空白の場合、システムは値が 1 であると想定します。

（注） Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスの場合、[最小 TTL（Minimum TTL）] および [TTL のリセット（Reset TTL）] オプションは無視されます。接続の最大 TTL は最初のパケットの TTL によって決定します。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。これにより、TTL 回避攻撃を阻止します。

パケット復号化の [プロトコル ヘッダー異常の検出（Detect Protocol Header Anomalies）] オプションが有効になっている場合、デコーダ ルール カテゴリで次のルールを有効にして、このオプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にトリガーするには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にトリガーするには、ルール 116:270 を有効にします。

TTL のリセット（Reset TTL）

[最小 TTL（Minimum TTL）] の値以上の値を設定した場合、以下のフィールドが正規化されます。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 TTL] フィールド
- [Normalize IPv6] が有効にされている場合は、[IPv6 Hop Limit] フィールド

パケット値が [最小 TTL（Minimum TTL）] を下回る場合、システムはパケットの TTL またはホップリミットの値をこのオプションに対して設定された値に変更して、パケットを正規化します。このフィールドを空白のままにするか、0 に設定するか、または [最小 TTL（Minimum TTL）] 未満の値に設定すると、このオプションは無効になります。

IPv4 の正規化（Normalize IPv4）

IPv4 トラフィックの正規化を有効にします。システムは、以下の場合にも必要に応じて TTL フィールドを正規化します。

- このオプションが有効になっていて、さらに、
- [TTL のリセット（Reset TTL）] に設定された値によって TTL の正規化が有効になっている。

このオプションを有効にすると、追加の IPv4 オプションを有効にすることもできます。

このオプションを有効にすると、システムは以下の基本の IPv4 正規化を実行します。

- 過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長まで切り捨てます。
- [Differentiated Services (DS)] フィールド（旧称 [Type of Service (TOS)] フィールド）をクリアします。
- すべてのオプション オクテットを 1（[操作なし（No Operation）]）に設定します。

このオプションは Firewall Threat Defense ルーテッド インターフェイスとトランスペアレント インターフェイスでは無視されます。Firewall Threat Defense デバイスは、ルーテッドインターフェイスまたはトランスペアレント インターフェイスのルーテッド アラート、End of Options List（EOOL）、オペレーションなし（NOP）オプション以外の IP オプションを含んでいるすべての RSVP パケットをドロップします。

フラグメント禁止ビットの正規化（Normalize Don't Fragment Bit）

[IPv4 Flags] 見出し フィールドの単一ビットの [Don’t Fragment] サブフィールドをクリアします。このオプションを有効にすると、ダウンストリームのルータがパケットをドロップする代わりに、必要に応じてパケットをフラグメント化できます。また、このオプションを有効にすることで、ドロップされるパケットを巧妙に作成してポリシーを回避する試みを防ぐこともできます。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

Normalize Reserved Bit

[IPv4 Flags] 見出し フィールドの単一ビットの [Reserved] サブフィールドをクリアします。通常は、このオプションを有効にします。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

TOS ビットの正規化（Normalize TOS Bit）

1バイトの差別化サービス（DS）フィールド（旧「タイプオブサービス（ToS）フィールド」）をクリアします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

Normalize Excess Payload

過剰なペイロードを持つパケットを、IP 見出しに指定されたデータグラム長にレイヤ 2（たとえば、イーサネット）見出しを合計した長さにまで切り捨てます。ただし、最小フレーム長より小さく切り捨てることはしません。このオプションを選択するには、[IPv4の正規化（Normalize IPv4）] を有効にする必要があります。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。過剰なペイロードを持つパケットは、常にこれらのインターフェイスでドロップされます。

IPv6 の正規化（Normalize IPv6）

[Hop-by-Hop Options] および [Destination Options] 拡張見出しに含まれるすべてのオプション タイプ フィールドを 00（スキップして処理を続行）に設定します。このオプションが有効にされていて、[Reset TTL] に設定された値が ホップ リミット正規化を有効にしている場合、システムは必要に応じてホップ リミット フィールドも正規化します。

Normalize ICMPv4

ICMPv4 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコードフィールドをクリアします。

Normalize ICMPv6

ICMPv6 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコードフィールドをクリアします。

予約済みビットの正規化またはクリア（Normalize/Clear Reserved Bits）

TCP ヘッダーの予約ビットをクリアします。

Normalize/Clear Option Padding Bytes

TCP オプションの埋め込みバイトをクリアします。

URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）

緊急（URG）制御ビットが設定されていない場合、16 ビットの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをクリアします。

空のペイロードに設定された緊急ポインタまたは URG をクリア（Clear Urgent Pointer/URG on Empty Payload）

ペイロードがない場合、TCP ヘッダーの緊急ポインタ フィールドと URG 制御ビットをクリアします。

Clear URG if Urgent Pointer is Not Set

緊急ポインタが設定されていない場合、TCP ヘッダーの緊急制御ビットをクリアします。

緊急ポインタの正規化（Normalize Urgent Pointer）

ポインタがペイロード長を上回る場合、2 バイトの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをペイロード長に設定します。

TCP ペイロードの正規化（Normalize TCP Payload）

再送信されるデータの一貫性が確保されるように [TCP データ（TCP Data）] フィールドの正規化を有効にします。正しく再構成できないセグメントはすべてドロップされます。

SYN に関するデータを削除（Remove Data on SYN）

TCP オペレーティング システム ポリシーが Mac OS 以外の場合、同期（SYN）パケットのデータを削除します。

また、このオプションにより、TCP ストリーム プリプロセッサの [ポリシー（Policy）] オプションが [Mac OS] に設定されていない場合にトリガー可能なルール 129:2 もまた無効になります。

RST に関するデータを削除（Remove Data on RST）

TCP リセット（RST）パケットからデータを削除します。

Trim Data to Window

TCP データ フィールドを [Window] フィールドで指定されたサイズに切り詰めます。

Trim Data to MSS

ペイロードが MSS より長い場合、[TCP データ（TCP Data）] フィールドを最大セグメント サイズ（MSS）にまで切り捨てます。

解決不可能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）

このオプションを有効にすると、システムは無効になり受信ホストによってブロックされる可能性が高い異常な TCP パケット（正規化されている場合）をブロックします。たとえば、システムは、確立されたセッションに送信される以降の SYN パケットをブロックします。

ルールが有効になっているかどうかに関係なく、以下に示す TCP ストリーム プリプロセッサのいずれかのルールに一致するパケットもすべてドロップされます。

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 ～129:19

[ブロックされたパケットの合計（Total Blocked Packets）] パフォーマンス グラフには、インライン展開でブロックされたパケットの数が示され、パッシブ展開とタップモードでのインライン展開の場合は、インライン展開でブロックされる予想数が示されます。

明示的な混雑通知（ECN）（Explicit Congestion Notification）

明示的輻輳通知（ECN）フラグのパケット単位またはストリーム単位の正規化を以下のように有効にします。

- [パケット（Packet）] を選択すると、ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされます。
- [ストリーム（Stream）] を選択すると、ECN の使用がネゴシエートされていない場合、ストリーム単位で ECN フラグがクリアされます。

[ストリーム（Stream）] を選択した場合、この正規化が実行されるようにするには、TCP ストリーム プリプロセッサの [TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] オプションも有効にされている必要があります。

既存の TCP オプションをクリア（Clear Existing TCP Options）

[これらの TCP オプションを許可（Allow These TCP Options）] を有効にします。

これらの TCP オプションを許可（Allow These TCP Options）

トラフィックで許可する特定の TCP オプションの正規化を無効にします。

明示的に許可されたオプションは、正規化されません。オプションを [操作なし（No Operation）]（TCP オプション 1）に設定して明示的に許可していないオプションは、正規化されます。

[これらの TCP オプションを許可（Allow These TCP Options）] の設定に関係なく、次のオプションは最適な TCP パフォーマンスに一般的に使用されるため、システムは常にこれらのオプションを許可します。

- 最大セグメント サイズ（MSS）（Maximum Segment Size (MSS)）
- ウィンドウ スケール（Window Scale）
- タイム スタンプ TCP（Time Stamp TCP）

他のそれほど一般的に使用されないオプションについては、システムは自動的に許可しません。

特定のオプションを許可するには、オプション キーワード、オプション番号、またはこの両方のカンマ区切りリストを設定します。以下に、一例を示します。

```
sack, echo, 19
```

オプション キーワードを指定するということは、そのキーワードと関連付けられた 1 つ以上の TCP オプションの番号を指定することと同じです。たとえば、`sack` を指定することは、TCP オプション 4（Selective Acknowledgement Permitted）および TCP オプション 5（Selective Acknowledgement）を指定することと同じです。オプション キーワードでは、大文字と小文字が区別されません。

また、`any` を指定すると、すべての TCP オプションが許可されるため、実質的にすべての TCP オプションの正規化が無効にされます。

次の表に、許可する TCP オプションを指定する方法を要約します。フィールドを空のままにすると、システムは MSS、ウィンドウ スケール、およびタイムスタンプのオプションのみを許可します。

指定するキーワード	許可されるオプション
sack	TCP オプション 4（Selective Acknowledgement Permitted）および 5（Selective Acknowledgement）
echo	TCP オプション 6（Echo Request）および 7（Echo Reply）
partial_order	TCP オプション 9（Partial Order Connection Permitted）および 10（Partial Order Service Profile）
conn_count	TCP 接続カウント オプション 11（CC）、12（CC.New）、および 13（CC.Echo）
alt_checksum	TCP オプション 14（Alternate Checksum Request）および 15（Alternate Checksum）
md5	TCP オプション 19（MD5 Signature）

指定するキーワード	許可されるオプション
オプション番号 2 ～ 255	キーワードのないオプションを含む、特定のオプション
any	すべての TCP オプション（この設定は、実質的に TCP オプションの正規化を無効にします）

このオプションに any を指定しない場合、正規化に以下が含まれます。

- MSS、ウィンドウ スケール、タイムスタンプ、およびその他の明示的に許可されたオプションを除き、すべてのオプションのバイトを [操作なし（No Operation）]（TCP オプション 1）に設定します。
- タイムスタンプは存在していても無効な場合、あるいは有効であってもネゴシエートされない場合、タイムスタンプ オクテットを [操作なし（No Operation）] に設定します。
- タイムスタンプがネゴシエートされているが存在しない場合、パケットをブロックします。
- 確認応答（ACK）制御ビットが設定されていない場合、タイムスタンプ エコー応答T（TSecr）オプション フィールドをクリアします。
- SYN 制御ビットが設定されていない場合、[MSS] および [ウィンドウ スケール（Window Scale）] オプションを [操作なし（No Operation）]（TCP オプション 1）に設定します。

関連トピック

インライン導入でのプリプロセッサによるトラフィックの変更 （2764 ページ）
アダプティブ プロファイルについて （2933 ページ）

インライン正規化の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

始める前に

- 問題を起こすパケットを正規化またはドロップするには、インライン導入でのプリプロセッサによるトラフィックの変更（2764 ページ）の説明に従って [インライン モード（Inline Mode）] を有効にします。また、管理対象デバイスは、インラインで展開する必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーションパネルで [設定（Settings）] をクリックします（キャレットではなく、単語をクリックします）。

ステップ 5 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] で [インライン正規化（Inline Normalization）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [インライン正規化（Inline Normalization）] の横にある [編集（Edit）]（✎） をクリックします。

ステップ 7 インライン正規化プリプロセッサ（2872ページ）で説明されているオプションを設定します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- インライン正規化 [最小TTL（Minimum TTL）] オプションで侵入イベントを生成する場合は、パケットデコーダルール 116:429（IPv4）と 116:270（IPv6）のいずれかまたは両方を有効にします。詳細については、侵入ルール状態の設定（2032ページ）およびインライン正規化オプション（2873 ページ）を参照してください。
- 設定変更を展開します設定変更の展開（172 ページ）を参照してください。

関連トピック

レイヤ管理（2185 ページ）

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更 （2764 ページ）
アダプティブ プロファイルについて （2933 ページ）

IP 最適化プリプロセッサ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

最大伝送ユニット（MTU）より大きいために IP データグラムが複数の小さい IP データグラムに分割されると、その IP データグラムはフラグメント化されたことになります。単一の IP データグラム フラグメントには、隠れた攻撃を識別するのに十分な情報が含まれない場合があります。そのため、攻撃者はエクスプロイトの検出を免れるために、フラグメント化されるパケットで攻撃データを送信する可能性があります。IP 最適化プリプロセッサは、ルール エンジンが IP データグラムに対してルールを実行する前に、パケットに仕込まれた攻撃をルールで識別しやすくするために、フラグメント化された IP データグラムを再構成します。フラグメント化されたデータグラムを再構成できない場合、それらのデータグラムに対しては、ルールが実行されません。

IP フラグメンテーション エクスプロイト

IP最適化を有効にすると、ネットワーク上のホストに対する攻撃（ティアドロップ攻撃など）や、システム自体に対するリソース消費攻撃（Jolt2 攻撃など）を検出するのに役立ちます。

ティアドロップ攻撃は、特定のオペレーティング システムのバグを悪用して、そのオペレーティング システムがオーバーラップした IP フラグメントを再構成しようとするとクラッシュするように仕掛けます。IP最適化プリプロセッサを有効にして、オーバーラップしたフラグメントを識別するように設定すれば、該当するフラグメントを識別できます。IP最適化プリプロセッサは、ティアドロップ攻撃などのオーバーラップ フラグメント攻撃で、最初のパケットを検出するだけで、同じ攻撃での後続のパケットは検出しません。

Jolt2 攻撃では、IP デフラグ機能を酷使させるという方法でサービス拒絶攻撃を仕掛けるために、フラグメント化された同じ IP パケットのコピーを大量に送信します。IP 最適化プリプロセッサでは、メモリ使用量の上限によって、このような攻撃を阻止し、包括的検査においてシステムを自己防衛状態にします。システムは攻撃によって過負荷にならず、運用可能な状態を維持し、ネットワーク トラフィックの検査を続行します。

フラグメント化されたパケットを再構成する方法は、オペレーティング システムによって異なります。ホストがどのオペレーティング システムで実行されているのかを攻撃者が特定できれば、その攻撃者はターゲット ホストが特定の方法で再構成するように不正なパケットをフラグメント化することも可能です。モニター対象のネットワーク上でホストを実行しているオペレーティング システムは、システムには不明です。したがって、プリプロセッサがパケットを誤った方法で再構成して検査し、それによってエクスプロイトが検出されないままパス スルー

する可能性があります。このような攻撃を軽減するために、ネットワーク上のホストごとに適切な方法でパケットを最適化するよう、最適化プリプロセッサを設定できるようになっています。

パッシブ展開でadaptive profile updatesを使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、IP 最適化プリプロセッサに適用するターゲット ベースのポリシーが動的に選択されるようにすることもできます。

ターゲット ベースの最適化ポリシー

ホストのオペレーティング システムは以下の3つの基準を使用して、パケットを再構成する際に優先するパケット フラグメントを決定します。

- オペレーティング システムがフラグメントを受信した順序
- フラグメントのオフセット（パケットの先頭からのそのフラグメントの距離（バイト単位））
- オーバーラップしているフラグメントとの相対開始位置と相対終了位置

これらの基準はすべてのオペレーティング システムで使用されているものの、フラグメント化されたパケットを再構成するときに優先するフラグメントは、オペレーティング システムによって異なります。したがって、ネットワーク上で異なるオペレーティング システムを使用する2台のホストが、同じオーバーラップ フラグメントをまったく異なる方法で再構成する場合も考えられます。

いずれかのホストのオペレーティング システムを認識している攻撃者が、オーバーラップしたパケット フラグメントに不正なコンテンツを忍ばせて送信することによって、エクスプロイトの検出を免れ、そのホストを悪用する可能性があります。このパケットが他のホストで再構成されて検査されても、パケットに害はないように見えますが、ターゲット ホストで再構成される場合には不正なエクスプロイトが含まれています。ただし、モニター対象のネットワーク セグメントで稼働するオペレーティング システムを認識するように IP 最適化プリプロセッサを設定すれば、このプリプロセッサがターゲット ホストと同じ方法でフラグメントを再構成することによって、攻撃を識別できます。

IP 最適化オプション

IP 最適化を有効または無効にすることだけを選択することもできますが、シスコでは、それよりも細かいレベルで、有効にする IP 最適化プリプロセッサの動作を指定することを推奨しています。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

次のグローバル オプションを構成できます。

事前に割り当てられたフラグメント（Preallocated Fragments）

プリプロセッサが一度に処理できる個々のフラグメントの最大数。事前割り当てするフラグメント ノードの数を指定すると、静的メモリ割り当てが有効になります。

⚠

注意 個々のフラグメントの処理には、約 1550 バイトのメモリが使用されます。プリプロセッサで個々のフラグメントを処理するために必要なメモリが、管理対象デバイスに事前定義された使用可能なメモリ量の制限を上回る場合は、管理対象デバイスのメモリ制限が優先されます。

IP 最適化ポリシーごとに、以下のオプションを設定できます。

Networks

最適化ポリシーを適用するホスト（複数可）の IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`すべて` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Policy

モニター対象ネットワーク セグメント上のホスト一式に使用する最適化ポリシー。

ターゲット ホストのオペレーティング システムに応じて、7 つの最適化ポリシーの 1 つを選択できます。以下の表に、7 つのポリシーと、それぞれのポリシーを使用するオペレーティング システムを記載します。First と Last というポリシー名は、これらのポリシーが元のオーバーラップ パケットまたは後続のオーバーラップ パケットのどちらを優先するかを反映しています。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

表 *227:* ターゲットベースの最適化ポリシー

ポリシー	オペレーティング システム
BSD	AIX FreeBSD IRIX VAX/VMS

ポリシー	オペレーティング システム
BSD-right	HP JetDirect
First	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

Timeout

プリプロセッサエンジンがフラグメント化されたパケットを再構成する際に使用できる最大時間（秒数）を指定します。指定された時間内にパケットを再構成できない場合、プリプロセッサ エンジンはパケットの再構成試行を停止し、受信したフラグメントを破棄します。

最小 TTL（Min TTL）

パケットに許容される最小 TTL 値を指定します。このオプションは、TTL ベースの挿入攻撃を検出します。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 123:11 を有効にします。

異常検知（Detect Anomalies）

オーバーラップ フラグメントのようなフラグメンテーション問題を識別します。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレントインターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 123:1 ～ 123:4
- 123:5（BSD ポリシー）
- 123:6 ～123:8

オーバーラップ範囲（Overlap Limit）

セッション内で重複しているセグメントの設定された数が検出されると、そのセッションの最適化を停止することを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値 0 は、無制限の重複セグメント数を指定します。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレントインターフェイスでは無視されます。重複フラグメントは、それらのインターフェイスでは常にドロップされます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 123:12 を有効にできます。

最小フラグメント サイズ（Minimum Fragment Size）

設定されたバイト数より小さい最後でないフラグメントが検出された場合、そのパケットは悪意のあるものとみなされることを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値 0 は、無制限のバイト数を指定します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 123:13 を有効にできます。

IP 最適化の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2748 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）

カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] で [IP 最適化（IP Defragmentation）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [IP最適化（IP Defragmentation）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 必要に応じて、[事前割り当て済みフラグメント（Preallocated Fragments）] フィールドに値を入力します。

ステップ 8 次の選択肢があります。

- サーバープロファイルの追加：ページの左側の [サーバー（Servers）] の横にある [追加（Add）] () をクリックし、[ホストアドレス（Host Address）] フィールドに値を入力して、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。
- サーバー プロファイルの編集：ページの左側の [サーバー（Servers）] で設定済みのアドレスをクリックするか、[デフォルト（default）] をクリックします。
- プロファイルの削除：ポリシーの横にある[削除（Delete）]（）をクリックします。

ステップ 9 IP 最適化オプション （2882 ページ）の説明に従ってオプションを変更します。

ステップ 10 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、IP 最適化ルール（GID 123）を有効にします。詳細については、「侵入ルール状態の設定（2032 ページ）」および「IP 最適化オプション （2882 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの基本 （2179 ページ）

競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

パケット デコーダ

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

キャプチャしたパケットをプリプロセッサに送信する前に、システムはパケットをパケットデコーダに送信します。パケット デコーダは、プリプロセッサやルール エンジンが容易に使用できる形式に、パケット ヘッダーおよびペイロードを変換します。データリンク層から開始して、ネットワーク層、トランスポート層へと、各スタック層が順にデコードされます。

パケット デコーダ オプション

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

GTP データ チャネルのデコード（Decode GTP Data Channel）

カプセル化された GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）データ チャネルをデコードします。デフォルトでは、デコーダはポート 3386 ではバージョン 0 のデータをデコードし、ポート 2152 ではバージョン 1 のデータをデコードします。`GTP_PORTS` デフォルト変数を使用して、カプセル化された GTP トラフィックを識別するポートを変更できます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:297 および 116:298 を有効にします。

[標準外ポートで Teredo を検知（Detect Teredo on Non-Standard Ports）]

ポート 3544 以外の UDP ポートで識別される IPv6 トラフィックの Teredo トンネリングを検査します。

IPv6 トラフィックが存在する場合、システムは常にこのトラフィックを検査します。デフォルトでは、IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP 見出しがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。

IPv4 ネットワークでは、IPv4 ホストが Teredo プロトコルを使用して、IPv4 Network Address Translation（NAT）デバイスを介して IPv6 トラフィックをトンネリングできます。Teredo は、IPv6 パケットを IPv4 UDP データグラムにカプセル化して、IPv4 NAT デバイスの背後で IPv6 接続を許可します。システムは通常、UDP ポート 3544 を使用して Teredo トラフィックを識別します。ただし、攻撃者が検出を免れるために標準以外のポートを使用する可能性も考えられ

ます。[Detect Teredo on Non-Standard Ports] を有効にすることで、システムに Teredo トンネリングのすべての UDP ペイロードを検査させることができます。

Teredo のデコードは、外側のネットワーク層に IPv4 が使用されている場合に限り、最初の UDP 見出しに対してのみ行われます。UDP データが IPv6 データにカプセル化されるため、Teredo IPv6 層の後に 2 つめの UDP 層が存在する場合、ルール エンジンは UDP 侵入ルールを使用して、内側および外側の両方の UDP 層を分析します。

policy-other ルール カテゴリの侵入ルール 12065、12066、12067、および 12068 は Teredo トラフィックを検出しますが、デコードはしないことに注意してください。（オプション）これらのルールを使用してインライン展開で Teredo トラフィックをドロップすることができます。ただし、[非標準ポートでの Teredo の検出（Detect Teredo on Non-Standard Ports）] を有効にする場合は、これらのルールを無効化するか、トラフィックをドロップせずにイベントを生成するように設定する必要があります。

[余長値の検知（Detect Excessive Length Value）]

パケット ヘッダーが実際のパケット長を超えるパケット長を指定しているかどうかを検出します。

このオプションは、Firewall Threat Defense ルーテッド、トランスペアレント、およびインラインインターフェイスでは無視されます。超過ヘッダー長を持つパケットは常にドロップされます。ただし、このオプションは Firewall Threat Defense インライン タップおよびパッシブ インターフェイスに適用されます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:6、116:47、116:97、および 116:275 を有効にできます。

[間違いな IP オプションを検知（Detect Invalid IP Options）]

無効な IP オプションを使用したエクスプロイトを識別するために、無効な IP ヘッダー オプションを検出します。たとえば、ファイアウォールに対するサービス拒絶攻撃は、システムをフリーズさせる原因になります。ファイアウォールが無効なタイムスタンプおよび IP セキュリティ オプションを解析しようとして、ゼロ長のチェックに失敗すると、回復不可能な無限ループが発生します。ルールエンジンはゼロ長のオプションを識別し、ファイアウォールでの攻撃を軽減するために使用できる情報を提供します。

Firewall Threat Defense デバイスは、各ルーテッドまたはトランスペアレント インターフェイスのルータ アラート、End of Options List（EOOL）、およびオペレーションなし（NOP）オプションを持つ RSVP パケットをドロップします。インライン、インライン タップ、またはパッシブ インターフェイスについては、IP オプションは上記のように処理されます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:4 および 116:5 を有効にします。

[実験的 TCP オプションを検知（Detect Experimental TCP Options）]

試験的な TCP オプションが設定された TCP ヘッダーを検出します。以下の表は、それらのオプションを示しています。

TCP オプション	説明
9	Partial Order Connection Permitted
10	Partial Order Service Profile
14	Alternate Checksum Request
15	Alternate Checksum Data
	Trailer Checksum
20	Space Communications Protocol Standards（SCPS）
21	Selective Negative Acknowledgements（SCPS）
22	Record Boundaries（SCPS）
23	Corruption（SPCS）
24	SNAP
26	TCP Compression Filter

これらのオプションは試験的なものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。

（注） 上記の表に記載されている試験的オプションに加えて、26 より大きいオプション番号を持つ TCP オプションは、試験的オプションと見なされます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:58 を有効にします。

廃止された TCP オプションを検知

廃止された TCP オプションが設定された TCP ヘッダーを検出します。これらのオプションは廃止されたものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。以下の表は、それらのオプションを示しています。

TCP オプション	説明
6	Echo
7	Echo Reply
16	Skeeter
17	Bubba

TCP オプション	説明
19	MD5 Signature
25	Unassigned（未定義）

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:57 を有効にします。

[T または TCP を検知（Detect T/TCP）]

CC.ECHO オプションが設定された TCP ヘッダーを検出します。CC.ECHO オプションは、TCP for Transactions（T/TCP）が使用されていることを確認します。T/TCP ヘッダー オプションは幅広く使用されていないため、一部のシステムでは考慮されず、悪用される恐れがあります。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:56 を有効にします。

[その他の TCP オプションを検知（Detect Other TCP Options）]

他の TCP デコード イベント オプションでは検出されない無効な TCP オプションが設定された TCP ヘッダーを検出します。たとえば、このオプションは、無効な長さ、またはオプション データが TCP ヘッダーに収まらない長さの TCP オプションを検出します。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。無効な TCP オプションを持つパケットは常にドロップされます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:54、116:55、および 116:59 を有効にできます。

[プロトコルヘッダの異常を検知（Detect Protocol Header Anomalies）]

より具体的な IP および TCP デコーダ オプションでは検出されない他のデコード エラーを検出します。たとえば、このデコーダは、不正な形式のデータ リンク プロトコル ヘッダーを検出する場合があります。

このオプションは、Firewall Threat Defense ルーテッド、トランスペアレント、およびインライン インターフェイスでは無視されます。ヘッダー異常があるパケットは常にドロップされます。ただし、このオプションは Threat Defense インライン タップおよびパッシブ インターフェイスに適用されます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、次のルールを有効にすることができます。

GID:SID	該当する場合にイベントを生成
116:467	パケットが Cisco FabricPath ヘッダーにカプセル化されるパケットの最小サイズより小さい。

GID:SID	該当する場合にイベントを生成
116:468	ヘッダーの Cisco メタデータ（CMD）フィールドに、有効な CMD ヘッダの最小サイズより小さいヘッダー長が含まれている。CMD フィールドは、Cisco TrustSec プロトコルと関連付けられています。
116:469	ヘッダーの CMD フィールドに、無効なフィールド長が含まれている。
116:470	ヘッダーの CMD フィールドに、無効なセキュリティ グループ タグ（SGT）オプションのタイプがあります。
116:471	ヘッダーの CMD フィールドに、値が予約されている SGT が含まれています。

その他のパケット デコーダ オプションに関連付けられていないパケット デコーダ ルールを有効にすることもできます。

関連トピック

定義済みデフォルト変数 （1409 ページ）

パケット復号化の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [パケット復号化（Packet Decoding）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [パケット復号（Packet Decoding）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 パケットデコーダオプション （2887ページ）で説明されているオプションを有効または無効にします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、パケット デコーダ ルール（GID 116）を有効にします。詳細については、侵入ルール状態の設定 （2032ページ）およびパケットデコーダオプション （2887ページ）を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤの基本 （2179 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

TCP ストリームの前処理

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

TCP プロトコルは、接続で生じ得るさまざまな状態を定義します。各 TCP 接続は、送信元と宛先の IP アドレス、および送信元と宛先のポートによって識別されます。TCP では、接続パラメータ値が同じ接続は、一度に 1 つしか存在できません。

状態に関連する TCP エクスプロイト

侵入ルールに `established` 引数と組み合わせた `flow` キーワードを追加すると、侵入ルール エンジンはステートフル モードでルールとフロー ディレクティブに一致するパケットを検査します。ステートフル モードでは、クライアントとサーバの間で正当な 3 ウェイ ハンドシェイクによって確立されたTCPセッションの一部となっているトラフィックだけが評価されます。

確立された TCP セッションの一部として識別できない TCP トラフィックをプリプロセッサが検出するようにシステムを設定することは可能です。しかし、このようなイベントは、システムをすぐに過負荷状態に陥らせ、しかも意味のあるデータを提供しないため、通常の使用法では推奨されません。

Stick や Snot などの攻撃では、システムの自身に対する広範なルール セットとパケット インスペクションを悪用します。これらのツールは、Snort ベースの侵入ルールのパターンに基づいてパケットを生成し、ネットワークに送信します。ステートフル インスペクションに対して設定するルールに `flow` または `flowbits` キーワードを含めなければ、パケットのそれぞれがルールをトリガーするため、システムが過負荷状態になります。ステートフル インスペクションを使用することで、確立された TCP セッションに含まれず、意味のある情報を提供しないこれらのパケットを無視できます。ステートフル インスペクションを実行すると、ルール エンジンは確立された TCP セッションに含まれる攻撃のみを検出するため、アナリストが stick や snot によって大量に生成されるイベントに時間を取られることがなくなります。

ターゲット ベースの TCP ポリシー

オペレーティング システムによって、TCP の実装方法は異なります。たとえば、セッションをリセットするために、Windowsやその他のオペレーティング システムの一部ではTCP リセットセグメントに正確なTCP シーケンス番号を割り当てる必要があるのに対し、Linuxや他のオペレーティング システムではシーケンス番号の範囲を使用できます。この例の場合、ストリーム プリプロセッサは、シーケンス番号に基づき、宛先ホストがリセットにどのように応答するかを正確に把握しなければなりません。ストリーム プリプロセッサがセッションの追跡を停止するのは、宛先ホストがリセットが有効であると見なした場合のみです。したがって、プリプロセッサがストリームの検査を停止した後は、パケットを送信することによって攻撃が検出を免れることはできません。TCP の実装方法の違いには、オペレーティング システムで TCP タイムスタンプ オプションを採用しているかどうか、採用している場合にはどのようにタイムスタンプを処理するか、そしてオペレーティング システムで SYN パケットのデータを受け入れるか、無視するかどうかも含まれます。

また、オーバーラップTCPセグメントを再構成する方法も、オペレーティングシステムによって異なります。オーバーラップ TCP セグメントは、確認応答済み TCP トラフィックの通常の再送信を反映する場合があります。あるいは、ホストのオペレーティングシステムを認識している攻撃者が、エクスプロイトの検出を免れるためにオーバーラップセグメントに不正なコンテンツを忍ばせて送信し、そのホストを悪用しようとしている場合もあります。ただし、モニター対象のネットワーク セグメント上で稼働するオペレーティング システムを認識するようにストリーム プリプロセッサを設定すれば、そのプリプロセッサがターゲット ホストと同じ方法でセグメントを再構成することによって、攻撃を識別できます。

モニター対象のネットワーク セグメント上のさまざまなオペレーティング システムに合わせてTCP ストリーム インスペクションおよび再構成を調整するために、1 つ以上の TCP ポリシーを作成することができます。ポリシーごとに、13 のオペレーティング システム ポリシーのうちの 1 つを特定します。異なるオペレーティング システムを使用するホストのいずれか、あるいはすべてを識別するために必要な数だけ TCP ポリシーを使用し、各 TCP ポリシーを特定の IP アドレスまたはアドレス ブロックにバインドします。デフォルトの TCP ポリシーは、他の TCP ポリシーで指定されていないモニタ対象ネットワーク上のすべてのホストに適用されます。したがって、デフォルトの TCP ポリシーに IP アドレスまたはアドレス ブロックを指定する必要はありません。

パッシブ展開で adaptive profile updates を使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、TCP ストリーム プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

TCP ストリームの再構成

ストリーム プリプロセッサは、TCP セッションでのサーバからクライアントへの通信ストリーム、クライアントからサーバへの通信ストリーム、またはその両方の通信ストリームに含まれるすべてのパケットを収集して再構成します。これにより、ルール エンジンは、特定のストリームに含まれる個々のパケットだけを検査するのではなく、ストリームを再構成された単一のエンティティとして検査できます。

ストリームの再構成により、ルールエンジンは、個々のパケットを検査する場合には検出できない可能性のあるストリームベースの攻撃を識別できます。ルールエンジンの再アセンブリ対象とする通信ストリームは、ネットワークのニーズに応じて指定できます。たとえば、Web サーバー上のトラフィックをモニターする際に、独自の Web サーバーから不正なトラフィックを受信する可能性がほとんどないため、クライアント トラフィックだけを検査するという場合もあります。

各 TCP ポリシーに、ストリーム プリプロセッサが再構成するトラフィックを識別するポートのカンマ区切りのリストを指定できます。adaptive profile updates が有効にされている場合、再構成するトラフィックを識別するサービスを、ポートの代わりとして、あるいはポートと組み合わせてリストすることもできます。

ポート、サービス、またはその両方を指定できます。クライアント ポート、サーバ ポート、またはその両方を任意に組み合わせた個別のポート リストを指定できます。また、クライアント サービス、サーバ サービス、またはその両方を任意に組み合わせた個別のサービス リストを指定することもできます。たとえば、以下を再構成する必要があるとします。

- クライアントからの SMTP（ポート 25）トラフィック
- FTP サーバ応答（ポート 21）
- 両方向の Telnet（ポート 23）トラフィック

この場合、以下のように設定できます。

- クライアント ポートとして、`23, 25` を指定
- サーバ ポートとして、`21, 23` を指定

あるいは、以下のように設定することもできます。

- クライアント ポートとして、25 を指定
- サーバー ポートとして、21 を指定
- 両方のポートとして、23 を指定

さらに、ポートとサービスを組み合わせた以下の設定例は、adaptive profile updates が有効にされている場合、有効になります。

- クライアント ポートとして、23 を指定
- クライアント サービスとして、smtp を指定
- サーバー ポートとして、21 を指定
- サーバー サービスとして、telnet を指定

ポートを否定すると（!80など）、そのポートのトラフィックがTCPストリームプリプロセッサで処理されなくなり、パフォーマンスが向上します。

all を引数として指定して、すべてのポートに対して再構成を指定することもできますが、ではポートを all に**設定しない**よう推奨しています。この設定では、このプリプロセッサで検査するトラフィックの量が増え、不必要にパフォーマンスが低下するためです。

TCP 再構成には、自動的かつ透過的にその他のプリプロセッサに追加するポートが含まれています。しかし、他のプリプロセッサの設定に追加した TCP 再構成リストにポートを明示的に追加する場合は、これらの追加したポートは通常処理されます。これには、次のプリプロセッサのポート リストが含まれています。

- FTP/Telnet（サーバ レベル FTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- Session Initiation Protocol
- POP
- IMAP
- SSL

追加のトラフィック タイプ（クライアント、サーバー、両方）を再構成すると、リソースの需要が増大することに注意してください。

TCP ストリームのプリプロセス オプション

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

次のグローバル TCP オプションを構成できます。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元ポートおよび宛先ポートの両方を any に設定した TCP ルールで、flow または flowbits オプションが使用されている場合を除き、有効化された侵入ルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、TCP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

TCP ポリシーごとに、以下のオプションを設定できます。

ネットワーク（Network）

TCP ストリーム再アセンブリ ポリシーを適用するホストの IP アドレスを指定します。

単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。

デフォルト ポリシーの default 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべて を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Policy

TCP ポリシーを適用するターゲット ホスト（複数可）のオペレーティング システムを識別します。[Mac OS] 以外のポリシーを選択すると、システムは同期（SYN）パケットからデータを削除し、ルール 129:2 に対するイベントの生成を無効にします。インライン正規化プリプロセッサの [SYN に関するデータを削除（Remove Data on SYN）] オプションを有効にすると、ルール 129:2 も無効になることに注意してください。

以下の表に、オペレーティング システム ポリシーとそれを使用するホスト オペレーティング システムをリストします。

表 *228 : TCP* オペレーティング システム ポリシー

ポリシー	オペレーティング システム
First	不明な OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD

ポリシー	オペレーティング システム
Linux	Linux 2.4 カーネル Linux 2.6 カーネル
Old Linux	Linux 2.2 以前のカーネル
Windows	Windows 98 Windows NT の場合 Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 以降
HPUX 10	HP-UX 10.2 以前
Mac OS	Mac OS 10（Mac OS X）

ヒント First オペレーティング システム ポリシーは、ホストのオペレーティング システムが不明な場合にはある程度の保護対策になります。ただし、攻撃を見逃す可能性もあります。オペレーティング システムが既知であれば、ポリシーを編集して、その正しいオペレーティング システムを指定してください。

Timeout

侵入ルール エンジンが非アクティブなストリームを状態テーブルで保持する秒数（1 ～ 86400 秒）。指定された期間内にストリームが再アセンブルされない場合、侵入ルールエンジンはそのストリームを状態テーブルから削除します。

（注） ネットワーク トラフィックがデバイスの帯域幅制限に到達しやすいセグメントに、管理対象デバイスが展開されている場合は、処理のオーバーヘッド量を削減するために、この値を大きい値（たとえば、600 秒）に設定することを検討してください。

Firewall Threat Defense デバイスはこのオプションを無視します。その代りに高度なおアクセス制御の **Threat Defense サービス ポリシー**の設定を使用します。詳細については、サービス ポリシー ルールの設定 （1924 ページ）を参照してください。

最大 TCP ウィンドウ（Maximum TCP Window）

受信側ホストで指定されている TCP ウィンドウの最大許容サイズを 1 ～ 1073725440 バイトの範囲で指定します。値を 0 に設定すると、TCP ウィンドウ サイズのチェックが無効になります。

⚠

注意 上限は RFC で許可される最大ウィンドウ サイズです。これは、攻撃者が検出を回避できないようにすることを目的としていますが、あまりにも大きな最大ウィンドウ サイズを設定すると、システム自体がサービス妨害を招く可能性があります。

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効になっている場合は、ルール 129:6 を有効にして、このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。

オーバーラップ範囲（Overlap Limit）

セッションで許容するオーバーラップ セグメントの数を 0（無制限）～ 255 の範囲で指定します。セッションで、この指定された値に達すると、セグメントの再構成が停止します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、それに付随するプリプロセッサ ルールが有効にされている場合、イベントも生成されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:7 を有効にします。

ファクタをフラッシュ（Flush Factor）

インライン展開では、ここで設定するサイズ減少なしのセグメントの数（1 ～ 2048）の後にサイズが減少したセグメントが検出されると、システムは検出用に累積されたセグメントデータをフラッシュします。値を 0 に設定すると、要求または応答の終わりを示す可能性のあるこのセグメント パターンの検出が無効になります。このオプションを有効にするには、インライン正規化の [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にする必要があることに注意してください。

ステートフル インスペクションの異常（Stateful Inspection Anomalies）

TCP スタックの異常な動作を検出します。付随するプリプロセッサ ルールが有効にされている場合、TCP/IP スタックが不完全に作成されていると、多数のイベントが生成される可能性があります。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 129:1 ～ 129:5
- 129:6（Mac OS のみ）
- 129:8 ～129:11
- 129:13 ～ 129:19

次の点に注意してください。

- ルール 129:6 でトリガーするには、さらに [最大 TCP ウィンドウ（Maximum TCP Window）] に 0 より大きい値を設定する必要があります。
- ルール 129:9 および 129:10 でトリガーするには、さらに [TCP セッションのハイジャック（TCP Session Hijacking）] を有効にする必要があります。

TCP セッションのハイジャック（TCP Session Hijacking）

スリーウェイ ハンドシェイク中に TCP 接続の両端から検出されたハードウェア（MAC）アドレスの有効性を、セッションで受信した後続のパケットに照合して検査することにより、TCP セッション ハイジャックを検出します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、2 つの対応するプリプロセッサ ルールのいずれかが有効にされている場合、接続のどちらかの側の MAC アドレスが一致しないと、システムがイベントを生成します。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 129:9 および 129:10 を有効にします。これらのルールのいずれかを使用してイベントを生成するには、[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] を有効にする必要があります。

連続した小型セグメント（Consecutive Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、連続する小さな TCP セグメントの許容数を 1 ～ 2048 の範囲で指定します。値を 0 に設定すると、連続する小さな TCP セグメントのチェックが無効になります。

このオプションは、[Small Segment Size] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。通常は、それぞれのセグメントの長さが 1 バイトであったとしても、ACK が介在することなく 2000 個もの連続するセグメントを受信することはないので注意してください。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 129:12 を有効にします。

小型セグメントのサイズ（Small Segment Size）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、小さいと見なされる TCP セグメントのサイズを 1 ～ 2048 バイトの範囲で指定します。値を 0 に設定すると、小さいセグメントのサイズの指定が無効になります。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションは、[連続する小さなセグメント（Consecutive Small Segments）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。2048 バイトの TCP セグメントは、標準的な 1500 バイトのイーサネット フレームより大きいことに注意してください。

小型セグメントを無視したポート（Ports Ignoring Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）]、[連続する小さなセグメント（Consecutive Small Segments）]、および [小さなセグメント サイズ（Small Segment Size）] が有効になっている場合は、小さい TCP セグメントの検出を無視する 1 つ以上のポートのカンマ区切りリストを指定します。このオプションを空白のままにすると、ポートはすべて無視されないように指定されます。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

リストには任意のポートを追加できますが、このリストが適用されるのは、TCP ポリシーの [ストリーム再構成を実行（Perform Stream Reassembly on）] ポート リストに指定されているポートのみです。

Require TCP 3-Way Handshake

TCP スリーウェイ ハンドシェイクの完了時に確立されたセッションだけを処理することを指定します。パフォーマンスを向上させ、SYN フラッド攻撃から保護し、部分的に非同期の環境での運用を可能にするには、このオプションを無効にします。確立された TCP セッションには含まれていない情報を送信して誤検出を発生させようとする攻撃を回避するには、このオプションを有効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:20 を有効にします。

3 ウェイ ハンドシェイク タイムアウト（3-Way Handshake Timeout）

[Require TCP 3-Way Handshake] が有効にされている場合、ハンドシェークを完了するまでの時間制限を 0（無制限）～ 86400 秒（24 時間）の範囲で指定します。このオプションの値を変更するには、[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] を有効にする必要があります。

Firepower ソフトウェア デバイスと Firewall Threat Defense インライン、インラインタップ、およびパッシブ インターフェイスの場合、デフォルトは 0 です。Firewall Threat Defense のルーティッド インターフェイスおよびトランスペアレント インターフェイスの場合、タイムアウトは常に 30 秒であり、ここで設定した値は無視されます。

パケット サイズ パフォーマンスの向上（Packet Size Performance Boost）

再アセンブリ バッファで大きいパケットをキューに入れないようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。1 ～ 20 バイトの小さなパケットを使用した検出回避の試行から保護するには、このオプションを無効にします。すべてのトラフィックが非常に大きなパケットからなるため、そのような攻撃は起こらないと確信できる場合は、このオプションを有効にします。

Legacy Reassembly

パケットを再構成する際に、廃止されたストリーム4プリプロセッサをエミュレートするようにストリーム プリプロセッサを設定します。これにより、ストリーム プリプロセッサで再構成されたイベントを、ストリーム4プリプロセッサで再構成された、同じデータ ストリームに基づくイベントと比較できます。

非同期ネットワーク（Asynchronous Network）

モニター対象ネットワークが非同期ネットワーク（システムにトラフィックの半分だけが見えるネットワーク）であるかどうかを指定します。このオプションを有効にすると、システムは TCP ストリームを再構成しないため、パフォーマンスが向上します。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

クライアント ポートでのストリーム再構成の実行（Perform Stream Reassembly on Client Ports）

接続のクライアント側のポートに基づくストリームの再アセンブリを有効にします。つまり、Web サーバー、メール サーバー、または一般に $HOME_NET で指定された IP アドレスによって定義されたその他の IP アドレスを宛先とするストリームが再アセンブルされます。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

クライアント サービスでのストリーム再構成の実行（Perform Stream Reassembly on Client Services）

接続のクライアント側のサービスに基づくストリームの再アセンブリを有効にします。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

選択するクライアント サービスごとに、1つ以上のクライアント ディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアント アプリケーションに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザー定義のディテクタをアプリケーションに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

サーバー ポートでのストリーム再構成の実行（Perform Stream Reassembly on Server Ports）

接続のサーバー側のポートに基づくストリームの再アセンブリのみを有効にします。つまり、Web サーバー、メール サーバー、または一般に $EXTERNAL_NET で指定された IP アドレスによって定義されたその他の IP アドレスから発信されたストリームが再アセンブリされます。サーバー側の攻撃を監視する必要がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

（注） サービスを徹底的に検査するには、Perform Stream Reassembly on Server Ports フィールドにポート番号を追加することに加えて、Perform Stream Reassembly on Server Services フィールドにサービス名を追加します。たとえば、HTTP サービスを検査するには、Perform Stream Reassembly on Server Ports フィールドにポート番号 80 を追加することに加えて、Perform Stream Reassembly on Server Services フィールドに **'HTTP'** サービスを追加します。

サーバー サービスでのストリーム再構成の実行（Perform Stream Reassembly on Server Services）

接続のサーバー側のサービスに基づくストリームの再アセンブリのみを有効にします。サーバー側の攻撃を監視する必要がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。サービスに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタを関連するアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザー定義のディテクタをアプリケーション プロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）

接続のクライアント側とサーバー側の両方のポートに基づくストリーム再構成を有効にします。同じポートで、不正なトラフィックがクライアントとサーバー間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

両方のサービスでのストリーム再構成の実行（Perform Stream Reassembly on Both Services）

接続のクライアント側とサーバー側の両方のサービスに基づくストリーム再構成を有効にします。同じサービスで、不正なトラフィックがクライアントとサーバー間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアントアプリケーションまたはアプリケーションプロトコルに対して有効になっているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションまたはアプリケーションプロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザー定義のディテクタをアプリケーションまたはアプリケーションプロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Firewall Threat Defense ルーテッドおよびトランスペアレントインターフェイスでは無視されます。

トラブルシューティング オプション：最大キューイング バイト（Troubleshooting Options: Maximum Queued Bytes）

トラブルシューティングについてサポートに問い合わせた際に、TCP 接続の片側でキューイングできるデータ量を指定するように指示されることがあります。値 0 は、無制限のバイト数を指定します。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響を与えるので、サポートからガイダンスを受けた場合にのみ変更してください。

Troubleshooting Options：Maximum Queued Segments

トラブルシューティングについてサポートに問い合わせた際に、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定するように指示されることがあります。値 0 は、無制限のデータ セグメント バイト数を指定します。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

関連トピック

ディテクタのアクティブおよび非アクティブの設定 （2653 ページ）
レイヤ管理 （2185 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

TCP ストリームの前処理の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

始める前に

- カスタム ターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、および VLAN のサブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2748 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 変更するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [TCPストリームの構成（TCP Stream Configuration）] 設定が無効になっている場合は、[有効化（Enabled）] をクリックして有効にします。

ステップ 6 [TCPストリームの構成（TCP Stream Configuration）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 [グローバル設定（Global Settings）] セクションの [パケット タイプ パフォーマンス ブースト（Packet Type Performance Boost）] チェックボックスをオンまたはオフにします。

ステップ 8 次の操作を実行できます。

- [ターゲット（Targets）] セクションの [ホスト（Hosts）] の横にある [追加（Add）] () をクリックします。[ホスト アドレス（Host Address）] フィールドに 1 つまたは複数の IP

アドレスを指定します。単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。作業が完了したら [OK] をクリックします。

- 既存のターゲットベースのポリシーの編集：[ホスト（Hosts）] の下で、編集するポリシーのアドレスをクリックするか、またはデフォルトの構成値を編集します。
- TCP ストリームの前処理オプションの変更：TCP ストリームのプリプロセス オプション（2895 ページ）を参照してください。

注意
サポートから指示がない限り、[最大キュー済みバイト（Maximum Queued Bytes）] または [最大キュー済みセグメント（Maximum Queued Segments）] を変更しないでください。

ヒント
クライアント サービス、サーバー サービス、またはその両方に基づくストリーム リアセンブル設定を変更するには、変更するフィールドの内側をクリックするか、そのフィールドの横にある [編集（Edit）] をクリックします。ポップアップ ウィンドウで矢印を使用して、サービスを [利用可能（Available）] リストと [有効化（Enabled）] リスト間で移動し、[OK] をクリックします。

- 既存のターゲットベースのポリシーの削除：削除するポリシーの横にある [削除（Delete）]（） をクリックします。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SMTP ストリーム プリプロセッサ ルール（GID 129）を有効にします。詳細については、侵入ルール状態の設定 （2032 ページ） および TCP ストリームのプリプロセス オプション（2895 ページ） を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤ管理 （2185 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）

UDP ストリームの前処理

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

UDP ストリームの前処理が行われるのは、ルール エンジンがパケットを処理するために使用する UDP ルールに、以下の引数のいずれかを使用した `flow` キーワードが含まれる場合です。

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDPデータ ストリームは一般に、セッションという観点で考慮されません。UDPはコネクションレス型プロトコルであり、2つのエンドポイントが通信チャネルを確立してデータを交換し、チャネルを終了する手段は提供していません。ただし、ストリームプリプロセッサは、カプセル化 IP データグラム ヘッダーの送信元および宛先 IP アドレス フィールドと、UDP ヘッダーのポート フィールドを使用して、フローの方向を判断し、セッションを識別します。セッションが終了するのは、設定可能なタイマーの時間を超えた場合、または一方のエンドポイントで、もう一方のエンドポイントが到達不能、あるいは要求されたサービスが利用不可という内容の ICMP メッセージを受け取った場合です。

システムは UDP ストリームの前処理に関連するイベントを生成しないことに注意してください。ただし、関連するパケット デコーダ ルールを有効にすることで、UDP プロトコル ヘッダーの異常を検出することができます。

関連トピック

TCP ヘッダー値とストリーム サイズ （2119 ページ）

UDP ストリームのプリプロセス オプション

Timeout

プリプロセッサが非アクティブなストリームを状態テーブルに保持する秒数を指定します。指定した時間内に追加のデータグラムが現れなかった場合、プリプロセッサはそのストリームを状態テーブルから削除します。

Firewall Threat Defense デバイスはこのオプションを無視します。その代りに高度なおアクセス制御の **Threat Defense サービス ポリシー**の設定を使用します。詳細については、サービス ポリシー ルールの設定 （1924 ページ）を参照してください。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元および宛先ポートの両方を `any` に設定した UDP ルールで `flow` または `flowbits` オプションが使用されている場合を除き、有効化されたルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、UDP トラフィックを無視するようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

関連トピック

TCP ヘッダー値とストリーム サイズ （2119 ページ）

UDP ストリームの前処理の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [UDP ストリームの構成（UDP Stream Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [UDPストリームの設定（UDP Stream Configuration）] の横にある[編集（Edit）]（）をクリックします。

ステップ 7 UDP ストリームのプリプロセス オプション （2906 ページ）で説明されているオプションを設定します。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

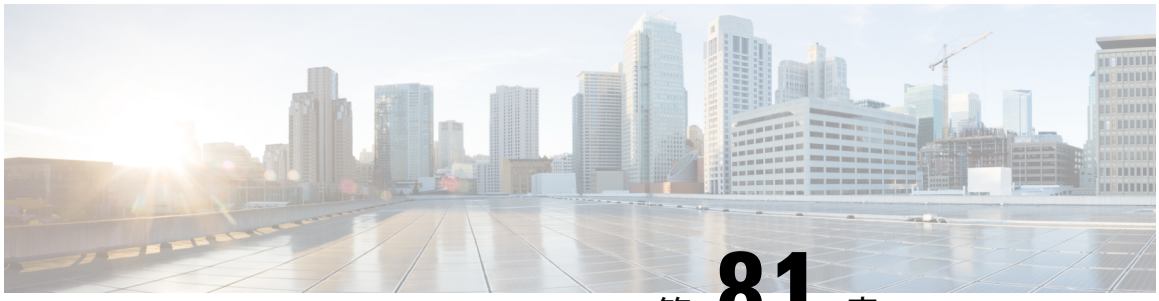
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、関連するパケット デコーダ ルール（GID 116）を有効にします。詳細については、「侵入ルール状態の設定 （2032ページ）」および「パケットデコーダ （2887ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

関連トピック

レイヤ管理 （2185 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー （1998 ページ）
TCP ヘッダー値とストリーム サイズ （2119 ページ）



第 81 章

特定の脅威の検出

次のトピックでは、特定の脅威を検出するためにネットワーク分析ポリシーでプリプロセッサを使用する方法について説明します。

- 特定の脅威の検出の概要 （2909 ページ）
- 特定の脅威の検出のライセンス要件 （2910 ページ）
- 特定の脅威の検出の要件と前提条件 （2910 ページ）
- Back Orifice の検出 （2910 ページ）
- ポートスキャン検出 （2912 ページ）
- レート ベースの攻撃防御 （2921 ページ）

特定の脅威の検出の概要

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニター対象ネットワークへの特定の攻撃、たとえば、Back Orifice 攻撃、複数のポートスキャン タイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃などを検出できます。プリプロセッサに固有の GID 署名が有効になっている場合、Web 上のネットワーク分析ポリシーは無効と表示されます。ただし、プリプロセッサは、使用可能なデフォルト設定を使用しているデバイスでオンになります。

侵入ポリシーで設定する機密データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

特定の脅威の検出のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

特定の脅威の検出の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

Back Orifice の検出

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Firepower システムは、Back Orifice プログラムの存在を検出するプリプロセッサを提供しています。Back Orifice プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。

Back Orifice 検出プリプロセッサ

Back Orifice プリプロセッサは、UDP トラフィックを分析し、Back Orifice マジック クッキー「*!*QWTY?」を調べます。このクッキーは、パケットの最初の 8 バイトにあり、XOR で暗号化されています。

Back Orifice プリプロセッサには設定ページがありますが、設定オプションはありません。Back Orifice プリプロセッサが有効になっていても、プリプロセッサ ルールを有効にしなければ、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *229 : Back Orifice GID:SID*

プリプロセッサ ルール **GID:SID**	説明
105:1	Back Orifice トラフィック検出
105:2	Back Orifice クライアント トラフィック検出
105:3	Back Orifice サーバー トラフィック検出
105:4	Back Orifice Snort バッファ攻撃検出

Back Orifice の検出

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [特定の脅威の検出（Specific Threat Detection）] の下の [Back Orifice の検出（Back Orifice Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

（注）
Back Orifice にユーザーが設定できるオプションはありません。

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、Back Orifice 検出ルール 105:1、105:2、105:3、または 105:4 を有効にします。詳細については、「侵入ルールの状態 （2031 ページ）」および「Back Orifice 検出プリプロセッサ （2910 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

ポートスキャン検出

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲットホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザーがネットワークで使用する可能性があるものもあります。Cisco のポートスキャン ディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性があるポートスキャンを判別できるように設計されています。

注目 内部リソースのデバイスの負荷分散試験。ポートスキャン検出が期待どおりに機能しない場合は、感度レベルを [高（High）] に設定する必要がある場合があります。

Snort 3 にアップグレードし、バージョン 7.2.0 で導入されたポートスキャン機能を使用することを強く推奨します。詳細については、Cisco Secure Firewall Management Center Snort 3 Configuration GuideおよびSnort 3 インスペクタリファレンスを参照してください。

ポートスキャン タイプ、プロトコル、フィルタリング感度レベル

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲットホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。

表 *230 :* プロトコル タイプ

プロトコル	説明
TCP	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、およびXmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。
UDP	UDP プローブを検出します。たとえば、ゼロ バイトの UDP パケットなどです。
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲットホストでサポートされている IP プロトコルを発見しようとするためのスキャンであるため、TCP スキャンおよびUDP スキャンとは異なります。

一般に、ターゲットホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。

表 *231 :* ポートスキャン タイプ

タイプ	説明
ポート スキャン検出	1 対 1 のポートスキャン。攻撃者が 1 つまたは少数のホストを使用して、単一のターゲット ホスト上の複数のポートをスキャンする場合です。 1 対 1 の ポートスキャンには次のような特徴があります。 • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン このオプションでは、TCP、UDP、および IP ポートスキャンが検出されます。
ポートスイープ	攻撃者が少数のホストを使用して、複数の対象ホスト上で 1 つのポートをスキャンする 1 対複数のポートスイープ。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン このオプションでは、TCP、UDP、ICMP、および IP ポートスイープが検出されます。
デコイ ポートスキャン	攻撃者がスプーフィングされた送信元 IP アドレスと実際にスキャンされた IP アドレスとを組み合わせた 1 対 1 ポートスキャン。 デコイ ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

タイプ	説明
分散型ポートスキャン	複数のホストが開いているポストに対して 1 つのホストをクエリする複数対 1 のポートスキャン。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

ポートスキャンディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバーに接続するときに、クライアントはサーバーのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバーをプローブする場合、そのサーバーがウェブ サービスを提供するかどうかを攻撃者があらかじめ知っていることはありません。ポートスキャンディテクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲット ホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャンディテクタは、選択された機密レベルに基づいてフィルタリングされた ポートスキャン イベントを生成することができます。

表 *232* : 感度レベル

レベル	説明
Low	ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。 このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。
Medium	ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。 [Ignore Scanned] フィールドにアクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。 このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。

レベル	説明
High	期間に基づいてポートスキャンが検出されます。したがって、時間ベースのポートスキャンを検出できます。ただし、このオプションを使用する場合は、[スキャン済みの無視（Ignore Scanned）] および [スキャナの無視（Ignore Scanner）] フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。 このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。

ポートスキャン イベント生成

ポートスキャン検出が有効の場合、さまざまなポートスキャンおよびポートスイープを検出するには、ジェネレータ ID（GID）122 および SID 1 ～ 27 の [Snort ID]（SID）によりルールを有効にする必要があります。

（注） イベントがポートスキャン接続ディテクタによって生成された場合、プロトコル番号は255に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、インターネット割り当て番号局（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

表 *233 :* ポートスキャン検出 *SID*（*GID 122*）

ポートスキャン タイプ	プロトコル	機密レベル	プリプロセッサ ルール SID
ポート スキャン検出	TCP	Low	1
	UDP	Medium または High	5
	ICMP	Low	21
	IP	Medium または High	イベントを生成しません。
		Low	イベントを生成しません。
		Medium または High	9
		Low	13
		Medium または High	

ポートスキャン タイプ	プロトコル	機密レベル	プリプロセッサ ルール SID
ポートスイープ	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	3、27 7 19 23 25 26 11 15
デコイ ポートスキャン	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	2 6 22 イベントを生成しません。 イベントを生成しません。 10 14
分散型ポートスキャン	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	4 8 20 24 イベントを生成しません。 イベントを生成しません。 12 16

ポートスキャン イベント パケット ビュー

関連するプリプロセッサ ルールを有効にすると、ポートスキャン ディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャン イベントのパケット ビューに表示される情報は、他のタイプの侵入イベントとは異なります。

侵入イベント ビューを出発点に、ポートスキャン イベントのパケット ビューまでドリルダウンします。各ポートスキャンイベントは複数のパケットに基づくため、単一のポートスキャンパケットをダウンロードすることはできません。ただし、ポートスキャンパケットビューで、使用可能なすべてのパケット情報を確認できます。

任意の IP アドレスをクリックしてコンテキスト メニューを表示し、[whois（whois）] を選択して、そのIPアドレスでルックアップを実行するか、[ホストプロファイルの表示（View Host Profile）] を選択して、そのホストのホスト プロファイルを表示できます。

表 *234 :* ポートスキャン パケット ビュー

情報	説明
デバイス	イベントを検出したデバイス。
時刻（Time）	イベントが発生した時刻。
Message	プリプロセッサによって生成されたイベント メッセージ。
送信元 IP	スキャン側ホストの IP アドレス。
Destination IP	スキャンされたホストの IP アドレス。
Priority Count	スキャンされたホストからの否定応答（TCP RST、ICMP 到達不能など）の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。
Connection Count	ホスト上でアクティブな接続数。この値は、TCP や IP などの接続ベースのスキャンより正確です。
IP カウント	スキャン対象のホストに接続するIPアドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、 3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。 プロキシやDNS サーバーなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
Scanner/Scanned IP Range	スキャン対象ホストまたはスキャン側ホスト（スキャンのタイプに依存）の IP アドレスの範囲。ポートスイープの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
Port/Proto Couont	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。

情報	説明
Port/Proto Range	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
Open Ports	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで1つ以上の開かれたポートが検出された場合にのみ表示されます。

ポートスキャン検出の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ポートスキャン検出の設定オプションを使用して、ポートスキャンディテクタによるスキャンアクティビティのレポート方法を微調整できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [設定（Settings）] をクリックします。

ステップ 5 [特定の脅威検出（Specific Threat Detection）] の下の [ポートスキャン検出（Portscan Detection）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [ポートスキャン検出（Portscan Detection）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 [プロトコル（Protocol）] フィールドで、有効にするプロトコルを指定します。

（注）
TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることを確認する必要があります。

ステップ 8 [スキャンタイプ（Scan Type）] フィールドで、検出するポートスキャンタイプを指定します。

ステップ 9 [重要度レベル（Sensitivity Level）] リストからレベルを選択します。ポートスキャンタイプ、プロトコル、フィルタリング感度レベル （2913 ページ）を参照してください。

ステップ 10 特定のホストのポートスキャン アクティビティのサインをモニターする場合は、[IP の監視（Watch IP）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。すべてのネットワーク トラフィックを監視するには、フィールドを空白のままにします。

ステップ 11 ホストをスキャナとして無視するには、[スキャナの無視（Ignore Scanners）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ステップ 12 ホストをスキャンのターゲットとして無視するには、[スキャン対象の無視（Ignore Scanned）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ヒント
特にアクティブなネットワーク上のホストを示すには、[スキャナの無視（Ignore Scanners）] と [スキャン対象の無視（Ignore Scanned）] を使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

ステップ 13 ミッドストリームでピックアップされたセッションのモニタリングを中断するには、[ACK スキャンの検出（Detect Ack Scans）] チェックボックスをオフにします。

（注）
ミッドストリームセッションの検出はACKスキャンの識別に役立ちますが、大量のトラフィックとパケットのドロップが発生するネットワークでは、誤ってイベントが生成される可能性があります。

ステップ 14 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- さまざまなポートスキャンおよびポートスイープを検出するためにポートスキャン検出を行う場合は、ルール 122:1 ～ 122:27 を有効にします。詳細については、「侵入ルールの状態（2031 ページ）」および「ポートスキャン イベント生成（2916 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

レート ベースの攻撃防御

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

レート ベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レート ベースの検出基準を使用することで、レート ベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の検出設定に戻すことができます。

レート ベース フィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インライン モードで展開されている管理対象デバイスでこの機能を使用すると、指定の期間だけレートベース攻撃をブロックし、その後イベントだけを生成してトラフィックをドロップしない状態に戻せます。

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1 つの IP アドレスからの SYN パケットの最大許容数を設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

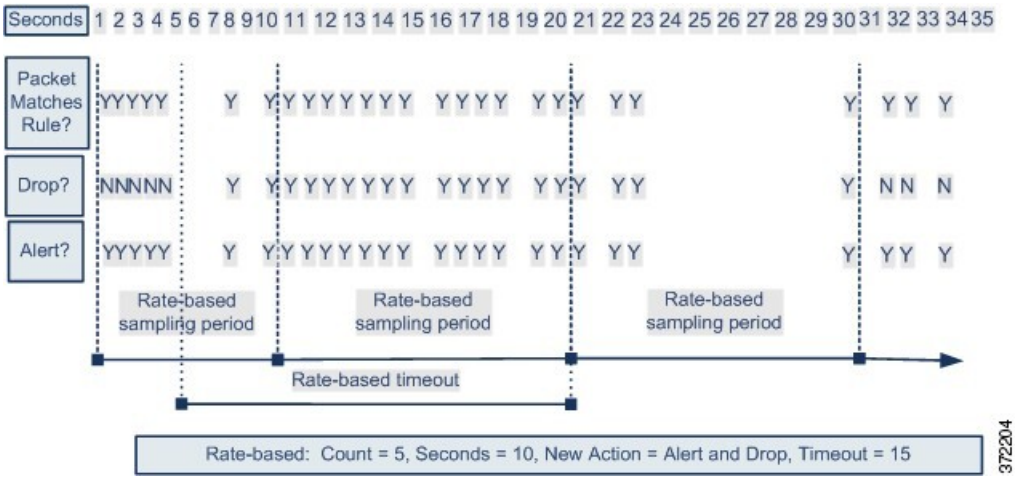
ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス妨害（DoS）攻撃や、ユーザーによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レート ベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

たとえば、1 つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

（注） デバイスは、内部リソースにインスペクションの負荷を分散させます。レート ベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。ユーザーにより規定の時間間隔内に送信された接続試行が多すぎると、アラートがトリガーされます。そのため、ルールをレート制限することを推奨します。正しいレートを決定する際に支援が必要な場合は、サポートに連絡してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値を超えている場合は、新しいアクションが続行されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



関連トピック

動的侵入ルール状態 （2040 ページ）

レート ベースの攻撃防御の例

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レート ベースの攻撃防御は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

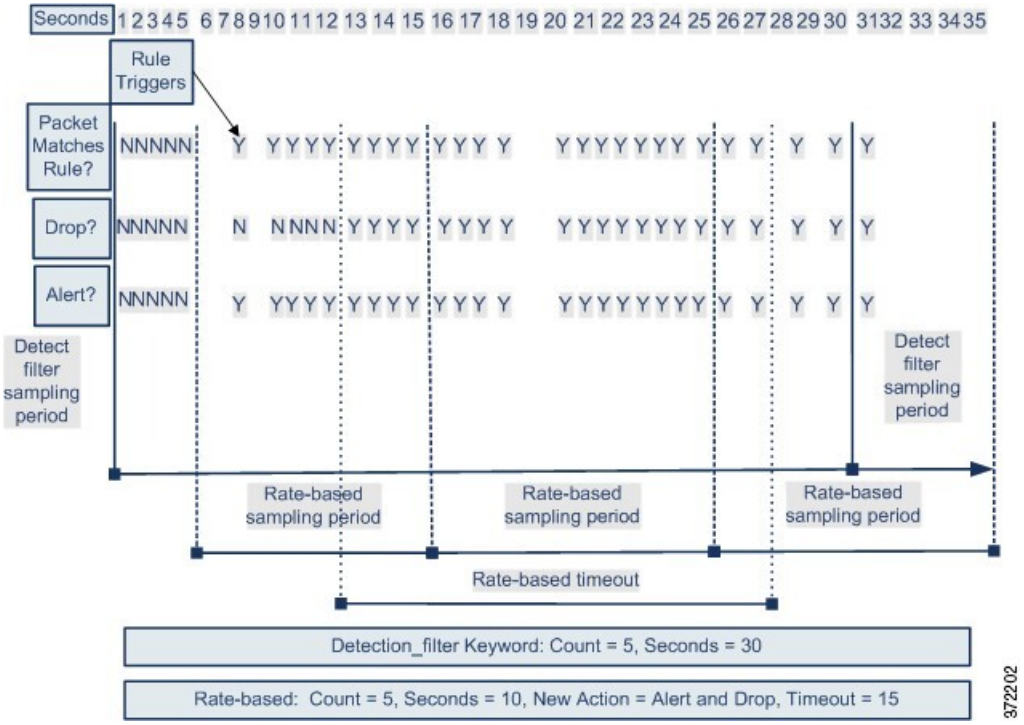
detection_filter キーワード、しきい値構成または抑制、およびレートベースの基準のすべてが同じトラフィックに適用される場合もあります。抑制をルールに適用すると、レートベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

detection_filter キーワードの例

以下に、攻撃者がブルートフォースログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された detection_filter キーワードも含むルールがトリガーされます。このルールには、レートベース攻撃防止が設定されています。10 秒以内にルールに 5 回ヒットすると、レートベースの設定により、ルール属性が 20 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベントは生成されません。それは、レートが detection_filter キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レートベースの基準によって新しいアクション [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。

レートベースの基準に一致すると、イベントが生成されて、パケットがドロップされます。これは、レートベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続きます。20 秒が経過すると、レートベース アクションがタイムアウトになります。タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レートベースのアクションは続行されます。



この例には示されていませんが、[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を `detection_filter` キーワードと組み合わせて使用することで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができることにも注意してください。ルールにレート ベースの設定を使用するかどうかを決定する際は、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合の結果と `detection_filter` キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。

関連トピック

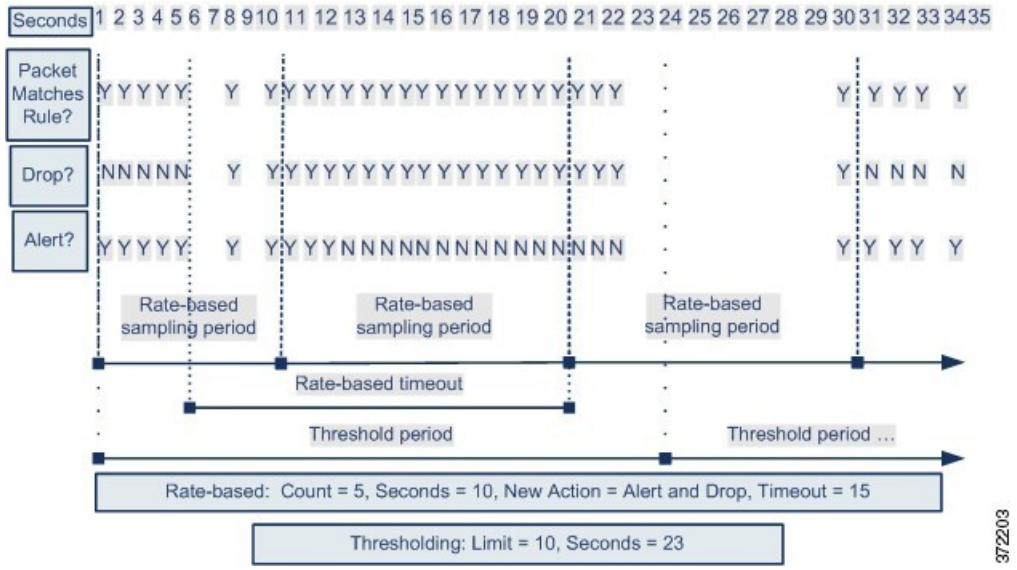
侵入ルールの状態 （2031 ページ）

ダイナミック ルール状態のしきい値構成または抑制の例

以下に、攻撃者がブルート フォース ログインを仕掛ける例を示します。パスワードを特定する試みが繰り返されると、レートベースの攻撃防止が設定されているルールがトリガーされます。10 秒以内にルールに 5 回ヒットすると、レートベースの設定により、ルール属性が 15 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が 23 秒間で 10 に制限されます。

図に示されているように、最初の 5 個のパケットが一致すると、ルールはイベントを生成します。5 個のパケットがルールに一致した後、レートベースの基準が新しいアクションとして [ドロップしてイベントを生成する（Drop and Generate Events）] をトリガーし、次の 5 個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。新しいアクションが元の [Generate Events] アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



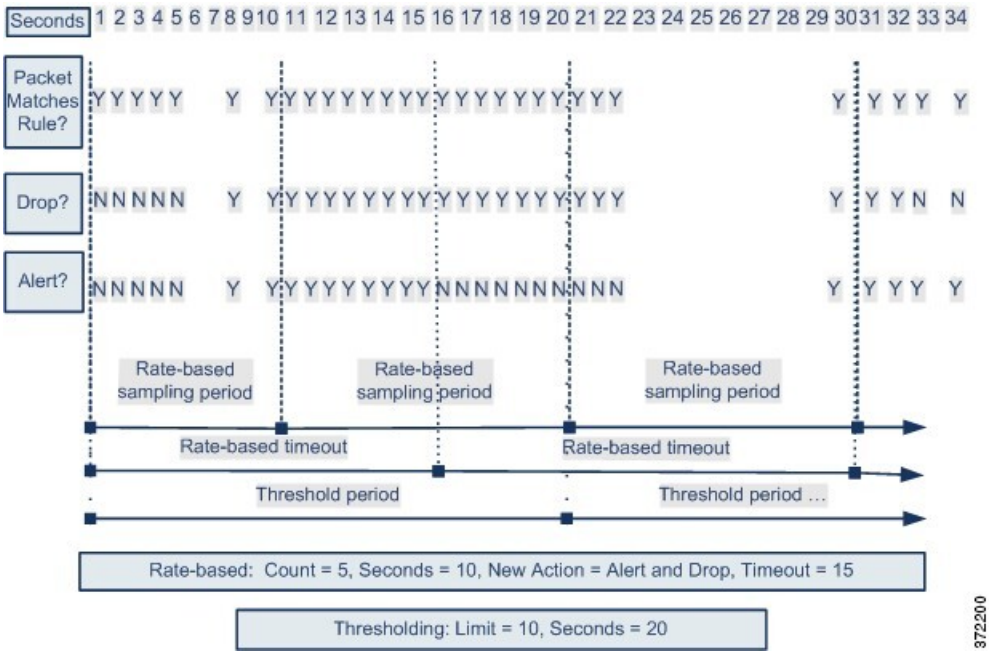
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [イベントを生成する（Generate Events）] から [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す11番目のイベントを生成します。

ポリシー全体のレート ベース検出としきい値構成または抑制の例

以下に、ネットワーク上のホストに対して、攻撃者がサービス妨害（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の [同時接続の制御（Control Simultaneous Connections）] 設定がトリガーされます。この設定は、1 つの送信元からの接続数が 10 秒間で 5 つに達すると、イベントを生成して悪意のあるトラフィックをドロップします。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が 20 秒間で 10 件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の 10 個のパケットに対してイベントが生成され、トラフィックがドロップされます。10個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レートベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レート ベース アクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



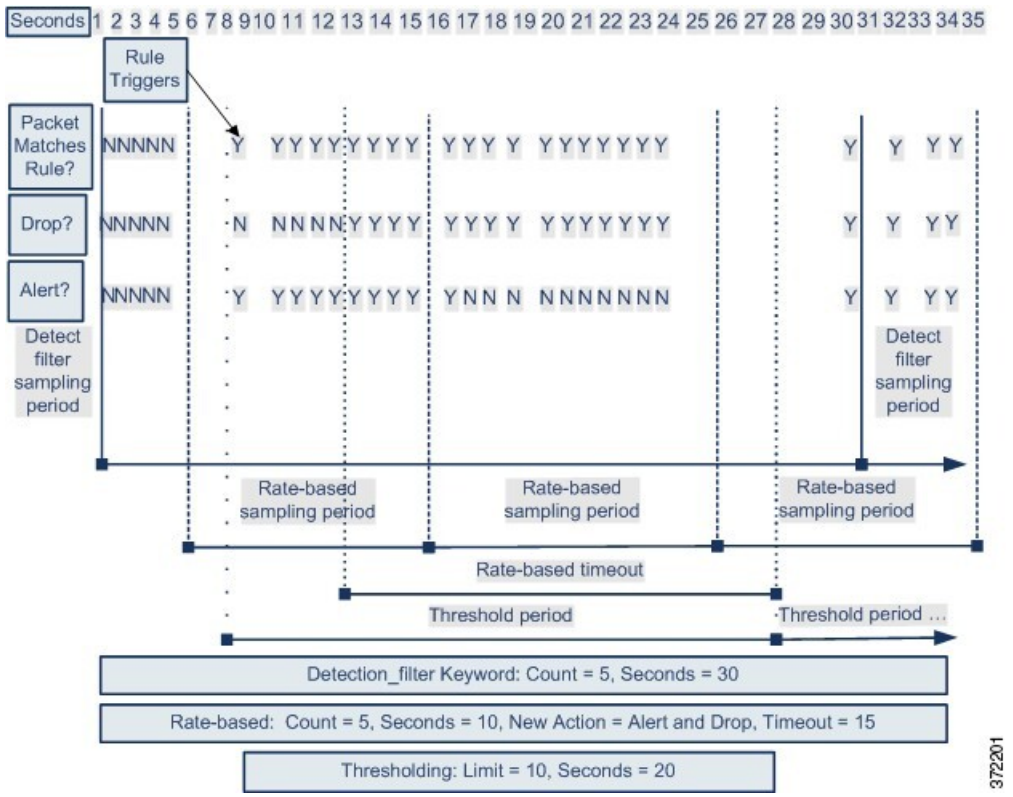
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

複数のフィルタリング方法によるレート ベース検出の例

以下に、攻撃者がブルートフォース ログインを仕掛ける例で、`detection_filter` キーワード、レートベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードを含むルールがトリガーされます。このルールには、レート ベースの攻撃防御も設定されています。その設定では、15 秒間にルールのヒット数が 5 に達すると、ルール属性が 30 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは 30 秒間で 10 件に制限されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベント通知は行われません。それは、`detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。レート ベースの基準が満たされると、システムは 11 個目から 15 個目のパケットに対してイベントを生成し、パケットをドロップします。15 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

レート ベースのタイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。



レート ベースの攻撃防御オプションと設定

レート ベース攻撃の防御では、異常なトラフィック パターンを識別して、そのトラフィックが正当な要求に与える影響を最小限に抑えるようにします。一般に、レートベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックに、ネットワーク上のホストに対して過剰な未完了接続が含まれています。これは、SYN フラッド攻撃を意味します。
- 任意のトラフィックには、ネットワーク上のホストに対して過剰な接続が含まれています。これは、TCP/IP 接続フラッド攻撃を意味します。
- 1 つ以上の特定の宛先 IP アドレスへのトラフィック、または 1 つ以上の特定の送信元 IP アドレスからのトラフィックで、ルールとの一致が過剰に発生します。
- すべてのトラフィックで、特定のルールとの一致が過剰に発生します。

ネットワーク分析ポリシーでは、ポリシー全体に対して SYN フラッドまたは TCP/IP 接続フラッドのいずれかの検出を設定することができます。または個々の侵入ルールもしくはプリプロセッサ ルールに対してレート ベース フィルタを設定できます。GID 135 ルールに手動でレート ベース フィルタを追加すること、またはルールの状態を変更することはできない点に注意してください。GID 135 のルールでは、クライアントを送信元の値、サーバーを宛先の値として使用します。

[SYN攻撃防止（SYN Attack Prevention）] が有効になっている場合、定義されたレート条件を超えるとルール 135:1 がトリガーされます。

[同時接続の制御（Control Simultaneous Connections）] が有効になっている場合、定義されたレート条件を超えるとルール 135:2 がトリガーされ、セッションがクローズまたはタイムアウトするとルール 135:3 がトリガーされます。

（注） デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。ユーザーにより規定の時間間隔内に送信された接続試行が多すぎると、アラートがトリガーされます。そのため、ルールをレート制限することを推奨します。正しいレートを決定する際に支援が必要な場合は、サポートに連絡してください。

各レート ベース フィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルール ベースの送信元/宛先の設定の場合、ネットワーク アドレスの指定
- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超過した場合に実行する新しいアクション

  ポリシー全体に対してレート ベースを設定すると、システムはレート ベース攻撃を検出した時点でイベントを生成します。インライン展開では、トラフィックをドロップすることもできます。個々のルールにレート ベース アクションを設定する場合は、[イベントの生成（Generate Events）]、[イベントのドロップと作成（Drop and Generate Events）]、[無効（Disable）] の 3 つの利用可能なアクションから選択できます。
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定が使用されていない場合、ルールが [イベントの生成（Generate Events）] に設定されていればイベントが生成されますが、そのルールのパケットがドロップされることはありません。ただし、攻撃トラフィックが、レートベースの基準が設定されているルールに一致した場合、それらのルールが当初 [イベントのドロップおよび生成（Drop and Generate Events）] に設定されていないとしても、レート アクションがアクティブである期間は、パケットがドロップされる場合があります。

（注） レート ベース アクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。ただし、ポリシー レベルでレート ベース フィルタを設定すると、指定した期間内の過剰な数のSYNパケットまたはSYN/ACKインタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに複数のレート ベース フィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベース フィルタ アクションが競合する場合は、最初のレート ベース フィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレート ベース フィルタと個々のルールに設定されたレート ベース フィルタが競合する場合は、ポリシー全体のレート ベース フィルタが優先されます。

関連トピック

[ルール（Rule）] ページからの動的ルール状態の設定 （2042 ページ）

レートベースの攻撃防御、検出フィルタリング、しきい値処理または抑制

キーワード `detection_filter` により、ルールに一致するしきい値が指定の時間内に発生するまで、ルールのトリガーを阻止します。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

しきい値処理と抑制を用いて、ルール、送信元または宛先に関するイベント通知数を制限することまたはそのルールをすべて一緒に通知を抑制することで、過剰なイベントを低減できます。また、オーバーライドする特定のしきい値がない各ルールに適用するグローバル ルールのしきい値を設定できます。

ルールに抑制を提供する場合、ポリシー全体またはルールにより指定されたレート ベースの設定であるため、レート ベースでアクションの変更が発生した場合でも、システムは、すべての適用可能な IP アドレスのそのルールのイベント通知を抑制します。

関連トピック

侵入イベントしきい値 （2033 ページ）
侵入ポリシー抑制の設定 （2037 ページ）
グローバル ルールのしきい値の基本 （2219 ページ）

レートベース攻撃防止の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ポリシー レベルでレートベース攻撃防止を設定することで、SYN フラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（注）
カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [設定（Settings）] をクリックします。

ステップ 5 [特定の脅威検出（Specific Threat Detection）] の下の [レートベース攻撃防止（Rate-Based Attack Prevention）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [レートベース攻撃防止（Rate-Based Attack Prevention）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 7 次の 2 つの選択肢があります。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN 攻撃の防止（SYN Attack Prevention）] の下にある [追加（Add）] をクリックします。
- 過剰な数の接続を防ぐには、[同時接続の制御（Control Simultaneous Connections）] の下にある [追加（Add）] をクリックします。

ステップ 8 トラフィックを追跡する方法を指定します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [送信元（Source）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。
- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [宛先（Destination）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

（注）
- すべてのサブネットまたは IP をモニターするために、[ネットワーク（Network）] フィールドに IP アドレス 0.0.0.0/0 を入力しないでください。システムは、（通常、

すべてのサブネットまたは IP を識別するために使用される）この IP アドレスをレートベースの攻撃防御ではサポートしていません。

- システムは、[ネットワーク（Network）] フィールドに含まれる各 IP アドレスのトラフィックを個別に追跡します。ある特定の IP アドレスからの設定されたレートを超過するトラフィックがある場合、その IP アドレスに関するイベントだけが生成されることになります。例として、ネットワーク設定で `10.1.0.0/16` の送信元 CIDR ブロックを設定し、10 個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21 から 8 つの接続が開始され、10.1.5.10 から 6 つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21 から 11 個の同時接続が開始されている場合、システムは 10.1.4.21 からの接続に対してだけイベントを生成します。

ステップ 9 レート追跡設定をトリガーとして使用するレートを指定します。

- SYN 攻撃に対する構成の場合は、[レート（Rate）] フィールドに、一定の秒数あたりの SYN パケット数を入力します。
- 同時接続に対する構成の場合は、[カウント（Count）] フィールドに、接続数を入力します。

デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。ユーザーにより規定の時間間隔内に送信された接続試行が多すぎると、アラートがトリガーされます。そのため、ルールをレート制限することを推奨します。正しいレートの決定する方法については、サポートに問い合わせてください。

ステップ 10 レートベース攻撃防止設定に一致するパケットをドロップするには、[ドロップ（Drop）]チェックボックスをオンにします。

ステップ 11 [タイムアウト（Timeout）] フィールドに、イベント生成のタイムアウト期間を入力します。この期間を経過すると、SYN または同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

注意
インライン展開では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

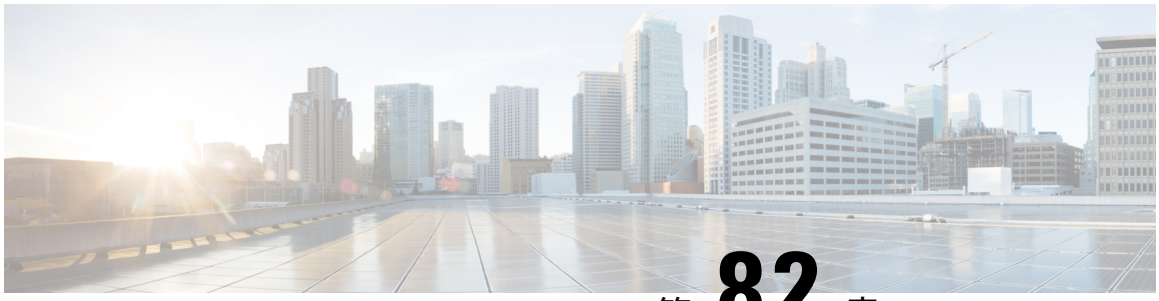
ステップ 12 [OK] をクリックします。

ステップ 13 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。



第 82 章

アダプティブ プロファイル

ここでは、適応型プロファイルの設定方法について説明します。

- アダプティブ プロファイルについて （2933 ページ）
- アダプティブプロファイルのライセンス要件 （2934 ページ）
- アダプティブプロファイルの要件と前提条件 （2934 ページ）
- アダプティブプロファイルの更新 （2934 ページ）
- アダプティブプロファイルの更新とシスコの推奨ルール （2935 ページ）
- 適応型プロファイルのオプション （2936 ページ）
- 適応型プロファイルの設定 （2937 ページ）

アダプティブ プロファイルについて

次のことを行うには、アダプティブプロファイルを有効にする必要があります。

- マルウェア保護（AMP）を含むアプリケーションとファイルの制御を実行し、侵入ルールがサービスメタデータを使用できるようにします。

⚠

注意 アクセスコントロールルールでマルウェア防御（AMP）を含むアプリケーション/ファイル制御を実行し、侵入ルールでサービスメタデータを使用するためには、適応型プロファイルの設定 （2937 ページ）の説明に従ってアダプティブプロファイルを有効（デフォルトの状態）にする**必要があります**。

- パッシブ展開では、アダプティブプロファイルの更新を有効にして、宛先ホストのオペレーティング システムに従って IP トラフィックに最適化とリアセンブルを行います。

（注） インライン展開では、アダプティブプロファイルの更新を有効にする代わりに、インライン正規化プリプロセッサを設定し、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にすることを推奨します。

アダプティブプロファイルのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

アダプティブプロファイルの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

アダプティブプロファイルの更新

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。adaptive profile updatesでは、ネットワーク検出で検出したホスト情報またはサードパーティからインポートしたホスト情報に合わせて、システムが処理動作を変更します。

Profile updatesは、ネットワーク分析ポリシーに手動で設定可能なターゲットベース プロファイルと同様に、ターゲット ホストのオペレーティング システムと同じ方法で、IP パケットの最適化およびストリームのリアセンブルを行うのに役立ちます。その後、侵入ルールエンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

手動で設定されたターゲットベースのプロファイルは、選択したデフォルトのオペレーティング システムか固有のホストに構築したプロファイルのいずれかに適用されます。ただし、Profile updatesは、ターゲット ホストのホスト プロファイルのオペレーティング システムに基づいて適切なオペレーティング システム プロファイルに切り替わります。

10.6.0.0/16 サブネット向けにprofile updatesを設定し、Linux にデフォルトの IP 最適化ターゲットベース ポリシーを設定するシナリオを考えてみます。設定を構成する Firewall Management Center には 10.6.0.0/16 サブネットを含むネットワーク マップがあります。

- システムが 10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲットベース ポリシーを使用して IP フラグメントのリアセンブルを行います。
- システムが 10.6.0.0/16 サブネット上にあるホスト B からのトラフィックを検出すると、ネットワーク マップからホスト B のオペレーティング システム データを取得します。システムは、このオペレーティング システムに基づいたプロファイルを使用し、ホスト B を宛先とするトラフィックを最適化します。

アダプティブプロファイルの更新とシスコの推奨ルール

adaptive profile updates機能は、アクセス コントロール ポリシーの詳細設定で、そのアクセス コントロールポリシーによって呼び出されるすべての侵入ポリシーにグローバルに適用されます。シスコの推奨ルール機能は、設定する個々の侵入ポリシーに適用されます。

シスコの推奨ルールと同様に、profile updatesはルールのメタデータをホスト情報と比較し、ルールを特定のホストに適用すべきかどうかを判別します。ただし、シスコの推奨ルールがその情報を使用してルールの有効化または無効化を行うための推奨事項を提供するのに対して、profile updatesはその情報を使用して特定のトラフィックに特定のルールを適用します。

シスコの推奨ルールでは、提案された変更をルール状態に実装するために、ユーザーの対話が必要になります。一方、Profile updates は侵入ポリシーを変更しません。プロファイル更新に基づくルールの処理は、パケット単位で行われます。

さらに、シスコの推奨ルールでは、結果として、無効化されたルールを有効にできます。これに対して、Profile updates では、侵入ポリシーですでに有効になっているルールの適用のみに影響を与えます。Profile updates はルール状態を変更することはありません。

profile updatesとシスコの推奨ルールは組み合わせて使用できます。侵入ポリシーを展開すると、Profile updatesはルールの状態を使用して適用の候補に含めるかどうかを判別し、推奨事項の承認または拒否はそのルール状態に反映されます。両方の機能を使用して、監視対象の各ネットワークに最適なルールを有効化または無効化することができ、特定のトラフィックに対する有効化したルールの適用を最も効率的に行うことができます。

関連トピック

シスコ推奨ルールについて （2197 ページ）

適応型プロファイルのオプション

有効（Enable）

このオプションを有効にする必要があるのは、次の場合です。

- アクセスコントロールルールでマルウェア保護（AMP）を含めたアプリケーションとファイルの制御を実行する
- 侵入ルールでサービス メタデータを使用する

このオプションは、デフォルトで有効です。

（注） Snort 3 でアダプティブプロファイルを有効にするには、[有効化（Enable）] オプションと [プロファイル更新の有効化（Enable Profile Updates）] オプションの両方を選択する必要があります。

プロファイルの更新を有効にする（Enable Profile Updates）

パッシブ展開で、プロファイルの更新を有効にして、ネットワーク マップでホストが使用するオペレーティング システムのプロファイルに応じて IP トラフィックがデフラグおよびリアセンブルされるようにします。

Snort 3 でアダプティブプロファイルが有効になっている場合は、これを有効にする必要があります。

アダプティブ プロファイル - 属性の更新間隔（Adaptive Profiles - Attribute Update Interval）

プロファイルの更新を有効にすると、Firewall Management Center から管理対象デバイスに対するネットワーク マップ データの同期の頻度を分単位で制御することができます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。このオプションの値を大きくすると、大規模なネットワークでパフォーマンスを向上させることができます。

アダプティブ プロファイル - ネットワーク（Adaptive Profiles - Networks）

任意で、プロファイルの更新を有効にすると、IP アドレス、アドレス ブロック、およびネットワーク変数のカンマ区切りリストに対する profile updates を制限して、パフォーマンスを向上させることができます。ネットワーク変数を使用すると、アクセス コントロール ポリシーのデフォルトの侵入ポリシーにリンクされている変数セットの変数の値が使用されるようになります。たとえば、**192.168.1.101**、**192.168.4.0/24**、**$HOME_NET** というように入力することができます。IPv4 と IPv6 がサポートされます。

デフォルト値（`0.0.0.0/0`）は、すべてのネットワークにアダプティブプロファイルの更新を適用します。

関連トピック

トラフィック識別の前に通過するパケットのインスペクション （2746 ページ）
変数セット （1406 ページ）

適応型プロファイルの設定

パッシブ展開では、adaptive profile updatesを設定することをお勧めします。インライン展開の場合、インライン正規化プリプロセッサの設定で [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にします。

注意 アクセス コントロール ルールが AMP を含むアプリケーション制御およびファイル制御を行い、侵入ルールがサービス メタデータを使用するためには、この手順で説明されているように、アダプティブ プロファイルが**必ず**有効になっている（デフォルト状態）必要があります。

始める前に

アクセス コントロール ポリシーには、ホスト/サービスの検出を実行できるように有効になっている、ネットワーク検出ポリシーが必要です。または、ホストデータをサードパーティのソースからインポートする必要があります。

手順

ステップ 1 アクセス制御ポリシーエディタで、変更するポリシーの [編集（Edit）]（ ） をクリックします。

ステップ 2 **[詳細（More）] > [詳細設定（Advanced Settings）]** の順にクリックし、[検出拡張の設定（Detection Enhancement Settings）] セクションの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 適応型プロファイルのオプション （2936ページ）の説明に従って適応型プロファイルのオプションを設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

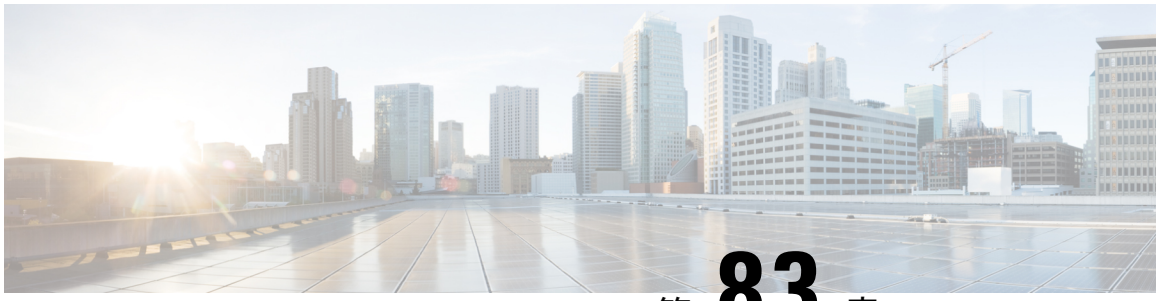
関連トピック

インライン正規化プリプロセッサ （2872 ページ）
Snort 再起動のシナリオ （162 ページ）

第 XV 部

Threat Intelligence Director

• Secure Firewall Threat Intelligence Director （2941 ページ）



第 83 章

Secure Firewall Threat Intelligence Director

この章のトピックでは、Threat Intelligence Director を設定および使用する方法について説明します。

- Secure Firewall Threat Intelligence Director の概要 （2941 ページ）
- Threat Intelligence Director の要件と前提条件 （2944 ページ）
- Threat Intelligence Director のセットアップ方法 （2947 ページ）
- Threat Intelligence Director インシデントおよびオブザベーション データの分析 （2958 ページ）
- Threat Intelligence Director 設定の表示および変更 （2975 ページ）
- Threat Intelligence Director のトラブルシューティング （2994 ページ）
- Threat Intelligence Director の履歴 （2996 ページ）

Secure Firewall Threat Intelligence Director の概要

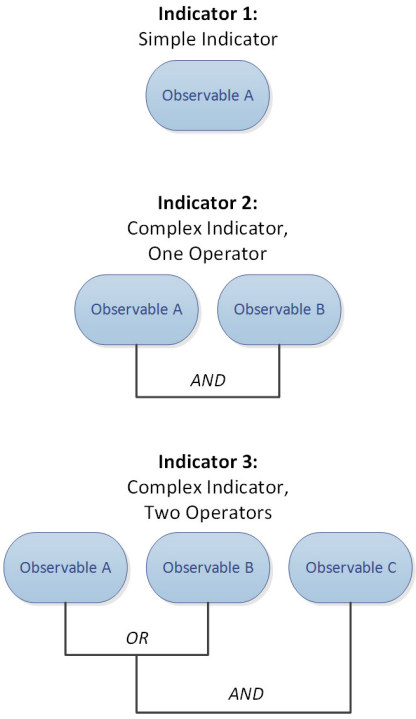
Secure Firewall Threat Intelligence Director は脅威インテリジェンス データを操作可能にし、インテリジェンスデータの集約、防衛アクションの設定、環境内の脅威の分析を支援します。この機能は、Firepower の他の機能を補完するもので、脅威に対する追加の防衛線を提供します。

Threat Intelligence Director をホスティング プラットフォームに設定すると、脅威インテリジェンス ソースからデータが取り込まれ、設定されたすべての管理対象デバイス（要素）にそのデータが公開されます。このリリースでサポートされているホスティングプラットフォームと要素の詳細については、プラットフォーム、要素、およびライセンスに関する要件 （2945 ページ） を参照してください。

ソースには、オブザーバブルを含むインジケータが含まれています。インジケータは、脅威に関連するすべての特性を伝達し、個々のオブザーバブルは、その脅威に関連付けられた個々の特性（例えば、SHA-256 値）を表します。単純なインジケータには単一のオブザーバブルが含まれ、複合インジケータには 2 つ以上のオブザーバブルが含まれます。

オブザーバブルとそれらの間の AND/OR 演算子は、次の例に示すように、インジケータのパターンを形成します。

図 *321* : 例：インジケータ パターン



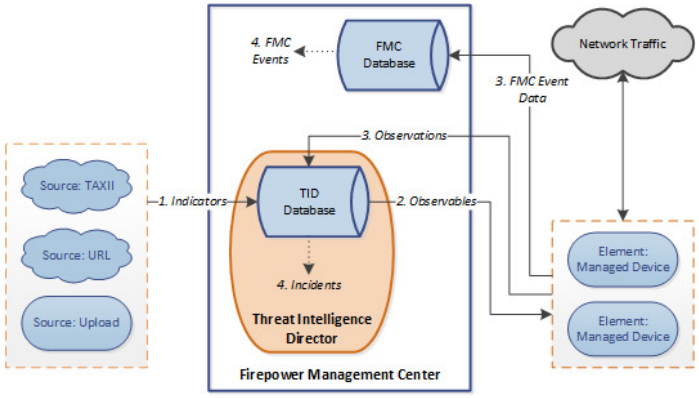
オブザーバブルが要素に公開された後、要素はトラフィックをモニタし、システムがトラフィック内のオブザーバブルを識別すると、Firewall Management Center にオブザベーションを報告します。

Firewall Management Center は、すべての要素からのオブザベーションを収集し、Threat Intelligence Director インジケータに対してオブザベーションを評価して、オブザーバブルの親インジケータに関連付けられたインシデントを生成または更新します。

インシデントは、インジケータのパターンが満たされたときに完全に実現されます。トラフィックがインジケータ内の 1 つまたは複数のオブザーバブルに一致するが、パターン全体では一致しない場合、インシデントは部分的に実現されます。詳細については、監視とインシデント生成 （2958 ページ）を参照してください。

次の図に、サンプルのシステム構成におけるデータフローを示します。

図 *322 : Firewall Management Centerデータ フロー*



Threat Intelligence Director インシデントが完全または部分的に実現されると、システムは設定されたアクション（モニタ、ブロック、部分的なブロック、またはアクションなし）を実行します。詳細については、「アクションに影響を与える要因（2968 ページ）」を参照してください。

Threat Intelligence Director およびセキュリティ インテリジェンス

アクセス コントロール ポリシーの一部として、セキュリティ インテリジェンスではレピュテーション インテリジェンスを使用して、IP アドレス、URL、およびドメインとの間の接続をすばやくブロックします。セキュリティ インテリジェンスは、Talos インテリジェンス グループからの業界をリードする脅威インテリジェンスへのアクセスを一意に提供します。セキュリティ インテリジェンスの詳細については、セキュリティ インテリジェンスについて（1851 ページ）を参照してください。

Threat Intelligence Director は、サードパーティのソースからのセキュリティ インテリジェンスに基づいて接続をブロックするシステムの機能を次のように拡張します。

- **Threat Intelligence Director は、追加のトラフィック フィルタリング基準をサポート**：セキュリティ インテリジェンスは、IP アドレス、URL、および（DNS ポリシーが有効な場合は）ドメイン名に基づいてトラフィックをフィルタリングできるようにします。Threat Intelligence Director でも、これらの基準によるフィルタリングをサポートし、SHA-256 ハッシュ値に基づくフィルタリングのサポートを追加します。
- **Threat Intelligence Director は、追加のインテリジェンス取り込み方法をサポート**：セキュリティ インテリジェンスおよび Threat Intelligence Director の両方を使用して、フラット ファイルを手動でアップロードするか、サードパーティ ホストからフラット ファイルを取得するようにシステムを構成することで、システムに脅威インテリジェンスをインポートできます。Threat Intelligence Director は、これらのフラット ファイルの管理における柔軟性を向上させます。また、Threat Intelligence Director は Structured Threat Information eXpression（STIX™）形式で提供されるインテリジェンスを取得して取り込むことができます。
- **Threat Intelligence Director は、フィルタリング処理のきめ細かい制御を提供**：セキュリティ インテリジェンスにより、ネットワーク、URL、またはDNSオブジェクトによるフィ

ルタリング基準を指定できます。セキュリティ インテリジェンス オブジェクト（特にリストおよびフィード）には、複数の IP アドレス、URL、DNS ドメイン名を含めることができますが、オブジェクトの個別のコンポーネントではなく、オブジェクト全体に基づいてのみ、ブロックまたはブロックしないことができます。Threat Intelligence Director を使用すると、個別の基準（つまり簡易インジケータまたは個別のオブザーバブル）に対するフィルタリング処理を構成できます。

- **Threat Intelligence Director 構成の変更には再展開は不要**：アクセス コントロール ポリシーでセキュリティ インテリジェンス設定を変更したら、管理対象デバイスに変更された構成を再展開する必要があります。Threat Intelligence Director では、管理対象デバイスへのアクセス コントロール ポリシーの初期展開後に、ソース、インジケータ、およびオブザーバブルを再展開せずに構成でき、システムによって新しい Threat Intelligence Director データが要素に自動的に公開されます。

セキュリティ インテリジェンスまたは Threat Intelligence Director が特定のインシデントに対処できるときに、システムがどのように機能するかについては、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）を参照してください。

Threat Intelligence Director のパフォーマンスへの影響

Secure Firewall Management Center

いくつかのケースで、次のような場合があります。

- 特に大きな STIX ソースを取り込んでいる間にシステムのパフォーマンスがわずかに低下することがあり、取り込みが完了するまでに時間がかかることがあります。
- 新しいまたは変更された Threat Intelligence Director データを要素に公開するまでに、最大 15 分かかることがあります。

管理対象デバイス（Managed Device）

例外的なパフォーマンスの影響はありません。Threat Intelligence Director は、Secure Firewall Management Center セキュリティ インテリジェンスの機能と同じようにパフォーマンスに影響します。

Threat Intelligence Director の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

管理者

脅威インテリジェンス ディレクタユーザー

追加の要件

次のトピックでは、Threat Intelligence Director を使用するための追加の要件について説明します。

プラットフォーム、要素、およびライセンスに関する要件

ホスティング プラットフォーム

次の物理および仮想 Secure Firewall Management Center で Threat Intelligence Director をホスティングできます。

- バージョン 6.2.2 以降を実行している。
- 最小 15 GB のメモリで構成されている。
- REST API アクセスが有効な状態で構成されている。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Enabling REST API Access」を参照してください。

要素

デバイスがバージョン 6.2.2 以降を実行している場合は、任意の Secure Firewall Management Center 管理対象デバイスを Threat Intelligence Director 要素として使用できます。

ライセンシング

SHA-256 の監視可能な公開のファイルポリシーを構成するには、次のライセンスを取得したデバイスが必要です。

- スマートライセンスデバイスの場合：
  - IPS ライセンス：IPv4、IPv6、URL、および DNS の検出と監視可能
  - マルウェア防御ライセンス：SHA-256 の検出と監視可能
- クラシック ライセンス デバイスの場合：
  - 保護ライセンス：IPv4、IPv6、URL、および DNS の検出と監視可能
  - マルウェアライセンス：SHA-256 の検出と監視可能

詳細については、Threat Intelligence Director をサポートするためのポリシーの設定 （2948 ページ） およびCisco Secure Firewall Management Center アドミニストレーション ガイドの「Licenses」の章を参照してください。

ソース要件

ソース タイプの要件：

STIX

ファイルは、STIX バージョン 1.0、1.1、1.1.1、または 1.2 であり、STIX ドキュメントのガイドライン（http://stixproject.github.io/documentation/suggested-practices/）に準拠していなければなりません。

STIX ファイルには複雑なインジケータを含めることができます。

URL ダウンロードまたはファイルアップロードで設定される場合、STIX ファイルの最大サイズは 40MB です。これより大きい STIX ファイルがある場合は、TAXII サーバーを使用することを推奨します。

フラット ファイル（Flat File）

ファイルは、1 行に 1 つのオブザーバブル値を持つ ASCII テキスト ファイルでなければなりません。

フラット ファイルには、簡易インジケータ（インジケータごとに 1 つのオブザーバブル）しか含まれていません。

フラットファイルは 500 MB 以下にする必要があります。

Threat Intelligence Director では、以下はサポートされません。

- オブザーバブル値を区切る区切り文字（たとえば、`observable,` は無効です）。
- オブザーバブル値を囲む囲み文字（たとえば、`"observable"` は無効です）。

各ファイルには、コンテンツ タイプを 1 つしか含めることができません。

- `SHA-256`：SHA-256 ハッシュ値。
- `Domain`：RFC 1035 で規定されているドメイン名。
- `URL`：RFC 1738 で規定されている URL。

（注） Threat Intelligence Director は、ポート、プロトコル、または認証情報を含む URL を正規化し、インジケータを検出するときに正規化されたバージョンを使用します。たとえば、Threat Intelligence Director は次の URL を正規化します。

```
http://example.com/index.htm
http://example.com:8080/index.htm
example.com:8080/index.htm
example.com/index.htm
```

as:

```
example.com/index.htm
```

または、Threat Intelligence Director はたとえば次の URL を正規化します。

```
http://abc@example.com:8080/index.htm
```

これを次のように更新します。

```
abc@example.com/index.htm/
```

- `IPv4`：RFC 791 で規定されている IPv4 アドレス。

  Threat Intelligence Director は CIDR ブロックを受け入れません。

- `IPv6`：RFC 4291 で規定されている IPv6 アドレス。

  Threat Intelligence Director はプレフィックス長を受け入れません。

ソース コンテンツの制限事項

システムにより、URL オブザーバブルの最初の 1000 文字のみが取り込まれ、照合されます。

Threat Intelligence Director のセットアップ方法

（注） Threat Intelligence Director の設定や操作中に問題が発生した場合は、Threat Intelligence Director のトラブルシューティング （2994 ページ）を参照してください。

手順

ステップ 1 インストールしたものが Threat Intelligence Director を実行するための要件を満たしていることを確認します。

プラットフォーム、要素、およびライセンスに関する要件（2945ページ）を参照してください

ステップ 2 管理対象デバイスごとに、Threat Intelligence Director をサポートするために必要なポリシーを設定し、それらのポリシーをデバイスに展開します。

Threat Intelligence Director をサポートするためのポリシーの設定（2948ページ）を参照してください。

インテリジェンス データ ソースを取り込む前または後で要素を設定できます。

ステップ 3 Threat Intelligence Director で取り込むインテリジェンス ソースを設定します。

ソース要件（2946ページ）とデータ ソースを取り込むためのオプション（2950ページ）の下のトピックを参照してください。

ステップ 4 要素にデータをまだ公開していない場合は、公開します。ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開（2990ページ）を参照してください。

次のタスク

- 定期的にスケジュールされたバックアップに Threat Intelligence Director を含めます。Threat Intelligence Director データのバックアップおよび復元について（2957ページ）を参照してください。

  Secure Firewall Management Center の展開が高可用性構成の場合は、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Firewall Management Center High Availability Disaster Recovery*」も参照してください。

- （オプション）必要に応じて、Threat Intelligence Director 機能に管理アクセスを付与します。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Firewall Management Center」を参照してくだい。

- 操作中に必要に応じて、設定を微調整します。たとえば、誤検出インシデントを生成するオブザーバブルを [ブロックしない（Do Not Block）] リストに追加します。「Threat Intelligence Director 設定の表示および変更（2975 ページ）」を参照してください。

Threat Intelligence Director をサポートするためのポリシーの設定

Firewall Management Center から管理対象デバイス（要素）に Threat Intelligence Director データを公開するには、アクセス コントロール ポリシーを設定する必要があります。さらに、最大限のオブザベーションおよび Firewall Management Center イベント生成を行うためにアクセス コントロール ポリシーを設定することを推奨します。

Threat Intelligence Director をサポートする各管理対象デバイスに対し、次の手順を実行して関連付けられたアクセス コントロール ポリシーを設定します。

データが公開された後に Threat Intelligence Director を使用するように設定されている要素は、現在公開されているすべてのオブザーバブルを自動的に受信します。

手順

ステップ 1 アクセス コントロール ポリシーの [一般設定（General Settings）] で、[Threat Intelligence Director を有効にする（Enable Threat Intelligence Director）] チェックボックスがオンになっていることを確認します。[一般設定（General Settings）] に移動するには、**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [編集（Edit）] > [詳細（More）] > [詳細設定（Advanced Settings）]** を選択します。このオプションは、デフォルトで有効です。

詳細については、アクセス コントロール ポリシーの詳細設定（1759 ページ）を参照してください。

ステップ 2 まだ設定されていない場合は、アクセス コントロール ポリシーに接続を（信頼ではなく）許可するルールを追加します。Threat Intelligence Director では、アクセス コントロール ポリシーで 1 つ以上のルールを指定する必要があります。

Threat Intelligence Director はインスペクションに依存しているため、トラフィックを信頼するのではなく、許可するようにしてください。トラフィックを信頼する目的はインスペクションをバイパスすることであるためです。詳細については、基本的なアクセス コントロール ポリシーの作成（1748 ページ）を参照してください。

ステップ 3 アクセス コントロール ポリシーのデフォルト アクションとして [侵入防御（Intrusion Prevention）] を選択し、TID 検出のためにトラフィックを復号する場合は、SSL ポリシーをアクセス コントロール ポリシーに関連付けます。アクセス制御への他のポリシーの関連付け（1765 ページ）を参照してください。

ステップ 4 `SHA-256` オブザーバブルにオブザベーションおよび Secure Firewall Management Center イベントを生成させる場合：

a) 1 つ以上の [マルウェアクラウドルックアップ（Malware Cloud Lookup）] または [マルウェアブロック（Block Malware）] ファイル ルールを含むファイル ポリシーを作成します。

詳細については、ファイル ポリシーの設定（2252 ページ）を参照してください。

b) このファイル ポリシーを、アクセス コントロール ポリシーの 1 つ以上のルールと関連付けます。

ステップ 5 [IPv4]、[IPv6]、[URL]、または [ドメイン名（Domain Name）] のオブザベーションで接続およびセキュリティ インテリジェンスイベントを生成する場合は、アクセス コントロール ポリシーで接続およびセキュリティ インテリジェンスのロギングを有効にします。

a) ファイル ポリシーを呼び出したアクセス コントロール ルールで、[接続の終了時にロギング（Log at End of Connection）] および [ファイル イベント：ログファイル（File Events: Log Files）] を有効にします（まだ有効になっていない場合）。

詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Logging Connections with Access Control Rules*」を参照してください。

b) セキュリティ インテリジェンス設定でデフォルトのロギング（[DNS ポリシー（DNS Policy）]、[ネットワーク（Networks）]、および [URL（URLs）]）が有効になっていることを確認します。

詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Logging Connections with Security Intelligence*」を参照してください。

ステップ 6 設定変更を展開します設定変更の展開 （172 ページ）を参照してください。

次のタスク

残りの項目を入力します。 Threat Intelligence Director のセットアップ方法 （2947 ページ）

データ ソースを取り込むためのオプション

使用するデータ タイプと配信メカニズムに基づいて構成オプションを選択します。

これらのデータ タイプの詳細については、ソース要件 （2946 ページ） を参照してください。

表 *235*：データ ソースを取り込むためのオプション

データ タイプ	取り込みオプション
STIX	• TAXII サーバーからの STIX フィードの取り込み： ソースとして使用する TAXII フィードの取得 （2950 ページ）を参照してください • URL からの STIX データのダウンロード： URL からのソースの取得 （2952 ページ）を参照してください • STIX ファイルのアップロード： ソースとして使用するローカルファイルのアップロード （2954 ページ）を参照してください
フラット ファイル	• URL からのデータのダウンロード： URL からのソースの取得 （2952 ページ）を参照してください • フラット ファイルのアップロード： 「ソースとして使用するローカル ファイルのアップロード （2954 ページ）」を参照してください。

ソースとして使用する TAXII フィードの取得

TID の設定や操作中に問題が発生した場合は、を参照してください。 Threat Intelligence Director のトラブルシューティング （2994 ページ）

手順

ステップ 1 次の要件をソースが満たしていることを確認します。 ソース要件 （2946 ページ）

ステップ 2 **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）]** を選択します。

ステップ 3 [追加（Add）]（＋） をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [TAXII] を選択します。

ステップ 5 情報を入力します。

- ホスト サーバーで暗号化された接続が必要な場合は、Threat Intelligence Director ソースの TLS/SSL 設定の構成 （2955 ページ） の説明に従って [SSL 設定（SSL Settings）] を構成します。
- TAXII ソースの [アクション（Action）] 選択を変更することはできません。

  STIX データに（システムがブロックできない）複雑なインジケータが含まれている可能性があるため、TAXII ソースの `Block` が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

  ただし、取り込み後は、個々のオブザーバブルと、そのソースから取得した簡易インジケータをブロックすることができます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ） を参照してください。
- フィードのリストが読み込まれるまでには時間がかかることがあります。
- [更新頻度（Update Every）] 間隔は、Threat Intelligence Director が TAXII ソースから更新を取得する頻度を指定します。

  データ ソースを更新する有効な更新頻度を設定します。たとえば、ソースを 1 日に 3 回更新する場合、更新間隔を 1440/3 または 480 分に設定して、定期的に最新データをキャプチャします。
- [TTL] に指定された日数の経過後に、Threat Intelligence Director が以下のものを削除します。
  - 以降のソース更新に含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

（注）
[TTL] に指定された日数内にソースに更新が含まれず、ソースのチェックサムが変更されない場合、ダウンロードは更新なしのフィードとして扱われます。オブザーバブルが新しい TTL 値を受信するには、ソースにいくつかの更新が含まれている必要があります。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（PUBLISH）] [スライダ（Slider）]（）が有効になっていることを確認します。

このオプションを有効にすると、システムは自動的に初期ソースデータとそれに続く変更を公開します。

詳細は、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- TAXII フィードには大量のデータが含まれている可能性があるため、システムがすべてのデータを取り込むまでに時間がかかることがあります。取り込みステータスを表示するには、[ソース（Sources）] ページを更新します。
- このソースのエラーが表示される場合は、ステータスにマウスオーバーすると詳細を確認できます。
- 初期の Threat Intelligence Director 設定を行っている場合は、Threat Intelligence Director のセットアップ方法 （2947 ページ） に戻ります。

URL からのソースの取得

Threat Intelligence Director でホストからファイルを取得する場合は、URL ソースを設定します。

TID の設定や操作中に問題が発生した場合は、を参照してください。 Threat Intelligence Director のトラブルシューティング （2994 ページ）

手順

ステップ 1 次の要件をソースが満たしていることを確認します。 ソース要件 （2946 ページ）

ステップ 2 **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）]** を選択します。

ステップ 3 [追加（Add）]（） をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [URL] を選択します。

ステップ 5 フォームに入力します。

- フラットファイルを取り込む場合は、ソース内に含まれるデータを記述する [タイプ（Type）] を選択します。
- ホスト サーバーで暗号化された接続が必要な場合は、Threat Intelligence Director ソースの TLS/SSL 設定の構成 （2955 ページ） の説明に従って **SSL 設定**を構成します。

- 名前の場合：Threat Intelligence Director インジケータに基づいてインシデントの並び替えと処理を簡単にするには、 送信元全体に一貫した命名スキームを使用します。例：<source>-<type>。

  ソース名も追加すると、追加の情報やフィードバックのためにソースに返信することが簡単になります。

  一貫性のある名前を入力してください。たとえば、IPv4アドレスを含むソースの場合、常に IPV4 を使用します（IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4、IP-V4 などは使用しません）。

- STIX ファイルを取り込む場合は、STIX データに（システムがブロックできない）複雑なインジケータが含まれている可能性があるため、`Block` が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

  ただし、取り込み後は、個々のオブザーバブルと、そのソースから取得した簡易インジケータをブロックすることができます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。

- データ ソースを更新する有効な更新頻度を設定します。たとえば、ソースを 1 日に 3 回更新する場合、更新間隔を 1440/3 または 480 分に設定して、定期的に最新データをキャプチャします。

- [TTL] 間隔に指定された日数の経過後に、Threat Intelligence Director が以下のものを削除します。

  - 以降のソース更新に含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

（注）
[TTL] に指定された日数内にソースに更新が含まれず、ソースのチェックサムが変更されない場合、ダウンロードは更新なしのフィードとして扱われます。オブザーバブルが新しい TTL 値を受信するには、ソースにいくつかの更新が含まれている必要があります。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）][スライダ（Slider）]（ ）が有効になっていることを確認します。

このオプションを有効にすると、システムは自動的に初期ソースデータとそれに続く変更を公開します。

詳細は、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 取り込みステータスを表示するには、[ソース（Sources）]ページを更新します。エラーが表示される場合は、ステータスにマウスオーバーすると詳細を確認できます。
- 初期の Threat Intelligence Director 設定を行っている場合は、Threat Intelligence Director のセットアップ方法 （2947 ページ） に戻ります。

ソースとして使用するローカル ファイルのアップロード

この手順は、ローカル ファイルのワンタイム手動アップロードに使用します。

STIX ファイルを取り込むと、Threat Intelligence Director によって STIX ファイルの内容から単純または複雑なインジケータが作成されます。

フラット ファイルを取り込むと、Threat Intelligence Director によってファイル内のオブザーバブル値ごとに簡易インジケータが作成されます。

Threat Intelligence Director の設定や操作中に問題が発生した場合は、Threat Intelligence Director のトラブルシューティング （2994 ページ）を参照してください。

手順

ステップ 1 の要件をファイルが満たしていることを確認します。 ソース要件 （2946 ページ）

ステップ 2 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 3 [追加（Add）] （＋） をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [アップロード（Upload）] を選択します。

ステップ 5 フォームに入力します。

- フラットファイルをアップロードする場合は、ソース内に含まれるデータを記述する [タイプ（Type）] を選択します。
- 名前の場合：Threat Intelligence Director インジケータに基づいてインシデントの並び替えと処理を簡単にするには、 送信元全体に一貫した命名スキームを使用します。例：<source>-<type>。

  ソース名も追加すると、追加の情報やフィードバックのためにソースに返信することが簡単になります。

  一貫性のある名前を入力してください。たとえば、IPv4アドレスを含むソースの場合、常に IPV4 を使用します（IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4、IP-V4 などは使用しません）。
- STIX ファイルをアップロードする場合は、STIX データに複雑なインジケータが含まれている可能性があるため、`Block` が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

ただし、インジケータまたはオブザーバブル レベルで簡易インジケータをブロックすることはできます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。

- [TTL] 間隔に指定された日数の経過後に、Threat Intelligence Director が以下のものを削除します。
  - 以降のアップロードに含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

（注）
[TTL] に指定された日数内にソースに更新が含まれず、ソースのチェックサムが変更されない場合、ダウンロードは更新なしのフィードとして扱われます。オブザーバブルが新しい TTL 値を受信するには、ソースにいくつかの更新が含まれている必要があります。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）][スライダ（Slider）]（ ）が有効になっていることを確認します。

取り込み時にソースを公開しない場合、後ですべてのソースインジケータを一度に公開することはできません。代わりに、各オブザーバブルを個別に公開する必要があります。「ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）」を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 取り込みステータスを表示するには、[ソース（Sources）]ページを更新します。エラーが表示される場合は、ステータスにマウスオーバーすると詳細を確認できます。
- 初期の Threat Intelligence Director 設定を行っている場合は、Threat Intelligence Director のセットアップ方法 （2947 ページ） に戻ります。

重複インジケータの処理

単一のインジケータが複数のソースに含まれている場合：

インジケータの各インスタンスがインシデントを生成するため、特定の脅威を一度検出すると複数のインシデントを生成する場合があります。

今後の重複インシデントを回避するには、重複インジケータの 1 つを除くすべてのインジケータの公開を一時停止します。「ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）」を参照してください。

Threat Intelligence Director ソースの TLS/SSL 設定の構成

ホスト サーバーで暗号化された接続が必要な場合は、**SSL 設定**を構成します。

始める前に

- ソースとして使用する TAXII フィードの取得 （2950 ページ） または URL からのソースの取得 （2952 ページ） の説明に従って、TAXII または URL ソースの設定を開始します。

手順

ステップ 1 [ソースの編集（Edit Source）] ダイアログボックスで、[SSL設定（SSL Settings）] セクションを展開します。

ステップ 2 サーバー証明書が自己署名されている場合：

a) [自己署名証明書（Self-Signed Certificate）] を有効にします。

b) [SSL ホスト名検証（SSL Hostname Verification）] 方式を選択します。

- [厳格（Strict）]：Threat Intelligence Director では、ソース **URL** がサーバー証明書に指定されたホスト名と一致する必要があります。

  ホスト名にワイルドカードが含まれる場合、TID は複数のサブドメインと一致することはできません。

- [ブラウザ互換性あり（Browser Compatible）]：Threat Intelligence Director では、ソース **URL** がサーバー証明書に指定されたホスト名と一致する必要があります。

  ホスト名にワイルドカードが含まれる場合、TID はすべてのサブドメインに一致します。

- [すべて許可（Allow All）]：Threat Intelligence Director では、ソース **URL** がサーバー証明書に指定されたホスト名と一致する必要はありません。

たとえば、subdomain1.subdomain2.cisco.com がソース **URL** で、*.cisco.com がサーバー証明書で指定されたホスト名である場合は、次のようになります。

- [厳格（Strict）] ホスト名検証は失敗します。
- [ブラウザ互換性あり（Browser Compatible）] ホスト名検証は成功します。
- [すべて許可（Allow All）] ホスト名検証では、ホスト名の値は完全に無視されます。

c) [サーバー証明書（Server Certificate）] の場合：

- PEM エンコードおよび自己署名されたサーバー証明書にアクセスできる場合は、テキストエディタで証明書を開き、BEGIN CERTIFICATE 行と END CERTIFICATE 行を含むテキストブロック全体をコピーします。この文字列全体をフィールドに入力します。
- 自己署名されたサーバー証明書にアクセスできない場合は、フィールドを空白のままにします。ソースを保存すると、Threat Intelligence Director はサーバーから証明書を取得します。

ステップ 3 サーバーにユーザー証明書が必要な場合：

a) [ユーザー証明書（User Certificate）] を入力します。

テキスト エディタで PEM エンコードされた証明書を開いて、`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含むテキストのブロック全体をコピーします。この文字列全体をフィールドに入力します。

b) [ユーザー秘密キー（User Private Key）] を入力します。

テキスト エディタで秘密キー ファイルを開き、`BEGIN RSA PRIVATE KEY` および `END RSA PRIVATE KEY` 行を含むテキスト ブロック全体をコピーします。この文字列全体をフィールドに入力します。

次のタスク

- 証明書の有効期限を記録します。現在の証明書の有効期限が切れた後に、新しいサーバー証明書を入力するためのカレンダー通知を設定することもできます。
- ソースの設定を続けます。
  - ソースとして使用する TAXII フィードの取得 （2950 ページ）
  - URL からのソースの取得 （2952 ページ）

Threat Intelligence Director アクセス権を持つユーザー ロール

Firewall Management Center ユーザー アカウントを使用して、Threat Intelligence Director のメニューやページにアクセスすることができます。

- [管理者（Admin）] または [Threat Intelligence Director ユーザ（Threat Intelligence Director User）] のユーザ ロールを持つアカウント。
- [インテリジェンス（Intelligence）]権限を含むカスタム ユーザ ロールを持つアカウント。

さらに、[管理者（Admin）]、[アクセス管理者（Access Admin）]、または [ネットワーク管理者（Network Admin）] のユーザ ロールを持つ Firewall Management Center ユーザ アカウントを使用して、アクセス コントロール ポリシーで Threat Intelligence Director を有効または無効にすることができます。

ユーザーアカウントの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Firewall Management Center*」の章を参照してください。

Threat Intelligence Director データのバックアップおよび復元について

Firewall Management Center を使用して、Threat Intelligence Director に必要なすべてのデータ（要素データ、セキュリティ インテリジェンス イベント、接続イベント、Threat Intelligence Director

構成、および Threat Intelligence Director データ）をバックアップおよび復元できます。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「the *Backup/Restore*」の章を参照してください。

（注） ハイ アベイラビリティ構成のアクティブな Firewall Management Center で Threat Intelligence Director をホスティングする場合、システムは Threat Intelligence Director 構成と Threat Intelligence Director データをスタンバイ Firewall Management Center に同期しません。フェールオーバー後にデータを復元できるように、アクティブ Firewall Management Center で Threat Intelligence Director データの定期的なバックアップを実行することを推奨します。

アクティブな Firewall Management Center で Threat Intelligence Director のデータの復元を試みる前に、アクティブピアで同期を一時停止します。詳細については、「」『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「*Pausing Communication Between Paired Firepower Management Centers*」を参照してください。

表 *236 : Threat Intelligence Director* 関連のバックアップおよび復元ファイルの内容

Threat Intelligence Director 関連ファイルの内容	**バックアップの選択**	**復元の選択**
要素データ	**バックアップ構成**	**設定データの復元（Restore Configuration Data）**
Secure Firewall Management Center イベント データ	**イベントのバックアップ**	**イベント データの復元（Restore Event Data）**
Threat Intelligence Director 構成および Threat Intelligence Director データ	**Threat Intelligence Director のバックアップ**	**Threat Intelligence Director データの復元（Restore Threat Intelligence Director Data）**

Threat Intelligence Director インシデントおよびオブザベーション データの分析

Threat Intelligence Director 要素によって生成されたインシデントおよびオブザベーション データを分析するには、インシデント表およびインシデント詳細ページを使用します。

監視とインシデント生成

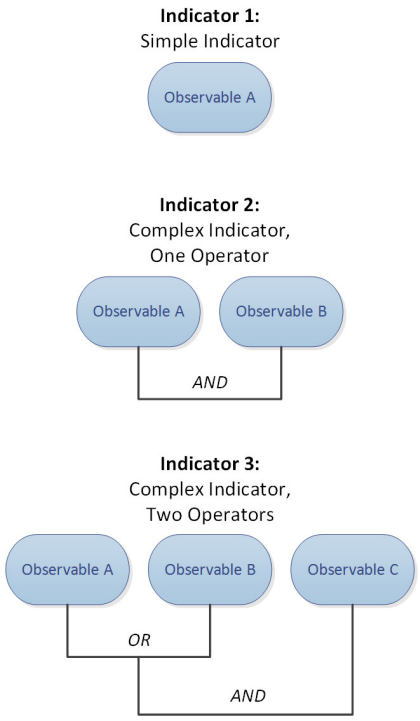
Threat Intelligence Director は、インジケータに対する最初のオブザーバブルがトラフィックに見られたときにインシデントを生成します。単一の監視後、簡易インジケータが完全に実現されます。複雑なインジケータは、1 つ以上の追加の監視がそのパターンを実行するまで、部分的に実現されます。複雑なインジケータは、必ずしも単一のトランザクション中に達成される

必要はありません。各オブザーバブルは、異なるトランザクションにより、時間の経過とともに個別に達成できます。

（注） インジケータのパターンを評価するときに、Threat Intelligence Director は、サポートされていない無効なオブジェクトと、ブロックしないリストにあるオブザーバブルを無視します。

インシデントが完全に実現された後、その後の監視で新しいインシデントがトリガーされます。

図 *323 :* 例：インジケータ パターン



Threat Intelligence Director が上記の例からのオブザーバブルを取り込み、オブザーバブルが順番に確認されると、インシデント生成は次のように進行します。

1. システムがトラフィック中のオブザーバブル A を識別すると、Threat Intelligence Director は次のようになります。
   - インジケータ 1 に対して完全に実現されたインシデントを生成します。
   - インジケータ 2 とインジケータ 3 に対して、部分的に実現されたインシデントを生成します。
2. システムがトラフィック中のオブザーバブル B を識別すると、Threat Intelligence Director は次のようになります。

- インジケータ 2 については、パターンが達成されたのでインシデントを [完全に実現（fully-realized）] に更新します。
- インジケータ 3 については、インシデントを [部分的に実現（partially-realized）] に更新します。

3. システムがトラフィック中のオブザーバブル C を識別すると、Threat Intelligence Director は次のようになります。
   - インジケータ 3 については、パターンが達成されたのでインシデントを [完全に実現（fully-realized）] に更新します。
4. システムがオブザーバブル A をもう一度識別すると、Threat Intelligence Director は次のようになります。
   - インジケータ 1 に対して新しい完全に実現されたインシデントを生成します。
   - インジケータ 2 とインジケータ 3 に対して、新しい部分的に実現されたインシデントを生成します。

特定のインジケータが複数のソースに存在する場合、重複インシデントが表示される場合があります。詳細については、Threat Intelligence Director のトラブルシューティング （2994 ページ）を参照してください。

インシデントは実際のトラフィックによってのみ生成されることに注意してください。URL B のオブザーバブルがあり、ユーザーが URL B へのリンクを表示する URL A にアクセスした場合は、ユーザーが URL B のリンクをクリックしない限り、インシデントは発生しません。

インシデントの表示と管理

[インシデント（Incidents）] ページには、最大 110 万件の最新の Threat Intelligence Director インシデントに関する要約情報が表示されます。（インシデント サマリー情報 （2961 ページ）を参照）。

始める前に

- Threat Intelligence Director のセットアップ方法 （2947 ページ）の説明に従って機能を設定します。
- 監視とインシデント生成 （2958 ページ）の説明を読んで、オブザベーションとインシデント生成について理解します。

手順

ステップ 1 **[統合（Integration）] > [インテリジェンス（Intelligence）] > [インシデント（Incidents）]** を選択します。

ステップ 2 次のようにインシデントを確認します。

- 1 つ以上のフィルタを追加するには、[フィルタ（Filter）]（ ）をクリックします。デフォルトのフィルタは 6 時間です。詳細については、テーブル ビューでの Threat Intelligence Director データのフィルタ処理 （2985 ページ）を参照してください。
- Threat Intelligence Director でインシデントが最後に更新された日時を表示するには、[最終更新日（Last Updated）] 列内の値の上にカーソルを置きます。
- インシデントに関連付けられているインジケータについての詳細を表示するには、[インジケータ名（Indicator Name）] 列内のテキストをクリックします（インジケータの表示と管理 （2980 ページ）を参照）。

ステップ 3 [インシデントID（Incident ID）] 列の値をクリックして、その他の詳細を表示します。

表示される詳細の説明については、インシデントの詳細 （2963 ページ）を参照してください。

- インジケータの詳細を表示するには、ウィンドウ下部の [インジケータ（Indicator）] 見出しのインジケータ値（IP アドレスや SHA-256 の値など）をクリックします。
- オブザベーションの詳細を表示するには、[オブザベーション（Observations）] 見出しのすぐ下のオブザベーションの左にある矢印をクリックします。
- [Security Intelligence Events（セキュリティ インテリジェンス イベント）] ページでこのインシデントを表示するには、オブザベーション詳細セクションで [イベント（Events）] リンクをクリックします。

ステップ 4 （オプション）インシデント詳細ページで詳細情報を入力します。

ヒント：次のオプションの一貫性と有用性を最大化するには、方針を作成したうえで、命名規則、カテゴリの選択、および信頼度レベル基準を文書化します。

- [名前（Name）]、[説明（Description）] および [カテゴリ（Category）] フィールドに任意の値を入力します。
- [信頼度（Confidence）] の評価レベルをクリックします。
- インシデントの調査ステータスを指定するには、[ステータス（Status）] フィールドのドロップダウン リストから値を選択します。

インシデント サマリー情報

[インシデント（Incidents）] ページには、すべての Threat Intelligence Director インシデントのサマリー情報が表示されます。

表 *237:* インシデント サマリー情報

フィールド	説明
最終更新日	システムまたはユーザが最後にインシデントを更新してからの日数。更新の日時を表示するには、この列の値にマウスオーバーします。
[インシデント ID（Incident ID）]	インシデントの固有識別子。この ID の形式は次のとおりです。 `<type>-<date>-<number>` • `<type>`：インシデントに関係するインジケータまたはオブザーバブルのタイプ。単純なインジケータの場合、この値はオブザーバブルのタイプ（`IP`（IPv4 または IPv6）、`URL`（URL）、`DOM`（ドメイン）、または `SHA`（SHA-256））を示します。複雑なインジケータの場合、この値は `COM` です。 • `<date>`：インシデントが作成された日付（*yyyymmdd*）。 • `<number>`：インシデント番号。これは、1 日に作成されたインシデントの中での順序を示す番号です。この順序は 0 で始まることに注意してください。たとえば、`DOM-20170828-10` はその日に作成された 11 番目のインシデントです。 識別子の隣には、インシデントが [部分的に実現（Partially Realized）] か、[完全に実現（Fully Realized）] かを示すアイコンが表示されます。詳細については、監視とインシデント生成（2958 ページ）を参照してください。
[インジケータ名（Indicator Name）]	インシデントに関係するインジケータの名前。インジケータの追加情報を表示するには、この列の値をクリックします。インジケータの表示と管理（2980 ページ）を参照してください。
Type	インシデントに関係するインジケータのタイプ。 • 単一のオブザーバブルを含むインジケータでは、データ型（`URL`、`SHA-256` など）が表示されます。 • 2 つ以上のオブザーバブルを含むインジケータは、`Complex` として表示されます。
[実施アクション（Action Taken）]	インシデントに関してシステムが実行するアクション。詳細については、インシデントの詳細（2963 ページ）を参照してください。
Status（ステータス）	インシデントに関する調査のステータスです。詳細については、インシデントの詳細（2963 ページ）を参照してください。
[削除（Delete）]（🗑）	このアイコンをクリックすると、インシデントが完全に削除されます。

インシデントの詳細

[インシデントの詳細（Incident Details）] ウィンドウには、単一の Threat Intelligence Director インシデントに関する情報が表示されます。このウィンドウは、2 つのセクションで構成されています。

- インシデントの詳細：基本情報 （2963 ページ）
- インシデントの詳細：インジケータとオブザベーション （2964 ページ）

インシデントの詳細：基本情報

[インシデントの詳細（Incident Details）] ウィンドウの上部セクションでは、次の情報が提供されます。

表 *238 :* 基本的なインシデント情報フィールド

フィールド	説明
[部分的に実現 *IncidentID*（Partially-Realized IncidentID）] または [完全に実現*IncidentID*（Fully-Realized IncidentID）]	インシデントのステータス（部分的に実現または完全に実現）およびインシデントの一意の ID を示すアイコン。 （注） インジケータのステータスを判断するときに、Threat Intelligence Director は、サポートされていない無効なオブザーバブルと、ブロックしないリストにあるオブザーバブルを無視します。
[既読（Opened）]	インシデントが最後に更新された日時。
Name	手動で入力するオプションのカスタム インシデント名。 ヒント：[説明（Description）] フィールド（ウィンドウの下部）にソースからの情報がある場合は、そのフィールドの情報を使用してインシデントに名前を付けます。
説明	手動で入力するオプションのカスタム インシデント説明。 ヒント：[説明（Description）] フィールド（ウィンドウの下部）にソースからの情報がある場合は、そのフィールドの情報を使用してインシデントについて説明します。
[オブザベーション（Observations）]	インシデント内のオブザベーションの数。
信頼性（Confidence）	インシデントの相対的な重要度を示すために手動で選択できるオプションの評価。

フィールド	説明
[実施アクション（Action Taken）]	システムによって実行されるアクション：[モニタ済み（Monitored）]、[ブロック済み（Blocked）]、または [部分的にブロック済み（Partially Blocked）]。 [部分的にブロック済み（Partially Blocked）] は、インシデントに [モニタ済み（Monitored）] と [ブロック済み（Blocked）] の両方のオブザベーションが含まれていることを示します。 （注） [実施アクション（Action Taken）] は、システムによって実行されるアクションを示しますが、必ずしも Threat Intelligence Director で選択されているアクションではありません。詳細については、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け（2969 ページ）を参照してください。
カテゴリ（Category）	インシデントに手動で追加するオプションのカスタム タグまたはキーワード。
Status（ステータス）	インシデントの分析の現在の段階を示す値。すべてのインシデントは、[ステータス（Status）] を初めて変更するまでは [新規（New）] です。 このフィールドは任意です。組織のニーズに応じて、以下のステータス値を使用することを検討してください。 • [新規（New）]：インシデントには調査が必要ですが、まだ調査を開始していません。 • [オープン（Open）]：現在インシデントを調査しています。 • [クローズ済み（Closed）]：インシデントを調査し、対処しました。 • [却下（Rejected）]：インシデントを調査し、実行するアクションはないと判断しました。
[削除（Delete）]（🗑）	このアイコンをクリックすると、このインシデントが完全に削除されます。

インシデントの詳細：インジケータとオブザベーション

[インシデントの詳細（Incident Details）] ウィンドウの下部セクションには、インジケータとオブザベーションの詳細情報が表示されます。この情報は、[インジケータ（Indicator）] フィールド、インジケータ パターン、および [オブザベーション（Observations）] フィールドとして編成されています。

[インジケータ（Indicator）] セクション

インジケータの詳細を初めて表示するときには、このセクションにはインジケータ名のみが表示されます。

[インジケータ（Indicator）] ページでインジケータを表示するには、インジケータ名をクリックします。

インジケータ名の隣にある下矢印をクリックすると、インシデントを閉じることなくインジケータの詳細を表示できます。詳細フィールドには、次のものがあります。

表 *239* : インジケータのフィールド

フィールド	説明
説明（**Description**）	ソースから提供されたインジケータの説明。
ソース（**Source**）	インジケータが含まれていたソース。このリンクをクリックすると、完全なソースの詳細にアクセスできます。
[有効期限（**Expires**）**]**	ソースの [TTL] 値に基づく、インシデントが期限切れになる日時。
操作（**Action**）	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。
[STIX のダウンロード（**Download STIX**）**]**	ソース タイプが `STIX` の場合は、このボタンをクリックして STIX ファイルをダウンロードします。

[インジケータ パターン（Indicator Pattern）]

インジケータ パターンは、インジケータを構成するオブザーバブルおよび演算子のグラフィカル表示です。演算子はインジケーター内のオブザーバブルをリンクします。AND 関係は [AND] 演算子で示されます。OR 関係は、**OR** 演算子、または複数のオブザーバブルの緊密なグループ化によって示されます。

パターンのオブザーバブルがすでに観測されている場合、オブザーバブル ボックスは白色です。オブザーバブルがまだ観測されていない場合、オブザーバブル ボックスは灰色です。

インジケータ パターンで、次のようにします。

- **[**ブロックしないリストに追加（**Add to Do-Not-Block List**）**]** ボタンをクリックして、オブザーバブルをブロックしないリストに追加します。このアイコンは、白色と灰色の両方のオブザーバブル ボックスに表示されます。詳細については、Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について （2992 ページ）を参照してください。
- 白色のオブザーバブル ボックスにマウスオーバーすると、[オブザベーション（Observations）] セクションで関連するオブザベーションが強調表示されます。
- 白色のオブザーバブル ボックスをクリックすると、[オブザベーション（Observations）] セクションで関連するオブザベーションが強調表示され、そのオブザベーションがスク

ロールされて表示されて（複数のオブザベーションが存在する場合）、そのオブザベーションの詳細表示が展開されます。

- インジケータ パターンで灰色のオブザーバブル ボックスをマウスオーバーまたはクリックした場合、[オブザベーション（Observations）] セクションに変化はありません。これは、オブザーバブルがまだ観測されていないため、表示するオブザベーションの詳細がないためです。

[オブザベーション（Observations）] セクション

デフォルトでは、[オブザベーション（Observations）] セクションには、次のような概要情報が表示されます。

- オブザベーションをトリガーしたオブザーバブルのタイプ（たとえば、[ドメイン（Domain）]）
- オブザーバブルを構成するデータ
- オブザベーションが最初のオブザベーションか、それ以降のオブザベーションか（たとえば、[最初の（1st）] または [3 つ目（3rd）]）

（注） 1 つのオブザーバブルが 3 回以上観測された場合、Threat Intelligence Director では最初と最後のオブザベーションの詳細を表示します。中間のオブザベーションの詳細は表示されません。

- オブザベーションの日時
- オブザーバブルに設定されているアクション

[オブザベーション（Observations）] セクションでオブザベーションにマウスオーバーすると、インジケータ パターンの関連するオブザーバブルが強調表示されます。

[オブザベーション（Observations）] セクションでオブザベーションをクリックした場合は、インジケータ パターンで関連するオブザーバブルが強調表示され、関連する最初のオブザーバブルがスクロールされて表示されます（複数のオブザーバブルが存在する場合）。また、オブザベーションをクリックすると、[オブザベーション（Observations）] セクションのオブザベーションの詳細が展開されます。

オブザベーションの詳細には、次のようなフィールドがあります。

表 *240*：オブザベーションの詳細のフィールド

フィールド	説明
[送信元（SOURCE）]	オブザベーションをトリガーしたトラフィックの送信元 IP アドレスおよびポート。

フィールド	説明
DESTINATION	オブザベーションをトリガーしたトラフィックの宛先 IP アドレスおよびポート。
[その他の情報（ADDITIONAL INFORMATION）]	オブザベーションをトリガーしたトラフィックに関連する DNS および認証情報。
イベント	このクリッカブル リンクは、オブザベーションによって接続、セキュリティ インテリジェンス、ファイル、またはマルウェア イベントが生成された場合に表示されます。リンクをクリックして、Secure Firewall Management Center イベント テーブルでイベントを表示します。Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

Threat Intelligence Director オブザベーションのイベントの表示

Threat Intelligence Director オブザベーションによって生成される Secure Firewall Management Center イベントについて詳しくは、Secure Firewall Management Center イベントでの Threat Intelligence Director オブザベーション （2968 ページ） を参照してください。

Threat Intelligence Director 関連のイベントについてログに記録されるシステム アクションは、Threat Intelligence Director の相互作用やその他の Secure Firewall Management Center 機能によって異なります。アクションの優先順位付けについて詳しくは、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）を参照してください。

始める前に

- Threat Intelligence Director のセットアップ方法 （2947 ページ）の説明に従って機能を設定します。
- Threat Intelligence Director をサポートするためのポリシーの設定 （2948 ページ）の説明に従って、アクセス コントロール ポリシーで Threat Intelligence Director に必要なイベント ロギングを有効にしたことを確認します。

手順

ステップ 1 **[統合（Integration）]** > **[インテリジェンス（Intelligence）]** > **[インシデント（Incidents）]** を選択します。

ステップ 2 インシデントの [インシデント ID（Incident ID）] 値をクリックします。

ステップ 3 [インジケータ（Indicator）] セクションでオブザベーションをクリックして、オブザベーション ボックスを表示します。

ステップ 4 オブザベーション ボックスの左上隅にある矢印をクリックしてボックスを展開します。

ステップ 5 オブザベーション情報で[イベント（Events）] リンクをクリックします。セキュリティ インテリジェンス イベントの詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「接続イベントとセキュリティ インテリジェンスのイベント」を参照してください。

Secure Firewall Management Center イベントでの Threat Intelligence Director オブザベーション

アクセス コントロール ポリシーを完全に制御する場合、Threat Intelligence Director オブザベーションによって、次の Secure Firewall Management Center イベントが生成されます。

表 *241* : オブザベーションによって生成される *Secure Firewall Management Center* イベント

オブザベーションの内容	接続イベントの表	セキュリティ インテリジェンス イベントの表	ファイル イベントの表	マルウェアイベントの表
SHA-256	はい	非対応	はい	○（判定結果がマルウェアまたはカスタム検出の場合）。
[ドメイン名（Domain Name）]、[URL]、または [IPv4/IPv6]	○ Threat Intelligence Director 関連の接続イベントは、Threat Intelligence Director 関連の [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] 値によって識別されます。	○ Threat Intelligence Director 関連のセキュリティ インテリジェンス イベントは、Threat Intelligence Director 関連の [セキュリティ インテリジェンス イベント（Security Intelligence Category）] 値により識別されます。	いいえ	非対応

アクションに影響を与える要因

システムがアクションを取るタイミングや、Threat Intelligence Director オブザーバブルと一致するトラフィックを検出したときにシステムが取るアクションは多くの要因によって決定されます。

- セキュリティ インテリジェンスのような機能は、Threat Intelligence Director がアクションを起こす前にアクションを起こします。詳細は、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）を参照してください。

- 実行されるアクションは一般に、オブザーバブルに対して構成されたアクション（親インジケータまたはソースに対して構成されたアクションとは異なる可能性がある）となります。
- STIX ソースには複雑なインジケータが含まれている可能性があるため、ソースのアクション設定は [モニター（Monitor）] にのみ設定できます。ただし、STIX フィードまたはファイルに含まれている個々の簡易インジケータまたはオブザーバブルは [ブロック（Block）] に設定できます。
- インジケータおよびオブザーバブルのアクション設定は、継承するかまたは継承をオーバーライドするように個別に設定できます。Threat Intelligence Director 設定における継承（2986 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。
- それ以外の場合は実用的なトラフィックが、[ブロックしない（Do Not Block）] リストに含まれている可能性があります。詳細は、Threat Intelligence Director オブザーバブルのブロックしないリストへの追加 （2993 ページ）を参照してください。
- 設定されたアクションは、部分的および完全に実現されたインシデントの両方に対して実行されます。
- 複雑なインジケータに基づくインシデントは部分的にブロックできます。これは、インジケータにモニタ対象のオブザーバブルとブロックされたオブザーバブルの両方が含まれている場合に発生する可能性があります。
- 公開の一時停止は、システムが実行するアクションに影響します。公開の一時停止について （2989 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。
- Threat Intelligence Director 機能を一時停止すると、すべての操作ができなくなります。この機能を再開した後、実行可能なデータが以前と異なる場合があります。詳細については、「Threat Intelligence Director の一時停止と要素からの Threat Intelligence Director データの消去 （2990 ページ）」を参照してください。

Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け

Threat Intelligence Director のオブザーバブルアクションが Firewall Management Center のポリシーアクションと競合する場合は、システムが次のようにアクションに優先順位を付けます。

- セキュリティ インテリジェンスのブロックしないリスト
- TID ブロック（TID Block）
- セキュリティ インテリジェンス ブロック
- TID モニター
- セキュリティ インテリジェンス モニター

具体的には次のとおりです。

表 *242 : Threat Intelligence Director URL* 監視可能アクション対セキュリティ インテリジェンス アクション

設定：セキュリティ インテリジェンス アクション	設定：**Threat Intelligence Director** 監視可能アクション	**Threat Intelligence Director** インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ（**Security Intelligence Category**）	理由（**Reason**）
[ブロックしない（Do Not Block）]	[モニター（Monitor）] または [ブロック（Block）]	TID インシデントなし	セキュリティ インテリジェンス イベントなし		
ブロック（Block）	モニター	ブロック	ブロック（Block）	システム分析により決定（を参照） セキュリティ インテリジェンス カテゴリ （1859 ページ）	URL Block
	ブロック（Block）	ブロック	ブロック（Block）	TID URL ブロック（TID URL Block）	URL Block
モニター	モニター	監視対象	セキュリティ インテリジェンスと TID の後に処理されたアクセス制御ルールによって決定されます。	TID URL モニター	URL Monitor
	ブロック（Block）	ブロック	ブロック（Block）	TID URL ブロック（TID URL Block）	URL Block

表 *243 : Threat Intelligence Director IPv4/IPv6* 監視可能アクション対セキュリティ インテリジェンス アクション

設定：セキュリティ インテリジェンス アクション	設定：**Threat Intelligence Director** 監視可能アクション	**Threat Intelligence Director** インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ（**Security Intelligence Category**）	理由（**Reason**）
[ブロックしない（Do Not Block）]	[モニター（Monitor）] または [ブロック（Block）]	TID インシデントなし	セキュリティ インテリジェンス イベントなし		
ブロック（Block）	モニター	TID インシデントなし	ブロック（Block）	システム分析により決定（を参照） セキュリティ インテリジェンス カテゴリ （1859 ページ）	IP Block
	ブロック（Block）	ブロック	ブロック（Block）	TID IPv4 Block TID IPv6 Block	IP Block
モニター	モニター	監視対象	セキュリティ インテリジェンスと TID の後に処理されたアクセス制御ルールによって決定されます。	TID IPv4 モニタ TID IPv6 Monitor	IP Monitor
	ブロック（Block）	ブロック	ブロック（Block）	TID IPv4 Block TID IPv6 Block	IP Block

表 *244 : Threat Intelligence Director* ドメイン名の監視可能アクション対 *DNS* ポリシー アクション

設定：**DNS** ポリシー アクション	設定：**Threat Intelligence Director** ドメイン名の監視可能アクション	**Threat Intelligence Director** インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ（**Security Intelligence Category**）	理由（**Reason**）
[ブロックしない（Do Not Block）]	[モニター（Monitor）] または [ブロック（Block）]	TID インシデントなし	セキュリティ インテリジェンス イベントなし		
Drop, Domain Not Found Sinkhole—Log Sinkhole—Block and Log	モニター	ブロック	ブロック（Block）	システム分析により決定（を参照）セキュリティ インテリジェンス カテゴリ （1859 ページ）	DNS ブロック（DNS Block）
	ブロック（Block）	ブロック	ブロック（Block）	TID ドメイン名ブロック	DNS ブロック（DNS Block）
モニター	モニター	監視対象	セキュリティ インテリジェンスと TID の後に処理されたアクセス制御ルールによって決定されます。	TID ドメイン名モニター	DNS モニター（DNS Monitor）
	ブロック（Block）	ブロック	ブロック（Block）	TID ドメイン名ブロック	DNS ブロック（DNS Block）

表 *245 : TID SHA-256* 監視可能アクション対マルウェア クラウド ルックアップ ファイル ポリシー

ファイル傾向（File Disposition）	Threat Intelligence Director SHA-256 監視可能アクション	Threat Intelligence Director インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
クリーン（Clean）	[モニター（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外
マルウェア	[モニター（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外
Custom	[モニター（Monitor）] または [ブロック（Block）]	監視対象	• SHA-256 がカスタム検出リストにない場合は、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）]。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出（Custom Detection）]。	• SHA-256 がカスタム検出リストにない場合は、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）]。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出（Custom Detection）]。
不明	[モニター（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外

（注） Threat Intelligence Director の一致は、システムが動的分析用にファイルを送信する前に発生します。

表 *246 : TID SHA-256* 監視可能アクション対マルウェア ブロック ファイル ポリシー

ファイル傾向（**File Disposition**）	**Threat Intelligence Director SHA-256** 監視可能アクション	**Threat Intelligence Director** インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
[正常（Clean）] または [不明（Unknown）]	モニター	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外
	ブロック（Block）	ブロック	• SHA-256 がカスタム検出リストにない場合は、[TID ブロック（TID Block）]。 変更されたファイル性質は [カスタム（Custom）] です。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出ブロック（Custom Detection Block）]。	TID ブロック（TID Block） 変更されたファイル性質は [カスタム（Custom）] です。

ファイル傾向（File Disposition）	Threat Intelligence Director SHA-256 監視可能アクション	Threat Intelligence Director インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
[マルウェア（Malware）] または [カスタム（Custom）]	モニター	ブロック	マルウェア ブロック（Block Malware）	マルウェア ブロック（Block Malware）
	ブロック（Block）	ブロック	• SHA-256 がカスタム検出リストにない場合は、[TID ブロック（TID Block）]。 変更されたファイル性質は [カスタム（Custom）] です。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出ブロック（Custom Detection Block）]。	TID ブロック（TID Block） 変更されたファイル性質は [カスタム（Custom）] です。

Threat Intelligence Director 設定の表示および変更

必要に応じて、次の情報を使用して設定を見直し、微調整します。

要素（管理対象デバイス）の Threat Intelligence Director ステータスの表示

管理対象デバイスとして Firewall Management Center に登録されているすべてのデバイスは、[要素（Elements）] ページに自動的に表示されます。すべての（Threat Intelligence Director をサポートするためのポリシーの設定（2948 ページ） で指定されたとおりに）適切に構成された要素は、要素が追加される前に取り込まれたものを含めて、現在公開されているすべてのオブザーバブルを受信します。

手順

ステップ 1 [統合（Integration）]>[インテリジェンス（Intelligence）]>[要素（Elements）]を選択します。>>

ステップ 2 要素が接続され、Threat Intelligence Director が有効になっているかどうかを確認するには、要素名の横にあるアイコンにカーソルを合わせます。

（注）
展開後、適用されたアクセス コントロール ポリシーと TID が有効かどうかなど、このページの情報が更新されるまで、最大 5 分かかる場合があります。

ソースの表示と管理

[ソース（Sources）]ページには、設定済みのすべてのソースに関する概要情報が表示されます（ソース サマリー情報 （2977 ページ）を参照）。

手順

ステップ 1 **[統合（Integration）]>[インテリジェンス（Intelligence）]>[ソース（Sources）]** を選択します。

ステップ 2 ソースを次のように表示します。

- ページに表示されるソースをフィルタ処理するには、[フィルタ（Filter）]（ ）をクリックします。詳細については、テーブル ビューでの Threat Intelligence Director データのフィルタ処理 （2985 ページ）を参照してください。
- 詳細な取り込みステータスを表示するには、[ステータス（Status）]列のテキストの上にカーソルを移動します。詳細については、ソース ステータスの詳細 （2978 ページ）を参照してください。

ステップ 3 ソースを次のように管理します。

- [アクション（Action）]設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。固定されているアクションがある場合、ソースの[タイプ（Type）]には、そのアクションだけがサポートされます。
- [公開（Publish）]設定を編集するには、[スライダ（Slider）]（ ）をクリックします。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。

- Threat Intelligence Director によるソースの更新を一時停止または再開する場合は、[更新の一時停止（Pause Updates）] または [更新の再開（Resume Updates）] をクリックします。更新を一時停止すると、更新は中断されますが、既存のインジケータとオブザーバブルは TID 内に残ります。
- ソースを削除するには、[削除（Delete）]（） をクリックします。ソースが現在処理中の場合、[削除（Delete）] はグレー表示になります。ソースを削除すると、そのソースに関連付けられているすべてのインジケータも削除されます。関連付けられているオブザーバブルも削除される可能性があります。ただし、システム内に残っているインジケータに関連付けられたオブザーバブルは保持されます。

ソース サマリー情報

[ソース（Sources）]ページには、設定されているすべてのソースの概要情報が表示されます。次の表で、概要表示に含まれるフィールドについて簡単に説明します。これらのフィールドの詳細については、ソースの関連設定トピックの説明を参照してください。データ ソースを取り込むためのオプション （2950 ページ） を参照してください。

表 *247 :* ソース サマリー情報

フィールド	説明
[名前（Name）]	ソース名。
Type	ソースのデータ形式（[STIX] または [フラットファイル（Flat File）]）。
配信	Threat Intelligence Director がソースを取得するのに使用する手法。
操作（Action）	このソースに含まれるデータと一致するトラフィックに対してシステムで実行するように設定されているアクション（[ブロック（Block）] または [モニター（Monitor）]）。 可用性、継承、および継承のオーバーライドを含むThreat Intelligence Director のアクションの詳細については、アクションに影響を与える要因 （2968 ページ） を参照してください。
パブリッシュ	[オン（On）] または [オフ（Off）] トグル。登録されている要素（Threat Intelligence Director をサポートするために設定された管理対象デバイス）に Threat Intelligence Director がソースからのデータを公開するかどうかを指定します。 インジケータは親ソースから [公開（Publish）] 設定を継承でき、オブザーバブルは親インジケータから [公開（Publish）] 設定を継承できます。詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。
最終更新日時（Last Updated）	Threat Intelligence Director が最後にソースを更新した日時。

フィールド	説明
Status（ステータス）	ソースの現在のステータス。 • [新規（New）]：ソースは新規に作成されます。 • [スケジュール済み（Scheduled）]：初回のダウンロードまたはその後の更新がスケジュールされていますが、まだ進行中ではありません。 • [ダウンロード 中（Downloading）]：Threat Intelligence Director が初回のダウンロードまたは更新を処理中です。 • [解析中（Parsing）] または [処理中（Processing）]：Threat Intelligence Director がソースを取り込んでいます。 • [完了（Completed）]：Threat Intelligence Director はソースの取り込みを終了しました。 • [完了（エラーあり）（Completed with Errors）]：Threat Intelligence Director はソースの取り込みを終了しましたが、一部のオブザーバブルがサポートされていないか無効です。 • [エラー（Error）]：Threat Intelligence Director による処理にエラーが発生しました。[更新間隔（Update Frequency）] が指定された TAXII ソースまたは URL ソースの場合、更新が一時停止でなければ、 Threat Intelligence Director はスケジュールされている次回の更新で再試行します。 ページを更新してステータスを更新します。
[編集（Edit）]（）	このアイコンをクリックすると、ソースの設定を編集できます。
[削除（Delete）]（）	このアイコンをクリックすると、ソースが完全に削除されます。

ソース ステータスの詳細

ソースの概要ページに表示されるソースの [ステータス（Status）] 値にマウスオーバーすると、Threat Intelligence Director は次の詳細情報を表示します。

データ	説明
ステータス メッセージ	ソースの現在のステータスを簡単に説明します。
最終更新日（Last Updated）	Threat Intelligence Director が最後にソースを更新した日時を表示します。
次回更新日（Next Update）	TAXII および URL ソースの場合、この値は Threat Intelligence Director が次にソースを更新する時期を指定します。

データ	説明
インジケータ（Indicators）	インジケータ カウントを表示します。 • [使用済み（Consumed）]：最近のソース更新中に Threat Intelligence Director が処理したインジケータの数。この数値は、取り込みや破棄が行われたかどうかに関係なく、その更新に含まれていたすべてのインジケータを表します。 • [破棄済み（Discarded）]：最近の更新でシステムが Threat Intelligence Director に追加しなかった無効なインジケータの数。 （注） TAXII ソースの場合、 Threat Intelligence Director は [最終更新（Last Update）] と [合計（Total）] とに分けてインジケータ数を表示します。これは、TAXII の場合、既存のデータを置換する形式ではなく、増分データを追加する形式で更新が行われるからです。他のソース タイプのインジケータの場合、これらのソースの更新では既存のデータ セットが完全に置換されるので、Threat Intelligence Director は [最終更新（Last Update）] の値のみを表示します。 あるインジケータのオブザーバブルがすべて [無効（Invalid）] の場合、 Threat Intelligence Director はそのインジケータを破棄します。
オブザーバブル（Observables）	オブザーバブルの数を表示します。 • [使用済み（Consumed）]：最近のソース更新中に Threat Intelligence Director が処理したオブザーバブルの数。この数値は、取り込みや破棄が行われたかどうかに関係なく、その更新に含まれていたすべてのオブザーバブルを表します。 • [サポート対象外（Unsupported）]：最近の更新でシステムが Threat Intelligence Director に追加しなかったサポートされないオブザーバブルの数。 サポートされているオブザーバブルのタイプに関する詳細については、ソース要件（2946 ページ） でコンテンツ タイプに関する情報を参照してください。 • [無効（Invalid）]：最近の更新でシステムが Threat Intelligence Director に追加しなかった無効なオブザーバブルの数。 オブザーバブルが正しく作成されていない場合は無効になります。たとえば、10.10.10.10.123 は有効な IPv4 アドレスではありません。 （注） TAXII ソースの場合、 Threat Intelligence Director は [最終更新（Last Update）] と [合計（Total）] とに分けてオブザーバブル数を表示します。これは、TAXII の場合、既存のデータを置換する形式ではなく、増分データを追加する形式で更新が行われるからです。他のソース タイプのオブザーバブルの場合、これらのソースの更新では既存のデータ セットが完全に置換されるので、Threat Intelligence Director は [最終更新（Last Update）] の値のみを表示します。

インジケータの表示と管理

インジケータは、取り込まれたソースから自動的に生成されます。このページの詳細については、インジケータ サマリー情報 （2981 ページ） を参照してください。

手順

ステップ 1 **[インテリジェンス（Intelligence）]** > **[ソース（Sources）]** の順に選択します。

ステップ 2 [インジケータ（Indicators）] をクリックします。

ステップ 3 現在のインジケータを次のように表示します。

- ページに表示されるインジケータをフィルタリングするには、[フィルタ（Filter）] （ ）をクリックします。詳細については、テーブル ビューでの Threat Intelligence Director データのフィルタ処理 （2985 ページ）を参照してください。
- インジケータの詳細情報（関連付けられているオブザーバブルなど）を表示するには、インジケータ名をクリックします。詳細については、インジケータの詳細 （2982ページ）を参照してください。
- インジケータに関連付けられているインシデントについての情報を表示するには、[インシデント（Incidents）]列内の番号をクリックします。また、インシデントの上にカーソルを移動すると、インシデントが完全に実現されたか、部分的に実現されたかを確認できます。
- ソースからのインジケータの調査が Threat Intelligence Director で完了したかどうかを判別するには、[ステータス（Status）] 列を確認します。

ステップ 4 現在のインジケータを次のように管理します。

- [アクション（Action）] を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。固定されているアクションがある場合、ソースの [タイプ（Type）] には、そのアクションだけがサポートされます。
- [公開（Publish）]設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。
- インジケータの 1 つ以上のオブザーバブルをブロックしないリストに追加するには、インジケータ名をクリックして [インジケータの詳細（Indicator Details）] ページにアクセスします。詳細については、「Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について （2992 ページ）」を参照してください。

インジケータ サマリー情報

[インジケータ（Indicators）]ページには、設定されたソースに関連付けられているすべてのインジケータの概要情報が表示されます。

表 *248*：インジケータ サマリー情報

フィールド	説明
[タイプ（Type）]	• 1 つオブザーバブルを持つインジケータには、そのオブザーバブルのデータ タイプがリストされます（URL、SHA-256 など）。 • 2 つ以上のオブザーバブルを持つインジケータは、[複合（Complex）] としてリストされます。 特定のオブザーバブルを確認するには、タイプの上にカーソルを移動します。
名前（**Name**）	インジケータ名。
ソース（**Source**）	インジケータが含まれていたソース（親ソース）。
[インシデント（Incidents）]	インジケータに関連付けられたすべてのインシデントに関する情報。 • インシデントが**部分的に実現**（）されるか、**完全に実現**（）されるかを指定するアイコン。 • インジケータに関連付けられたインシデント数。
操作（**Action**）	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。 インジケータは親ソースから[アクション（Action）]設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。 インジケータは親ソースから[公開（Publish）]設定を継承でき、オブザーバブルは親インジケータから[公開（Publish）]設定を継承できます。詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。
最終更新日時（**Last Updated**）	Threat Intelligence Director が最後にインジケータを更新した日時。

フィールド	説明
Status（ステータス）	インジケータの現在のステータス。 • [保留中（Pending）]：Threat Intelligence Director はインジケータのオブザーバブルを取り込み中です。 • [完了（Completed）]：Threat Intelligence Director はインジケータのオブザーバブルをすべて正常に取り込みました。 • [完了（エラーあり）（Completed With Errors）]：Threat Intelligence Director はインジケータを取り込みましたが、一部のオブザーバブルがサポートされていないか無効です。

インジケータの詳細

[インジケーターの詳細（Indicator Details）] ページには、インシデントのインジケータとオブザーバブル（監視可能）データが表示されます。

表 *249*：インジケータの詳細情報

フィールド	説明
[名前（Name）]	インジケータ名。
Description	ソースから提供されたインジケータの説明。
ソース（Source）	インジケータが含まれていたソース。
有効期限	ソースの [TTL] 値に基づく、インジケータが期限切れになる日時。
操作（Action）	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。 インジケータは親ソースから [アクション（Action）] 設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。 インジケータは親ソースから [パブリッシュ（Publish）] 設定を継承でき、オブザーバブルは親インジケータから [パブリッシュ（Publish）] 設定を継承できます。詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。

フィールド	説明
インジケータのパターン（Indicator Pattern）	インジケーターのパターンを形成するオブザーバブルと演算子。演算子はインジケーター内のオブザーバブルをリンクします。AND 関係は [AND] 演算子で示されます。OR 関係は、**OR** 演算子、または複数のオブザーバブルの緊密なグループ化によって示されます。 必要に応じて、**[ブロックしないリストに追加（Add to Do-Not-Block List）]** ボタンをクリックして、オブザーバブルをブロックしないリストに追加します。詳細については、「Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について （2992 ページ）」を参照してください。

オブザーバブルの表示と管理

[オブザーバブル（Observables）] ページには、正常に取り込まれたすべてのオブザーバブルが表示されます（オブザーバブル サマリー情報 （2984 ページ）を参照）。

始める前に

- ソースとして使用する TAXII フィードの取得 （2950 ページ）、URL からのソースの取得 （2952 ページ）、またはソースとして使用するローカルファイルのアップロード （2954 ページ）の説明に従って 1 つ以上のソースを設定します。

手順

ステップ 1 **[インテリジェンス（Intelligence）]** > **[ソース（Sources）]** の順に選択します。

ステップ 2 [オブザーバブル（Observables）] をクリックします。

ステップ 3 現在のオブザーバブルを次のように表示します。

- ページに表示されるオブザーバブルをフィルタリングするには、[フィルタ（Filter）] （🔍）をクリックします。詳細については、テーブル ビューでの Threat Intelligence Director データのフィルタ処理 （2985 ページ）を参照してください。
- [値（Value）] 列の情報が途切れている場合は、値の上にカーソルを移動します。
- そのオブザーバブルを含むインジケータを表示するには、[インジケータ（Indicators）] 列内の番号をクリックします。[インシデント（Incidents）] ページが開き、オブザーバブルの値がフィルタとして適用されます。詳細については、インジケータの表示と管理 （2980 ページ）を参照してください。

ステップ 4 現在のオブザーバブルを次のように管理します。

- [アクション（Action）] を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。

- オブザーバブルの[公開（Publish）]設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。
- オブザーバブルの有効期限を変更するには、親ソースの[TTL]を変更します。詳細については、ソースの表示と管理 （2976 ページ）を参照してください。
- オブザーバブルをブロックしないリストに追加するには、**[ブロックしないリストに追加（Add to Do-Not-Block List）]** ボタンをクリックします。詳細については、「Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について （2992 ページ）」を参照してください。

オブザーバブル サマリー情報

[オブザーバブル（Observables）]ページには、取り込まれたすべてのオブザーバブルの概要情報が表示されます。

表 *250*：オブザーバブル サマリー情報

フィールド	説明
[タイプ（Type）]	オブザーバブル（監視可能）データのタイプ：`SHA-256`、`Domain`、`URL`、`IPv4`、または `IPv6`。
値	オブザーバブルを構成するデータ。
インジケータ（Indicators）	オブザーバブルを含む親インジケータの数。
操作（Action）	オブザーバブルに対して設定されている操作。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集 （2988 ページ）を参照してください。 インジケータは親ソースから[アクション（Action）]設定を継承でき、オブザーバブルは親インジケータから[アクション（Action）]設定を継承できます。詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。
パブリッシュ	オブザーバブルのパブリッシュ設定（ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照）。 インジケータは親ソースから[公開（Publish）]設定を継承でき、オブザーバブルは親インジケータから[公開（Publish）]設定を継承できます。詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。

フィールド	説明
更新時刻（**Updated At**）	Threat Intelligence Director が最後にオブザーバブルを更新した日時。
有効期限	親インジケータの [TTL] に基づいて、オブザーバブルが Threat Intelligence Director から自動的に消去される日付。
[ブロックしないリストに追加（Add to Do-Not-Block List）] ボタン	このボタンをクリックすると、オブザーバブルがブロックしないリストに追加されます。Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について （2992 ページ）を参照してください。

テーブル ビューでの Threat Intelligence Director データのフィルタ処理

手順

ステップ 1 次のいずれかの Threat Intelligence Director テーブル ビューを選択します。

- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [インシデント（Incidents）]**
- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）]**
- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）]**
- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [監視可能（Observables）]**

ステップ 2 [フィルタ（Filter）]（🔍）をクリックし、フィルタ属性を選択します。

ステップ 3 そのフィルタ属性の値を選択または入力します。

フィルタでは大文字/小文字が区別されます。

ステップ 4 （オプション）複数の属性でフィルタリングするには、[フィルタ（Filter）]（🔍）をクリックし、手順 2 と手順 3 を繰り返します。

ステップ 5 前回フィルタを適用してから行った変更を取り消すには、[キャンセル（Cancel）] をクリックします。

ステップ 6 フィルタを適用してテーブルを更新するには、[適用（Apply）] をクリックします。

ステップ 7 フィルタ属性を個別に削除するには、フィルタ属性の横にある**削除**（ ）をクリックし、[適用（Apply）] をクリックしてテーブルを更新します。

Threat Intelligence Director 設定における継承

Threat Intelligence Director はソースからインテリジェンス データを取り込むと、そのソースの子オブジェクトとしてインジケータとオブザーバブルを作成します。作成時に、これらの子オブジェクトは、親設定から [アクション（Action）] および [公開（Publish）] 設定を継承します。

インジケータは、親ソースからこれらの設定を継承します。インジケータは、親ソースを1つしか持てません。

オブザーバブルは、親インジケータからこれらの設定を継承します。オブザーバブルは、複数の親インジケータを持つことができます。

詳細については、以下を参照してください。

- 複数の親からの TID 設定の継承 （2986 ページ）
- 継承された TID 設定の上書きについて （2987 ページ）

複数の親からの TID 設定の継承

オブザーバブルに複数の親インジケータがある場合、システムはすべての親から継承した設定を比較し、オブザーバブルに最もセキュアなオプションを割り当てます。つまり、

- [アクション（Action）] : [ブロック（Block）] は [モニタ（Monitor）] よりもセキュアです。
- [公開（Publish）] : [オン（On）] は [オフ（Off）] よりもセキュアです。

たとえば、SourceA は IndicatorA と関連する ObservableA に関与する可能性があります。

設定	SourceA	IndicatorA	ObservableA
アクション	ブロック	ブロック（Block）	ブロック（Block）
パブリッシュ	オフ（Off）	オフ（Off）	オフ（Off）

SourceB が後で ObservableA を含む IndicatorB に関与する場合、システムは ObservableA を次のように変更します。

設定	SourceB	IndicatorB	ObservableA
操作（Action）	モニター	モニター	[ブロック（Block）]（IndicatorA から継承）

設定	SourceB	IndicatorB	ObservableA
パブリッシュ	オン（On）	オン（On）	[オン（On）]（IndicatorB から継承）

この例では、ObservableA には 2 つの親があります。1 つは [アクション（Action）] 設定の親で、もう 1 つは [公開（Publish）] 設定の親です。オブザーバブルの設定を手動で編集してから設定を元に戻した場合、[アクション（Action）] 設定が IndicatorA 値に設定され、[公開（Publish）] 設定が IndicatorB 値に設定されます。

継承された TID 設定の上書きについて

継承された設定を上書きするには、子レベルで設定を変更します。ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集（2988 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開（2990 ページ）を参照してください。継承された設定を上書きすると、親オブジェクトに変更にかかわらず、子オブジェクトではその設定が保持されます。

たとえば、上書きを設定せずに、次の元の設定で開始するとします。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オフ（Off）	オフ（Off）	オフ（Off）

IndicatorA の設定を上書きした場合、設定は次のようになります。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オン（On）	オン（On）	オン（On）

この場合、SourceA の [公開（Publish）] 設定への変更は、IndicatorA に自動的にはカスケードされなくなります。ただし、オブザーバブルの設定は現在値を上書きするようには設定されていないため、IndicatorA から ObservableA1 および ObservableA2 への継承は続行されます。

後から ObservableA1 の設定を上書きする場合は、次のようになります。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オン（On）	オフ（Off）	オン（On）

IndicatorA の [公開（Publish）] 設定への変更は、ObservableA1 に自動的にはカスケードされなくなります。ただし、ObservableA2 は上書き値には設定されていないため、これらの変更は引き続き ObservableA2 にカスケードされます。

オブザーバブル レベルでは、上書き設定から継承された設定に戻すことができ、システムは、親インジケータからそのオブザーバブルへの設定変更のカスケードを自動的に再開します。

ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director アクションの編集

（注）

- 親のアクションを編集すると、すべての子に対しアクションが設定されます。ソース レベルでアクションを編集すると、そのすべてのインジケータにアクションが設定されます。インジケータ レベルでアクションを編集すると、そのオブザーバブルのすべてに対してアクションが設定されます。
- 子のアクションを編集すると、継承が中断されます。インジケータ レベルでアクションを編集し、続いてソース レベルで編集すると、個々のインジケータのアクションを編集するまで、インジケータのアクションが保持されます。監視可能レベルでアクションを編集し、続いてインジケータ レベルで編集すると、個々のオブザーバブルのアクションを編集するまで、オブザーバブルのアクションが保持されます。監視可能レベルでは、親インジケータのアクションに自動的に復元できます。継承の詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。

他の アクションに影響を与える要因 （2968 ページ） を確認することもできます。

手順

ステップ 1 次のいずれかを選択します。

- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）]**

  （注）
  Threat Intelligence Director は、ソース レベルでの TAXII ソースのブロックをサポートしていません。TAXII ソースに簡易インジケータが含まれている場合、インジケータ レベルまたは監視可能レベルでブロックすることができます。

- [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）] > > >

  （注）
  Threat Intelligence Director は、複雑なインジケータのブロックをサポートしていません。代わりに、複雑なインジケータ内で個々のオブザーバブルをブロックします。

- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [監視可能（Observables）]**

ステップ 2 [アクション（Action）] ドロップダウンを使用して、 または **Block** ( ) を選択します。

ステップ 3 （オブザーバブルのみ）親インジケータからアクション設定を継承し直すには、オブザーバブルの [アクション（Action）] 設定の横にある [復元（Revert）] をクリックします。

公開の一時停止について

- 機能レベルで公開を一時停止すると、要素に保存されているすべての Threat Intelligence Director オブザーバブルが消去されます。つまり、Threat Intelligence Director は脅威を検出、監視、ブロックすることはできません。システム上の他のセキュリティ機能は影響を受けません。
- ソース、インジケータ、またはオブザーバブル レベルで公開を一時停止すると、システムは一時停止された Threat Intelligence Director オブザーバブルを要素から削除し、トラフィックと一致しないようにします。
- 親のパブリケーションを一時停止すると、すべての子が一時停止します。ソース レベルで公開を一時停止すると、そのすべてのインジケータの公開が一時停止されます。インジケータ レベルで公開を一時停止すると、そのすべてのオブザーバブルの公開が一時停止されます。
- 子のパブリケーションを一時停止すると、継承が中断されます。インジケータ レベルで公開を一時停止し、その後にソース レベルで公開すると、インジケータの個別設定を変更するまで、インジケータの公開は一時停止されたままになります。監視可能レベルで公開を一時停止し、その後にインジケータ レベルで公開すると、オブザーバブルの個別設定を変更するまで、オブザーバブルの公開は一時停止されたままになります。監視可能レベルでは、親インジケータの公開ステータスに自動的に復元できます。継承の詳細については、Threat Intelligence Director 設定における継承 （2986 ページ）を参照してください。
- アップロードされたソースの公開は、インジケータ レベルでのみ一時停止することができます。
- オブザーバブルの公開を一時停止することと、オブザーバブルをブロックしないリストに追加することの比較については、Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について （2992 ページ）を参照してください。
- 個々のオブザーバブルまたはインジケータに対して公開または一時停止の設定を指定した場合、更新プログラムに同じオブザーバブルまたはインジケータが含まれている場合、ソースの更新によってその設定が変わることはありません。
- オブジェクト管理ページで公開を無効にすることができます。オブザーバブルのパブリケーション頻度の変更 （2991 ページ）を参照してください。
- 更新を一時停止する [ソース（Sources）] ページ上のオプションは、要素へのデータの公開には関連しません。フィードから Firewall Management Center 上のソースを更新する場合に適用されます。

Threat Intelligence Director の一時停止と要素からの Threat Intelligence Director データの消去

注意 この設定により、すべての要素への公開が一時停止され、要素に保存されたすべての Threat Intelligence Director オブザーバブルが消去され、Threat Intelligence Director 機能を使用したトラフィックの検査が停止されます。

より細かいレベルでオブザーバブルを無効にするには、ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ）を参照してください。

管理センター上のデータ（既存のインシデントと設定済みのソース、インジケータ、オブザーバブル、およびソースの取り込み）は、この設定の影響を受けません。

手順

ステップ 1 **[インテリジェンス（Intelligence）] > [設定（Settings）]** の順に選択します。

ステップ 2 [一時停止（Pause）] をクリックします。

次のタスク

要素への Threat Intelligence Director データの同期とオブザベーションの生成を再開する準備ができたら、このページから手動で公開を [再開（Resume）] します。管理センター上の既存のオブザーバブルがすべての要素に公開されます。

ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開

ソース レベルで公開が有効になっている場合、システムは最初のソース データとそれに続く以下のような変更を自動的に公開します。

- 定期的なソースの更新からの変更
- システム アクションに起因する変更（**TTL** の有効期限など）
- ユーザーが開始した変更（インジケータやオブザーバブルの [アクション（Action）] 設定の変更など）

（注） デバイス（要素）から一度にすべての Threat Intelligence Director オブザーバブルを消去するには、Threat Intelligence Director の一時停止と要素からの Threat Intelligence Director データの消去（2990 ページ） を参照してください。

始める前に

公開を一時停止する前に、公開の一時停止について（2989ページ） に記載されている影響を把握してください。

手順

ステップ 1 次のいずれかを選択します。

- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）]**
- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）]**
- **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [監視可能（Observables）]**

ステップ 2 [公開（Publish）][スライダ（Slider）]（ ）を検索して、要素への公開を切り替えるために使用します。

ステップ 3 （オブザーバブルのみ）親インジケータからパブリケーション設定を継承し直す場合は、オブザーバブルの [公開（Publish）] 設定の横にある [復元（Revert）] をクリックします。

次のタスク

- 要素が変更を受け取るまで少なくとも 10 分間待機します。大規模なソースが含まれる変更には時間がかかります。
- （オプション）オブザーバブル レベルで TID データのパブリケーション頻度を変更します。オブザーバブルのパブリケーション頻度の変更（2991 ページ） を参照してください。

オブザーバブルのパブリケーション頻度の変更

デフォルトでは、監視可能データ（オブザーバブル）が TID 要素に 5 分ごとに公開されます。この間隔を別の値に設定するには、次の手順を実行します。

始める前に

- 監視可能レベルで TID データのパブリケーションを有効にします。ソース、インジケータ、またはオブザーバブル レベルでの Threat Intelligence Director データの一時停止または公開 （2990 ページ） を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 **[セキュリティインテリジェンス（Security Intelligence）]** > **[ネットワークリストとフィード（Network Lists and Feeds）]** を選択します。

ステップ 3 [Cisco-TIDフィード（Cisco-TID-Feed）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 4 [更新間隔:（Update Frequency）] ドロップダウンリストから値を選択します。

- 監視可能なデータの要素への公開を停止するには、[無効（Disable）] を選択します。
- その他の値を選択して、監視可能なパブリケーションの間隔を設定します。

ステップ 5 [保存（Save）] をクリックします。

Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について

指定された [アクション（Action）] から簡易インジケータ内の 1 つのオブザーバブルを除外する（モニタリング/ブロッキングなしでトラフィックを通過させる）には、オブザーバブルをブロックしないリストに追加することができます。

複雑なインジケータでは、Threat Intelligence Director はトラフィックを評価するときにブロックしないリストのオブザーバブルを無視しますが、そのインジケータ内の他のオブザーバブルは引き続き評価されます。たとえば、インジケータにAND演算子でリンクされているオブザーバブル 1 とオブザーバブル 2 が含まれていて、オブザーバブル 1 をブロックしないリストに追加すると、Threat Intelligence Director はオブザーバブル 2 が認識されたときに完全に実現されたインシデントを生成します。

これに対して、同じ複雑なインジケータで、オブザーバブル 1 をブロックしないリストに追加するのではなく、その公開を無効にすると、Threat Intelligence Director はオブザーバブル 2 が認識されたときに部分的に実現されたインシデントを生成します。

（注） オブザーバブルをブロックしないリストに追加する場合、オブザーバブルの設定が継承されるか上書き値であるかにかかわらず、常に [アクション（Action）] 設定より優先されます。

更新プログラムに同じオブザーバブルが含まれている場合、ソースの更新は個々のオブザーバブルのブロックしないリスト設定に影響しません。

Threat Intelligence Director オブザーバブルのブロックしないリストへの追加

ブロックしないリストの使用の詳細については、Threat Intelligence Director オブザーバブルのブロックしないリストへの追加について （2992 ページ）を参照してください。

ヒント Web インターフェイスのいくつかの場所に [ブロックしないリストに追加（Add to Do Not Block List）] ボタン（）が表示されます。このボタンをクリックすると、これらの場所にあるいずれかのブロックしないリストにオブザーバブルを追加できます。

手順

ステップ 1 **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [監視可能（Observables）]** を選択します。

ステップ 2 許可するオブザーバブルに移動します。

ステップ 3 そのオブザーバブルの （**[ブロックしないリストに追加（Add to Do-Not-Block List）]**）をクリックします。

次のタスク

（オプション）ブロックしないリストからオブザーバブルを削除する必要がある場合は、ボタンをもう一度クリックします。

STIX ソース ファイルの表示

手順

ステップ 1 **[統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）]**を選択します。

ステップ 2 インジケータ名をクリックします。

ステップ 3 [STIXのダウンロード（Download STIX）] をクリックします。

ステップ 4 テキスト エディタでこのファイルを開きます。

Threat Intelligence Director のトラブルシューティング

以下のセクションでは、Threat Intelligence Director の一般的な問題について、可能な解決策と軽減策を説明します。

フラット ファイル ソースを取得またはアップロードするとエラーが発生する

システムがフラット ファイル ソースを取得またはアップロードできない場合は、フラット ファイル内のデータが [インテリジェンス（Intelligence）] > [ソース（Sources）] ページの [タイプ（Type）] 列と一致することを確認してください。

TAXII または URL のソース アップデートでエラーが発生する

TAXII または URL のソース アップデートでソース ステータス エラーが発生した場合は、サーバー証明書の期限が切れていないことを確認してください。証明書の有効期限が切れている場合は、新しい**サーバー証明書**を入力するか、または既存の**サーバー証明書**を削除して、Threat Intelligence Director が新しい証明書を取得できるようにします。詳細については、Threat Intelligence Director ソースの TLS/SSL 設定の構成 （2955 ページ）を参照してください。

インジケータまたはソースに対して「ブロック」アクションは使用できず、「モニター」アクションのみを使用できます。

インジケータまたはソースの個々のオブザーバブルのアクションを変更できます。

Threat Intelligence Director テーブル ビューで「結果なし」と表示される

テーブル ビューには、[ソース（Sources）]、[インジケータ（Indicators）]、[オブザーバブル（Observables）]、および [インシデント（Incidents）] ページが含まれます。

いずれかの Threat Intelligence Director テーブル ビューにデータが表示されない場合：

- テーブル フィルタを確認し、[最終更新日（Last Updated）] フィルタ属性の時間枠を拡大することを検討します（テーブル ビューでの Threat Intelligence Director データのフィルタ処理 （2985 ページ）を参照）。
- ソースが正しく設定されていることを確認します（データ ソースを取り込むためのオプション （2950 ページ）を参照）。
- Threat Intelligence Director をサポートするのに必要なアクセス コントロール ポリシー、および関連するポリシーが設定されていることを確認します（Threat Intelligence Director をサポートするためのポリシーの設定 （2948 ページ）を参照）。たとえば、SHA 256 オブザーバブルがオブザベーションを生成していない場合、展開されているアクセス コントロール ポリシーに、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ポリシーを呼び出すアクセス制御ルールが 1 つ以上含まれていることを確認します。

- Threat Intelligence Director をサポートするアクセス コントロール ポリシーおよび関連するポリシーが要素に展開されていることを確認します（設定変更の展開 （172 ページ）を参照）。
- 機能レベルで Threat Intelligence Director データ パブリケーションを一時停止していないことを確認します（Threat Intelligence Director の一時停止と要素からの Threat Intelligence Director データの消去 （2990 ページ）を参照）。

システムが低速またはパフォーマンス低下を起こしている

パフォーマンスの影響の詳細については、Threat Intelligence Director のパフォーマンスへの影響 （2944 ページ） を参照してください。

Secure Firewall Management Center テーブル ビューに Threat Intelligence Director データが表示されない

オブザーバブルを要素に公開しても、接続、セキュリティ インテリジェンス、ファイル、またはマルウェア イベントのテーブルに Threat Intelligence Director データが表示されない場合は、要素に展開されたアクセス コントロール ポリシーとファイル ポリシーを確認してください。詳細については、Threat Intelligence Director をサポートするためのポリシーの設定 （2948 ページ）を参照してください。

1 つまたは複数の要素が Threat Intelligence Director データによって圧倒される

Threat Intelligence Director データが 1 つまたは複数のデバイスを圧倒している場合は、Threat Intelligence Director による要素に保存されているデータの公開と消去を一時停止することを検討してください。詳細については、Threat Intelligence Director の一時停止と要素からの Threat Intelligence Director データの消去 （2990 ページ）を参照してください。

システムが TID ブロックの代わりにマルウェア クラウド ルックアップを実行している

これは設計によるものです。詳細については、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）を参照してください。

システムが TID アクションではなく、セキュリティ インテリジェンスまたは DNS ポリシー アクションを実行している

これは設計によるものです。詳細については、Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け （2969 ページ）を参照してください。

TID が無効化されている

- アプライアンスにメモリを追加します。Threat Intelligence Director を使用するには、少なくとも 15 GB のメモリをアプライアンスに搭載する必要があります。
- Secure Firewall Management Center の REST API アクセスを有効化します。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Enabling REST API Access*」を参照してください。

システムが Threat Intelligence Director インシデントを生成しないか、または予期される Threat Intelligence Director アクションを実行しない

- すべての管理対象デバイスが Threat Intelligence Director に対し適切に有効になっており、設定されていることを確認します。要素（管理対象デバイス）の Threat Intelligence Director ステータスの表示 （2975 ページ）およびThreat Intelligence Director をサポートするためのポリシーの設定 （2948 ページ）を参照してください。
- 変更内容が要素に公開されるまでには少なくとも 5 ～ 10 分かかり、大規模なデータ フィードを公開する場合は、かかる時間がそれよりも著しく長くなります。
- オブザーバブルに対するアクション設定を確認します。オブザーバブルの表示と管理 （2983 ページ）を参照してください。
- システムが実行する Threat Intelligence Director アクションに影響を与える他の要因のリストについては、アクションに影響を与える要因 （2968 ページ） を参照してください。
- 要素（管理対象デバイス）に、予想していた脅威データが含まれていない可能性があります。公開の一時停止について （2989 ページ）を参照してください。

特定の脅威との一度の遭遇によって、複数のインシデントが生成される

これは、単一のインジケータが複数のソースに含まれている場合に発生します。

詳細については、「重複インジケータの処理 （2955 ページ）」を参照してください。

Threat Intelligence Director の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
複数の STIX フィードに含まれるインジケータの扱い	7.1	任意（Any）	STIX フィードに同一のインジケータが含まれている場合、フィードごとにインジケータが作成され、同じインジケータに対して複数のインシデントが生成される可能性があります。以前は、最後にダウンロードされたフィードのみが有効でした。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細

アクションの優先順位付けの変更	6.5	任意（Any）	これらの変更は、複数の Firepower 機能を特定の 1 つのオブザーバブルに適用可能な場合に適用されます。
			
			TID ブロッキングおよびモニタリング監視可能アクションが、セキュリティインテリジェンスを使用したブロッキングおよびモニタリングよりも優先されるようになりました。
			
			重要
			システムは引き続き、トラフィックを以前と同様に効果的に処理します。以前にブロックされたトラフィックは引き続きブロックされ、モニター対象トラフィックは引き続きモニターされます。これは、アクションに関与しているとイベント内で報告されるコンポーネントを変更するだけです。さらに、より多くの TID インシデントが生成されている場合もあります。
			
			• [ブロック（Block）]TID監視可能アクションを設定した場合は、トラフィックがセキュリティインテリジェンスブロックアクションにも一致していても、次のようになります。
			  • 接続イベントのセキュリティ インテリジェンス カテゴリは TID ブロックのバリアントです。
			  • システムは、[Blocked] のアクション実施を伴う TIDインシデントを生成します。
			
			• [モニター（Monitor）] TID 監視可能アクションを設定した場合は、トラフィックがセキュリティインテリジェンスモニタールールにも一致していても、次のようになります。
			  • 接続イベントのセキュリティ インテリジェンス カテゴリは TID モニターのバリアントです。
			  • システムは、[Monitored] のアクション実施を伴う TIDインシデントを生成します。
			
			以前は、どちらの場合も、システムではカテゴリが分析別に報告され、TID インシデントは生成されませんでした。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Secure Firewall Threat Intelligence Director	6.2.2	いずれか	導入された機能：外部送信元から脅威のインテリジェンスを使用して脅威を特定し処理できます。 新規画面：複数のタブがあるトップレベルの新しい [インテリジェンス（Intelligence）] メニュー サポートされているプラットフォーム： Secure Firewall Management Center

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。