CLI ブック 2：Cisco Secure Firewall ASA ファイアウォール CLI 9.22 コンフィギュレーション ガイド

最終更新：2026 年 10 月 5 日

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

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

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

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

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

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

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

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

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

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

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

© 2026 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

このマニュアルについて xxi

本書の目的 xxi

関連資料 xxi

表記法 xxi

通信、サービス、およびその他の情報 xxiii

第 1 章

Cisco Secure Firewall ASA ファイアウォール サービスの概要 1

ファイアウォール サービスの実装方法 1

基本アクセス制御 2

URL フィルタリング 2

データ保護 3

仮想環境のファイアウォール サービス 3

ネットワーク アドレス変換 4

アプリケーション インスペクション 5

使用例：サーバーの公開 5

第 I 部：

アクセス コントロール 9

第 2 章

アクセス制御のオブジェクト 11

オブジェクトのガイドライン 11

オブジェクトの設定 12

ネットワーク オブジェクトとグループの設定 12

ネットワーク オブジェクトの設定 12

ネットワーク オブジェクト グループの設定 13

サービス オブジェクトとサービス グループの設定 14
サービス オブジェクトの設定 15
サービス グループの設定 16
ネットワーク サービス オブジェクトとネットワーク サービス オブジェクト グループの設定 18
ネットワーク サービス オブジェクトのガイドライン 18
信頼できる DNS サーバの構成 19
ネットワーク サービス オブジェクトの設定 21
ネットワーク サービス オブジェクト グループの設定 22
ローカル ユーザー グループの設定 24
セキュリティ グループ オブジェクト グループの設定 25
時間範囲の設定 27
オブジェクトのモニタリング 28
オブジェクトの履歴 29

第 3 章 アクセス コントロール リスト 33
ACL について 33
ACL タイプ 33
ACL 名 35
アクセス コントロール エントリの順序 36
許可/拒否と一致/不一致 36
アクセス コントロールによる暗黙的な拒否 36
NAT 使用時に拡張 ACL で使用する IP アドレス 37
時間ベース ACE 38
アクセス制御リストのライセンス 38
ACL のガイドライン 39
ACL の設定 40
基本的な ACL 設定および管理オプション 40
拡張 ACL の設定 41
IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 42
ポートベースの照合に使用する拡張 ACE の追加 44

ICMP ベースの照合に使用する拡張 ACE の追加 45
ユーザーベースの照合（アイデンティティ ファイアウォール）に使用する拡張 ACE の追加 46
セキュリティ グループ ベースの照合（Cisco TrustSec）に使用する拡張 ACE の追加 47
拡張 ACL の例 48
アドレスを拡張 ACL のオブジェクトに変換する例 49
標準 ACL の設定 50
Webtype ACL の設定 50
URL 照合に使用する Webtype ACE の追加 51
IP アドレス照合に使用する Webtype ACE の追加 52
Webtype ACL の例 53
EtherType ACL の設定 55
EtherType ACL の例 56
隔離されたコンフィギュレーション セッションでの ACL の編集 57
ACL のモニタリング 59
ACL の履歴 59

第 4 章 アクセス ルール 63
ネットワーク アクセスの制御 63
ルールに関する一般情報 64
インターフェイス アクセス ルールとグローバル アクセス ルール 64
インバウンド ルールとアウトバウンド ルール 64
ルールの順序 66
暗黙的な許可 66
暗黙的な拒否 66
NAT とアクセス ルール 67
同一のセキュリティ レベル インターフェイスとアクセスルール 67
拡張アクセス ルール 68
リターン トラフィックに対する拡張アクセス ルール 68
ブロードキャストとマルチキャスト トラフィックの許可 68
管理アクセス ルール 69

EtherType ルール 69
サポートされている EtherType およびその他のトラフィック 69
リターン トラフィックに対する EtherType ルール 70
MPLS の許可 70
アクセス ルールのライセンス 70
アクセス制御に関するガイドライン 71
アクセス制御の設定 73
アクセス グループの設定 73
ICMP アクセス ルールの設定 74
アクセス ルールのモニタリング 76
アクセス ルールの syslog メッセージの評価 77
ネットワーク アクセスの許可または拒否の設定例 78
アクセス ルールの履歴 79

第 5 章 **ASA および Cisco TrustSec** 83
Cisco TrustSec について 83
Cisco TrustSec の SGT および SXP サポートについて 84
Cisco TrustSec 機能のロール 85
セキュリティ グループ ポリシーの適用 86
ASA によるセキュリティ グループベースのポリシーの適用 87
セキュリティ グループに対する変更が ISE に及ぼす影響 89
ASA での送信者および受信者のロール 90
ISE への ASA の登録 91
ISE でのセキュリティ グループの作成 91
PAC ファイルの生成 92
Cisco TrustSec のガイドライン 92
Cisco TrustSec と統合するための ASA の設定 95
Cisco TrustSec と統合するための AAA サーバーの設定 96
PAC ファイルのインポート 98
Security Exchange Protocol の設定 100
SXP 接続のピアの追加 102

環境データの更新 103
セキュリティ ポリシーの設定 104
レイヤ 2 セキュリティ グループのタギング インポジションの設定 106
使用シナリオ 107
インターフェイスでのセキュリティ グループ タグの設定 108
IP-SGT バインディングの手動設定 109
トラブルシューティングのヒント 110
Cisco TrustSec の例 110
セキュアクライアントCisco TrustSec に対する VPN のサポート 111
リモート アクセス VPN グループ ポリシーおよびローカル ユーザーへの SGT の追加 112
Cisco TrustSec のモニタリング 113
Cisco TrustSec の履歴 114

第 6 章 **Cisco Umbrella** 117
Cisco Umbrella Connector について 117
Cisco Umbrella エンタープライズ セキュリティ ポリシー 118
Cisco Umbrella の登録 118
Cisco Umbrella Connector のライセンス要件 119
Cisco Umbrella のガイドラインと制限事項 119
Cisco Umbrella Connector の設定 121
Cisco Umbrella 登録サーバーからの CA 証明書のインストール 122
Umbrella Connector のグローバル設定 123
DNS インスペクション ポリシー マップでの Umbrella のイネーブル化 125
Umbrella の登録確認 127
Umbrella Connector の例 128
例：グローバル DNS インスペクション ポリシーでの Umbrella のイネーブル化 128
例：カスタム インスペクション ポリシーを使用したインターフェイス上での Umbrella のイネーブル化 129
例：Umbrella からの特定のホストまたはネットワークのグローバルな除外 131
Umbrella Connector のモニタリング 132
Umbrella サービス ポリシーの統計情報のモニタリング 132

Umbrella の syslog メッセージのモニタリング 134
Cisco Umbrella Connector の履歴 135

第 II 部： 仮想環境のファイアウォール サービス 137

第 7 章 属性ベースのアクセス制御 139
属性ベースのネットワーク オブジェクトのガイドライン 139
属性ベースのアクセス制御の設定 140
vCenter 仮想マシンの属性の設定 140
VM 属性エージェントの設定 142
属性ベースのネットワーク オブジェクトの設定 144
属性ベースのネットワーク オブジェクトを使用したアクセス制御の設定 146
属性ベースのネットワーク オブジェクトのモニタリング 148
属性ベースのアクセス制御の履歴 149

第 III 部： ネットワーク アドレス変換 151

第 8 章 Network Address Translation（NAT） 153
NAT の機能 153
NAT の基本 154
NAT の用語 154
NAT タイプ 155
ネットワークオブジェクト NAT および twice NAT 155
ネットワークオブジェクト NAT 156
twice NAT 156
ネットワークオブジェクト NAT と twice NAT の比較 156
NAT ルールの順序 157
NAT インターフェイス 159
NAT のガイドライン 160
NAT のファイアウォールモードのガイドライン 160
IPv6 NAT のガイドライン 161

IPv6 NAT のベストプラクティス 161
NAT のその他のガイドライン 162
マッピング アドレス オブジェクトのネットワーク オブジェクト NAT のガイドライン 166
実際のアドレス オブジェクトおよびマッピング アドレス オブジェクトの Twice NAT のガイドライン 167
FQDN 接続先のガイドライン 169
実際のポートおよびマッピング ポートのサービス オブジェクトの Twice NAT のガイドライン 169
ダイナミック NAT 170
ダイナミック NAT について 170
ダイナミック NAT の欠点と利点 172
ダイナミック ネットワーク オブジェクト NAT の設定 172
ダイナミック Twice NAT の設定 175
ダイナミック PAT 178
ダイナミック PAT について 178
ダイナミック PAT の欠点と利点 179
PAT プールオブジェクトのガイドライン 180
ダイナミック ネットワーク オブジェクト PAT の設定 181
ダイナミック Twice PAT の設定 184
ポート ブロック割り当てによる PAT の設定 188
Per-Session PAT または Multi-Session PATの設定 191
スタティック NAT 193
スタティック NAT について 193
ポート変換を設定したスタティック NAT 194
一対多のスタティック NAT 195
他のマッピングシナリオ（非推奨） 196
スタティック ネットワーク オブジェクト NAT またはポート変換を設定したスタティック NAT の設定 198
スタティック Twice NAT またはポート変換を設定したスタティック NAT の設定 201
アイデンティティ NAT 205
アイデンティティ ネットワーク オブジェクト NAT の設定 205
アイデンティティ Twice NAT の設定 208

NAT のモニタリング 210
NAT の履歴 211

第 9 章 NAT の例と参照 221
ネットワーク オブジェクト NAT の例 221
内部 Web サーバーへのアクセスの提供（スタティック NAT） 221
内部ホストの NAT（ダイナミック NAT）および外部 Web サーバーの NAT（スタティック NAT） 222
複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ 224
FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック NAT） 225
Twice NAT の例 227
宛先に応じて異なる変換（ダイナミック Twice PAT） 227
宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT） 228
ルーテッドモードとトランスペアレントモードの NAT 230
ルーテッドモードの NAT 230
トランスペアレントモードまたはブリッジグループ内の NAT 231
NAT パケットのルーティング 233
マッピング アドレスとルーティング 233
マッピングインターフェイスと同じネットワーク上のアドレス 233
一意のネットワーク上のアドレス 234
実際のアドレスと同じアドレス（アイデンティティ NAT） 234
リモート ネットワークのトランスペアレント モードのルーティング要件 236
出力インターフェイスの決定 236
VPN の NAT 237
NAT とリモート アクセス VPN 237
NAT およびサイト間 VPN 239
NAT および VPN 管理アクセス 242
NAT と VPN のトラブルシューティング 243
IPv6 ネットワークの変換 244
NAT64/46：IPv6 アドレスの IPv4 への変換 245

NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット 245
NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク 246
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換 248
NAT66 の例：ネットワーク間のスタティック変換 248
NAT66 の例：シンプルな IPv6 インターフェイス PAT 249
NAT を使用した DNS クエリと応答の書き換え 250
DNS 応答修正：外部の DNS サーバー 251
DNS 応答修正：別々のネットワーク上の DNS サーバー、ホスト、およびサーバー 253
DNS 応答修正：ホスト ネットワーク上の DNS サーバー 254
DNS64 応答修正 255
PTR の変更、ホスト ネットワークの DNS サーバー 256

第 10 章 アドレスとポートのマッピング（MAP） 259
アドレスとポートのマッピング（MAP）について 259
変換によるアドレスとポートのマッピング（MAP-T）について 259
アドレスとポートのマッピング（MAP）に関するガイドライン 261
MAP-T ドメインの設定 262
MAP のモニタリング 264
MAP ドメイン構成の確認 264
MAP syslog メッセージのモニタリング 265
MAP の履歴 266

第 IV 部： サービス ポリシーとアプリケーション インスペクション 267

第 11 章 サービス ポリシー 269
サービス ポリシーについて 269
サービス ポリシーのコンポーネント 269
サービス ポリシーで設定される機能 271
機能の方向性 272
サービス ポリシー内の機能照合 273

複数の機能アクションが適用される順序 274
特定の機能アクションの非互換性 275
複数のサービス ポリシーの機能照合 276
サービス ポリシーのガイドライン 277
サービス ポリシーのデフォルト 279
デフォルトのサービス ポリシー設定 279
デフォルトのクラス マップ（トラフィック クラス） 279
サービス ポリシーの設定 280
トラフィックの特定（レイヤ 3/4 クラス マップ） 282
通過トラフィック用のレイヤ 3/4 クラス マップの作成 282
管理トラフィック用のレイヤ 3/4 クラス マップの作成 285
アクションの定義（レイヤ 3/4 ポリシー マップ） 286
インターフェイス（サービス ポリシー）へのアクションの適用 288
サービス ポリシーのモニタリング 289
サービス ポリシー（モジュラ ポリシー フレームワーク）の例 289
HTTP トラフィックへのインスペクションと QoS ポリシングの適用 289
HTTP トラフィックへのインスペクションのグローバルな適用 290
特定のサーバーへの HTTP トラフィックに対するインスペクションと接続制限値の適用 291
NAT による HTTP トラフィックへのインスペクションの適用 292
サービス ポリシーの履歴 292

第 12 章 アプリケーション レイヤ プロトコル インスペクションの準備 295
アプリケーション レイヤ プロトコル インスペクション 295
アプリケーション プロトコル インスペクションを使用するタイミング 295
インスペクション ポリシー マップ 296
使用中のインスペクション ポリシー マップの交換 297
複数のトラフィック クラスの処理方法 297
アプリケーション インスペクションのガイドライン 298
アプリケーション インスペクションのデフォルト 300
デフォルト インスペクションと NAT に関する制限事項 300

デフォルトのインスペクション ポリシー マップ 305
アプリケーション レイヤ プロトコル インスペクションの設定 305
インスペクションの適切なトラフィック クラスの選択 312
正規表現の設定 313
正規表現の作成 314
正規表現クラス マップの作成 317
インスペクション ポリシーのモニタリング 317
アプリケーション インスペクションの履歴 319

第 13 章 基本インターネット プロトコルのインスペクション 321
DCERPC インスペクション 322
DCERPC の概要 322
DCERPC インスペクション ポリシー マップの設定 323
DNS インスペクション 325
DNS インスペクションのデフォルト 325
DNS インスペクション ポリシー マップの設定 326
FTP インスペクション 331
FTP インスペクションの概要 331
厳密な FTP 332
FTP インスペクション ポリシー マップの設定 333
HTTP インスペクション 337
HTTP インスペクションの概要 337
HTTP インスペクション ポリシー マップの設定 337
ICMP インスペクション 342
ICMP エラー インスペクション 342
ILS インスペクション 343
インスタント メッセージ インスペクション 344
IP オプション インスペクション 347
IP オプション インスペクションのデフォルト 348
IP オプション インスペクション ポリシー マップの設定 348
IPsec パススルー インスペクション 350

IPsec パス スルー インスペクションの概要 350
IPsec パススルー インスペクション ポリシー マップの設定 351
IPv6 インスペクション 352
IPv6 インスペクションのデフォルト 352
IPv6 インスペクション ポリシー マップの設定 353
NetBIOS インスペクション 355
PPTP インスペクション 356
RSH インスペクション 356
SMTP および拡張 SMTP インスペクション 357
SMTP および ESMTP インスペクションの概要 357
ESMTP インスペクションのデフォルト 358
ESMTP インスペクション ポリシー マップの設定 359
SNMP インスペクション 362
SQL*Net インスペクション 363
Sun RPC インスペクション 363
Sun RPC インスペクションの概要 364
Sun RPC サービスの管理 364
TFTP インスペクション 365
XDMCP インスペクション 366
VXLAN インスペクション 366
基本的なインターネット プロトコル インスペクションの履歴 367

第 14 章 音声とビデオのプロトコルのインスペクション 371
CTIQBE インスペクション 371
CTIQBE インスペクションの制限事項 371
H.323 インスペクション 372
H.323 インスペクションの概要 372
H.323 の動作 373
H.245 メッセージでの H.239 サポート 374
H.323 インスペクションの制限事項 374
H.323 インスペクション ポリシー マップの設定 375

MGCP インスペクション 378
MGCP インスペクションの概要 379
MGCP インスペクション ポリシー マップの設定 381
RTSP インスペクション 382
RTSP インスペクションの概要 382
RealPlayer 設定要件 383
RSTP インスペクションの制限事項 383
RTSP インスペクション ポリシー マップの設定 384
SIP インスペクション 386
SIP インスペクションの概要 387
SIP インスペクションの制限事項 387
デフォルトの SIP インスペクション 389
SIP インスペクション ポリシー マップの設定 389
Skinny（SCCP）インスペクション 393
SCCP インスペクションの概要 394
Cisco IP Phone のサポート 394
SCCP インスペクションの制限事項 395
デフォルトの SCCP インスペクション 395
Skinny（SCCP）インスペクション ポリシー マップの設定 395
STUN インスペクション 397
音声とビデオのプロトコル インスペクションの履歴 398

第 15 章 モバイル ネットワークのインスペクション 401
モバイル ネットワーク インスペクションの概要 401
GTP インスペクションの概要 401
モバイル端末の場所変更の追跡 402
GTP インスペクションの制限事項 402
Stream Control Transmission Protocol（SCTP）インスペクションとアクセス制御 403
SCTP ステートフル インスペクション 404
SCTP アクセス制御 405
SCTP NAT 405

SCTP アプリケーション レイヤのインスペクション 405
SCTP に関する制限事項 406
Diameter インスペクション 407
M3UA インスペクション 408
M3UA プロトコル準拠 408
M3UA インスペクションの制限事項 409
RADIUS アカウンティング インスペクションの概要 410
モバイル ネットワーク プロトコル インスペクションのライセンス 410
GTP インスペクションのデフォルト 411
モバイル ネットワーク インスペクションの設定 412
GTP インスペクション ポリシー マップの設定 412
SCTP インスペクション ポリシー マップの設定 417
Diameter インスペクション ポリシー マップの設定 419
カスタム Diameter 属性値ペア（AVP）の作成 424
暗号化された Diameter セッションの検査 425
Diameter クライアントとのサーバー信頼関係の設定 427
Diameter インスペクション用のスタティック クライアント証明書によるフル TLS プロキシの設定 429
Diameter インスペクション用のローカル ダイナミック証明書によるフル TLS プロキシの設定 432
Diameter インスペクション用の TLS オフロードによる TLS プロキシの設定 436
M3UA インスペクション ポリシー マップの設定 438
モバイル ネットワーク インスペクションのサービス ポリシーの設定 442
RADIUS アカウンティング インスペクションの設定 444
RADIUS アカウンティング インスペクション ポリシー マップの設定 444
RADIUS アカウンティング インスペクションのサービス ポリシーの設定 446
モバイル ネットワーク インスペクションのモニタリング 447
GTP インスペクションのモニタリング 447
SCTP のモニタリング 449
Diameter のモニタリング 450
M3UA のモニタリング 451

モバイル ネットワーク インスペクションの履歴 452

第 V 部： 接続管理と脅威の検出 457

第 16 章 接続設定 459

接続の設定 459

接続の設定 460

グローバル タイムアウトの設定 462

SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信） 464

異常な TCP パケット処理のカスタマイズ（TCP マップ、TCP ノーマライザ） 467

非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス） 472

非対称ルーティングの問題 472

TCP ステートバイパスのガイドラインと制限事項 474

TCP ステート バイパスの設定 474

TCP シーケンスのランダム化の無効化 476

大規模フローのオフロード 478

フローオフロード導入の制約事項 478

フロー オフロードの設定 480

IPSec フローのオフロード 482

IPsec フローオフロードの制限事項 483

IPsec フローオフロードの設定 483

DTLS 暗号化アクセラレーション 484

DTLS 暗号化アクセラレーション 485

DTLS 暗号化アクセラレーションのモニタリング 485

特定のトラフィック クラスの接続の設定（すべてのサービス） 486

TCP オプションの構成 492

接続のモニタリング 493

接続設定の履歴 494

第 17 章 QoS 499

QoS について 499

サポートされている QoS 機能 499
トークン バケットとは 500
ポリシング 500
プライオリティ キューイング 501
QoS 機能の相互作用のしくみ 501
DSCP（DiffServ）の保存 501
QoS のガイドライン 501
QoS の設定 502
プライオリティ キューのキューおよび TX リング制限の決定 502
キュー制限のワークシート 502
TX リング制限のワークシート 503
インターフェイスのプライオリティ キューの設定 504
プライオリティ キューイングとポリシング用のサービス ルールの設定 506
QoS のモニター 508
QoS ポリシーの統計情報 508
QoS プライオリティの統計情報 509
QoS プライオリティ キューの統計情報 509
プライオリティ キューイングとポリシングの設定例 510
VPN トラフィックのクラス マップの例 510
プライオリティとポリシングの例 511
QoS の履歴 512

第 18 章 脅威の検出 513
脅威の検出 513
基本脅威検出統計情報 514
拡張脅威検出統計情報 515
スキャン脅威検出 515
脅威検出のガイドライン 516
脅威検出のデフォルト 517
脅威検出の設定 518
基本脅威検出統計情報の設定 518

拡張脅威検出統計情報の設定 519
スキャン脅威検出の設定 521
VPN サービスの脅威検出の設定 522
脅威検出のモニタリング 524
基本脅威検出統計情報のモニタリング 524
拡張脅威検出統計情報のモニタリング 525
ホストの脅威検出統計情報の評価 527
スキャン脅威検出の排除されたホスト、攻撃者、ターゲットのモニタリング 530
VPN サービスの脅威検出のモニタリング 531
VPN サービスの脅威検出の Syslog モニタリング 531
VPN サービスの脅威検出の show コマンドによるモニタリング 531
VPN サービス違反に適用された排除の削除 533
脅威検出の例 534
脅威検出の履歴 535

このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

- 本書の目的 （xxi ページ）
- 関連資料 （xxi ページ）
- 表記法 （xxi ページ）
- 通信、サービス、およびその他の情報 （xxiii ページ）

本書の目的

このマニュアルは、コマンドライン インターフェイスを使用して Secure Firewall ASA シリーズのファイアウォール機能を設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

また、Web ベースの GUI アプリケーションである適応型セキュリティ デバイス マネージャ（ASDM）を使用して ASA を設定、監視することもできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

関連資料

詳細については、『*Navigating the Cisco ASA Series Documentation*』（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、文字、表示、および警告に関する次の規則に準拠しています。

文字表記法

表記法	説明
boldface	コマンド、キーワード、ボタン ラベル、フィールド名、およびユーザー入力テキストは、**boldface**で示しています。メニューベース コマンドの場合は、メニュー項目を [ ] で囲み、コマンドのフル パスを示しています。
italic	ユーザーが値を指定する変数は、イタリック体で示しています。 イタリック体は、マニュアル タイトルと一般的な強調にも使用されています。
等幅	システムが表示するターミナル セッションおよび情報は、等幅文字で記載されます。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[ ]	角かっこの中の要素は、省略可能です。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
[ ]	システム プロンプトに対するデフォルトの応答も、角カッコで囲んで記載されます。
< >	パスワードなどの出力されない文字は、山カッコ（<>）で囲んで示しています。
!、#	コードの先頭に感嘆符（!）または番号記号（#）がある場合は、コメント行であることを示します。

読者への警告

このマニュアルでは、読者への警告に以下を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

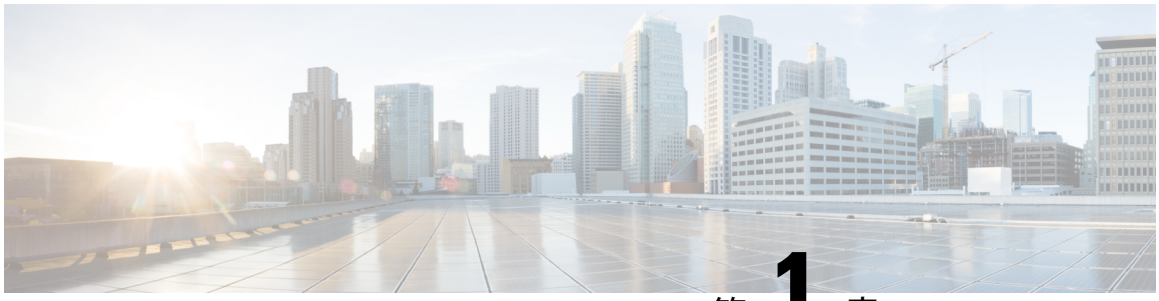
警告 **「警告」の意味です。人身事故を予防するための注意事項が記述されています。**

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービスリクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

シスコのバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



第 1 章

Cisco Secure Firewall ASA ファイアウォール サービスの概要

ファイアウォールサービスとは、トラフィックをブロックするサービス、内部ネットワークと外部ネットワーク間のトラフィック フローを可能にするサービスなど、ネットワークへのアクセス制御に重点を置いた ASA の機能です。これらのサービスには、サービス妨害（DoS）、その他の攻撃などの脅威からネットワークを保護するサービスが含まれています。

以降のトピックでは、ファイアウォール サービスの概要を示します。

- ファイアウォール サービスの実装方法 （1 ページ）
- 基本アクセス制御 （2 ページ）
- URL フィルタリング （2 ページ）
- データ保護 （3 ページ）
- 仮想環境のファイアウォール サービス （3 ページ）
- ネットワーク アドレス変換 （4 ページ）
- アプリケーション インスペクション （5 ページ）
- 使用例：サーバーの公開 （5 ページ）

ファイアウォール サービスの実装方法

次の手順は、ファイアウォールサービスを実装するための一般的な手順を示します。ただし、各手順は任意であり、サービスをネットワークに提供する場合にのみ必要です。

始める前に

一般的な操作の設定ガイドに従って ASA を設定してください（最小限の基本設定、インターフェイス コンフィギュレーション、ルーティング、管理アクセスなど）。

手順

ステップ 1 ネットワークのアクセス制御を実装します。基本アクセス制御 （2 ページ）を参照してください。

ステップ 2 URL フィルタリングを実装します。URL フィルタリング （2 ページ）を参照してください。

ステップ 3 脅威からの保護を実装します。データ保護 （3 ページ）を参照してください。

ステップ 4 仮想環境に適合するファイアウォール サービスを実装します。仮想環境のファイアウォール サービス （3 ページ）を参照してください。

ステップ 5 ネットワーク アドレス変換（NAT）を実装します。ネットワーク アドレス変換 （4 ページ）を参照してください。

ステップ 6 デフォルト設定がネットワークに十分でない場合は、アプリケーションインスペクションを実装します。アプリケーション インスペクション （5 ページ） を参照してください。

基本アクセス制御

インターフェイスごとに、またはグローバルに適用するアクセス ルールは、防御の最前線となります。エントリ時に、特定のタイプのトラフィック、または特定のホストあるいはネットワーク間のトラフィックをドロップできます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。

アクセス ルールは、内部から外部へのトラフィックを制限するため、または外部から内部へのトラフィックを許可するために使用できます。

基本的なアクセス ルールでは、送信元アドレスとポート、宛先アドレスとポート、およびプロトコルの「5タプル」を使用してトラフィックを制御します。アクセス ルール （63 ページ）およびアクセス コントロール リスト （33 ページ） を参照してください。

ルールをアイデンティティ アウェアにすることで、ルールを増やすことができます。ID 制御を実装するには、Cisco Identity Services Engine（ISE）を別のサーバーにインストールして、Cisco Trustsec を実装します。その後、セキュリティ グループ基準をアクセス ルールに追加できます。ASA および Cisco TrustSec （83 ページ）を参照してください。

URL フィルタリング

URL フィルタリングは、宛先サイトの URL をベースにしたトラフィックを拒否または許可します。

URL フィルタリングを実装するには、Cisco Umbrella サービスをサブスクライブします。このサービスで、エンタープライズ セキュリティ ポリシーを設定して、完全修飾ドメイン名（FQDN）に基づいて悪意のあるサイトをブロックできます。疑わしいと見なされた FQDN の

場合は、ユーザー接続を Cisco Umbrella インテリジェント プロキシにリダイレクトし、URL フィルタリングを実行します。Umbrella サービスは、ユーザーの DNS ルックアップ要求を処理し、ブロック ページの IP アドレスまたはインテリジェント プロキシの IP アドレスを返すことによって機能します。このサービスは、許可されたドメインの FQDN の実際の IP アドレスを返します。Cisco Umbrella （117 ページ） を参照してください。

データ保護

スキャニング、サービス妨害（DoS）、および他の攻撃から保護するために多くの手段を実装できます。ASA の数多くの機能は、接続制限を適用して異常な TCP パケットをドロップすることで、攻撃から保護するのに役立ちます。一部の機能は自動ですが、ほとんどの場合でデフォルトが適切である設定可能な機能もあれば、完全に任意で必要な場合に設定する必要がある機能もあります。

次に、ASA で使用可能な脅威からの保護サービスを示します。

- IP パケット フラグメンテーションの保護：ASA は、すべての ICMP エラー メッセージの完全リアセンブリ、および ASA を介してルーティングされる残りの IP フラグメントの仮想リアセンブリを実行し、セキュリティ チェックに失敗したフラグメントをドロップします。コンフィギュレーションは必要ありません。
- 接続制限、TCP 正規化、およびその他の接続関連機能：TCP と UDP の接続制限値とタイムアウト、TCP シーケンス番号のランダム化、TCP ステート バイパスなどの接続関連サービスを設定します。TCP 正規化は、正常に見えないパケットをドロップするように設計されています。接続設定 （459 ページ）を参照してください。

  たとえば、TCP と UDP の接続、および初期接続（信元と宛先の間で必要になるハンドシェイクを完了していない接続要求）を制限できます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。
- 脅威検出：攻撃を識別できるように統計情報の収集するために脅威検出を ASA に実装します。基本脅威検出はデフォルトでイネーブルになっていますが、高度な統計情報とスキャン脅威検出を実装できます。スキャン脅威であると特定されたホストを遮断できます。脅威の検出 （513 ページ）を参照してください。

仮想環境のファイアウォール サービス

仮想環境は仮想マシンとしてサーバーを導入します（VMware ESXi など）。仮想環境でのファイアウォールは、従来のハードウェアデバイスでも実現できますが、ASA 仮想 などの仮想マシンのファイアウォールも実現できます。

従来のファイアウォールと次世代のファイアウォール サービスは、仮想マシン サーバーを使用しない環境に適用する場合と同じ方法で、仮想環境に適用されます。ただし、仮想環境では、サーバーの作成と切断が容易なため、追加の課題を提供できます。

さらに、データセンター内のサーバー間のトラフィックは、データセンターと外部ユーザー間のトラフィックと同じ程度の保護を必要とする可能性があります。たとえば、攻撃者がデータセンター内のあるサーバーの制御を手に入れた場合、データセンターのその他のサーバーに攻撃を広げる可能性があります。

仮想環境のファイアウォール サービスは、ファイアウォール保護を特に仮想マシンに適用する機能を追加します。以下に、仮想環境で使用可能なファイアウォール サービスを示します。

- 属性ベースのアクセス制御：属性に基づいて一致するトラフィックにネットワーク オブジェクトを設定し、アクセス制御ルールでこれらのオブジェクトを使用します。これにより、ネットワーク トポロジからファイアウォール ルールを分離することができます。たとえば、Engineering 属性を持つすべてのホストに Lab Server 属性を持つホストへのアクセスを許可できます。これらの属性を持つホストを追加および削除することができ、ファイアウォール ポリシーは、アクセス ルールを更新する必要なく自動的に適用されます。詳細については、属性ベースのアクセス制御 （139 ページ）を参照してください。

ネットワーク アドレス変換

ネットワーク アドレス変換（NAT）の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリック アドレスだけを外部に最小限にアドバタイズすることができるからです。

NAT の他の機能には、次のおりです。

- セキュリティ：内部 IP アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティングソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常通りに適用されます。

参照先：

- Network Address Translation（NAT） （153 ページ）
- NAT の例と参照 （221 ページ）

アプリケーション インスペクション

インスペクション エンジンは、ユーザーのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、必要なピンホールを開く、およびネットワーク アドレス変換（NAT）を適用するために ASA で詳細なパケット インスペクションを行う必要があります。

デフォルトの ASA ポリシーは、すでに DNS、FTP、SIP、ESMTP、TFTP などの数多くの一般的なプロトコルのインスペクションをグローバルに適用しています。デフォルトのインスペクションでネットワークに必要なすべてが揃うことがあります。

ただし、他のプロトコルのインスペクションをイネーブルにしたり、インスペクションを微調整したりする必要がある場合があります。多くのインスペクションには、それらの内容に基づいてパケットを制御できる詳細なオプションがあります。プロトコルを十分に理解している場合には、そのトラフィックをきめ細かく制御できます。

サービス ポリシーを使用して、アプリケーション インスペクションを設定します。グローバル サービス ポリシーを設定するか、サービス ポリシーを各インターフェイスに適用するか、またはその両方を行うことができます。

参照先：

- サービス ポリシー （269 ページ）
- アプリケーション レイヤ プロトコル インスペクションの準備 （295 ページ）
- 基本インターネット プロトコルのインスペクション （321 ページ）
- 音声とビデオのプロトコルのインスペクション （371 ページ）
- モバイル ネットワークのインスペクション （401 ページ）。

使用例：サーバーの公開

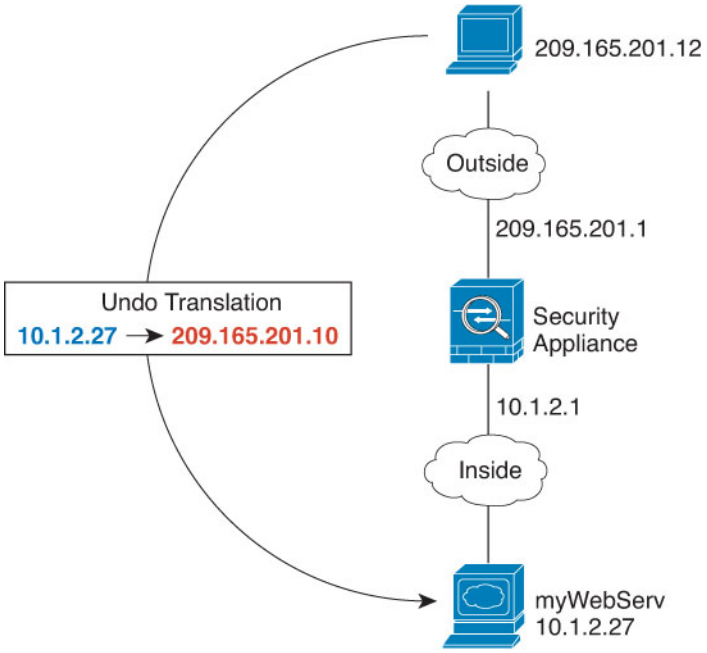
一般公開されているサーバーで特定のアプリケーション サービスを実行できます。たとえば、ユーザーが Web ページに接続でき、それ以外のサーバーへの接続を確立しないように Web ページを公開することができます。

サーバーを一般公開するには、通常、接続および NAT ルールによってサーバーの内部 IP アドレスと一般ユーザーが使用できる外部アドレス間で変換を行うことができるアクセス ルールを作成する必要があります。さらに、外部に公開したサービスで内部サーバーと同じポートを使

用しない場合には、ポートアドレス変換（PAT）を使用して内部ポートを外部ポートにマッピングすることができます。たとえば、内部 Web サーバーが TCP/80 で実行されていない場合、外部ユーザーが容易にアクセスできるようにそのサーバーを TCP/80 にマッピングできます。

次の例では、内部プライベート ネットワーク上の Web サーバーをパブリック アクセスで使用可能にします。

図 *1 :* 内部 *Web* サーバーのスタティック *NAT*



手順

ステップ 1 内部 Web サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

ステップ 2 オブジェクトのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

ステップ 3 外部インターフェイスに接続されているアクセス グループにアクセス ルールを追加して、サーバーへの Web アクセスを許可します。

```
hostname(config)# access-list outside_access_in line 1 extended
permit tcp any4 object myWebServ eq http
```

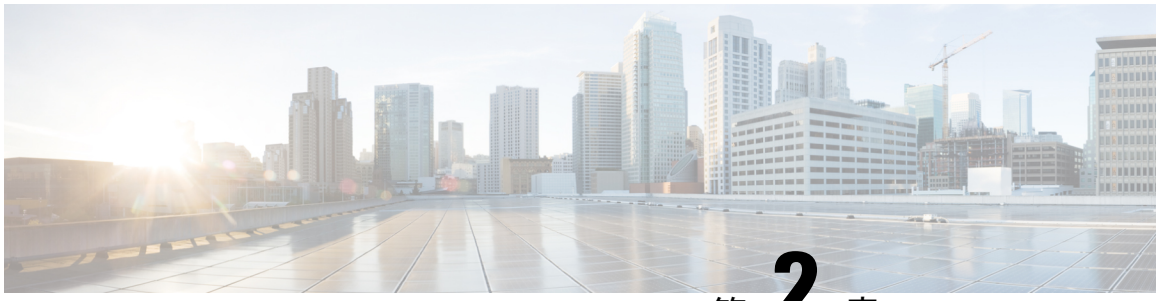
ステップ 4 外部インターフェイスにアクセス グループがない場合は、access-group コマンドを使用してアクセス グループを適用します。

```
hostname(config)# access-group outside_access_in in interface outside
```

第 部

アクセス コントロール

- アクセス制御のオブジェクト （11 ページ）
- アクセス コントロール リスト （33 ページ）
- アクセス ルール （63 ページ）
- ASA および Cisco TrustSec （83 ページ）
- Cisco Umbrella （117 ページ）



第 2 章

アクセス制御のオブジェクト

オブジェクトとは、コンフィギュレーションで使用するための再利用可能なコンポーネントです。インライン IP アドレス、サービス、名前などの代わりに、Cisco ASA コンフィギュレーションでオブジェクトを定義し、使用できます。オブジェクトを使用すると、コンフィギュレーションのメンテナンスが容易になります。これは、一箇所でオブジェクトを変更し、このオブジェクトを参照している他のすべての場所に反映できるからです。オブジェクトを使用しなければ、1 回だけ変更するのではなく、必要に応じて各機能のパラメータを変更する必要があります。たとえば、ネットワーク オブジェクトによって IP アドレスおよびサブネット マスクが定義されており、このアドレスを変更する場合、この IP アドレスを参照する各機能ではなく、オブジェクト定義でアドレスを変更することだけが必要です。

- オブジェクトのガイドライン （11 ページ）
- オブジェクトの設定 （12 ページ）
- オブジェクトのモニタリング （28 ページ）
- オブジェクトの履歴 （29 ページ）

オブジェクトのガイドライン

IPv6 のガイドライン

IPv6 のサポートには次の制約が伴います。

- 1 つのネットワーク オブジェクト グループの中で IPv4 および IPv6 のエントリを混在させることができますが、NAT に対しては、混合オブジェクト グループは使用できません。

その他のガイドラインと制限事項

- オブジェクトおよびオブジェクト グループは同じネーム スペースを共有するため、オブジェクトの名前は固有のものでなければなりません。「Engineering」という名前のネットワーク オブジェクト グループと「Engineering」という名前のサービス オブジェクト グループを作成する場合、少なくとも 1 つのオブジェクト グループ名の最後に識別子（または「タグ」）を追加して、その名前を固有のものにする必要があります。たとえば、

「Engineering_admins」と「Engineering_hosts」という名前を使用すると、オブジェクト グループの名前を固有のものにして特定可能にすることができます。

- オブジェクト名は、文字、数字、および .!@#$%^&()-_{} を含めて、64 文字までに制限されています。オブジェクト名は、大文字と小文字が区別されます。

オブジェクトの設定

次の各項では、主にアクセス コントロールで使用されるオブジェクトを設定する方法について説明します。

ネットワーク オブジェクトとグループの設定

ネットワーク オブジェクトおよびグループは、IP アドレスまたはホスト名を特定します。これらのオブジェクトをアクセス コントロール リストで使用して、ルールを簡素化できます。

ネットワーク オブジェクトの設定

1 つのネットワーク オブジェクトには、1 つのホスト、ネットワーク IP アドレス、IP アドレスの範囲、または完全修飾ドメイン名（FQDN）を入れることができます。

また、オブジェクトに対して NAT ルールをイネーブルにすることもできます（FQDN オブジェクトを除く）。オブジェクト NAT の設定の詳細については、Network Address Translation（NAT）（153 ページ） を参照してください。

手順

ステップ 1 オブジェクト名を使用して、ネットワーク オブジェクトを作成または編集します： **object network** *object_name*

例：

```
hostname(config)# object network email-server
```

ステップ 2 次のいずれかのコマンドを使用して、オブジェクトにアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **host** {*IPv4_address*|*IPv6_address*}：単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask*|*IPv6_address/IPv6_prefix*}：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

- **range** *start_address end_address*：アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。
- **fqdn** [**v4** | **v6**] *fully_qualified_domain_name*：完全修飾ドメイン名。つまり、www.example.com のようなホスト名アドレスを IPv4 に制限するには **v4**、IPv6 に制限するには **v6** を指定します。アドレス タイプを指定しない場合、IPv4 が使用されます。

例：

```
hostname(config-network-object)# host 10.2.2.2
```

ステップ 3 （任意）説明を追加します。**description** *string*

ネットワーク オブジェクト グループの設定

ネットワーク オブジェクト グループには、インライン ネットワークやホストと同様に複数のネットワーク オブジェクトを含めることができます。ネットワーク オブジェクト グループは、IPv4 と IPv6 の両方のアドレスの混在を含めることができます。

ただし、IPv4 と IPv6 が混在するオブジェクト グループや、FQDN オブジェクトが含まれているオブジェクト グループを、NAT に使用することはできません。

手順

ステップ 1 オブジェクト名を使用して、ネットワーク オブジェクト グループを作成または編集します。**object-group network** *group_name*

例：

```
hostname(config)# object-group network admin
```

ステップ 2 次のコマンドの 1 つまたは複数を使用して、ネットワーク オブジェクト グループにオブジェクトとアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **network-object host** {*IPv4_address* | *IPv6_address*}：単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **network-object** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*}：ネットワークまたはホストのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **network-object object** *object_name*：既存のネットワーク オブジェクトの名前。
- **group-object** *object_group_name*：既存のネットワーク オブジェクト グループの名前。

例：

```
hostname(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
hostname(config-network-object-group)# network-object 2001:db8:0:cd30::/60
hostname(config-network-object-group)# network-object host 10.1.1.1
hostname(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
hostname(config-network-object-group)# network-object object existing-object-1
hostname(config-network-object-group)# group-object existing-network-object-group
```

ステップ 3 （任意）説明を追加します。**description** *string*

例

3 人の管理者の IP アドレスを含むネットワーク グループを作成するには、次のコマンドを入力します。

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```

次のコマンドを入力して、さまざまな部門に所属する特権ユーザーのネットワーク オブジェクト グループを作成します。

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

その後、3 つすべてのグループを次のようにネストします。

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

サービス オブジェクトとサービス グループの設定

サービス オブジェクトとグループでは、プロトコルおよびポートを指定します。これらのオブジェクトをアクセス コントロール リストで使用して、ルールを簡素化できます。

サービス オブジェクトの設定

サービス オブジェクトには、単一のプロトコル仕様を含めることができます。

手順

ステップ 1 オブジェクト名を使用して、サービス オブジェクトを作成または編集します。**object service** *object_name*

例：

```
hostname(config)# object service web
```

ステップ 2 次のいずれかのコマンドを使用して、オブジェクトにサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service** *protocol*：IP プロトコルの名前または番号（0 ～ 255）。**ip** を指定すると、すべてのプロトコルに適用されます。
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]：ICMP または ICMP バージョン 6 のメッセージ用。ICMP タイプを名前または番号（0～255）で指定することで、オブジェクトをそのメッセージ タイプに制限できます（オプション）。タイプを指定する場合、そのタイプ（1 ～ 255）に対する ICMP コードを任意で指定できます。コードを指定しない場合は、すべてのコードが使用されます。
- **service** {**tcp** | **udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*]：TCP、UDP、または SCTP 用。送信元、宛先、またはその両方に対して、任意でポートを指定できます。ポートは、名前または番号で指定できます。operator には次のいずれかを指定できます。
  - **lt**：小なり。
  - **gt**：大なり。
  - **eq**：等しい。
  - **neq**：非同値。
  - **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します（例：**range 100 200**）。

例：

```
hostname(config-service-object)# service tcp destination eq http
```

ステップ 3 （任意）説明を追加します。**description** *string*

サービス グループの設定

1つのサービス オブジェクト グループには、さまざまなプロトコルが混在しています。必要に応じて、それらを使用するプロトコルの送信元および宛先ポート、およびICMPのタイプおよびコードを入れることができます。

始める前に

ここで説明する一般的なサービス オブジェクト グループを使用して、すべてのサービスをモデル化できます。ただし、ASA 8.3(1)よりも前に使用可能であったサービス グループ オブジェクトのタイプを設定することもできます。こうした従来のオブジェクトには、TCP/UDP/TCP-UDPポート グループ、プロトコル グループ、およびICMPグループが含まれます。これらのグループのコンテンツは、ICMP6またはICMPコードをサポートしないICMPグループを除く、一般的なサービス オブジェクト グループの関連する設定に相当します。これらの従来のオブジェクトを使用したい場合は、object-service コマンドに関する説明を Cisco.com のコマンド リファレンスで確認してください。

手順

ステップ 1 オブジェクト名を使用して、サービス オブジェクト グループを作成または編集します。
object-group service *object_name*

例：

```
hostname(config)# object-group service general-services
```

ステップ 2 次のコマンドの 1 つまたは複数を使用して、サービス オブジェクト グループにオブジェクトとサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service-object** *protocol*：IP プロトコルの名前または番号（0 ～ 255）。**ip** を指定すると、すべてのプロトコルに適用されます。
- **service-object** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]：ICMP または ICMP バージョン 6 のメッセージ用。ICMPタイプを名前または番号（0～255）で指定することで、オブジェクトをそのメッセージタイプに制限できます（オプション）。タイプを指定する場合、そのタイプ（1 ～ 255）に対する ICMP コードを任意で指定できます。コードを指定しない場合は、すべてのコードが使用されます。
- **service-object** {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*]：TCP、UDP、その両方、または SCTP 用。送信元、宛先、またはその両方に対して、任意でポートを指定できます。ポートは、名前または番号で指定できます。operator には次のいずれかを指定できます。
  - **lt**：小なり。
  - **gt**：大なり。
  - **eq**：等しい。

- **neq**：非同値。
- **range**：値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します（例：**range 100 200**）。

- **service-object object** *object_name*：既存のサービス オブジェクトの名前。
- **group-object** *object_group_name*：既存のサービス オブジェクト グループの名前。

例：

```
hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
```

ステップ 3 （任意）説明を追加します。**description** *string*

例

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object tcp destination eq ftp
hostname(config-service-object-group)# service-object tcp-udp destination eq www
hostname(config-service-object-group)# service-object tcp destination eq h323
hostname(config-service-object-group)# service-object tcp destination eq https
hostname(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# object service SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# object service HTTPS
hostname(config-service-object)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
hostname(config-service-object-group)# service-object object HTTPS
```

ネットワークサービスオブジェクトとネットワークサービスオブジェクト グループの設定

ネットワークサービス オブジェクトまたはネットワークサービス オブジェクト グループでは、単一のアプリケーションを定義します。アプリケーションは、DNS ドメイン名 （example.com など）、IP サブネット、およびオプションでプロトコルとポート （TCP/80 など） で構成できます。したがって、ネットワーク サービス オブジェクトまたはネットワーク サービス オブジェクト グループを使用することで、個別のネットワーク オブジェクトとサービス オブジェクトの内容を 1 つのオブジェクトに結合できます。

拡張 ACL でネットワークサービス オブジェクト グループを作成して、ルートマップ（ポリシーベースルーティングで使用）、アクセスコントロールルール、および VPN フィルタで使用できます。ACL ではネットワークサービス オブジェクト（グループではない）を直接使用できないことに注意してください。グループオブジェクトを使用するには、最初にオブジェクトをグループオブジェクトに追加する必要があります。

ドメイン名の仕様を使用すると、DNS スヌーピングによって、接続の開始前にユーザーの DNS 要求を通じて取得した IP アドレスが取得されます。これにより、接続の開始時に IP アドレスが使用可能になり、最初のパケットからルートマップとアクセスコントロールルールによって接続が正しく処理されます。

ネットワーク サービス オブェクトのガイドライン

- ネットワーク サービス オブェクトに DNS ドメイン名の仕様を含める場合は、DNS インスペクションが必要です。DNS インスペクションはデフォルトでイネーブルになっています。ネットワーク サービス オブジェクトを使用する場合は、無効にしないでください。
- DNS スヌーピングは、UDP DNS パケットでのみ実行され、TCP または HTTP DNS パケットでは実行されません。完全修飾ドメイン名オブジェクトとは異なり、アクセスリストでオブジェクトを使用しなくても、ネットワーク サービス ドメインの指定は即座にスヌープされます。
- DNS インスペクション ポリシーマップで dnscrypt を有効にすることはできません。dnscrypt は、ネットワーク サービス オブジェクトで使用されるドメインの IP アドレスを取得するために必要な DNS スヌーピングと互換性がありません。ドメインの指定を含むネットワーク サービス オブジェクトは動作不能になり、関連するアクセス コントロール エントリは一致しません。
- 最大 1024 のネットワーク サービス グループを定義できます。ただし、この制限はアイデンティティ ファイアウォールのローカルユーザ グループと共有されます。定義されたネットワーク サービス グループごとに、2 つ少ないユーザー グループを作成できます。
- ネットワーク サービス グループの内容は重複してもかまいませんが、ネットワーク サービス グループの完全な複製を作成することはできません。
- ネットワーク サービス オブジェクトまたはグループが ACL で使用されている場合、オブジェクトを削除しても、オブジェクトの内容がクリアされるだけです。オブジェクト自体は、設定で定義されたままになります。

- オブジェクトまたはグループの **dynamic** キーワードは、オブジェクトが実行コンフィギュレーションに保存されず、**show object** 出力にのみ表示されることを示しています。このキーワードを直接設定しないでください。これは主に外部のデバイスマネージャが使用します。
- ネットワークサービス オブジェクトの **app-id** コマンドは、特定のアプリケーションにシスコが割り当てる番号を 1 ～ 4294967295 の範囲で定義します。このコマンドを直接設定しないでください。このコマンドは、主に外部デバイスマネージャを使用する場合に使用します。

信頼できる DNS サーバの構成

ネットワークサービス オブジェクトでドメイン名を設定すると、DNS 要求/応答トラフィックのスヌーピングによって DNS ドメイン名に対応する IP アドレスが収集され、その結果がキャッシュされます。すべての DNS 要求/応答をスヌーピングできます。

スヌーピングされるレコードは、A、AAAA、および MX です。解決された各名前には存続可能時間（TTL）が適用され、最小値は 2 分、最大値は 24 時間です。これにより、キャッシュが古くならないように保証されます。

セキュリティ上の理由から、信頼する DNS サーバーを定義することで DNS スヌーピングの範囲を制限できます。信頼されていない DNS サーバーへの DNS トラフィックは無視され、ネットワークサービス オブジェクトのマッピングの取得に使用されません。デフォルトでは、設定および学習されたすべての DNS サーバーが信頼されます。信頼できるリストを制限する場合のみ変更が必要になります。

（注） 重要なのは、クライアントが使用する DNS サーバーを信頼できるサーバーとして定義することです。

始める前に

DNS スヌーピングは、デフォルトで有効になっている DNS インスペクションに依存しています。DNS インスペクションが無効になっていないことを確認してください。また、DSN スヌーピングは **dnscrypt** 機能と互換性がないため、DNS インスペクション ポリシー マップでそのコマンドを有効にしないでください。

手順

ステップ 1 **show dns trusted-source detail** コマンドを使用して、データパスにダウンロードされている現在の信頼できるサーバーを特定し、ネットワークサービス オブジェクト ドメインの解決に使用します。

デフォルトでは、DNS グループで構成するか、DHCP クライアント/サーバーまたはリレーを介して構成された DNS サーバーを信頼します。このコマンドにより、現在の設定と信頼されているサーバーが表示されます。

例：

```
ciscoasa# show dns trusted-source detail
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 10.163.47.11: management : N/A
    DNS Server Configured: 10.37.137.85: management : N/A
    DNS Server Configured: 10.37.142.73: management : N/A
Data-Path DNS Trusted Source (count 3): <ip>/<refcnt>; Trust-any disabled
  10.37.142.73/1
  10.37.137.85/1
  10.163.47.11/1
```

ステップ 2 （オプション）明示的に設定された信頼できる DNS サーバーを追加または削除します。

dns trusted-source *ip_list*

ip_list は、信頼できる DNS サーバーの IP アドレスのスペース区切りリストです。IPv4 アドレスと IPv6 アドレスを最大 12 個までリストできます。すべての DNS サーバーを含める場合は **any** を指定します。サーバーを削除するには、このコマンドの **no** 形式を使用します。

ステップ 3 （オプション）DNS サーバーグループで設定されたサーバーを信頼するかどうかを指定します。

dns trusted-source configured-servers

設定済みサーバーには、DNS グループまたはネームサーバーのコマンドで指定されたサーバーが含まれます。このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

ステップ 4 （オプション）デバイスインターフェイスで実行されている DHCP サーバーを介してアドレスを取得するクライアントの DHCP プールに設定されている DNS サーバーを信頼するかどうかを指定します。

dns trusted-source dhcp-pools

これらは **dhcpd dns** コマンドで設定されているサーバーであるため、IPv4 のみになります。このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

ステップ 5 （オプション）DHCP クライアントと DHCP サーバー間のスヌーピング リレー メッセージによって学習されたサーバーが、信頼できる DNS サーバーと見なされるかどうかを指定します。

dns trusted-source dhcp-relay

このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

ステップ 6 （オプション）DHCP クライアントと DHCP サーバー間のスヌーピングメッセージによって学習されたサーバーが、信頼できる DNS サーバーと見なされるかどうかを指定します。

dns trusted-source dhcp-client

このオプションは、DHCP クライアントを使用して IP アドレスを取得するデバイスインターフェイスから取得した情報を使用して内部インターフェイスの DHCP サーバーを設定するように **dhcpd auto_config** コマンドを設定する場合に適用されます。このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

ネットワーク サービス オブジェクトの設定

ネットワーク サービス オブジェクトでは、単一のアプリケーションを定義します。また、サブネット仕様やより一般的には DNS ドメイン名のいずれかによってアプリケーションの場所を定義します。必要に応じて、プロトコルとポートを含めて、アプリケーションの範囲を絞り込めます。

ネットワーク サービス オブジェクトは、ネットワーク サービス グループ オブジェクトでのみ使用できます。アクセス制御リストエントリ（ACE）でネットワーク サービス オブジェクトを直接使用することはできません。

手順

ステップ 1 オブジェクト名を使用して、ネットワーク サービス オブジェクトを作成または編集します。

object network-service *object_name*

名前は最大 128 文字で、スペースを含めることができます。スペースを含める場合、名前を二重引用符で囲む必要があります。

例：

```
ciscoasa(config)# object network-service webex
```

ステップ 2 次のいずれかのコマンドを使用して、1 つ以上のアプリケーションの場所とオプションサービスをオブジェクトに追加します。場所を削除するには、このコマンドの **no** 形式を使用します。これらのコマンドは、複数回入力できます。

- **domain** *domain_name* [*service*]：最大 253 文字の DNS 名。この名前は、完全修飾名（www.example.com など）または部分的な名前（example.com など）にすることができます。部分的な名前の場合、すべてのサブドメイン、つまりその名前を含むすべてのサーバー（www.example.com、www1.example.com、long.server.name.example.com など）に一致します。完全一致がある場合は、最も長い名前で接続が照合されます。ドメイン名は複数の IP アドレスに解決できます。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*]：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含め

ます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

これらのコマンドのサービス仕様は同じです。一致する接続の範囲を制限する場合にのみ、サービスを指定します。デフォルトでは、解決済みの IP アドレスへのすべての接続がオブジェクトと一致します。

protocol [*operator port*]

引数の説明

- *protocol* は、tcp、udp、ip など、接続で使用されるプロトコルです。プロトコルのリストを確認するには ? を使用します。
- （TCP/UDP のみ）*operator* は次のいずれかです。
  - **eq** は、指定したポート番号と等しいポートを意味します。
  - **lt** は、指定したポート番号より小さい任意のポートを意味します。
  - **gt** は、指定したポート番号より大きい任意のポートを意味します。
  - **range** は、指定した 2 つのポートの間の任意のポートを意味します。
- （TCP/UDP のみ）*port* は 1 ～ 65535 のポート番号か www などのニーモニックです。ニーモニックを確認するには ? を使用します。範囲の場合は 2 つのポートを指定する必要があります。最初のポートを 2 番目のポートよりも小さい番号にします。

ステップ 3 （任意）最大 200 文字で説明を追加します。 **description** *string*

例

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

ネットワーク サービス オブジェクト グループの設定

ネットワーク サービス グループには、ネットワーク サービス オブジェクトと明示的なサブネットまたはドメインの指定を含めることができます。ポリシーベース ルーティング、アクセス コントロール、および VPN フィルタのアクセス コントロール リスト エントリ（ACE）でネットワーク サービス オブジェクトを使用できます。

ネットワーク サービス グループを使用して、同じ方法で処理する必要があるアプリケーションのカテゴリを定義します。たとえば、企業ハブへのサイト間 VPN トンネルではなく、イン

ターネットにトラフィックを送信するアプリケーションを定義する単一のグループを作成できます。

ネットワーク サービス オブジェクト グループに、明示的に、またはネットワーク サービス オブジェクトへの参照によって含めるアプリケーションの数に制限はありません。

手順

ステップ 1 グループ名を使用して、ネットワーク オブジェクト グループを作成または編集します。

object-group network-service *group_name*

名前は最大 128 文字で、スペースを含めることができます。スペースを含める場合、名前を二重引用符で囲む必要があります。

例：

```
ciscoasa(config)# object-group network-service SaaS_Applications
```

ステップ 2 次のいずれかのコマンドを使用して、1 つ以上のアプリケーションの場所とオプションサービスをオブジェクトに追加します。場所を削除するには、このコマンドの**no**形式を使用します。これらのコマンドは、複数回入力できます。

- **network-service-member***object_name*：グループに含めるネットワーク サービス オブジェクトの名前。名前にスペースが含まれている場合は、その名前を二重引用符で囲みます。
- **domain** *domain_name* [*service*]：最大 253 文字の DNS 名。この名前は、完全修飾名（www.example.com など）または部分的な名前（example.com など）にすることができます。部分的な名前の場合、すべてのサブドメイン、つまりその名前を含むすべてのサーバー（www.example.com、www1.example.com、long.server.name.example.com など）に一致します。完全一致がある場合は、最も長い名前で接続が照合されます。ドメイン名は複数の IP アドレスに解決できます。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*]：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

これらのコマンドのサービス仕様は同じです。一致する接続の範囲を制限する場合にのみ、サービスを指定します。デフォルトでは、解決済みの IP アドレスへのすべての接続がオブジェクトと一致します。

protocol [*operator port*]

引数の説明

- *protocol* は、tcp、udp、ip など、接続で使用されるプロトコルです。プロトコルのリストを確認するには ? を使用します。
- （TCP/UDP のみ）*operator* は次のいずれかです。

- **eq** は、指定したポート番号と等しいポートを意味します。
- **lt** は、指定したポート番号より小さい任意のポートを意味します。
- **gt** は、指定したポート番号より大きい任意のポートを意味します。
- **range** は、指定した 2 つのポートの間の任意のポートを意味します。

- （TCP/UDP のみ）*port* は 1 ～ 65535 のポート番号か www などのニーモニックです。ニーモニックを確認するには ? を使用します。範囲の場合は 2 つのポートを指定する必要があります。最初のポートを 2 番目のポートよりも小さい番号にします。

ステップ 3 （任意）最大 200 文字で説明を追加します。 **description** *string*

例

事前に定義されたネットワーク サービス オブジェクトを使用して、一連の SaaS アプリケーションを設定します。

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

ローカル ユーザー グループの設定

作成したローカル ユーザー グループは、アイデンティティ ファイアウォールをサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールでも使用できるようになります。

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザー グループについて、Active Directory サーバーに LDAP クエリを送信します。ASA は、そのグループをアイデンティティ ベースのルール用にインポートします。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザー グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザー グループには、Active Directory からインポートされる、ネストされたグループおよびユーザー グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。

ユーザーは、ローカル ユーザー グループと Active Directory からインポートされたユーザー グループに属することができます。

ACL でユーザー名とユーザー グループ名を直接使用できるため、次の場合にだけローカル ユーザー グループを設定する必要があります。

- ローカル データベースで定義されているユーザーのグループを作成する。

- AD サーバーで定義されている単一のユーザー グループでキャプチャされなかったユーザーまたはユーザー グループのグループを作成する。

手順

ステップ 1 オブジェクト名を使用して、ユーザー オブジェクト グループを作成または編集します。**object-group user** *group_name*

例：

```
hostname(config)# object-group user admins
```

ステップ 2 次のコマンドの 1 つまたは複数を使用して、ユーザー オブジェクト グループにユーザーとグループを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **user** [*domain_NETBIOS_name*\]*username*：ユーザー名。ドメイン名またはユーザー名にスペースが含まれている場合は、ドメイン名とユーザー名を引用符で囲む必要があります。ドメイン名には、LOCAL（ローカル データベースで定義されているユーザー向け）、または **user-identity domain** *domain_NetBIOS_name* **aaa-server** *aaa_server_group_tag* コマンドで指定されている Active Directory（AD）のドメイン名を指定できます。AD ドメインに定義されているユーザーを追加する場合、*user_name* には、一意ではない可能性がある Common Name（CN）ではなく、一意の Active Directory sAMAccountName を指定する必要があります。ドメイン名を指定しない場合、デフォルト値が使用されます。デフォルト値は、LOCAL または **user-identity default-domain** コマンドで定義されている値のいずれかです。
- **user-group** [*domain_NETBIOS_name*\\]*username*：ユーザー グループ。ドメイン名またはグループ名にスペースが含まれている場合は、ドメイン名とグループ名を引用符で囲む必要があります。ドメイン名とグループ名を区切る二重の \\ に注意してください。
- **group-object** *object_group_name*：既存のユーザー オブジェクト グループの名前。

例：

```
hostname(config-user-object-group)# user EXAMPLE\admin
hostname(config-user-object-group)# user-group EXAMPLE\\managers
hostname(config-user-object-group)# group-object local-admins
```

ステップ 3 （任意）説明を追加します。**description** *string*

セキュリティ グループ オブジェクト グループの設定

作成したセキュリティ グループ オブジェクト グループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールで使用できるようになります。

Cisco TrustSec と統合されているときは、ASA は ISE からセキュリティ グループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザー アイデンティティへのマッピングと、Cisco TrustSec タグからサーバー リソースへのマッピングを行います。セキュリティ グループ ACL のプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、ローカライズされたセキュリティ ポリシーを持つローカル セキュリティ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル セキュリティ グループには、ISE からダウンロードされた、ネストされたセキュリティ グループを含めることができます。ASA は、ローカルと中央のセキュリティ グループを統合します。

ASA 上でローカル セキュリティ グループを作成するには、ローカル セキュリティ オブジェクト グループを作成します。1 つのローカル セキュリティ オブジェクト グループに、1 つ以上のネストされたセキュリティ オブジェクト グループまたはセキュリティ ID またはセキュリティ グループ名を入れることができます。ユーザーは、ASA 上に存在しない新しいセキュリティ ID またはセキュリティ グループ名を作成することもできます。

ASA 上で作成したセキュリティ オブジェクト グループは、ネットワーク リソースへのアクセスの制御に使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

ヒント　ASA にとって不明なタグや名前を使用してグループを作成する場合、そのタグや名前が ISE で解決されるまで、そのグループを使用するすべてのルールが非アクティブになります。

手順

ステップ 1　オブジェクト名を使用して、セキュリティ グループ オブジェクト グループを作成または編集します。**object-group security** *group_name*

例：

```
hostname(config)# object-group security mktg-sg
```

ステップ 2　次のコマンドの 1 つまたは複数を使用して、サービス グループ オブジェクト グループにオブジェクトを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **security-group** {**tag** *sgt_number* | **name** *sg_name*}：セキュリティ グループ タグ（SGT）または名前。タグは、1 から 65533 までの数字であり、IEEE 802.1X 認証、Web 認証、または ISE による MAC 認証バイパス（MAB）を通じてデバイスに割り当てられます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。有効なタグと名前については、ISE の設定を参照してください。

- **group-object** *object_group_name*：既存のセキュリティ グループ オブジェクト グループの名前。

例：

```
hostname(config-security-object-group)# security-group tag 1
hostname(config-security-object-group)# security-group name mgkt
hostname(config-security-object-group)# group-object local-sg
```

ステップ 3 （任意）説明を追加します。**description** *string*

時間範囲の設定

時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能または資産に時間ベースでアクセスするためにACLルールで使用されます。たとえば、勤務時間中にのみ特定のサーバーへのアクセスを許可するアクセス ルールを作成できます。

（注） 時間範囲オブジェクトには複数の定期的エントリを含めることができます。1 つの時間範囲に absolute 値と periodic 値の両方が指定されている場合は、periodic 値は absolute の開始時刻に到達した後にのみ評価され、absolute の終了時刻に到達した後は評価されません。

時間範囲を作成してもデバイスへのアクセスは制限されません。この手順では、時間範囲だけを定義します。その後、アクセス コントロール ルールでオブジェクトを使用する必要があります。

手順

ステップ 1 時間範囲を作成します。**time-range** *name*

ステップ 2 （任意）時間範囲に開始時刻または終了時刻（または両方）を追加します。

absolute [**start** *time date*] [**end** *time date*]

開始時刻を指定しない場合、現在の時刻がデフォルトの開始時刻になります。

time は 24 時間形式（*hh*:*mm*）で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

date は *day month year* の形式で指定します（たとえば、**1 January 2014**）。

ステップ 3 （任意）繰り返しの期間を追加します。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

days-of-the-week には次の値を指定できます。最初の引数に曜日を 1 つ指定した場合にのみ、2 番目の曜日を指定できることに注意してください。

- **Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday**、または **Sunday**。最初の *days-of-the-week* 引数には、複数の曜日をスペースで区切って指定できます。
- **daily**
- **weekdays**
- **weekend**

time は 24 時間形式（*hh*:*mm*）で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

このコマンドを繰り返して、複数の繰り返し期間を設定できます。

例

次に、2006 年 1 月 1 日の午前 8 時に始まる絶対的な時間範囲の例を示します。終了時刻も終了日も指定されていないため、時間範囲は事実上無期限になります。

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

次に、平日の午前 8 時～午後 6 時に毎週繰り返される定期的な時間範囲の例を示します。

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

次の例では、時間範囲の終了日を設定し、平日の期間を午前 8 時～午後 5 時に設定し、火曜日、木曜日と比較して月曜日、水曜日、金曜日に対して午後 5 時の後に異なる時間数を加算します。

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

オブジェクトのモニタリング

オブジェクトおよびグループをモニターするには、次のコマンドを入力します。

- **show access-list**

アクセス リストのエントリを表示します。オブジェクトを含むエントリは、オブジェクトのコンテンツに基づいて個々のエントリへも拡大しています。

- **show running-config object** [**id** *object_id*]

  現在のすべてのオブジェクトを表示します。**id** キーワードを使用すると、単一のオブジェクトを名前別に表示できます。

- **show running-config object** *object_type*

  現在のオブジェクトをタイプ、ネットワーク、またはサービス別に表示します。

- **show running-config object-group** [**id** *group_id*]

  現在のすべてのオブジェクト グループを表示します。**id** キーワードを使用すると、単一のオブジェクト グループを名前別に表示できます。

- **show running-config object-group** *grp_type*

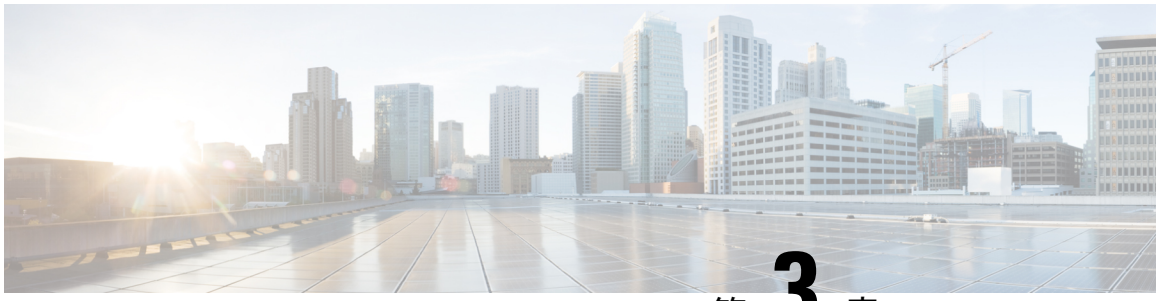
  現在のオブジェクト グループをグループ タイプごとに表示します。

オブジェクトの履歴

機能名	プラットフォーム リリース	説明
オブジェクト グループ	7.0(1)	オブジェクト グループによって、ACL の作成とメンテナンスが簡素化されます。 **object-group** *protocol*、**object-group** *network*、**object-group** *service*、**object-group** *icmp_type* の各コマンドが導入または変更されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
オブジェクト	8.3(1)	オブジェクトのサポートが導入されました。 次のコマンドが導入または変更されました。**object-network**、**object-service**、**object-group** ネットワーク、**object-group** サービス、**network object**、**access-list extended**、**access-list webtype**、**access-list remark**。
アイデンティティ ファイアウォールでのユーザー オブジェクト グループの使用	8.4(2)	アイデンティティ ファイアウォールのためのユーザー オブジェクト グループが導入されました。 **object-network user**、**user** のコマンドが導入されました。

機能名	プラットフォーム リリース	説明
Cisco TrustSec のためのセキュリティ グループ オブジェクト グループ	8.4(2)	Cisco TrustSec のためのセキュリティ グループ オブジェクト グループが導入されました。 **object-network security** および **security** コマンドが導入されました。
IPv4 および IPv6 の混合ネットワーク オブジェクト グループ	9.0(1)	以前は、ネットワーク オブジェクト グループに含まれているのは、すべて IPv4 アドレスであるか、すべて IPv6 アドレスでなければなりませんでした。現在では、ネットワーク オブジェクト グループが、IPv4 と IPv6 の両方のアドレスの混合をサポートするようになりました。 （注） 混合オブジェクト グループを NAT に使用することはできません。 **object-group network** コマンドが変更されました。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 **access-list extended**、**service-object**、**service** の各コマンドが導入または変更されました。
Stream Control Transmission Protocol（SCTP）のサービス オブジェクトのサポート	9.5(2)	特定の SCTP ポートに対するサービス オブジェクトおよびグループを作成できるようになりました。 次のコマンドが変更されました。**service-object**、**service**

機能名	プラットフォーム リリース	説明
ネットワークサービス オブジェクトと、ポリシーベースのルーティングおよびアクセス制御におけるネットワークサービス オブジェクトの使用	9.17(1)	ネットワークサービス オブジェクトを設定し、それらを拡張アクセス コントロール リストで使用して、ポリシーベース ルーティング ルート マップおよびアクセス コントロール グループで使用できます。ネットワークサービス オブジェクトには、IP サブネットまたは DNS ドメイン名の仕様が含まれ、オプションでプロトコルとポートの仕様が含まれます。これらは、基本的にネットワークオブジェクトとサービスオブジェクトを結合します。この機能には、信頼できる DNS サーバーを定義して、DNS ドメイン名解決が信頼できる送信元から IP アドレスを確実に取得できるようにする機能も含まれています。 次のコマンドが追加または変更されました：**access-list extended**、**app-id**、**clear configure object network-service**、**clear configure object-group network-service**、**clear dns ip-cache**、**clear object**、**clear object-group**、**debug network-service**、**description**、**dns trusted-source**、**domain**、**network-service-member**、**network-service reload**、**object-group network-service**、**object network-service**、**policy-route cost**、**set adaptive-interface cost**、**show asp table classify**、**show asp table network-service**、**show dns trusted-source**、**show dns ip-cache**、**show object**、**show object-group**、**show running-config**、**subnet**
ネットワークサービス グループのサポート	9.19(1)	最大 1024 のネットワーク サービス グループを定義できるようになりました。



第 3 章

アクセス コントロール リスト

アクセス コントロール リスト（ACL）は、さまざまな機能で使用されます。ACL をアクセス ルールとしてインターフェイスに適用するか、グローバルに適用すると、アプライアンスを通過するトラフィックが許可または拒否されます。ACL では、他の機能のために、機能を適用するトラフィックを選択し、制御サービスではなく照合サービスを実行します。

ここでは、ACL の基本と ACL を設定およびモニターする方法について説明します。アクセス ルールとは、グローバルに、またはインターフェイスに適用される ACL のことです。これについては、「アクセス ルール （63 ページ）」で詳しく説明します。

- ACL について （33 ページ）
- アクセス制御リストのライセンス （38 ページ）
- ACL のガイドライン （39 ページ）
- ACL の設定 （40 ページ）
- 隔離されたコンフィギュレーション セッションでの ACL の編集 （57 ページ）
- ACL のモニタリング （59 ページ）
- ACL の履歴 （59 ページ）

ACL について

アクセス コントロール リスト（ACL）では、ACL のタイプに応じてトラフィック フローを 1 つまたは複数の特性（送信元および宛先 IP アドレス、IP プロトコル、ポート、EtherType、その他のパラメータを含む）で識別します。ACL は、さまざまな機能で使用されます。ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。

ACL タイプ

ASA では、次のタイプの ACL が使用されます。

- 拡張 ACL：主に使用されるタイプです。この ACL は、サービス ポリシー、AAA ルール、WCCP、ボットネット トラフィック フィルタ、VPN グループおよび DAP ポリシーを含むさまざまな機能で、トラフィックがデバイスを通過するのを許可および拒否するアクセス

ルールとトラフィックの照合に使用されます。 拡張 ACL の設定 （41 ページ）を参照してください。

- EtherType ACL：EtherType ACL はブリッジ グループ メンバーのインターフェイスの非 IP レイヤ 2 トラフィックにのみ適用されます。これらのルールを使用して、レイヤ 2 パケット内の EtherType 値に基づいてトラフィックを許可または破棄できます。EtherType ACL では、デバイスでの非 IP トラフィック フローを制御できます。EtherType ACL の設定 （55 ページ）を参照してください。
- Webtype ACL：クライアントレス SSL VPN トラフィックのフィルタリングに使用されます。この ACL では、URL または宛先アドレスに基づいてアクセスを拒否できます。Webtype ACL の設定 （50 ページ）を参照してください。
- 標準 ACL：宛先アドレスだけでトラフィックを識別します。このタイプの ACL は、少数の機能（ルート マップと VPN フィルタ）でしか使用されません。VPN フィルタでは拡張アクセス リストも使用できるので、標準 ACL の使用はルート マップだけにしてください。 標準 ACL の設定 （50 ページ）を参照してください。

次の表に、ACL の一般的な使用目的と使用するタイプを示します。

表 *1*：*ACL* のタイプと一般的な使用目的

ACL の使用目的	ACL タイプ	説明
IP トラフィックのネットワーク アクセスの制御（ルーテッド モードおよびトランスペアレント モード）	拡張	ASA では、拡張 ACL により明示的に許可されている場合を除き、低位のセキュリティ インターフェイスから高位のセキュリティインターフェイスへのトラフィックは認められません。ルーテッドモードでは、ACLを使用して、ブリッジグループメンバーのインターフェイスと同じブリッジ グループの外部のインターフェイスとの間のトラフィックを許可する必要があります。 （注） また、ASAインターフェイスに管理アクセスの目的でアクセスするには、ホストIPアドレスを許可するACLは必要ありません。必要なのは、一般的な操作の設定ガイドに従って管理アクセスを設定することだけです。
AAA ルールでのトラフィック識別	拡張	AAAルールでは、ACLを使用してトラフィックを識別します。
特定のユーザーの IP トラフィックに対するネットワーク アクセス コントロールの強化	拡張、ユーザーごとに AAA サーバーからダウンロード	ユーザーに適用するダイナミック ACLをダウンロードするように RADIUS サーバーを設定できます。または、ASA 上に設定済みの ACL の名前を送信するようにサーバーを設定できます。

ACL の使用目的	ACL タイプ	説明
VPN アクセスおよびフィルタリング	拡張 規格	リモート アクセスおよびサイト間 VPN のグループ ポリシーでは、標準または拡張ACLがフィルタリングに使用されます。リモート アクセス VPN では、クライアントファイアウォール設定とダイナミック アクセス ポリシーにも拡張 ACL が使用されます。
トラフィック クラス マップでのモジュラポリシーフレームワークのトラフィックの識別	拡張	ACLを使用すると、クラスマップ内のトラフィックを識別できます。このマップは、モジュラ ポリシー フレームワークをサポートする機能に使用されます。モジュラ ポリシーフレームワークをサポートする機能には、TCP および一般的な接続設定やインスペクションなどがあります。
ブリッジ グループ メンバーのインターフェイスに対する非 IP トラフィックのネットワーク アクセスの制御	EtherType	ブリッジ グループのメンバーであるすべてのインターフェイスのEtherTypeに基づいて、トラフィックを制御をする ACL を設定できます。
ルート フィルタリングおよび再配布の特定	規格 拡張	各種のルーティング プロトコルでは、IP アドレスのルートフィルタリングと（ルートマップを介した）再配布にACLが使用されます（IPv4アドレスの場合は標準 ACL が、IPv6 アドレスの場合は拡張 ACL がそれぞれ使用されます）。
クライアントレス SSL VPN のフィルタリング	Webtype	Webtype ACL は、URL と宛先をフィルタリングするように設定できます。

ACL 名

各 ACL には、outside_in、OUTSIDE_IN、101 などの名前または数値 ID があります。名前は 241 文字以下にする必要があります。実行コンフィギュレーションを表示するときに名前を簡単に見つけられるように、すべて大文字にすることを検討してください。

ACL の目的を識別するのに役立つ命名規則を作成します。ASDM では、「*interface-name_purpose_direction*」などの命名規則が使用されます。たとえば、「外部」インターフェイスにインバウンド方向で適用される ACL の場合には、「outside_access_in」のようになります。

従来、 ACL ID は数値でした。標準 ACL は、1 ～ 99 または 1300 ～ 1999 の範囲にありました。拡張 ACL は、100 ～ 199 または 2000 ～ 2699 の範囲にありました。ASA では、これらの範囲は強制されませんが、数値を使用する場合は、IOS ソフトウェアを実行するルータとの一貫性を保つために、これらの命名規則を引き続き使用することをお勧めします。

アクセス コントロール エントリの順序

1 つの ACL は、1 つまたは複数の ACE で構成されます。特定の行に明示的に ACE を挿入しない限り、ある ACL 名について入力した各 ACE はその ACL の末尾に追加されます。

ACE の順序は重要です。ASA は、パケットを転送するかドロップするかを決定するとき、エントリがリストされている順序で各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。

したがって、一般的なルールの後に具体的なルールを配置した場合、具体的なルールは決してヒットしない可能性があります。たとえば、ネットワーク 10.1.1.0/24 を許可し、そのサブネット上のホスト 10.1.1.15 からのトラフィックをドロップする場合、10.1.1.15 を拒否する ACE は 10.1.1.0/24 を許可する ACE の前に置く必要があります。10.1.1.0/24 を許可する ACE を先にすると、10.1.1.15 は許可され、拒否 ACE は決して一致しません。

拡張 ACL では、**access-list** コマンドで **line** *number* パラメータを使用して適切な場所にルールを挿入します。どの番号を使用すればよいか判断できるように ACL エントリとその行番号を表示するには、**show access-list** *name* コマンドを使用します。その他のタイプの ACL の場合は、ACL を作成（できれば ASDM を使用）して ACE の順序を変更します。

許可/拒否と一致/不一致

アクセス コントロール エントリでは、ルールに一致するトラフィックを「許可」または「拒否」します。グローバルアクセスルールやインターフェイスアクセスルールなど、トラフィックが ASA の通過を許可されるか、ドロップされるかを決定する機能に ACL を適用する場合、「許可」と「拒否」は文字どおりの意味を持ちます。

サービスポリシールールなどのその他の機能の場合、「許可」と「拒否」は実際には「一致」または「不一致」を意味します。この場合、ACL では、アプリケーション インスペクションやサービスモジュールへのリダイレクトなど、その機能のサービスを受けるトラフィックを選択しています。「拒否される」トラフィックは、単に ACL に一致せず、したがってサービスを受けないトラフィックのことです

アクセス コントロールによる暗黙的な拒否

through-the-box アクセス ルールに使用する ACL には末尾に暗黙の deny ステートメントがあります。したがって、インターフェイスに適用される ACL などのトラフィック制御 ACL では、あるタイプのトラフィックを明示的に許可しない場合、そのトラフィックはドロップされます。たとえば、1 つまたは複数の特定のアドレス以外のすべてのユーザーが ASA 経由でネットワークにアクセスできるようにするには、特定のアドレスを拒否してから、その他のすべてのアドレスを許可する必要があります。

管理（コントロール プレーン）の ACL は to-the-box トラフィックを管理していますが、インターフェイスの一連の管理ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセス ルールに一致しない接続は通常のアクセス制御ルールで評価されます。

サービス対象のトラフィックの選択に使用されるACLの場合は、明示的にトラフィックを「許可」する必要があります。「許可」されていないトラフィックはサービスの対象になりません。「拒否された」トラフィックはサービスをバイパスします。

EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によって、拡張 ACL で以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE で明示的にすべてのトラフィックを拒否すると、IP および ARP トラフィックが拒否されます。許可されるのは、自動ネゴシエーションなどの物理プロトコル トラフィックだけです。

NAT 使用時に拡張 ACL で使用する IP アドレス

NAT または PAT を使用すると、アドレスまたはポートが変換され、通常は内部アドレスと外部アドレスがマッピングされます。変換されたポートまたはアドレスに適用される拡張 ACL を作成する必要がある場合は、実際の（変換されていない）アドレスまたはポートを使用するか、マッピングされたアドレスまたはポートを使用するかを決定する必要があります。要件は機能によって異なります。

実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。

実際の IP アドレスを使用する機能

次のコマンドおよび機能では、インターフェイスに表示されるアドレスがマッピング アドレスである場合でも、実際の IP アドレスを使用します。

- アクセス ルール（access-group コマンドで参照される拡張 ACL）
- サービス ポリシー ルール（モジュラ ポリシー フレームワークの match access-list コマンド）
- ボットネット トラフィック フィルタのトラフィック分類（dynamic-filter enable classify-list コマンド）
- AAA ルール（aaa ... match コマンド）
- WCCP（wccp redirect-list group-list コマンド）

たとえば、内部サーバー 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバーに付与する場合は、この内部サーバーへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバーのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

```
hostname(config)# object network server1
hostname(config-network-object)# host 10.1.1.5
hostname(config-network-object)# nat (inside,outside) static 209.165.201.5

hostname(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
```

```
hostname(config)# access-group OUTSIDE in interface outside
```

マッピング IP アドレスを使用する機能

次の機能は、ACL を使用しますが、これらの ACL は、インターフェイス上で認識されるマッピングされた値を使用します。

- IPsec ACL
- capture コマンドの ACL
- ユーザー単位 ACL
- ルーティング プロトコルの ACL
- 他のすべての機能の ACL

時間ベース ACE

ルールが一定期間だけアクティブになるように、拡張 ACE と Webtype ACE に時間範囲オブジェクトを適用することができます。このタイプのルールを使用すると、特定の時間帯には許容できるものの、それ以外の時間帯には許容できないアクティビティを区別できます。たとえば、勤務時間中に追加の制限を設け、勤務時間後または昼食時にその制限を緩めることができます。逆に、勤務時間外は原則的にネットワークをシャットダウンすることもできます。

時間範囲オブジェクトが含まれていないルールでは、プロトコル、送信元、宛先、およびサービス基準が正確に同じ時間ベースのルールを作成することはできません。時間ベースではないルールは、重複した時間ベースのルールを常にオーバーライドします（冗長であるため）。

（注） ACL を非アクティブにするための指定の終了時刻の後、約 80 ～ 100 秒の遅延が発生する場合があります。たとえば、指定の終了時刻が 3:50 の場合、この 3:50 は終了時刻に含まれているため、コマンドは、3:51:00 ～ 3:51:59 の間に呼び出されます。コマンドが呼び出された後、ASA は現在実行されているすべてのタスクを終了し、コマンドに ACL を無効にさせます。

アクセス制御リストのライセンス

アクセス制御リストは特別なライセンスを必要としません。

ただし、エントリ内でプロトコルとして **sctp** を使用する場合は、キャリア ライセンスが必要です。

ACL のガイドライン

ファイアウォール モード

- 標準 ACL と拡張 ACL は、ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされます。
- Webtype ACL は、ルーテッド モードのみでサポートされます。
- EtherType ACL は、ルーテッドおよびトランスペアレント モードで、ブリッジ グループ メンバーのインターフェイスに対してのみサポートされます。

フェールオーバーとクラスタリング

コンフィギュレーション セッションは、フェイルオーバーまたはクラスタ ユニット間で同期されません。あるセッションで変更をコミットすると、通常どおりすべてのフェイルオーバーおよびクラスタ ユニットでその変更が反映されます。

IPv6

- 拡張 ACL と Webtype ACL では、IPv4 アドレスと IPv6 アドレスを組み合わせて使用できます。
- 標準 ACL では、IPv6 アドレスは使用できません。
- EtherType ACL では、IP アドレスは使用しません。

その他のガイドライン

- ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。ASA では、ネットワーク マスク（たとえば、Class C マスクの 255.255.255.0）が使用されます。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。
- （拡張 ACL のみ）次の機能では、ACL を使用しますが、アイデンティティ ファイアウォール（個人またはグループ名を指定）、FQDN（完全修飾ドメイン名）、または Cisco TrustSec 値を含む ACL は使用できません。
  - VPN の crypto map コマンド
  - VPN の group-policy コマンド、ただし、vpn-filter を除く
  - WCCP
  - DAP

ACL の設定

次の各セクションでは、さまざまなタイプの ACL の設定方法について説明します。まず ACL の基本に関するセクションを読んで全体像を把握し、次に特定のタイプの ACL に関するセクションを読んで詳細を確認してください。

基本的な ACL 設定および管理オプション

1 つの ACL は、同じ ACL ID または ACL 名を持つ 1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。新しい ACL を作成するには、新しい ACL 名で ACE を作成します。作成した ACE は、新しい ACL の最初のルールになります。

ACL の操作では、次のことを実行できます。

ACL の内容を確認し、行番号とヒット数を決定する

ACL の内容を表示するには、**show access-list** *name* コマンドを使用します。各行は ACE で、行番号を含みます。行番号は、拡張 ACL に新しいエントリを挿入する場合に知っておく必要があります。情報には、各 ACE のヒット カウントも含まれます。ヒット カウントは、トラフィックがルールに一致した回数です。次に例を示します。

```
hostname# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group
LOCAL\\usergroup any any (hitcnt=0) 0xb0f5b1e1
```

ACE を追加する

ACE を追加するためのコマンドは **access-list** *name* [**line** *line-num*] *type parameters* です。行番号引数は、拡張 ACL でのみ使用できます。行番号を指定すると、ACE は ACL のその場所に挿入されます。その場所にあった ACE は、残りの ACE とともに下に移動します（つまり、ある行番号の位置に ACE を挿入しても、その行にあった古い ACE は置き換えられません）。行番号を指定しない場合、ACE は ACL の末尾に追加されます。使用可能なパラメータは、ACL のタイプによって異なります。詳細については、各 ACL タイプのトピックを参照してください。

コメントを ACL に追加する（Webtype 以外のすべてのタイプ）

ACE の目的を説明するのに役立つ注釈を ACL に追加するには、**access-list** *name* [**line** *line-num*] **remark** *text* コマンドを使用します。ベスト プラクティスは、ACE の前に注釈を挿入することです。ASDM で設定を表示すると、注釈は、その注釈に続く ACE に関連付けられます。ACE の前に複数の注釈を入力してコメントを拡張できます。各注釈は 100 文字に制限されます。先頭にスペースを置いて注釈を強調することができます。行番号を指定しない場合、注釈は ACL の末尾に追加されます。たとえば、各 ACE を追加する前に注釈を追加できます。

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

ACE または注釈を編集または移動する

ACE または注釈を編集または移動することはできません。代わりに、目的の値を持つ新しい ACE または注釈を（行番号を使用して）適切な場所に作成してから、古い ACE または注釈を削除します。ACE を挿入できるのは拡張 ACL だけなので、標準、Webtype、または EtherType の ACL の ACE を編集または移動する必要がある場合は、それらのタイプの ACL を再作成する必要があります。これは ASDM を使用して長い ACL を再編成するよりもはるかに簡単です。

ACE または注釈を削除する

ACE または注釈を削除するには、**no access-list** *parameters* コマンドを使用します。入力する必要があるパラメータ文字列を表示するには、**show access-list** コマンドを使用します。この文字列は、削除する ACE または注釈に正確に一致する必要があります。ただし、**line** *line-num* 引数は除きます。この引数は、**no access-list** コマンドのオプションです。

注釈を含む ACL 全体を削除する

clear configure access-list *name* コマンドを使用します。注意してください。このコマンドでは、確認は求められません。名前を含めないと、ASA のすべてのアクセス リストが削除されます。

ACL の名前を変更する

access-list *name* **rename** *new_name* コマンドを使用します。

ACL をポリシーに適用する

ACL を作成しただけでは、トラフィックには何の処理も実行されません。ポリシーに ACL を適用する必要があります。たとえば、access-group コマンドを使用してインターフェイスに拡張 ACL を適用すると、このインターフェイスを通過するトラフィックを拒否または許可できます。

拡張 ACL の設定

拡張 ACL は、同じ ACL ID または ACL 名を持つすべての ACE で構成されます。拡張 ACL は、最も複雑で機能豊富な ACL タイプで、さまざまな機能に使用できます。拡張 ACL の最も注目すべき用途は、グローバルに、またはインターフェイスに適用され、デバイスを通過するのを拒否または許可されるトラフィックを決定するアクセス グループとしての使用です。ただし、拡張 ACL は、その他のサービスの適用対象のトラフィックを決定するのにも使用されます。

拡張 ACL は複雑であるため、次の各セクションでは、ACE を作成して特定のタイプのトラフィック照合を提供することに焦点を当てます。最初のセクションでは、基本的なアドレス ベースの ACE と TCP/UDP ACE について説明し、残りのセクションの基礎を作ります。

IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加

基本的な拡張 ACE では、IPv4 および IPv6 アドレスや、www.example.com などの完全修飾ドメイン名（FQDN）を含む送信元アドレスと宛先アドレスに基づいてトラフィックを照合します。実際、どのタイプの拡張 ACE にも、送信元アドレスと宛先アドレスに関する詳細を含める必要があります。したがって、このトピックでは、最小限の拡張 ACE について説明します。

ヒント　ヒント：FQDN に基づいてトラフィックを照合する場合は、各 FQDN を表すネットワーク オブジェクトを作成する必要があります。

IP アドレスまたは FQDN 照合に使用する ACE を追加するには、次のコマンドを使用します。

access-list *access_list_name* ［**line** *line_number*］ **extended** ｛**deny** ｜ **permit**｝ *protocol_argument source_address_argument dest_address_argument* ［**log** ［［*level*］ ［**interval** *secs*］ ｜ **disable** ｜ **default**］］ ［**time-range** *time_range_name*］ ［**inactive**］

例：

```
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-list ACL_IN extended permit object service-obj-http any any
```

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。
- 行番号：**line***line_number*オプションでは、ACE を挿入する位置の行番号を指定します。指定しない場合は、ACL の末尾に追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- プロトコル：*protocol_argument* では、IP プロトコルを指定します。プロトコルとポートを指定するネットワークサービス オブジェクト グループを使用する場合は、この引数で **ip** を指定します。
  - *name* または *number*：プロトコルの名前または番号を指定します。**ip** を指定すると、すべてのプロトコルに適用されます。
  - **object-group** *protocol_grp_id*：**object-group protocol** コマンドを使用して作成されたプロトコルオブジェクトを指定します。
  - **object** *service_obj_id*：**object service** コマンドを使用して作成されたサービスオブジェクトを指定します。オブジェクトには、ポートまたは ICMP タイプとコード仕様を含めることができます（必要に応じて）。
  - **object-group** *service_grp_id*：**object-group service** コマンドを使用して作成されたサービス オブジェクト グループを指定します。

- 送信元アドレス、宛先アドレス：*source_address_argument* ではパケットの送信元の IP アドレスまたは FQDN を指定し、*dest_address_argument* ではパケットの送信先の IP アドレスまたは FQDN を指定します。
  - **host** *ip_address*：IPv4 ホストアドレスを指定します。
  - *ip_address mask*：10.100.10.0 255.255.255.0 などの IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
  - *ipv6-address/prefix-length*：IPv6 ホストまたはネットワークアドレスとプレフィックスを指定します。
  - **any**、**any4**、および **any6**：**any** は IPv4 と IPv6 の両方のトラフィックを指定します。**any4** は IPv4 トラフィックのみを指定します。**any6** は IPv6 トラフィックのみを指定します。
  - **interface** *interface_name*：ASA インターフェイスの名前を指定します。IP アドレスではなくインターフェイス名を使用して、トラフィックの送信元または宛先のインターフェイスに基づいてトラフィックを照合します。
  - **object** *nw_obj_id*：**object network** コマンドを使用して作成されたネットワークオブジェクトを指定します。
  - **object-group** *nw_grp_id*：**object-group network** コマンドを使用して作成されたネットワーク オブジェクト グループを指定します。
  - **object-group-network-service** *name*：ネットワークサービス オブジェクト グループの名前を指定します。
- ロギング：**log** 引数では、ACE がネットワークアクセス用の接続に一致するとき（**access-group** コマンドで ACL が適用されます）のロギングオプションを設定します。引数を指定せずに **log** オプションを入力すると、syslog メッセージ 106100 はデフォルトレベル（6）とデフォルト間隔（300 秒）で有効になります。ログ オプションは次のとおりです。
  - *level*：0 ～ 7 のシビラティ（重大度）。デフォルトは 6（情報）です。アクティブな ACE に対してこのレベルを変更する場合、新しいレベルは新規接続に適用され、既存の接続は引き続き前のレベルでロギングされます。
  - **interval** *secs*：syslog メッセージ間の時間間隔（秒）。1 ～ 600 で指定します。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。
  - **disable**：すべての ACE ロギングをディセーブルにします。
  - **default**：拒否されたパケットに関するメッセージ 106023 のロギングを有効にします。この設定は、**log** オプションを指定しないのと同じです。

- 時間範囲： **time-range** *time_range_name* オプションでは、ACE をアクティブにする時間帯と曜日を決定する時間範囲オブジェクトを指定します。時間範囲を指定しない場合、ACE は常にアクティブです。
- アクティベーション：ACE を削除せずに無効化するには、 **inactive** オプションを使用します。再度イネーブルにするには、inactive キーワードを使用せずに ACE 全体を入力します。

ポートベースの照合に使用する拡張 ACE の追加

ACE でサービス オブジェクトを指定する場合は、サービス オブジェクトに TCP/80 などのポートが指定されたプロトコルを含めることができます。または、ACE にポートを直接指定できます。ポートベースの照合を使用すると、プロトコルのすべてのトラフィックではなく、ポートベースのプロトコルの特定のタイプのトラフィックを対象にすることができます。

（注） プロトコルとポートを指定するネットワークサービス オブジェクト グループを使用する場合は、このトピックで説明しているとおり、ポートを指定しないでください。オブジェクトに定義されているプロトコル/ポートが一致するように、プロトコルとして**ip**を指定します。

ポートベースの 拡張 ACE は、プロトコルが **tcp**、**udp**、または **sctp** である基本的なアドレス照合 ACE です。ポート仕様を追加するには、次のコマンドを使用します。

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **sctp**} *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**] [**time-range** *time-range-name*] [**inactive**]

例：

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

port_argument オプションでは、送信元ポートまたは宛先ポートを指定します。ポートを指定しなかった場合は、すべてのポートが照合されます。使用可能な引数は次のとおりです。

- *operator port*：*port* は、整数またはポートの名前にできます。*operator* には次のいずれかを指定できます。
  - **lt**：より小さい
  - **gt**：より大きい
  - **eq**：等しい
  - **neq**：等しくない
  - **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します（例：**range 100 200**）。

（注） DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。

- **object-group** *service_grp_id*：**object-group service**{**tcp** | **udp** | **tcp-udp**} コマンドを使用して作成されたサービス オブジェクト グループを指定します。これらのオブジェクト タイプは推奨されなくなりました。

  ポート引数としてプロトコルおよびポートがオブジェクト内で定義されている場合は、推奨される一般的なサービス オブジェクトは指定できません。IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 （42 ページ） で説明されているように、これらのオブジェクトはプロトコル引数の一部として指定します。

その他のキーワードの詳細と、サービス オブジェクトを使用してプロトコルおよびポートを指定する方法については、IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 （42 ページ） を参照してください。

ICMP ベースの照合に使用する拡張 ACE の追加

ICMP トラフィックを照合するには、ICMP プロトコルキーワード **icmp** または **icmp6**のいずれかを使用します。**icmp** プロトコルは IPv4 アドレスのみに一致し、 **icmp6** プロトコルは IPv6 アドレスのみに一致します。ネットワークアドレスが選択したプロトコルと一致することを確認します。そうでない場合、ACE はどの接続とも一致しません。

ACE でサービス オブジェクトを指定する場合は、サービス オブジェクトに ICMP/ICMP6 プロトコルの ICMP タイプとコード仕様を含めることができます。または、ACE に ICMP タイプとコードを直接指定できます。たとえば、ICMP エコー要求（ping）トラフィックをターゲットにできます。

ICMP 拡張 ACE は、プロトコルが **icmp** または **icmp6** である基本的なアドレス照合 ACE です。これらのプロトコルにはタイプおよびコード値があるため、ACE にタイプおよびコード仕様を追加できます。

プロトコルが ICMP または ICMP6 である IP アドレスまたは FQDN 照合に使用する ACE を追加するには、次のコマンドを使用します。

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**} *source_address_argument dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

例：

```
hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
hostname(config)# access-list abc extended permit icmp any any echo
```

icmp_argument オプションでは、ICMP のタイプとコードを指定します。

- *icmp_type* [*icmp_code*]：ICMP タイプを名前または番号で指定し、そのタイプの ICMP コード（省略可能）を指定します。コードを指定しない場合は、すべてのコードが使用されます。
- **object-group** *icmp_grp_id*：（廃止予定）**object-group icmp-type** コマンドを使用して作成された ICMP/ICMP6 用のオブジェクト グループを指定します。

  ICMP 引数としてプロトコルおよびタイプがオブジェクト内で定義されている場合は、推奨される一般的なサービス オブジェクトは指定できません。IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 （42 ページ） で説明されているように、これらのオブジェクトはプロトコル引数の一部として指定します。

他のキーワードの説明については、IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 （42 ページ）を参照してください。

ユーザーベースの照合（アイデンティティ ファイアウォール）に使用する拡張ACEの追加

ユーザーベースの拡張 ACE は、ユーザー名またはユーザー グループを送信元の一致条件に含める基本的なアドレス照合 ACE です。ユーザー ID に基づくルールを作成すると、ルールがスタティックなホストまたはネットワーク アドレスに縛られるのを回避できます。たとえば、user1 のルールを定義し、アイデンティティ ファイアウォール機能によってそのユーザーがあるホストにマッピングされているとします。さらに、このホストにある日 10.100.10.3 が割り当てられ、その翌日に 192.168.1.5 が割り当てられたとします。この場合でも、ユーザーベースのルールは適用されます。

送信元アドレスと宛先アドレスは引き続き指定する必要があります。そのため、送信元アドレスは、ユーザーに（通常は DHCP 経由で）割り当てられる可能性があるアドレスが含まれるように広く設定してください。たとえば、ユーザー「LOCAL\user1 any」は、割り当てられているアドレスに関係なく LOCAL\user1 ユーザーに一致しますが、「LOCAL\user1 10.100.1.0 255.255.255.0」は、アドレスが 10.100.1.0/24 ネットワーク上にある場合にのみユーザーに一致します。

グループ名を使用すると、学生、教師、マネージャ、エンジニアなどユーザーのクラス全体に基づいてルールを定義できます。

ユーザーまたはグループ照合に使用する ACE を追加するには、次のコマンドを使用します。

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

例：

```
hostname(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

user_argument オプションでは、送信元アドレスに加えて、トラフィックを照合するユーザーまたはグループを指定します。使用可能な引数は次のとおりです。

- **object-group-user** *user_obj_grp_id*：**object-group user** コマンドを使用して作成されたユーザー オブジェクト グループを指定します。
- **user** {[*domain_nickname*\]*name* | **any** | **none**}：ユーザー名を指定します。ユーザー クレデンシャルを含むすべてのユーザーを照合するには **any** を指定し、ユーザー名にマッピングされていないアドレスを照合するには **none** を指定してください。これらのオプションが特に役立つのは、**access-group** と **aaa authentication match** のポリシーを結合する場合です。
- **user-group** [*domain_nickname*\\]*user_group_name*：ユーザー グループ名を指定します。\\ はドメインとグループ名の区切りです。

他のキーワードの説明については、IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 （42 ページ）を参照してください。

ヒント　特定の ACE にユーザーと Cisco Trustsec セキュリティ グループの両方を含めることができます。

セキュリティ グループ ベースの照合（Cisco TrustSec）に使用する拡張 ACE の追加

セキュリティ グループ拡張 ACE は、セキュリティ グループまたはタグを送信元または宛先の一致条件に含める基本的なアドレス照合 ACE です。セキュリティ グループに基づくルールを作成すると、ルールがスタティックなホストまたはネットワーク アドレスに縛られるのを回避できます。送信元アドレスと宛先アドレスは引き続き指定する必要があります。そのため、アドレスは、ユーザーに（通常は DHCP 経由で）割り当てられる可能性があるアドレスが含まれるように広く設定してください。

ヒント　このタイプの ACE を追加する前に、Cisco TrustSec 設定してください。

セキュリティ グループ照合に使用する ACE を追加するには、次のコマンドを使用します。

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

例：

```
hostname(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

security_group_argument オプションでは、送信元または宛先アドレスに加えて、トラフィックを照合するセキュリティ グループを指定します。使用可能な引数は次のとおりです。

- **object-group-security** *security_obj_grp_id*：**object-group security** コマンドを使用して作成されたセキュリティ オブジェクト グループを指定します。

- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*}：セキュリティ グループの名前またはタグを指定します。

他のキーワードの説明については、IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 （42 ページ）を参照してください。

ヒント　特定の ACE にユーザーと Cisco Trustsec セキュリティ グループの両方を含めることができます。

拡張 ACL の例

次に示す ACL は ASA を通るすべてのホスト（ACL を適用するインターフェイス上の）を許可します。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次の ACL は、192.168.1.0/24 のホストが TCP ベースのトラフィックで 209.165.201.0/27 のネットワークにアクセスすることを拒否します。その他のアドレスはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

選択したホストだけにアクセスを制限する場合は、限定的な許可 ACE を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次の ACL では、すべてのホスト（この ACL を適用するインターフェイス上の）からアドレス 209.165.201.29 の Web サイトへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

オブジェクト グループを使用する次の ACL では、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバーへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

次の例では、あるネットワーク オブジェクト グループ（A）から別のネットワーク オブジェクト グループ（B）へのトラフィックを許可する ACL を一時的にディセーブルにします。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

時間ベース ACE を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲を ACE にバインドします。次の例では、「Sales」ACL の ACE を「New_York_Minute」という時間範囲にバインドしています。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

次の例では、IPv4/IPv6 混在 ACL が表示されています。

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

アドレスを拡張 ACL のオブジェクトに変換する例

次に示す、オブジェクト グループを使用しない通常の ACL では、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバーへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

2 つのネットワーク オブジェクト グループ（内部ホスト用に 1 つ、Web サーバー用に 1 つ）を作成すると、コンフィギュレーションが簡略化され、簡単に修正してホストを追加できるようになります。

```
hostname(config)# object-group network denied
```

```
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config)# access-list ACL_IN extended deny tcp object-group denied object-group

web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

標準 ACL の設定

標準 ACL は、ACL ID または名前が同じすべての ACE で構成されます。標準 ACL は、ルートマップや VPN フィルタなどの限られた数の機能に使用されます。標準 ACL では、 IPv4 アドレスのみを使用して、宛先アドレスのみを定義します。

標準アクセス リスト エントリを追加するには、次のコマンドを使用します。

access-list *access_list_name* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address mask*}

例：

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

次のオプションがあります。

- 名前：*access_list_name* 引数には、ACL の名前または番号を指定します。標準 ACL の従来の数値は 1 ～ 99 または 1300 ～ 1999 ですが、任意の名前または数値を使用できます。ACL がまだ存在しない場合は、新しい ACL を作成します。ACL が存在する場合、エントリは ACL の末尾に追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- 宛先アドレス：**any4** キーワードは、すべての IPv4 アドレスに一致します。**host** *ip_address* 引数は、ホストの IPv4 アドレスに一致します。*ip_address ip_mask* 引数は、IPv4 サブネット（10.1.1.0 255.255.255.0 など）に一致します。

Webtype ACL の設定

Webtype ACL は、クライアントレス SSL VPN トラフィックのフィルタリング、特定のネットワーク、サブネット、ホスト、および Web サーバーへのユーザー アクセスの制限に使用されます。フィルタを定義しない場合は、すべての接続が許可されます。Webtype ACL は、同じ ACL ID または ACL 名を持つすべての ACE で構成されます。

Webtype ACL では、URL または宛先アドレスに基づいてトラフィックを照合できます。単一の ACE でこれらの仕様を組み合わせることはできません。次の各セクションでは、各タイプの ACE について説明します。

URL 照合に使用する Webtype ACE の追加

ユーザーがアクセスしようとしている URL に基づいてトラフィックを照合するには、次のコマンドを使用します。

access-list *access_list_name* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *time_range_name*] [**inactive**]

例：

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。ACL がすでに存在する場合は、ACL の末尾に ACE が追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- URL：**url** キーワードでは、照合する URL を指定します。すべての URL ベースのトラフィックに一致させるには、**url any** を使用します。そうでない場合は、URL 文字列を入力します。URL 文字列には、ワイルドカードを含めることができます。以下では、URL の指定に関するヒントと制限事項をいくつか示します。
  - すべての URL に一致させるには、**any** を指定します。
  - 「Permit url any」と指定すると、「プロトコル://サーバー IP/パス」の形式の URL はすべて許可され、このパターンに一致しないトラフィック（ポート転送など）はブロックされます。暗黙的な拒否が発生しないよう、必要なポート（Citrix の場合はポート 1494）への接続を許可する ACE を使用してください。
  - スマート トンネルと ica プラグインは、smart-tunnel:// と ica:// のタイプにのみ一致するため、「permit url any」を使用した ACL によって影響を受けることはありません。
  - 使用できるプロトコルは、cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel://、および smtp:// です。プロトコルでワイルドカードを使用することもできます。たとえば、htt* は http および https に一致し、アスタリスク * はすべてのプロトコルに一致します。たとえば、*://*.example.com は、example.com ネットワークへのすべてのタイプの URL ベース トラフィックに一致します。
  - smart-tunnel:// URL を指定すると、サーバー名だけを含めることができます。URL にパスを含めることはできません。たとえば、smart-tunnel://www.example.com は受け入れ可能ですが、smart-tunnel://www.example.com/index.html は受け入れ不可です。

- アスタリスク（*）：空の文字列を含む任意の文字列に一致します。すべての http URL に一致させるには、http://*/* と入力します。
- 疑問符 ? は任意の 1 文字に一致します。
- 角カッコ（[]）：文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、http://www.cisco.com:80/ と http://www.cisco.com:81/ の両方に一致させるには、「**http://www.cisco.com:8[01]/**」と入力します。

- ロギング：**log** 引数では、パケットが ACE に一致した場合のロギング オプションを設定します。引数を指定せずに **log** オプションを入力すると、syslog メッセージ 106102 はデフォルト レベル（6）とデフォルト間隔（300 秒）でイネーブルになります。ログ オプションは次のとおりです。
  - *level*：0 ～ 7 のシビラティ（重大度）。デフォルト値は 6 です。
  - **interval** *secs*：syslog メッセージ間の時間間隔（秒）。1 ～ 600 で指定します。デフォルトは 300 です。
  - **disable**：すべての ACL ロギングをディセーブルにします。
  - **default**：メッセージ 106103 のロギングをイネーブルにします。この設定は、**log** オプションを指定しないのと同じです。
- 時間範囲：**time-range** *time_range_name* オプションでは、ACE がアクティブになっている時間帯と曜日を決定する時間範囲オブジェクトを指定します。時間範囲を指定しない場合、ACE は常にアクティブです。
- アクティベーション：ACE を削除せずにディセーブルにするには、**inactive** オプションを使用します。再度イネーブルにするには、inactive キーワードを使用せずに ACE 全体を入力します。

IP アドレス照合に使用する Webtype ACE の追加

ユーザーがアクセスしようとしている宛先アドレスに基づいてトラフィックを照合するには、次のコマンドを使用します。Webtype ACL には、URL 仕様に加えて IPv4 アドレスと IPv6 アドレスの組み合わせを含めることができます。

IP アドレス照合に使用する Webtype ACE を追加するには、次のコマンドを使用します。

access-list *access_list_name* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *time_range_name*]] [**inactive**]]

例：

```
hostname(config)# access-list acl_company webtype permit tcp any
```

ここで説明していないキーワードの説明については、URL 照合に使用する Webtype ACE の追加 （51 ページ）を参照してください。このタイプの ACE に固有のキーワードと引数は次のとおりです。

- **tcp**：TCP プロトコル。Webtype ACL では、TCP トラフィックのみを照合します。
- 宛先アドレス：*dest_address_argument* では、パケットの送信先の IP アドレスを指定します。
  - **host** *ip_address*：IPv4 ホスト アドレスを指定します。
  - *dest_ip_address mask*：10.100.10.0 255.255.255.0 など、IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
  - *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。
  - **any**、**any4**、および **any6**： **any** は IPv4 と IPv6 トラフィックの両方を指定します。**any4** は IPv4 トラフィックのみを指定し、**any6** は IPv6 トラフィックのみを指定します。
- *operator port*：宛先ポート。ポートを指定しなかった場合は、すべてのポートが照合されます。*port* には、TCP ポートの番号（整数）または名前を指定できます。*operator* は次のいずれかになります。
  - **lt**：より小さい
  - **gt**：より大きい
  - **eq**：等しい
  - **neq**：等しくない
  - **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します（例：**range 100 200**）。

Webtype ACL の例

次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

次の例は、特定の Web ページへのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

次の例は、特定サーバー上にある任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

次の例は、Webtype ACL でワイルドカードを使用する方法を示しています。

- 次に、http://www.example.com/layouts/1033 などの URL に一致させる例を示します。

```
access-list VPN-Group webtype permit url http://www.example.com/*
```

- 次に、http://www.example.com/ や http://www.example.net/ などの URL に一致させる例を示します。

```
access-list test webtype permit url http://www.example.*
```

- 次に、http://www.example.com や ftp://wwz.example.com などの URL に一致させる例を示します。

```
access-list test webtype permit url *://ww?.e*co*/
```

- 次の例は、http://www.cisco.com:80 や https://www.cisco.com:81 などの URL に一致します。

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

  上記の例の範囲演算子「[ ]」は、文字 **0** または **1** がその場所で出現する可能性があることを示しています。

- 次に、http://www.example.com や http://www.example.net などの URL に一致させる例を示します。

```
access-list test webtype permit url http://www.[a-z]xample?*/
```

  上記の例に示した range 演算子「[]」は、**a** ～ **z** の範囲内の任意の 1 文字が出現可能であることを指定します。

- 次に、ファイル名またはパスのどこかに「cgi」が含まれる http または https URL に一致させる例を示します。

```
access-list test webtype permit url htt*://*/*cgi?*
```

（注） すべての http URL に一致させるには、「 http://*」ではなく「**http://*/***」と入力する必要があります。

次の例は、Web-type ACL を適用して、特定の CIFS 共有へのアクセスをディセーブルにする方法を示しています。

このシナリオでは、「shares」というルート フォルダに「Marketing_Reports」および「Sales_Reports」という 2 つのサブフォルダが格納されています。「shares/Marketing_Reports」フォルダへのアクセスを明示的に拒否しようとしています。

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

ただし、ACL の末尾に暗黙的な「deny all」があるため、上記の ACL を指定すると、ルート フォルダ（「shares」）とすべてのサブ フォルダ（「shares/Sales Reports」と「shares/Marketing Reports」）にアクセスできなくなります。

この問題を修正するには、ルート フォルダと残りのサブフォルダへのアクセスを許可する新しい ACL を追加します。

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

EtherType ACL の設定

EtherType ACL は、ブリッジ グループ メンバーのインターフェイスの非 IP レイヤ 2 トラフィックに適用されます。これらのルールを使用して、レイヤ 2 パケット内の EtherType 値に基づいてトラフィックを許可または破棄できます。EtherType ACL では、ブリッジ グループを経由する非 IP トラフィックのフローを制御できます。802.3 形式フレームでは、type フィールドではなく length フィールドが使用されるため、ACL では処理されません。

EtherType ACE を追加するには、次のコマンドを使用します。

access-list *access_list_name* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} | **eii-ipx** | **ipx** | **isis** | **mpls-multicast** | **mpls-unicast** | *hex_number*}

例：

```
hostname(config)# access-list ETHER ethertype deny mpls-multicast
```

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。ACL がすでに存在する場合は、ACL の末尾に ACE が追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否されます。**permit** キーワードは、条件が一致した場合にパケットを許可します。
- トラフィック一致条件：次のオプションを使用してトラフィックを照合できます。
  - **any**：すべてのレイヤ 2 トラフィックと一致します。
  - **bpdu**：デフォルトで許可されるブリッジ プロトコル データ ユニット（dsap 0x42）。このキーワードは **dsap bpdu** に変換されます。
  - **dsap**{*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**}：IEEE 802.2 論理リンク制御（LLC）パケットの宛先サービス アクセス ポイントのアドレス。ユーザーが許可または拒否するア

ドレスを 16 進数（0x01 ～ 0xff）で含めます。また、次のキーワードを使用して共通の値のルールを作成することもできます。

- **bpdu** 0x42 では、ブリッジ プロトコル データ ユニット。
- **ipx** 0xe0 では、Internet Packet Exchange（IPX）802.2 LLC。
- **isis** 0xfe では、Intermediate System to Intermediate System（IS-IS）
- **raw-ipx** 0xff では、Raw IPX 802.3 形式。

- **eii-ipx**：Ethernet II IPX 形式、EtherType 0x8137。
- **ipx**：Internetwork Packet Exchange（IPX）。このキーワードは、3 つの個別のルールを設定するための **dsap ipx**、**dsap raw-ipx**、および **eii-ipx** のショートカットです。
- **isis**：Intermediate System to Intermediate System（IS-IS）このキーワードは **dsap isis** に変換されます。
- **mpls-multicast**：MPLS マルチキャスト。
- **mpls-unicast**：MPLS ユニキャスト。
- [hex_number]：16 ビットの 16 進数 0x600 ～ 0xffff で指定できる任意の EtherType。EtherType のリストについては、http://www.ietf.org/rfc/rfc1700.txt にアクセスして、RFC 1700「Assigned Numbers」を参照してください。

EtherType ACL の例

次の例は、EtherType ACL の設定方法（インターフェイスへの適用方法を含む）を示しています。

たとえば、次のサンプル ACL では、内部インターフェイスで発信される一般的な EtherType が許可されます。

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

次の例では、ASA を通過する一部の EtherType が許可されますが、それ以外はすべて拒否されます。

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次の例では、両方のインターフェイスで EtherType 0x1256 のトラフィックが拒否されますが、他のトラフィックはすべて許可されます。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

隔離されたコンフィギュレーション セッションでの ACL の編集

アクセス ルールまたは他の目的に使用する ACL を編集すると、その変更はすぐに実装され、トラフィックに影響を与えます。新しいルールがアクティブになるのはルールのコンパイルが完了した後のみとし、そのコンパイルは各 ACE を編集した後に発生することを、トランザクション コミット モデルによって保証するために、アクセス ルールを使用できます。

ACL 編集の影響をさらに分離するには、「コンフィギュレーション セッション」で変更を行うことができます。このセッションは、変更内容を明示的にコミットする前に、複数の ACE やオブジェクトを編集できる隔離されたモードです。このため、デバイスの動作を変更する前に、目的のすべての変更が完了したことを確認できます。

始める前に

- access-group コマンドによって参照されるコマンドは編集できますが、その他のコマンドによって参照される ACL は編集できません。参照されない ACL を編集したり、新しいオブジェクトを作成したりすることもできます。
- オブジェクトとオブジェクト グループを作成または編集できますが、あるセッションで 1 つのオブジェクトまたはオブジェクト グループを作成する場合、同じセッションでそのオブジェクトまたはオブジェクト グループを編集することはできません。オブジェクトが希望どおりに定義されていない場合は、変更をコミットしてからオブジェクトを編集するか、セッション全体を廃棄してもう一度やり直す必要があります。
- access-group コマンド（アクセス ルール）によって参照される ACL を編集する場合は、セッションをコミットするときにトランザクション コミット モデルが使用されます。このため、ACL は、古い ACL が新しい ACL に置き換えられる前に完全にコンパイルされます。

手順

ステップ 1 セッションを開始します。

```
hostname#configure session session_name
hostname(config-s)#
```

session_name がすでに存在する場合は、そのセッションを開きます。存在しない場合は、新しいセッションを作成します。

既存のセッションを表示するには、**show configuration session** コマンドを使用します。一度にアクティブにできるセッションは最大で 3 つです。古い未使用のセッションを削除する必要がある場合は、**clear configuration session** *session_name* コマンドを使用します。

他のユーザーが編集中であるために既存のセッションを開くことができない場合は、セッションが編集中であることを示すフラグをクリアできます。この操作は、セッションが実際には編集中でないことが確実な場合にのみ行ってください。フラグをリセットするには、**clear session** *session_name* **access** コマンドを使用します。

ステップ 2 （コミットされたセッションのみ）変更を行います。次の基本コマンドとそれらのパラメータのいずれかを使用できます。

- **access-list**
- **object**
- **object-group**

ステップ 3 セッションで実行することを決定します。使用できるコマンドは、前にセッションをコミット済みかどうかによって異なります。使用できる可能性があるコマンドは次のとおりです。

- **exit**：セッションを単に終了し、変更のコミットや廃棄は行わないため、後で戻ることができます。
- **commit** [**noconfirm** [**revert-save** | **config-save**]]：（コミットされていないセッションのみ）変更を保存します。セッションを保存するかどうか尋ねられます。リバートセッションを保存（**revert-save**）しておくと、**revert** コマンドで変更を元に戻すことができます。また、コンフィギュレーションセッションを保存（**config-save**）しておくと、そのセッションで変更したすべての内容を、必要に応じて再度コミットできます。リバートセッションまたはコンフィギュレーション セッションを保存した場合は、変更はコミットされますが、セッションはアクティブのままになります。セッションを開いて、変更を元に戻したり同じ変更を再コミットしたりできます。**noconfirm** オプションと任意の適切な save オプションを指定すると、プロンプトが表示されないようにすることができます。
- **abort**：（コミットされていないセッションのみ）変更を破棄し、セッションを削除します。セッションを保持する場合は、セッションを終了して **clear session** *session_name* **configuration** コマンドを使用します。このコマンドは、セッションを削除せずに空にします。
- **revert**：（コミットされたセッションのみ）変更を元に戻し、セッションをコミットする前のコンフィギュレーションに戻して、そのセッションを削除します。
- **show configuration session** [*session_name*]：セッションで行った変更を表示します。

ACL のモニタリング

ACL をモニターするには、次のいずれかのコマンドを入力します。

- **show access-list** [*name*]：各 ACE の行番号とヒット カウントを含むアクセス リストを表示します。ACL 名を指定してください。そうしないと、すべてのアクセス リストが表示されます。
- **show running-config access-list** [*name*]：現在実行しているアクセス リスト コンフィギュレーションを表示します。ACL名を指定してください。そうしないと、すべてのアクセス リストが表示されます。

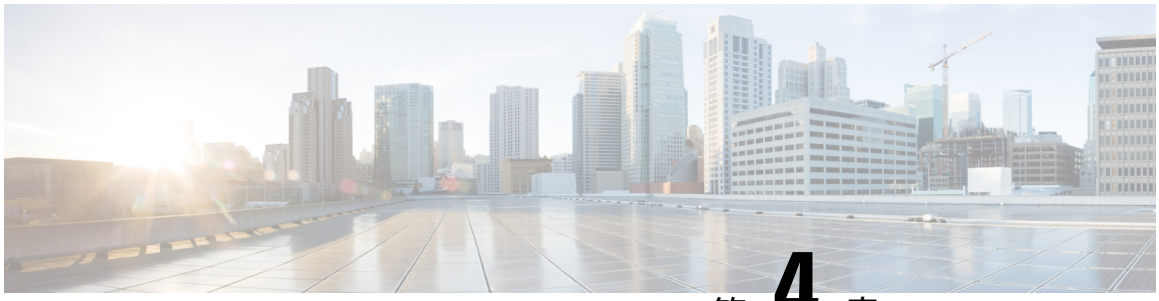
ACL の履歴

機能名	リリース	説明
標準、拡張、Webtype ACL	7.0(1)	ACL は、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。拡張アクセス コントロール リストは、 through-the-box アクセス コントロールとその他のいくつかの機能に使用されます。標準 ACL は、ルート マップと VPN フィルタで使用されます。Webtype ACL は、クライアントレス SSL VPN フィルタリングで使用されます。EtherType ACL は、IP 以外のレイヤ 2 トラフィックを制御します。 **access-list extended**、**access-list standard**、**access-list webtype**、**access-list ethertype** の各コマンドが導入されました。
拡張 ACL での実際の IP アドレス	8.3(1)	NAT または PAT を使用するときは、さまざまな機能で、ACL でのマッピング アドレスおよびポートの使用が不要になります。これらの機能については、変換されていない実際のアドレスとポートを使用する必要があります。実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。
拡張 ACL でのアイデンティティ ファイアウォールのサポート	8.4(2)	アイデンティティ ファイアウォールのユーザーおよびグループを発信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL はアクセス ルールや AAA ルールとともに、および VPN 認証に使用できます。 **access-list extended** コマンドが変更されました。

機能名	リリース	説明
EtherType ACL が IS-IS トラフィックをサポート	8.4(5)、9.1(2)	トランスペアレント ファイアウォール モードでは、ASA が EtherType ACL を使用して IS-IS トラフィックを制御できるようになりました。 **access-list ethertype** {**permit** | **deny**} **isis** コマンドが変更されました。
拡張 ACL での Cisco TrustSec のサポート	9.0(1)	Cisco TrustSec セキュリティ グループを送信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL をアクセス ルールとともに使用できます。 **access-list extended** コマンドが変更されました。
拡張 ACL と Webtype ACL での IPv4 アドレスと IPv6 アドレスの統合	9.0(1)	拡張 ACL と Webtype ACL で IPv4 アドレスと IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。any キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す any4 キーワードと、IPv6 のみのトラフィックを表す any6 キーワードが追加されました。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 次のコマンドが変更されました。**access-list extended**、**access-list webtype** **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コマンドが削除されました。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 **access-list extended** 、**service-object**、**service** の各コマンドが導入または変更されました。
ACL およびオブジェクトを編集するためのコンフィギュレーション セッション アクセス ルール内でのオブジェクトおよび ACL の前方参照	9.3(2)	独立したコンフィギュレーション セッションで ACL およびオブジェクトを編集できるようになりました。オブジェクトおよび ACL を前方参照することも可能です。つまり、まだ存在していないオブジェクトや ACL に対するルールおよびアクセス グループを設定することができます。 **clear configuration session**、**clear session**、**configure session**、**forward-reference**、および **show configuration session** の各コマンドが導入されました。
Stream Control Transmission Protocol（SCTP）の ACL のサポート	9.5(2)	**sctp** プロトコルを使用して、ポートの仕様を含む ACL ルールを作成できるようになりました。 次のコマンドが変更されました。**access-list extended** 。

機能名	リリース	説明
Ethertype ルールで、IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレスがサポートされます。	9.6(2)	IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレスに対する Ethertype のアクセス制御ルールを作成できるようになりました。この追加により、**bpdu** キーワードが対象トラフィックに一致しなくなります。**dsap 0x42** に対して **bpdu** ルールを書き換えます。 次のコマンドが変更されました。 **access-list ethertype**
ブリッジ グループ メンバーのインターフェイスで Ethertype ルールのルーテッド モード、およびブリッジ グループの仮想インターフェイス（BVI）の拡張アクセス ルールのサポート。	9.7(1)	Ethertype ACL を作成し、ルーテッド モードのブリッジ グループ メンバーのインターフェイスに適用できるようになりました。また、メンバー インターフェイスに加えて、ブリッジ仮想インターフェイス（BVI）に拡張アクセス ルールを適用することもできます。 次のコマンドが変更されました。**access-group**、**access-list ethertype**
EtherType アクセス制御リストの変更。	9.9(1)	EtherType アクセス コントロール リストは、Ethernet II IPX（EII IPX）をサポートするようになりました。さらに、DSAP キーワードに新しいキーワードが追加され、共通 DSAP 値（BPDU（0x42）、IPX（0xE0）、Raw IPX（0xFF）、および ISIS（0xFE））をサポートします。その結果、BPDU または ISIS キーワードを使用する既存の EtherType アクセス制御エントリは自動的に DSAP 仕様を使用するように変換され、IPX のルールは 3 つのルール（DSAP IPX、DSAP Raw IPX、および EII IPX）に変換されます。さらに、IPX を EtherType 値として使用するパケット キャプチャは廃止されました。これは、IPX が 3 つの個別の EtherType に対応するためです。 次のコマンドが変更されました：**access-list ethertype** キーワード **eii-ipx** および **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}が追加されました。**capture ethernet-typeipx** キーワードはサポートされなくなりました。
拡張 ACL でのネットワーク サービスのオブジェクト グループのサポート。	9.17(1)	拡張 ACL およびアクセス制御ルールの送信元および宛先基準としてネットワーク サービス オブジェクトを使用できます。 以下のコマンドが変更されました。**access-list extended**

機能名	リリース	説明
ACL とオブジェクトの前方参照は常に有効にです。さらに、アクセス制御のオブジェクトグループ検索がデフォルトで有効になりました。	9.18(1)	アクセスグループまたはアクセスルールを設定するときに、まだ存在していない ACL またはネットワークオブジェクトを参照できます。 さらに、オブジェクトグループ検索が新規展開のアクセス制御に対してデフォルトで有効になりました。デバイスをアップグレードしても、引き続きこのコマンドは無効になります。有効にする場合（推奨）、手動で行う必要があります。 **forward-reference enable** コマンドを削除し、**object-group-search access-control** のデフォルトを有効に変更しました。



第 4 章

アクセス ルール

この章では、アクセス ルールを使用して ASA へのネットワーク アクセスや ASA を通過するネットワーク アクセスを制御する方法について説明します。ルーテッドファイアウォールモードの場合もトランスペアレント ファイアウォール モードの場合も、ネットワーク アクセスを制御するには、アクセスルールを使用します。トランスペアレントモードでは、アクセスルール（レイヤ 3 トラフィックの場合）と EtherType ルール（レイヤ 2 トラフィックの場合）の両方を使用できます。

（注） ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセスルールは必要ありません。必要なのは、一般的な操作の設定ガイドに従って管理アクセスを設定することだけです。

- ネットワーク アクセスの制御 （63 ページ）
- アクセス ルールのライセンス （70 ページ）
- アクセス制御に関するガイドライン （71 ページ）
- アクセス制御の設定 （73 ページ）
- アクセス ルールのモニタリング （76 ページ）
- ネットワーク アクセスの許可または拒否の設定例 （78 ページ）
- アクセス ルールの履歴 （79 ページ）

ネットワーク アクセスの制御

アクセス ルールは、ASA の通過を許可するトラフィックを定義したものです。複数の異なるレイヤのルールを組み合わせてアクセス コントロール ポリシーを実装できます。

- インターフェイスに割り当てられる拡張アクセスルール（レイヤ3以上のトラフィック）：着信方向と発信方向のそれぞれで異なるルールセット（ACL）を適用できます。拡張アクセスルールでは、送信元と宛先のトラフィックの基準に基づいてトラフィックが許可または拒否されます。

- ブリッジ仮想インターフェイス（BVI、ルーテッドモード）に割り当てられている拡張アクセス ルール（レイヤ3以上のトラフィック）：BVIを指定すると、着信方向と発信方向のそれぞれで異なるルールセットを適用でき、ブリッジグループメンバーのインターフェイスにもルールセットを適用できます。BVIとメンバーのインターフェイスの両方にアクセスルールがあると、処理の順序は方向によって異なります。着信方向、メンバーのアクセス ルールが最初に、次に BVI のアクセス ルールが評価されます。発信方向、BVI ルールが最初に、メンバーのインターフェイスのルールが次に考慮されます。
- グローバルに割り当てられる拡張アクセス ルール：デフォルトのアクセス コントロールとして使用する単一のグローバル ルール セットを作成できます。グローバル ルールはインターフェイス ルールの後に適用されます。
- 管理アクセス ルール（レイヤ 3 以上のトラフィック）：インターフェイスに対するトラフィック（通常は管理トラフィック）を制御する単一のルールセットを適用できます。これらのルールは、CLI の「コントロール プレーン」アクセス グループに相当します。デバイスに対する ICMP トラフィックについては、代わりに ICMP ルールを設定できます。
- インターフェイスに割り当てられるEtherTypeルール（レイヤ2のトラフィック）（ブリッジ グループ メンバーのインターフェイスのみ）：着信方向と発信方向のそれぞれで異なるルール セットを適用できます。EtherType ルールは、IP 以外のトラフィックのネットワーク アクセスを制御するルールです。EtherType ルールでは、EtherType に基づいてトラフィックが許可または拒否されます。また、ブリッジ グループ メンバーのインターフェイスに拡張アクセス ルールを適用して、レイヤ 3 以上のトラフィックを制御できます。

ルールに関する一般情報

次のトピックでは、アクセス ルールおよび EtherType ルールに関する一般的な情報を提供します。

インターフェイス アクセス ルールとグローバル アクセス ルール

アクセス ルールを特定のインターフェイスに適用するか、またはアクセス ルールをすべてのインターフェイスにグローバルに適用できます。インターフェイス アクセス ルールと一緒にグローバル アクセス ルールを設定できます。この場合、特定の着信インターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも先に処理されます。グローバル アクセス ルールは、着信トラフィックにだけ適用されます。

インバウンド ルールとアウトバウンド ルール

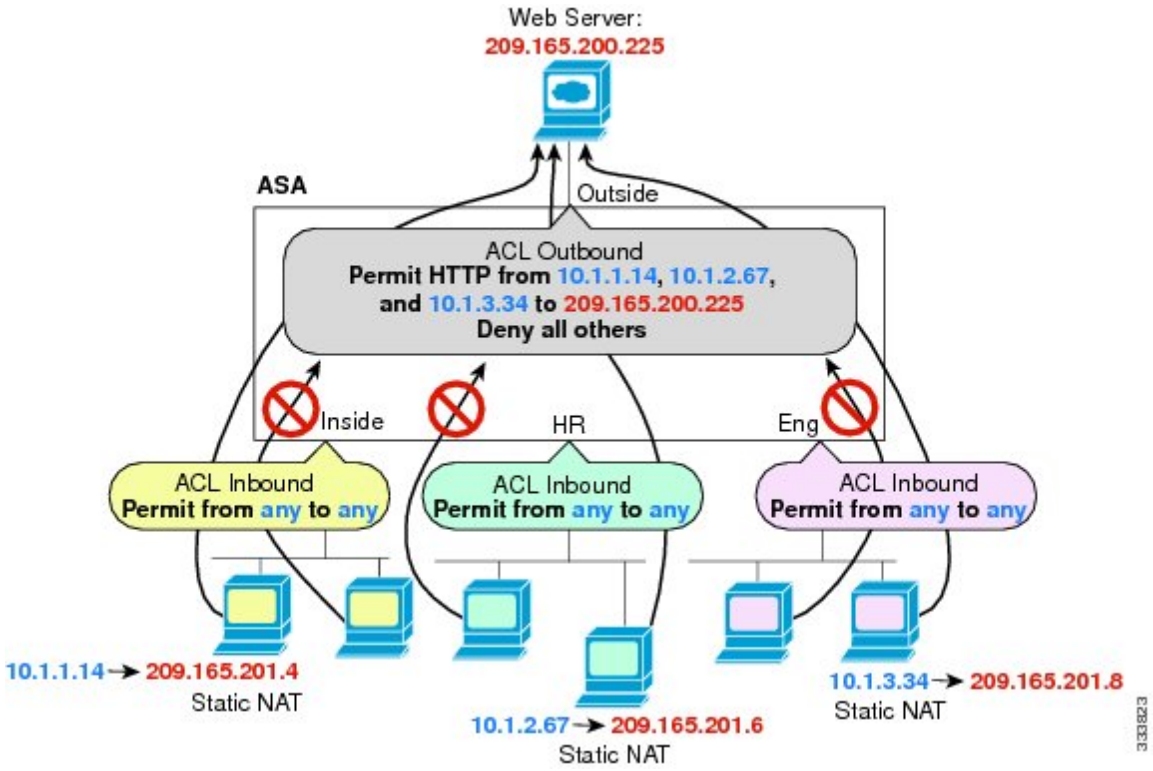
トラフィックの方向に基づいてアクセス ルールを設定できます。

- インバウンド：インバウンド アクセス ルールは、インターフェイスに入ってくるトラフィックに適用されます。グローバル アクセス ルールおよび管理アクセス ルールは常にインバウンド ルールになります。
- アウトバウンド：アウトバウンドルールは、インターフェイスから送信されるトラフィックに適用されます。

（注） 「インバウンド」および「アウトバウンド」は、インターフェイスにおける ACL の適用対象を表したもので、前者は、インターフェイスにおいて ASA により受信されるトラフィックに ACL が適用されることを表し、後者はインターフェイスにおいて ASA から送信されるトラフィックに ACL が適用されることを表しています。これらの用語は、一般に着信と呼ばれる、セキュリティの低いインターフェイスから高いインターフェイスへのトラフィックの移動や、一般に発信と呼ばれる、セキュリティの高いインターフェイスから低いインターフェイスへのトラフィックの移動を意味しません。

たとえば、内部ネットワーク上の特定のホストに限って、外部ネットワーク上の Web サーバーにアクセスできるようにする場合などには、アウトバウンド ACL が有用です。複数のインバウンド ACL を作成してアクセスを制限することもできますが、指定したホストだけアクセスを許可するアウトバウンド ACL を 1 つだけ作成する方が効率的です（次の図を参照してください）。他のすべてのホストは、アウトバウンド ACL により外部ネットワークから遮断されます。

図 *2 : Outbound ACL*



この例について、次のコマンドを参照してください。

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67
host 209.165.200.225 eq www
```

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

ルールの順序

ルールの順序が重要です。ASAにおいて、パケットを転送するかドロップするかの判断が行われる場合、ASAでは、パケットと各ルールとの照合が、適用されるACLにおけるそれらのルールの並び順に従って行われます。いずれかのルールに合致した場合、それ以降のルールはチェックされません。たとえば、先頭に作成したアクセスルールが、インターフェイスに対してすべてのトラフィックを明示的に許可するものであれば、それ以降のルールはチェックされません。

暗黙的な許可

高セキュリティ インターフェイスから低セキュリティ インターフェイスへのIPv4およびIPv6のユニキャスト トラフィックはデフォルトで許可されます。これには標準のルーテッド インターフェイスとルーテッドモードでのブリッジ仮想インターフェイス（BVI）間のトラフィックが含まれます。

ブリッジ グループ メンバーのインターフェイスでは、高セキュリティ インターフェイスから低セキュリティ インターフェイスへのこの暗黙の許可が、同じブリッジ グループ内でのみインターフェイスに適用されます。ブリッジ グループ メンバーのインターフェイスとルーテッド インターフェイスまたは別のブリッジ グループのメンバーとの間には暗黙の許可はありません。

ブリッジ グループ メンバーのインターフェイス（ルーテッドまたはトランスペアレント モード）も次をデフォルトで許可します。

- 双方向の ARP。ARP トラフィックの制御には ARP インスペクションを使用します。アクセス ルールでは制御できません。
- 双方向の BPDU。（Ethertype ルールを使用してこれらを制御できます）

他のトラフィックには、拡張アクセス ルール（IPv4 および IPv6）、または EtherType ルール（非 IP）のいずれかを使用する必要があります。

暗黙的な拒否

ACLの最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザーに、ASA経由でのネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザーを許可します。

管理（コントロール プレーン）の ACL は to-the-box トラフィックを管理していますが、インターフェイスの一連の管理ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセス ルールに一致しない接続は通常のアクセス制御ルールで評価されます。

EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によっ

て、拡張 ACL で以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ルールですべてのトラフィックを明示的に拒否した場合は、IP と ARP のトラフィックが拒否され、物理的なプロトコルのトラフィック（自動ネゴシエーションなど）だけが許可されます。

グローバル アクセス ルールを設定すると、暗黙的な拒否はグローバル ルールが処理された後になります。次の動作の順序を参照してください。

1. インターフェイス アクセス ルール
2. ブリッジ グループ メンバーのインターフェイスでは、ブリッジ仮想インターフェイス（BVI）のアクセス ルール
3. グローバル アクセス ルール
4. 暗黙的な拒否

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致を決定する際に常に実際の IP アドレスを使用します。たとえば、内部サーバー 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバーに付与する場合は、この内部サーバーへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバーのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

同一のセキュリティ レベル インターフェイスとアクセスルール

各インターフェイスにはセキュリティレベルがあり、アクセスルールが考慮される前にセキュリティレベルのチェックが実行されます。したがって、アクセスルールで接続を許可した場合でも、インターフェイスレベルでの同じセキュリティレベルのチェックにより、接続がブロックされる可能性があります。構成で同じセキュリティレベルの接続が許可されるようにすることで、許可/拒否の決定でアクセスルールが常に考慮されるようにする必要がある場合があります。

- 同じセキュリティレベルの入力インターフェイスと出力インターフェイス間の接続は、同じセキュリティトラフィックのインターフェイス間チェックの対象となります。

  これらの接続を許可するには、 **same-security-traffic permit inter-interface** コマンドを入力します。

  これらの接続を許可するには、**[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interface）]**の順に選択し、**[同じセキュリティレベルで構成された2つ以上のインターフェイス間のトラフィックを有効にする（Enable traffic between two or more interfaces which are configured with the same security levels）]** オプションを選択します。

- 同じ入力インターフェイスと出力インターフェイスを持つ接続は、同じセキュリティトラフィックのインターフェイス内チェックの対象となります。

これらの接続を許可するには、**same-security-traffic permit intra-interface** コマンドを入力します。

これらの接続を許可するには、**[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interface）]** の順に選択し、**[同じインターフェイスに接続された2つ以上のホスト間のトラフィックを有効にする（Enable traffic between two or more hosts connected to the same interface）]** オプションを選択します。

拡張アクセス ルール

この項では、拡張アクセス ルールについて説明します。

リターン トラフィックに対する拡張アクセス ルール

ルーテッド モードとトランスペアレント モードの両方に対する TCP、UDP、および SCTP 接続については、リターン トラフィックを許可するためのアクセス ルールは必要ありません。ASA は、確立された双方向接続のリターン トラフィックをすべて許可します。

ただし、ICMP などのコネクションレス型プロトコルについては、ASA は単方向セッションを確立します。したがって、（ACL を送信元インターフェイスと宛先インターフェイスに適用することで）アクセス ルールで双方向の ICMP を許可するか、ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。たとえば、ping を制御するには、**echo-reply**（**0**）（ASA からホストへ）または **echo**（**8**）（ホストから ASA へ）を指定します。

ブロードキャストとマルチキャスト トラフィックの許可

ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセス ルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP が含まれます。ダイナミック ルーティング プロトコルまたは DHCP リレーを、このトラフィックを許可するように設定する必要があります。

トランスペアレントまたはルーテッド ファイアウォール モードで同じブリッジ グループのメンバーであるインターフェイスでは、アクセス ルールを使用して IP トラフィックを許可することができます。

（注） これらの特殊なタイプのトラフィックはコネクションレス型であるため、アクセス ルールを着信および発信の両方のインターフェイスに適用して、リターン トラフィックの通過を許可する必要があります。

次の表に、同じブリッジ グループのメンバーであるインターフェイス間のアクセス ルールを使用して、ユーザーが許可できる一般的なトラフィック タイプを示します。

表 *2*: 同じブリッジ グループのメンバー間のアクセス ルールの特別なトラフィック

トラフィック タイプ	プロトコルまたはポート	注
DHCP	UDP ポート 67 および 68	DHCP サーバーがイネーブルの場合、ASA は DHCP パケットの通過を拒否します。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートは、アプリケーションによって異なります。	マルチキャスト ストリームは、常に Class D アドレス（224.0.0.0 to 239.x.x.x）に送信されます。
RIP（v1 または v2）	UDP ポート 520	—

管理アクセス ルール

ASA 宛ての管理トラフィックを制御するアクセス ルールを設定できます。to-the-box 管理トラフィック（**http**、**ssh**、**telnet** などのコマンドで定義）に対するアクセス制御ルールは、**control-plane** オプションを使用して適用される管理アクセス ルールよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box ACL で明示的に拒否されている場合でも着信が許可されます。

通常のアクセス ルールとは異なり、インターフェイスの一連の管理ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセス ルールに一致しない接続は通常のアクセス制御ルールで評価されます。

また、デバイスへの ICMP トラフィックは、ICMP ルールを使用して制御できます。デバイスを通過する ICMP トラフィックの制御には、通常の拡張アクセス ルールを使用します。

EtherType ルール

この項では、EtherType ルールについて説明します。

サポートされている EtherType およびその他のトラフィック

EtherType ルールは次を制御します。

- 一般的なタイプの IPX および MPLS ユニキャストまたはマルチキャストを含む、16 ビットの 16 進数値で示された EtherType。
- イーサネット V2 フレーム。
- デフォルトで許可される BPDU。BPDU は、SNAP でカプセル化されており、ASA は特別に BPDU を処理するように設計されています。

- トランク ポート（シスコ専用）BPDU。トランク BPDU のペイロードには VLAN 情報が含まれるため、BPDU を許可すると、ASA により、発信 VLAN を使用してペイロードが修正されます。
- Intermediate System to Intermediate System（IS-IS）。
- IEEE 802.2 論理リンク制御パケット。宛先サービス アクセス ポイントのアドレスに基づいてアクセスを制御できます。

次のタイプのトラフィックはサポートされていません。

- 802.3 形式フレーム：type フィールドではなく length フィールドが使用されるため、ルールでは処理されません。

リターン トラフィックに対する EtherType ルール

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる必要がある場合は、両方のインターフェイスにルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合は、Label Distribution Protocol および Tag Distribution Protocol の TCP 接続が ASA を経由して確立されるようにしてください。これには、ASA インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、ASA に接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。*interface* は、ASA に接続されているインターフェイスです。

mpls ldp router-id *interface* **force**

または

tag-switching tdp router-id *interface* **force**

アクセス ルールのライセンス

アクセス制御ルールは特別なライセンスを必要としません。

ただし、ルール内でプロトコルとして **sctp** を使用する場合は、キャリア ライセンスが必要です。

アクセス制御に関するガイドライン

IPv6 のガイドライン

IPv6 をサポートします。送信元アドレスと宛先アドレスには IPv4 アドレスと IPv6 アドレスの組み合わせを含めることができます。

Per-User ACL の注意事項

- ユーザーごとの ACL では、**timeout uauth** コマンドの値が使用されますが、この値は AAA のユーザーごとのセッション タイムアウト値でオーバーライドできます。
- ユーザーごとの ACL のためにトラフィックが拒否された場合、syslog メッセージ 109025 がログに記録されます。トラフィックが許可された場合、syslog メッセージは生成されません。ユーザーごとの ACL の **log** オプションの効果はありません。

その他のガイドラインと制限事項

- 時間の経過とともにアクセスルールのリストが増え、多数の廃止されたルールが含まれるようになることがあります。最終的に、アクセスグループの ACL が非常に大きくなり、システム全体のパフォーマンスに影響を与える可能性があります。syslog メッセージの送信、フェールオーバー同期のための通信、SSH/HTTPS 管理アクセス接続の確立と維持などに問題がある場合は、アクセスルールのプルーニングが必要かもしれません。一般に、ルールリストを積極的に維持管理して、古いルール、ヒットしないルール、解決できなくなった FQDN オブジェクトなどを削除する必要があります。また、オブジェクトグループ検索の実装も検討してください。
- 新しい展開ではオブジェクトグループ検索はデフォルトで有効化されます。

  オブジェクト グループ検索をイネーブルにすると、ルックアップのパフォーマンスは低下し、CPU 使用率は増加しますが、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索を有効にした場合、ネットワーク オブジェクトまたはサービス オブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。このオプションを設定するには、**object-group-search access-control** コマンドを使用します。

  object-group-search threshold コマンドを使用してしきい値をイネーブルにし、パフォーマンスの低下を防止することができます。しきい値を使用した動作では、接続ごとに送信元と宛先の両方の IP アドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の 1 万倍を超えると接続が切断されます。一致件数が膨大になることを防ぐためにルールを設定します。

（注） オブジェクト グループの検索は、ネットワーク オブジェクトとサービス オブジェクトのみで動作します。セキュリティ グループまたはユーザー オブジェクトでは動作しません。ACL にセキュリティ グループが含まれている場合は、この機能を有効にしないでください。ACL が非アクティブになったり、その他の予期しない動作となる可能性があります。

- アクセス グループにトランザクション コミット モデルを使用することで、システムのパフォーマンスと信頼性を高めることができます。ただし、解決が頻繁に変わる可能性があるホスト名にFQDNオブジェクトを使用する場合は、アクセスグループのコンパイルが完全に解決されない可能性があるため、トランザクションコミットは推奨されません。詳細については、一般的な操作設定ガイドの基本設定の章を参照してください。**asp rule-engine transactional-commit access-group** コマンドを使用します。
- ASDM では、ACL のルールの前にあるアクセス リストのコメントに基づいてルールの説明が設定されます。ASDM で新しいルールを作成した場合も、関連するルールの前にあるコメントが説明として設定されます。ただし、ASDM のパケット トレーサは、CLI の照合ルール後に設定されたコメントに一致します。
- 完全修飾ドメイン名（FQDN）ネットワークオブジェクトを送信元または宛先の基準として使用するには、データインターフェイスの DNS も設定する必要があります。

  FQDN によるアクセスの制御はベストエフォート型のメカニズムであることに注意してください。次の点を考慮してください。

  - DNS 応答はスプーフィングされる可能性があるため、完全に信頼できる内部 DNS サーバーのみを使用します。
  - 一部の FQDN は、特に非常に人気の高いサーバーの場合、数千とはいかなくても、数百の IP アドレスを持つことがあり、それらが頻繁に変更されることがあります。システムはキャッシュされている DNS ルックアップの結果を使用するため、ユーザーはキャッシュに存在しないアドレスを取得する可能性があり、その接続は FQDN ルールに合致しません。FQDN ネットワークオブジェクトを使用するルールは、100 未満のアドレスに解決される名前に対してのみ効果的に機能します。

    100 を超えるアドレスに解決される FQDN のネットワーク オブジェクト ルールを作成しないことを推奨します。接続のアドレスが解決され、デバイスの DNS キャッシュで使用可能である可能性は低いからです。
  - 人気のある FQDN では、異なる DNS サーバーが異なるセットの IP アドレスを返す場合があります。したがって、ユーザーが設定したものとは異なる DNS サーバーを使用している場合、FQDN ベースのアクセス制御ルールがクライアントで使用されているサイトのすべての IP アドレスに適用されないことがあり、ルールで意図した結果が得られません。

- 一部の FQDN DNS エントリには、非常に短い存続可能時間（TTL）値が設定されています。この結果、ルックアップテーブルで頻繁に再コンパイルが発生し、全体的なシステムパフォーマンスに影響を与える場合があります。

アクセス制御の設定

ここでは、アクセス コントロールを設定する方法について説明します。

アクセス グループの設定

アクセス グループを作成するには、まず、ACL を作成します。

ACL をインターフェイスにバインドするかグローバルに適用するには、次のコマンドを使用します。

access-group *access_list* { {**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**] | **global**}

インターフェイス固有のアクセス グループの場合は、次の手順を実行します。

- 拡張または EtherType ACL 名を指定します。ACL タイプ、インターフェイス、方向ごとに 1 つの access-group コマンドを設定し、1 つのコントロール プレーン ACL を設定できます。コントロール プレーン ACL は、拡張 ACL である必要があります。Ethertype ACL はブリッジ グループ メンバーのインターフェイスでのみ許可されます。ルーテッド モードのブリッジ グループでは、ブリッジ仮想インターフェイス（BVI）と各ブリッジ グループ メンバーのインターフェイスの両方に各方向の拡張 ACL を指定できます。
- **in** キーワードによって、ACL が着信トラフィックに適用されます。 **out** キーワードによって、ACL が発信トラフィックに適用されます。
- **interface** 名を指定します。
- per-user-override キーワードを使用すると（着信拡張 ACL の場合に限る）、ユーザー許可用にダウンロードしたダイナミック ユーザー ACL により、インターフェイスに割り当てられている ACL を上書きできます。たとえば、インターフェイス ACL が 10.0.0.0 からのトラフィックをすべて拒否し、ダイナミック ACL が 10.0.0.0 からのトラフィックをすべて許可する場合、そのユーザーに関しては、ダイナミック ACL によってインターフェイス ACL が上書きされます。

  デフォルトでは、VPN リモート アクセス トラフィックはインターフェイス ACL と照合されません。ただし、**no sysopt connection permit-vpn** コマンドを使用してこのバイパスをオフにする場合、動作は、グループ ポリシーに適用される **vpn-filter** があるかどうか、および **per-user-override** オプションを設定するかどうかによって異なります。

  - **per-user-override** なし、**vpn-filter** なし：トラフィックはインターフェイス ACL と照合されます。

- **per-user-override** なし、**vpn-filter**：トラフィックはまずインターフェイス ACL と照合され、次に VPN フィルタと照合されます。
- **per-user-override**、**vpn-filter**：トラフィックは VPN フィルタのみと照合されます。

- 拡張 ACL の対象が to-the-box トラフィックである場合、**control-plane** キーワードを指定します。

  通常のアクセスルールとは異なり、インターフェイスの一連の管理（コントロールプレーン）ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセス ルールに一致しない接続は通常のアクセス制御ルールで評価されます。

グローバル アクセス グループの場合は、global キーワードを指定して、すべてのインターフェイスの着信方向に拡張 ACL を適用します。

例

次の例は、**access-group** コマンドを使用する方法を示しています。

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access in interface outside
```

access-list コマンドでは、任意のホストからポート 80 を使用してホスト アドレスにアクセスできるようにしています。**access-group** コマンドでは、外部インターフェイスに入るトラフィックに **access-list** コマンドを適用するように指定しています。

ICMP アクセス ルールの設定

デフォルトでは、IPv4 または IPv6 を使用して任意のインターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- ASA は、ブロードキャストアドレス宛ての ICMP エコー要求に応答しません。
- ASA は、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセスルールと同様に順序があり、パケットに最初に一致したルールのアクションが適用されます。

インターフェイスに対していずれかの ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージタイプだけを拒否する場合は、残りのメッセージタイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP 到達不能メッセージ タイプ（タイプ 3）には常にアクセス許可を付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリが無効化され、IPsec および PPTP トラフィックが停止することがあります。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスに使用されます。

手順

ステップ 1 ICMP トラフィックのルールを作成します。

icmp {**permit** | **deny**} {**host** *ip_address* | *ip_address mask* | **any**} [*icmp_type*] *interface_name*

icmp_type を指定しない場合、すべてのタイプにルールが適用されます。番号または名前を入力できます。ping を制御するには、echo-reply（0）（ASA からホストへ）または echo（8）（ホストから ASA へ）を指定します。

すべてのアドレス（**any**）、単一のホスト（**host**）、またはネットワーク（*ip_address mask*）にルールを適用できます。

ステップ 2 ICMPv6（IPv6）トラフィックのルールを作成します。

ipv6 icmp {**permit** | **deny**} {**host** *ipv6_address* | *ipv6-network*/*prefix-length* | **any**} [*icmp_type*] *interface_name*

icmp_type を指定しない場合、すべてのタイプにルールが適用されます。

すべてのアドレス（**any**）、単一のホスト（**host**）、またはネットワーク（*ipv6-network*/*prefix-length*）にルールを適用できます。

ステップ 3 （任意）トレース ルートの出力に ASA が表示されるように、ICMP の到達不能メッセージに対するレート制限を設定します。

icmp unreachable rate-limit *rate* **burst-size** *size*

レート制限は 1 ～ 100 の範囲で設定できます。デフォルトは 1 です。バースト サイズは 1 ～ 10 です。応答のバーストサイズ数が送信されますが、後続の応答は、レート制限に達するまで送信されません。

例：

ASA をホップの 1 つとして表示するトレース ルートに対して ASA の通過を許可するためには、**set connection decrement-ttl** コマンドをイネーブルにするほか、レート制限を大きくする必要があります。たとえば、次のポリシーでは、ASA を通過するすべてのトラフィックについて、レート制限を引き上げ、Time-to-Live（TTL; 存続可能時間）の値をデクリメントしています。

```
icmp unreachable rate-limit 50 burst-size 10
class-map global-class
  match any
policy-map global_policy
  class global-class
```

```
set connection decrement-ttl
```

例

次の例は、10.1.1.15 のホストを除くすべてのホストで内部インターフェイスへの ICMP の使用を許可する方法を示しています。

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

次の例は、10.1.1.15 のアドレスを持つホストに内部インターフェイスへの ping だけを許可する方法を示しています。

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

次に、外部インターフェイスですべての ping 要求を拒否し、すべての packet-too-big メッセージを許可する（パス MTU ディスカバリをサポートするため）方法を示します。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次の例は、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに対して外部インターフェイスへの ping を許可する方法を示しています。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

アクセス ルールのモニタリング

ネットワーク アクセスをモニターするには、次のコマンドを入力します。

- **clear access-list** *id* **counters**

  アクセス リストのヒット数を消去します。

- **show access-list** [*name*]

  各 ACE の行番号とヒット カウントを含むアクセス リストを表示します。ACL 名を指定してください。そうしないと、すべてのアクセス リストが表示されます。

- **show running-config access-group**

  インターフェイスにバインドされている現在の ACL を表示します。

アクセス ルールの syslog メッセージの評価

アクセス ルールに関するメッセージは、syslog イベントのビューア（ASDM のビューアなど）を使用して確認できます。

デフォルトのロギングを使用している場合、明示的に拒否されたフローに対する syslog メッセージ 106023 だけが表示されます。ルールのリストの最後にある「暗黙の deny」に一致するトラフィックは記録されません。

ASA が攻撃を受けた場合、拒否されたパケットを示す syslog メッセージの数が非常に大きくなることがあります。代わりに、syslog メッセージ 106100 を使用するロギングをイネーブルにすることをお勧めします。このメッセージは各ルール（許可ルールも含む）の統計情報を示すもので、これを使用することにより、生成される syslog メッセージの数を制限できます。また、特定のルールについて、すべてのロギングをディセーブルにする方法もあります。

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフローエントリを作成して、指定された間隔内で受信したパケットの数を追跡します。ASA は、最初のヒットがあったとき、および各間隔の終わりに syslog メッセージを生成し、その間隔におけるヒットの合計数と最後のヒットのタイムスタンプを示します。各間隔の終わりに、ASA はヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、ASA はそのフロー エントリを削除します。ルールのロギングの設定では、それぞれのルールについて、ログ メッセージの間隔のほか、シビラティ（重大度）も制御することができます。

フローは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびポートで定義されます。同じ 2 つのホスト間の新しい接続では、送信元ポートが異なる場合があるため、接続のための新しいフローが作成されると、同じフローの増加は示されない場合があります。

確立された接続に属する、許可されたパケットを ACL でチェックする必要はありません。最初のパケットだけがロギングされ、ヒット数に含められます。ICMP などのコネクションレス型プロトコルの場合は、許可されているパケットもすべてロギングされ、拒否されたパケットはすべてロギングされます。

これらのメッセージの詳細については、*syslog* メッセージ ガイドを参照してください。

ヒント メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフロー エントリを作成して、指定された間隔内で受信したパケットの数を追跡します。ASA では、ACE 用のロギング フローを最大 32 K 保持できます。どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU リソースが無制限に消費されないようにするために、ASA は同時拒否フロー数に制限を設定します。この制限は、拒否フローに対してだけ設定されます（許可フローには設定されません）。これは、拒否フローは攻撃を示している可能性があるためです。制限に達すると、ASA は既存の拒否フローが期限切れになるまでロギング用の新しい拒否フローを作成せず、メッセージ 106101 を発行します。このメッセージの頻度は **access-list alert-interval** *secs* コマンドを使用して、拒否フローのキャッシュの最大数は **access-list deny-flow-max** *number* コマンドを使用して制御できます。

ネットワーク アクセスの許可または拒否の設定例

次に、ネットワーク アクセスの許可または拒否の一般的な設定例のいくつかを示します。

拡張 ACL の例

次の例は、内部サーバー1のネットワークオブジェクトを追加し、サーバーに対してスタティック NAT を実行し、内部サーバー 1 への外側からのアクセスをイネーブルにします。

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12

hostname(config)# access-list outside_access extended permit tcp any object inside-server1
 eq www
hostname(config)# access-group outside_access in interface outside
```

次の例では、すべてのホストに内部ネットワークと hr ネットワークの間での通信を許可しますが、外部ネットワークへのアクセスは特定のホストだけに許可されます。

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

次の例では、オブジェクトグループを使用して内部インターフェイスの特定のトラフィックを許可します。

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
 inside any
```

EtherType の例

たとえば、次のサンプル ACL では、内部インターフェイスで発信される一般的な EtherType が許可されます。

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
```

```
hostname(config)# access-group ETHER in interface inside
```

次の例では、ASA を通過する一部の EtherType が許可されますが、それ以外はすべて拒否されます。

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次の例では、両方のインターフェイスで EtherType 0x1256 のトラフィックが拒否されますが、他のトラフィックはすべて許可されます。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

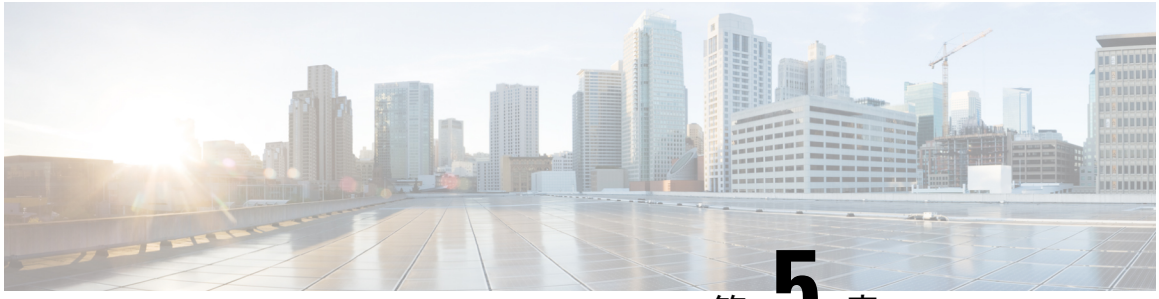
アクセス ルールの履歴

機能名	プラットフォームリリース	説明
インターフェイス アクセス ルール	7.0(1)	ACL を使用した、ASA 経由のネットワーク アクセスの制御。 access-group コマンドが導入されました。
グローバル アクセス ルール	8.3(1)	グローバル アクセス ルールが導入されました。 次のコマンドが変更されました。 **access-group.**
アイデンティティ ファイアウォールのサポート	8.4(2)	アイデンティティ ファイアウォールのユーザーおよびグループを発信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL はアクセス ルールや AAA ルールとともに、および VPN 認証に使用できます。 **access-list extended** コマンドが変更されました。
EtherType ACL が IS-IS トラフィックをサポート	8.4(5)、9.1(2)	トランスペアレント ファイアウォール モードでは、ASA が EtherType ACL を使用して IS-IS トラフィックを渡すことができるようになりました。 **access-list ethertype** {**permit** | **deny**} **isis** コマンドが変更されました。

機能名	プラットフォームリリース	説明
TrustSec のサポート	9.0(1)	TrustSec セキュリティ グループを送信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL をアクセス ルールとともに使用できます。 **access-list extended** コマンドが変更されました。
IPv4 および IPv6 の統合 ACL	9.0(1)	ACL で IPv4 および IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。any キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す any4 キーワードと、IPv6 のみのトラフィックを表す any6 キーワードが追加されました。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 次のコマンドが変更されました。**access-list extended**、**access-list webtype** **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コマンドが削除されました。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 **access-list extended** 、**service-object**、**service** の各コマンドが導入または変更されました。
アクセス グループ ルール エンジンのトランザクション コミット モデル	9.1(5)	イネーブルの場合、ルールの編集の完了後、ルールの更新が適用されます。ルールの照合パフォーマンスへの影響はありません。 asp rule-engine transactional-commit、show running-config asp rule-engine transactional-commit、clear configure asp rule-engine transactional-commit の各コマンドが導入されました。
ACL およびオブジェクトを編集するためのコンフィギュレーション セッション アクセス ルール内でのオブジェクトおよび ACL の前方参照	9.3(2)	独立したコンフィギュレーション セッションで ACL およびオブジェクトを編集できるようになりました。オブジェクトおよび ACL を前方参照することも可能です。つまり、まだ存在していないオブジェクトや ACL に対するルールおよびアクセス グループを設定することができます。 clear config-session、clear session、configure session、forward-reference、show config-session の各コマンドが導入されました。

機能名	プラットフォームリリース	説明
Stream Control Transmission Protocol（SCTP）のアクセス ルールのサポート	9.5(2)	**sctp** プロトコルを使用して、ポートの仕様を含むアクセス ルールを作成できるようになりました。 次のコマンドが変更されました。**access-list extended** 。
Ethertype ルールで、IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレスがサポートされます。	9.6(2)	IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレスに対する Ethertype のアクセス制御ルールを作成できるようになりました。この追加により、**bpdu** キーワードが対象トラフィックに一致しなくなります。**dsap 0x42** に対して **bpdu** ルールを書き換えます。 次のコマンドが変更されました。 **access-list ethertype**
ブリッジ グループ メンバーのインターフェイスで Ethertype ルールのルーテッド モード、およびブリッジ グループの仮想インターフェイス（BVI）の拡張アクセス ルールのサポート。	9.7(1)	Ethertype ACL を作成し、ルーテッド モードのブリッジ グループ メンバーのインターフェイスに適用できるようになりました。また、メンバー インターフェイスに加えて、ブリッジ仮想インターフェイス（BVI）に拡張アクセス ルールを適用することもできます。 次のコマンドが変更されました。**access-group**、**access-list ethertype**
EtherType アクセス制御リストの変更。	9.9(1)	EtherType アクセス コントロール リストは、Ethernet II IPX（EII IPX）をサポートするようになりました。さらに、DSAP キーワードに新しいキーワードが追加され、共通 DSAP 値（BPDU（0x42）、IPX（0xE0）、Raw IPX（0xFF）、および ISIS（0xFE））をサポートします。その結果、BPDU または ISIS キーワードを使用する既存の EtherType アクセス制御エントリは自動的に DSAP 仕様を使用するように変換され、IPX のルールは 3 つのルール（DSAP IPX、DSAP Raw IPX、および EII IPX）に変換されます。さらに、IPX を EtherType 値として使用するパケット キャプチャは廃止されました。これは、IPX が 3 つの個別の EtherType に対応するためです。 次のコマンドが変更されました：**access-list ethertype** キーワード **eii-ipx** および **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}が追加されました。**capture ethernet-typeipx** キーワードはサポートされなくなりました。
オブジェクト グループの検索しきい値がデフォルトで無効になりました。	9.12(1)	これまではオブジェクト グループの検索が有効になると、この機能によりしきい値が適用され、パフォーマンスの低下を防止していました。そのしきい値が、デフォルトで無効になりました。しきい値は、**object-group-search threshold** コマンドを使用して有効にできます。 **object-group-search threshold** コマンドが追加されました。

機能名	プラットフォームリリース	説明
ACL とオブジェクトの前方参照は常に有効にです。さらに、アクセス制御のオブジェクトグループ検索がデフォルトで有効になりました。	9.18(1)	アクセスグループまたはアクセスルールを設定するときに、まだ存在していない ACL またはネットワークオブジェクトを参照できます。 さらに、オブジェクトグループ検索が新規展開のアクセス制御に対してデフォルトで有効になりました。デバイスをアップグレードしても、引き続きこのコマンドは無効になります。有効にする場合（推奨）、手動で行う必要があります。 **forward-reference enable** コマンドを削除し、**object-group-search access-control** のデフォルトを有効に変更しました。
オブジェクトグループ検索の最適化。	9.22(1)	オブジェクトグループ検索機能が拡張され、アクセスコントロールルールを評価して接続を照合する際のオブジェクトルックアップ時間が短縮され、CPU オーバーヘッドが削減されました。オブジェクトグループ検索の設定に変更はありません。最適化された動作は自動的に行われます。 デバイス CLI に次のコマンドが追加されました。または、コマンド出力が拡張されました。 **clear asp table network-object**、 **debug ac logs**、 **packet-tracer**、 **show access-list**、 **show asp table network-group**、 **show object-group**。



第 5 章

ASA および Cisco TrustSec

この章では、ASA に Cisco TrustSec を実装する方法について説明します。

- Cisco TrustSec について （83 ページ）
- Cisco TrustSec のガイドライン （92 ページ）
- Cisco TrustSec と統合するための ASA の設定 （95 ページ）
- Cisco TrustSec の例 （110 ページ）
- セキュアクライアントCisco TrustSec に対する VPN のサポート （111 ページ）
- Cisco TrustSec のモニタリング （113 ページ）
- Cisco TrustSec の履歴 （114 ページ）

Cisco TrustSec について

従来、ファイアウォールなどのセキュリティ機能は、事前定義されている IP アドレス、サブネット、およびプロトコルに基づいてアクセスコントロールを実行していました。しかし、企業のボーダレス ネットワークへの移行に伴い、ユーザーと組織の接続に使用されるテクノロジーおよびデータとネットワークを保護するためのセキュリティ要件が大幅に向上しています。エンドポイントは、ますます遊動的となり、ユーザーは通常さまざまなエンドポイント（ラップトップとデスクトップ、スマートフォン、タブレットなど）を使用します。つまり、ユーザー属性とエンドポイント属性の組み合わせにより、ファイアウォール機能または専用ファイアウォールを持つスイッチやルータなどの実行デバイスがアクセスコントロール判断のために信頼して使用できる既存の 6 タプルベースのルール以外の主要な特性が提供されます。

その結果、お客様のネットワーク全体、ネットワークのアクセス レイヤ、分散レイヤ、コアレイヤ、およびデータセンターのセキュリティを有効にするためには、エンドポイント属性またはクライアントアイデンティティ属性のアベイラビリティと伝搬がますます重要な要件となります。

Cisco TrustSec は、既存の ID 認証インフラストラクチャを基盤とするアクセス コントロールです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec 機能では、実行デバイスはユーザー属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセスコントロールを決定します。この情報のアベイラビリティおよび伝

搬によって、ネットワークのアクセス レイヤ、分散レイヤ、およびコア レイヤでのネットワーク全体におけるセキュリティが有効になります。

ご使用の環境に Cisco TrustSec を実装する利点は、次のとおりです。

- デバイスからの適切でより安全なアクセスにより、拡大する複雑なモバイル ワークフォースを提供します。
- 有線または無線ネットワークへの接続元を包括的に確認できるため、セキュリティ リスクが低減されます。
- 物理またはクラウドベースの IT リソースにアクセスするネットワーク ユーザーのアクティビティに対する非常に優れた制御が実現されます。
- 中央集中化、非常にセキュアなアクセス ポリシー管理、およびスケーラブルな実行メカニズムにより、総所有コストが削減されます。
- 詳細については、次の URL を参照してください。
  - 企業向けの Cisco TrustSec システムおよびアーキテクチャの説明。

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
  - コンポーネントの設計ガイドへのリンクなど、Cisco TrustSec ソリューションを企業に導入する場合の手順。

    http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html
  - Cisco TrustSec ソリューションを ASA、スイッチ、ワイヤレス LAN（WLAN）コントローラ、およびルータと共に使用する場合の概要。

    http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf
  - Cisco TrustSec プラットフォームのサポート一覧。Cisco TrustSec ソリューションをサポートしているシスコ製品を確認できます。

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

Cisco TrustSec の SGT および SXP サポートについて

Cisco TrustSec 機能では、セキュリティ グループ アクセスは、トポロジ認識ネットワークをロールベースのネットワークに変換するため、ロールベース アクセス コントロール（RBAC）に基づいて実施されるエンドツーエンド ポリシーがイネーブルになります。認証時に取得されたデバイスおよびユーザー クレデンシャルは、パケットをセキュリティ グループごとに分類するために使用されます。Cisco TrustSec クラウドに着信するすべてのパケットは、セキュリティ グループ タグ（SGT）でタグ付けされます。タギングは、信頼できる中継がパケットの送信元のアイデンティティを識別し、データ パスでセキュリティ ポリシーを適用するのに役立ちます。SGT は、SGT を使用してセキュリティ グループ ACL を定義する場合に、ドメイン全体の特権レベルを示すことができます。

SGT は、RADIUS ベンダー固有属性で発生する IEEE 802.1X 認証、Web 認証、または MAC 認証バイパス（MAB）を使用してデバイスに割り当てられます。SGT は、特定の IP アドレスま

たはスイッチ インターフェイスにスタティックに割り当てることができます。SGT は、認証の成功後にスイッチまたはアクセス ポイントにダイナミックに渡されます。

セキュリティ グループ交換プロトコル（SXP）は、SGT およびセキュリティ グループ ACL をサポートしているハードウェアに対する SGT 対応ハードウェア サポートがないネットワーク デバイスに IP-to-SGT マッピング データベースを伝搬できるよう Cisco TrustSec 向けに開発されたプロトコルです。コントロール プレーン プロトコルの SXP は、IP-SGT マッピングを認証ポイント（レガシー アクセス レイヤ スイッチなど）からネットワークのアップストリーム デバイスに渡します。

SXP 接続はポイントツーポイントであり、基礎となる転送プロトコルとして TCP を使用します。SXP は TCP ポート番号 64999 を使用して接続を開始します。また、SXP 接続は、送信元および宛先 IP アドレスによって一意に識別されます。

Cisco TrustSec 機能のロール

アイデンティティおよびポリシーベースのアクセス実施を提供するために、Cisco TrustSec 機能には、次のロールがあります。

- アクセス要求側（AR）：アクセス要求側は、ネットワークの保護されたリソースへのアクセスを要求するエンドポイントデバイスです。これらのデバイスはアーキテクチャのプライマリ対象であり、そのアクセス権限はアイデンティティ クレデンシャルによって異なります。

  アクセス要求側には、PC、ラップトップ、携帯電話、プリンタ、カメラ、MACsec 対応 IP フォンなどのエンドポイント デバイスが含まれます。

- ポリシー デシジョン ポイント（PDP）：ポリシー デシジョン ポイントはアクセス コントロール判断を行います。PDP は 802.1x、MAB、Web 認証などの機能を提供します。PDP は VLAN、DACL および Security Group Access（SGACL/SXP/SGT）による許可および適用をサポートします。

  Cisco TrustSec 機能では、Cisco Identity Services Engine（ISE）が PDP として機能します。Cisco ISE はアイデンティティおよびアクセス コントロール ポリシーの機能を提供します。

- ポリシー情報ポイント（PIP）：ポリシー情報ポイントは、ポリシー デシジョン ポイントに外部情報（たとえば、評価、場所、および LDAP 属性）を提供する送信元です。

  ポリシー情報ポイントには、Session Directory、IPS センサー、Communication Manager などのデバイスが含まれます。

- ポリシー管理ポイント（PAP）：ポリシー管理ポイントはポリシーを定義し、許可システムに挿入します。PAP はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザー アイデンティティへのマッピングと、Cisco TrustSec タグからサーバー リソースへのマッピングを行います。

  Cisco TrustSec 機能では、Cisco Secure Access Control System（802.1x および SGT サポートと統合されたポリシー サーバー）が PAP として機能します。

- ポリシー エンフォースメント ポイント（PEP）：ポリシー エンフォースメント ポイントは、各 AR の PDP による決定（ポリシー ルールおよびアクション）を実行するエンティティです。PEPデバイスは、ネットワーク全体に存在するプライマリ通信パスを介してアイデンティティ情報を学習します。PEPデバイスは、エンドポイントエージェント、許可サーバー、ピア実行デバイス、ネットワーク フローなど、さまざまな送信元から各ARのアイデンティティ属性を学習します。同様に、PEP デバイスは SXP を使用して、ネットワーク全体で相互信頼できるピア デバイスに IP-SGT マッピングを伝搬します。

  ポリシー エンフォースメント ポイントには、Catalyst Switches、ルータ、ファイアウォール（具体的にはASA）、サーバー、VPNデバイス、SANデバイスなどのネットワーク デバイスが含まれます。

Cisco ASA は、アイデンティティ アーキテクチャの中で PEP の役割を果たします。SXP を使用して、ASAは、認証ポイントから直接アイデンティティ情報を学習し、その情報を使用してアイデンティティベースのポリシーを適用します。

セキュリティ グループ ポリシーの適用

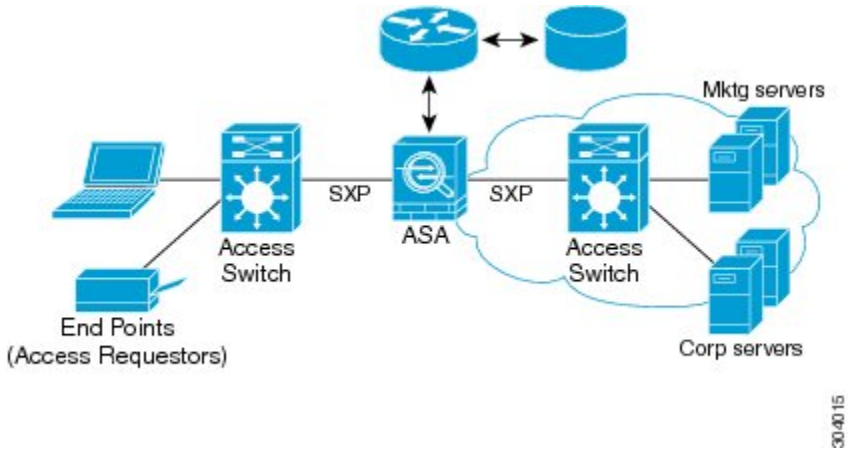
セキュリティ ポリシーの適用はセキュリティ グループの名前に基づきます。エンドポイントデバイスは、データセンターのリソースへのアクセスを試行します。ファイアウォールで設定された従来の IP ベースのポリシーと比較して、アイデンティティベースのポリシーは、ユーザーおよびデバイス アイデンティティに基づいて設定されます。たとえば、mktg-contractor が mktg-server にアクセスできるとします。mktg-corp-user は、mktg-server および corp-server にアクセスできます。

このタイプの導入には次のような利点があります。

- ユーザー グループとリソースが1つのオブジェクト（SGT）を使用して定義されます（簡易ポリシー管理）。
- ユーザー アイデンティティとリソース アイデンティティは、Cisco TrustSec 対応スイッチ インフラストラクチャ全体で保持されます。

次の図に、セキュリティ グループの名前ベースのポリシー適用のための展開を示します。

図 *3:* セキュリティ グループ名に基づくポリシー適用の導入



Cisco TrustSec を実装すると、サーバーのセグメンテーションをサポートするセキュリティ ポリシーを設定できます。また、Cisco TrustSec の実装には次のような特徴があります。

- 簡易ポリシー管理用に、サーバーのプールに SGT を割り当てることができます。
- SGT 情報は、Cisco TrustSec 対応スイッチのインフラストラクチャ内に保持されます。
- ASA は、Cisco TrustSec ドメイン全体にポリシーを適用するために IP-SGT マッピングを利用できます。
- サーバーの 802.1x 許可が必須であるため、導入を簡略化できます。

ASA によるセキュリティ グループベースのポリシーの適用

（注） ユーザーベースのセキュリティ ポリシーおよびセキュリティ グループベースのポリシーは、ASA で共存できます。セキュリティ ポリシーでは、ネットワーク属性、ユーザーベースの属性、およびセキュリティ グループベースの属性の任意の組み合わせを設定できます。

Cisco TrustSec と連携するように ASA を設定するには、ISE から Protected Access Credential（PAC）ファイルをインポートする必要があります。

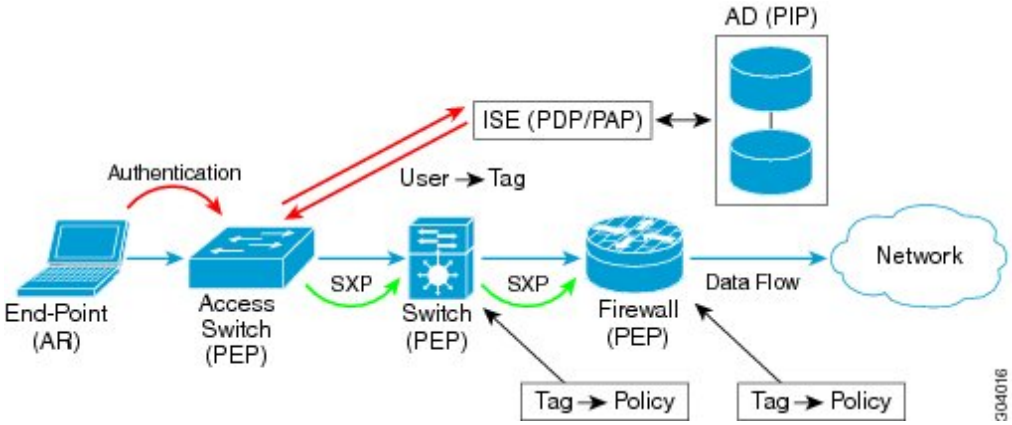
PAC ファイルを ASA にインポートすると、ISE との安全な通信チャネルが確立されます。チャネルが確立されると、ASA は、ISE を使用して PAC セキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします（具体的には、セキュリティ グループ テーブル）。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。

ASA は、最初にセキュリティ グループ テーブルをダウンロードするときに、テーブル内のすべてのエントリを順を追って調べ、そこで設定されているセキュリティ ポリシーに含まれるすべてのセキュリティ グループの名前を解決します。次に、ASA は、それらのセキュリティ ポ

リシーをローカルでアクティブ化します。ASA がセキュリティ グループの名前を解決できない場合、不明なセキュリティ グループ名に対して syslog メッセージを生成します。

次の図に、セキュリティ ポリシーが Cisco TrustSec で適用される仕組みを示します。

図 *4:* セキュリティ ポリシーの適用



1. エンドポイント デバイスは、アクセス レイヤ デバイスに直接アクセスするか、またはリモート アクセスを介してアクセスし、Cisco TrustSec で認証します。
2. アクセス レイヤ デバイスは 802.1X や Web 認証などの認証方式を使用して ISE のエンドポイント デバイスを認証します。エンドポイント デバイスは、ロールおよびグループ メンバーシップ情報を渡して、デバイスを適切なセキュリティ グループに分類します。
3. アクセス レイヤ デバイスは SXP を使用して、アップストリーム デバイスに IP-SGT マッピングを伝搬します。
4. ASA はパケットを受信すると、SXP から渡された IP-SGT マッピングを使用して、送信元および宛先 IP アドレスの SGT を調べます。

   マッピングが新規の場合、ASA はそのマッピングをローカル IP-SGT マネージャ データベースに記録します。コントロール プレーンで実行される IP-SGT マネージャ データベースは、各 IPv4 または IPv6 アドレスの IP-SGT マッピングを追跡します。データベースでは、マッピングが学習された送信元が記録されます。SXP 接続のピア IP アドレスがマッピングの送信元として使用されます。各 IP-SGT にマップされたエントリには、送信元が複数存在する可能性があります。

   ASA が送信者として設定されている場合、ASA は SXP ピアに IP-SGT マッピング エントリをすべて送信します。
5. ASA で SGT またはセキュリティ グループの名前を使用してセキュリティ ポリシーが設定されている場合、ASA はそのポリシーを適用します。（ASA では、SGT またはセキュリティ グループの名前を含むセキュリティ ポリシーを作成できます。セキュリティ グループの名前に基づいてポリシーを適用するには、ASA はセキュリティ グループ テーブルで SGT にセキュリティ グループの名前をマッピングする必要があります）。

   ASA がセキュリティ グループ テーブルでセキュリティ グループの名前を見つけることができず、その名前がセキュリティ ポリシーに含まれている場合、ASA は、セキュリティ

グループの名前を不明と見なし、syslogメッセージを生成します。ISEからのセキュリティ グループ テーブルの更新とセキュリティ グループの名前の学習後、ASA はセキュリティ グループの名前がわかっていることを示す syslog メッセージを生成します。

セキュリティ グループに対する変更が ISE に及ぼす影響

ASA は、ISE から最新のテーブルをダウンロードして、セキュリティ グループ テーブルを定期的に更新します。セキュリティ グループは、ダウンロードの合間にISEで変更できます。これらの変更は、セキュリティ グループ テーブルが更新されるまで、ASAには反映されません。

ヒント ISE のポリシー設定の変更は、メンテナンス時間中にスケジュールすることをお勧めします。さらに、セキュリティ グループの変更を確実に行うには、ASA でセキュリティ グループ テーブルを手動で更新します。

このようにポリシー設定の変更を行うことで、セキュリティ グループの名前を解決し、セキュリティ ポリシーを即座にアクティブ化できる可能性が最大限に高まります。

セキュリティ グループ テーブルは、環境データのタイマーが期限切れになると自動的に更新されます。セキュリティ グループ テーブルの更新は、オンデマンドでトリガーすることも可能です。

ISE でセキュリティ グループを変更する場合、ASA がセキュリティ グループ テーブルを更新するときに次のイベントが発生します。

- セキュリティ グループの名前を使用して設定されたセキュリティ グループ ポリシーだけは、セキュリティ グループ テーブルを通じて解決する必要があります。セキュリティ グループ タグを含むポリシーは、常にアクティブになります。
- セキュリティ グループ テーブルが初めて利用できるようになったときに、セキュリティ グループの名前を含むすべてのポリシーが確認され、セキュリティ グループの名前が解決され、ポリシーがアクティブ化されます。また、タグ付きのすべてのポリシーが確認されます。不明なタグの場合は syslog が生成されます。
- セキュリティ グループ テーブルの期限が切れていても、そのテーブルをクリアするか、新しいテーブルを使用できるようになるまで、最後にダウンロードしたセキュリティ グループ テーブルに従って引き続きポリシーが適用されます。
- ASA で解決済みのセキュリティ グループの名前が不明になると、セキュリティ ポリシーが非アクティブ化されます。ただし、ASA の実行コンフィギュレーションではセキュリティ ポリシーが保持されます。
- PAP で既存のセキュリティ グループが削除されると、既知のセキュリティ グループ タグが不明になる可能性がありますが、ASA のポリシー ステータスは変化しません。既知のセキュリティ グループの名前は未解決になる可能性があり、その場合、ポリシーは非アクティブになります。セキュリティ グループの名前が再利用される場合、新しいタグを使用してポリシーが再コンパイルされます。

- PAP で新しいセキュリティ グループが追加されると、不明なセキュリティ グループ タグが既知になる可能性があり、syslog メッセージが生成されます。ただし、ポリシー ステータスは変化しません。不明なセキュリティ グループの名前が解決される可能性があり、その場合、関連付けられているポリシーがアクティブ化されます。
- PAP でタグの名前が変更された場合、タグを使用して設定されたポリシーによって新しい名前が表示されます。ポリシー ステータスは変化しません。セキュリティ グループの名前を使用して設定されたポリシーは、新しいタグ値を使用して再コンパイルされます。

ASA での送信者および受信者のロール

ASA では、SXP の他のネットワーク デバイスとの間の IP-SGT マッピング エントリの送受信がサポートされます。SXP を使用すると、セキュリティデバイスとファイアウォールが、ハードウェアをアップグレードまたは変更する必要なく、アクセス スイッチからのアイデンティティ情報を学習できます。また、SXP を使用して、アップストリーム デバイス（データセンター デバイスなど）からの IP-SGT マッピング エントリをダウンストリーム デバイスに渡すこともできます。ASA は、アップストリームおよびダウンストリームの両方向から情報を受信できます。

ASA での SXP ピアへの SXP 接続を設定する場合は、アイデンティティ情報を交換できるように、ASA を送信者または受信者として指定する必要があります。

- 送信者モード：ASA で収集されたアクティブな IP-SGT マッピング エントリをすべてポリシー適用のためアップストリーム デバイスに転送できるように ASA を設定します。
- 受信者モード：ダウンストリーム デバイス（SGT 対応スイッチ）からの IP-SGT マッピング エントリを受信し、ポリシー定義作成のためにこの情報を使用できるように ASA を設定します。

SXP 接続の一方の端が送信者として設定されている場合、もう一方の端は受信者として設定する必要があります。逆の場合も同様です。SXP 接続の両端の両方のデバイスに同じロール（両方とも送信者または両方とも受信者）が設定されている場合、SXP 接続が失敗し、ASA は syslog メッセージを生成します。

SXP 接続が複数ある場合でも、IP-SGT マッピング データベースからダウンロードされた IP-SGT マッピング エントリを学習できます。ASA で SXP ピアへの SXP 接続が確立されると、受信者が送信者から IP-SGT マッピング データベース全体をダウンロードします。この後に行われる変更はすべて、新しいデバイスがネットワークに接続されたときにのみ送信されます。このため、SXP の情報が流れる速さは、エンドホストがネットワーク認証を行う速さに比例します。

SXP 接続を通じて学習された IP-SGT マッピング エントリは、SXP IP-SGT マッピング データベースで管理されます。同じマッピング エントリが異なる SXP 接続を介して学習される場合もあります。マッピング データベースは、学習した各マッピング エントリのコピーを 1 つ保持します。同じ IP-SGT マッピング値の複数のマッピング エントリは、マッピングを学習した接続のピア IP アドレスによって識別されます。SXP は IP-SGT マネージャに対して、新しいマッピングが初めて学習された場合にはマッピング エントリを追加するように、SXP データベース内の最後のコピーが削除された場合にはマッピングエントリを削除するように要求します。

SXP 接続が送信者として設定されている場合は必ず、SXP は IP-SGT マネージャに対して、デバイスで収集したすべてのマッピングエントリをピアに転送するよう要求します。新しいマッピングがローカルで学習されると、IP-SGT マネージャは SXP に対して、送信者として設定されている接続を介してそのマッピングを転送するよう要求します。

ASA を SXP 接続の送信者および受信者の両方として設定すると、SXP ループが発生する可能性があります。つまり、SXP データが最初にそのデータを送信した SXP ピアで受信される可能性があります。

ISE への ASA の登録

ASA が PAC ファイルを正常にインポートするには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。ISE に ASA を登録するには、次の手順を実行します。

手順

ステップ 1 ISE にログインします。

ステップ 2 [Administration] > [Network Devices] > [Network Devices] を選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 ASA の IP アドレスを入力します。

ステップ 5 ISE がユーザー認証用に使用されている場合、[Authentication Settings] 領域に共有秘密を入力します。

ASA で AAA サーバーを設定する場合は、ISE でここで作成した共有秘密を指定します。ASA の AAA サーバーはこの共有秘密を使用して、ISE と通信します。

ステップ 6 ASA のデバイス名、デバイス ID、パスワード、およびダウンロード間隔を指定します。これらのタスクの実行方法については、ISE のマニュアルを参照してください。

ISE でのセキュリティ グループの作成

ISE と通信するように ASA を設定する場合は、AAA サーバーを指定します。AAA サーバーを ASA で設定する場合は、サーバー グループを指定する必要があります。セキュリティ グループは、RADIUS プロトコルを使用するように設定する必要があります。ISE でセキュリティ グループを作成するには、次の手順を実行します。

手順

ステップ 1 ISE にログインします。

ステップ 2 [Policy] > [Policy Elements] > [Results] > [Security Group Access] > [Security Group] を選択します。

ステップ 3 ASAのセキュリティ グループを追加します。（セキュリティ グループは、グローバルであり、ASA に固有ではありません）。

ISE は、タグを使用して [Security Groups] でエントリを作成します。

ステップ 4 [Security Group Access] 領域で、ASA のデバイス ID クレデンシャルおよびパスワードを設定します。

PAC ファイルの生成

PAC ファイルを生成するには、次の手順を実行します。

（注） PAC ファイルには、ASA および ISE がその間で発生する RADIUS トランザクションを保護できる共有キーが含まれています。このため、必ずこのキーを安全にASAに保存してください。

手順

ステップ 1 ISE にログインします。

ステップ 2 [Administration] > [Network Resources] > [Network Devices] を選択します。

ステップ 3 デバイスのリストから ASA を選択します。

ステップ 4 [Security Group Access (SGA)] で、[Generate PAC] をクリックします。

ステップ 5 PAC ファイルを暗号化するには、パスワードを入力します。

PAC ファイルを暗号化するために入力するパスワード（または暗号キー）は、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

ISE はPACファイルを生成します。ASA は、フラッシュ、またはTFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバーから PAC ファイルをインポートできます。（PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。

Cisco TrustSec のガイドライン

ここでは、Cisco TrustSec を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

フェールオーバー

- アクティブ/アクティブおよびアクティブ/スタンバイ コンフィギュレーションの両方で ASA のセキュリティ グループベースのポリシーを設定できます。

- ASA がフェールオーバー設定の一部である場合、プライマリ ASA デバイスに PAC ファイルをインポートする必要があります。また、プライマリ デバイスで環境データを更新する必要もあります。
- ASA は、ハイ アベイラビリティ（HA）用に設定された ISE と通信できます。
- ASA では複数の ISE サーバーを設定できます。最初のサーバーが到達不能の場合、引き続き 2 番目以降のサーバーに接続を試みます。ただし、サーバー リストが Cisco TrustSec 環境データの一部としてダウンロードされた場合、そのリストは無視されます。
- ISE からダウンロードされた PAC ファイルが ASA で期限切れとなり、ASA が更新されたセキュリティ グループ テーブルをダウンロードできない場合、ASA が更新されたテーブルをダウンロードするまで、最後にダウンロードされたセキュリティ グループ テーブルに基づいてセキュリティ ポリシーを適用し続けます。

クラスタ

- ASA がクラスタリング構成の一部である場合、制御ユニットに PAC ファイルをインポートする必要があります。
- ASA がクラスタリング構成の一部である場合、制御ユニットで環境データを更新する必要があります。

IPv6

ASA は、IPv6 と IPv6 対応ネットワーク デバイス用に SXP をサポートします。AAA サーバーは IPv4 アドレスを使用する必要があります。

レイヤ 2 SGT インポジション

- 物理インターフェイス、サブインターフェイス、冗長インターフェイス、EtherChannel インターフェイス、およびでのみサポートされます。
- 論理インターフェイスまたは仮想インターフェイス（BVI など）ではサポートされません。
- SAP ネゴシエーションおよび MACsec を使用したリンク暗号化はサポートされていません。
- フェールオーバー リンクではサポートされません。
- クラスタ制御リンクではサポートされません。
- SGT が変更されても、ASA は既存のフローを再分類しません。以前の SGT に基づいて行われたポリシーに関する決定が、フローのライフサイクルにわたって適用され続けます。ただし、ASA は、パケットが以前の SGT に基づいて分類されたフローに属していても、SGT の変更内容を出力パケットに即座に反映できます。
- Firepower 1010 スイッチポートおよび VLAN インターフェイスは、レイヤ 2 セキュリティ グループ タグ インポジションをサポートしていません。

その他のガイドライン

- ASA は、SXP バージョン 3 をサポートしています。ASA は、さまざまな SXP 対応ネットワーク デバイスの SXP バージョンをネゴシエートします。
- ASAは、Cisco TrustSec（CTS）環境データの認可変更（CoA）をサポートしていません。
- SXP 調整タイマーの期限が切れたときにセキュリティ グループ テーブルを更新するように ASA を設定できます。セキュリティ グループ テーブルはオンデマンドでダウンロードできます。ASA のセキュリティ グループ テーブルが ISE から更新された場合、この変更が適切なセキュリティ ポリシーに反映されます。
- Cisco TrustSec は、シングル コンテキスト モードおよびマルチ コンテキスト モード（システム コンテキスト モードを除く）で Smart Call Home 機能をサポートしています。
- ASA は、単一の Cisco TrustSec ドメインでのみ相互運用するように設定できます。
- ASA は、デバイスの SGT 名のマッピングのスタティック コンフィギュレーションをサポートしていません。
- NAT は SXP メッセージでサポートされません。
- SXP はネットワークのエンフォースメント ポイントに IP-SGT マッピングを伝搬します。アクセス レイヤ スイッチがエンフォースメント ポイントと異なる NAT ドメインに属している場合、アップロードする IP-SGT マップは無効であり、実行デバイスに対する IP-SGT マッピング データベース検索から有効な結果を得ることはできません。その結果、ASA は実行デバイスにセキュリティ グループ対応セキュリティ ポリシーを適用できません。
- SXP 接続に使用する ASA にデフォルト パスワードを設定するか、またはパスワードを使用しないようにします。ただし、接続固有パスワードは SXP ピアではサポートされません。設定されたデフォルト SXP パスワードは導入ネットワーク全体で一貫している必要があります。接続固有パスワードを設定すると、接続が失敗する可能性があり、警告メッセージが表示されます。デフォルトパスワードを使用して接続を設定しても設定されていない場合、結果はパスワードなしで接続を構成した場合と同じです。
- ASA を SXP 送信者または受信者、あるいはその両方として設定できます。ただし、SXP 接続のループは、デバイスにピアへの双方向の接続がある場合、またはデバイスがデバイスの単方向に接続されたチェーンの一部である場合に発生します。（ASA は、データセンターのアクセス レイヤからのリソースの IP-SGT マッピングを学習できます。ASA は、これらのタグをダウンストリーム デバイスに伝搬する必要がある場合があります）。SXP 接続ループによって、SXP メッセージ転送の予期しない動作が発生する可能性があります。ASA が送信者および受信者として設定されている場合、SXP 接続ループが発生し、SXP データが最初にそのデータを送信したピアで受信される可能性があります。
- ASA のローカル IP アドレスを変更する場合は、すべての SXP ピアでピア リストが更新されていることを確認する必要があります。さらに、SXP ピアがその IP アドレスを変更する場合は、変更が ASA に反映されていることを確認する必要があります。
- 自動 PAC ファイル プロビジョニングはサポートされません。ASA 管理者は、ISE 管理インターフェイスの PAC ファイルを要求し、それを ASA にインポートする必要があります。

- PAC ファイルには有効期限があります。現在の PAC ファイルが期限切れになる前に更新された PAC ファイルをインポートする必要があります。そうしないと、ASA は環境データの更新を取得できません。ISE からダウンロードされた PAC ファイルが ASA で期限切れとなり、ASA が更新されたセキュリティ グループ テーブルをダウンロードできない場合、ASA が更新されたテーブルをダウンロードするまで、最後にダウンロードされたセキュリティ グループ テーブルに基づいてセキュリティ ポリシーを適用し続けます。
- セキュリティ グループが ISE で変更された（名前変更、削除など）場合、ASA は、変更されたセキュリティ グループに関連付けられた SGT またはセキュリティ グループ名を含む ASA セキュリティ ポリシーのステータスを変更しません。ただし、ASA は、それらのセキュリティ ポリシーが変更されたことを示す syslog メッセージを生成します。
- マルチキャスト タイプは ISE 1.0 ではサポートされていません。
- SXP 接続は、次の例に示すように、ASA によって相互接続された 2 つの SXP ピア間で初期化状態のままとなります。

```
(SXP peer A) - - - - (ASA) - - - (SXP peer B)
```

したがって、Cisco TrustSec と統合するように ASA を設定する場合は、SXP 接続を設定するために、ASA で、no-NAT、no-SEQ-RAND、MD5-AUTHENTICATION TCP オプションをイネーブルにする必要があります。SXP ピア間の SXP ポート TCP 64999 宛てのトラフィックに対して TCP 状態バイパス ポリシーを作成します。そして、適切なインターフェイスにポリシーを適用します。

たとえば、次のコマンド セットは、TCP 状態バイパス ポリシーの ASA の設定方法を示しています。

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

Cisco TrustSec と統合するための ASA の設定

Cisco TrustSec と統合するように ASA を設定するには、次のタスクを実行します。

始める前に

Cisco TrustSec と統合するように ASA を設定する前に、ISE で次のタスクを実行する必要があります。

- ISE への ASA の登録 （91 ページ）
- ISE でのセキュリティ グループの作成 （91 ページ）
- PAC ファイルの生成 （92 ページ）

手順

ステップ 1 Cisco TrustSec と統合するための AAA サーバーの設定 （96 ページ）

ステップ 2 PAC ファイルのインポート （98 ページ）

ステップ 3 Security Exchange Protocol の設定 （100 ページ）

このタスクでは、SXP のデフォルト値を有効にし、設定します。

ステップ 4 SXP 接続のピアの追加 （102 ページ）

ステップ 5 環境データの更新 （103 ページ）

必要に応じてこれを実行してください。

ステップ 6 セキュリティ ポリシーの設定 （104 ページ）

ステップ 7 レイヤ 2 セキュリティ グループのタギング インポジションの設定 （106 ページ）

Cisco TrustSec と統合するための AAA サーバーの設定

ここでは、Cisco TrustSec の AAA サーバーを統合する方法について説明します。ASA で ISE と通信するように AAA サーバー グループを設定するには、次の手順を実行します。

始める前に

- 参照先のサーバー グループは、RADIUS プロトコルを使用するように設定する必要があります。ASA に非 RADIUS サーバー グループを追加すると、設定は失敗します。
- ISE もユーザー認証に使用する場合は、ISE に ASA を登録したときに ISE で入力した共有秘密を取得します。この情報については、ISE 管理者に問い合わせてください。

手順

ステップ 1 AAA サーバー グループを作成し、ISE サーバーと通信するように ASA の AAA サーバー パラメータを設定します。

aaa-server *server-tag* **protocol radius**

例：

```
ciscoasa(config)# aaa-server ISEserver protocol radius
```

server-tag 引数には、サーバー グループ名を指定します。

ステップ 2 AAA サーバー グループ コンフィギュレーション モードを終了します。

exit

例：

```
ciscoasa(config-aaa-server-group)# exit
```

ステップ 3 AAA サーバーを AAA サーバー グループの一部として設定し、ホスト固有の接続データを設定します。

```
ciscoasa(config)# aaa-server server-tag(interface-name) host server-ip
```

例：

```
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
```

interface-name 引数には、ISE サーバーが配置されているネットワーク インターフェイスを指定します。このパラメータにはカッコが必要です。*server-tag* 引数は、AAA サーバー グループの名前です。*server-ip* 引数には、ISE サーバーの IP アドレスを指定します。

ステップ 4 ISE サーバーで ASA の認証に使用されるサーバー秘密値を指定します。

key *key*

例：

```
ciscoasa(config-aaa-server-host)# key myexclusivekey
```

key 引数は、最大 127 文字の英数字キーワードです。

ISE もユーザー認証に使用する場合は、ISE に ASA を登録したときに ISE で入力した共有秘密を入力します。

ステップ 5 AAA サーバー ホスト コンフィギュレーション モードを終了します。

exit

例：

```
ciscoasa(config-aaa-server-host)# exit
```

ステップ 6 環境データ取得のために Cisco TrustSec によって使用される AAA サーバー グループを識別します。

```
cts server-group AAA-server-group-name
```

例：

```
ciscoasa(config)# cts server-group ISEserver
```

AAA-server-group-name 引数は、ステップ 1 で *server-tag* 引数に指定した AAA サーバー グループの名前です。

（注） ASA では、サーバー グループの 1 つのインスタンスだけを Cisco TrustSec 用に設定できます。

次に、Cisco TrustSec との統合のために ISE サーバーと通信するように ASA を設定する例を示します。

```
ciscoasa(config)#aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

PAC ファイルのインポート

ここでは、PAC ファイルをインポートする方法について説明します。

始める前に

- ASA が PAC ファイルを生成するには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。
- ISE での PAC ファイルの生成時に PAC ファイルを暗号化するために使用されたパスワードを取得します。ASA は、PAC ファイルをインポートし、復号化する場合にこのパスワードが必要となります。
- インポートすると、PAC ファイルは NVRAM に常駐します。HA モードで動作している場合、フェールオーバーリンクとステートフルリンクを正しく設定すると、PAC ファイルをアクティブユニットにインポートすることで、セカンダリに複製されます。インポートされたファイルは NVRAM にあるため、ソフトウェアのアップグレード後など、デバイスがリブートするたびに、同ファイルを再インポートする必要があります。

- デバイスは単一の PAC ファイルを使用します。複数の PAC ファイルをインポートすると、以前にインポートされたファイルが、インポートした各 PAC ファイルで置き換えられます。
- ASA は、ISE で生成された PAC ファイルにアクセスする必要があります。ASA は、フラッシュ、または TFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバーから PAC ファイルをインポートできます。（PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。
- ASA のサーバー グループを設定します。

手順

Cisco TrustSec PAC ファイルをインポートします。

cts import-pac*filepath* **password** *value*

例：

```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

value 引数には、PAC ファイルの暗号化に使用するパスワードを指定します。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。*filepath* 引数には、次のオプションのいずれか 1 つを入力します。

シングル モード

- **disk0**：disk0 のパスおよびファイル名
- **disk1**：disk1 のパスおよびファイル名
- **flash**：フラッシュのパスおよびファイル名
- **ftp**：FTP のパスおよびファイル名
- **http**：HTTP のパスおよびファイル名
- **https**：HTTPS のパスおよびファイル名
- **smb**：SMB のパスおよびファイル名
- **tftp**：TFTP のパスおよびファイル名

マルチ モード

- **http**：HTTP のパスおよびファイル名
- **https**：HTTPS のパスおよびファイル名
- **smb**：SMB のパスおよびファイル名
- **tftp**：TFTP のパスおよびファイル名

次に、PAC ファイルを ASA にインポートする例を示します。

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

Security Exchange Protocol の設定

Cisco TrustSec を使用するように Security Exchange Protocol（SXP）を有効にして設定する必要があります。

始める前に

少なくとも 1 つのインターフェイスを UP/UP ステートにする必要があります。すべてのインターフェイスがダウンした状態で SXP がイネーブルになっている場合、ASA では、SXP が動作していない、あるいは SXP をイネーブルにできなかったことを示すメッセージは表示されません。show running-config コマンドを入力して設定を確認すると、コマンドの出力に次のメッセージが表示されます。

```
"WARNING: SXP configuration in process, please wait for a few moments and try again."
```

手順

ステップ 1 ASA で SXP をイネーブルにします。SXP は、デフォルトで、ディセーブルに設定されています。

cts sxp enable

例：

```
ciscoasa(config)# cts sxp enable
```

ステップ 2 （任意。推奨されません）SXP 接続のデフォルトの送信元 IP アドレスを設定します。

cts sxp default source-ip *ipaddress*

例：

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

ipaddress 引数は、IPv4 または IPv6 アドレスです。

SXP 接続のデフォルトの送信元 IP アドレスを設定する場合は、ASA 発信インターフェイスと同じアドレスを指定する必要があります。送信元 IP アドレスが発信インターフェイスのアドレスと一致しない場合、SXP 接続は失敗します。

SXP 接続の送信元 IP アドレスが設定されていない場合、ASA は、route/ARP 検索を実行して、SXP 接続用の発信インターフェイスを判別します。SXP 接続のデフォルトの送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。

ステップ 3 （任意）SXP ピアでの TCP MD5 認証のデフォルト パスワードを設定します。デフォルトでは、SXP 接続にパスワードは設定されていません。

cts sxp default password [**0** | **8**] *password*

例：

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

デフォルトのパスワードを使用するように SXP 接続ピアを設定した場合、または設定した場合にのみ、デフォルトのパスワードを設定します。

パスワードの長さは復号レベルによって異なります。指定しない場合、デフォルトは 0 になります。

- **0**：暗号化されていないクリアテキスト。パスワードには、最大 80 文字を指定できます。
- **8**：暗号化テキスト。パスワードには、最大 162 文字を指定できます。

ステップ 4 （任意）ASA が SXP ピア間での新しい SXP 接続の設定を試行する時間間隔を指定します。

cts sxp retry period *timervalue*

例：

```
ciscoasa(config)# cts sxp retry period 60
```

ASA は、成功した接続が確立されるまで接続を試み続け、失敗した試行後、再度試行するまでに再試行間隔の間待機します。再試行期間には 0 ～ 64000 秒の値を指定できます。デフォルトは 120 秒です。0 秒を指定すると、ASA は SXP ピアへの接続を試行しません。

再試行タイマーは、SXP ピア デバイスとは異なる値に設定することを推奨します。

ステップ 5 （任意）調整タイマーの値を指定します。

cts sxp reconciliation period *timervalue*

例：

```
ciscoasa(config)# cts sxp reconciliation period 60
```

SXP ピアが SXP 接続を終了すると、ASA はホールド ダウン タイマーを開始します。ホールド ダウン タイマーの実行中に SXP ピアが接続されると、ASA は調整タイマーを開始します。次に、ASA は、SXP マッピング データベースを更新して、最新のマッピングを学習します。

調整タイマーの期限が切れると、ASA は、SXP マッピング データベースをスキャンして、古いマッピング エントリ（前回の接続セッションで学習されたエントリ）を識別します。ASA

は、これらの接続を廃止としてマークします。調整タイマーが期限切れになると、ASA は、SXP マッピング データベースから廃止エントリを削除します。

調整期間には 1 ～ 64000 秒の値を指定できます。デフォルトは 120 秒です。

ステップ 6 （任意）SXP ピアが SXP 接続を終了した後にピアから学習した IP-SGT マッピングに削除ホールド ダウン タイマーを設定します。

cts sxp delete-hold-down period *timervalue*

タイマーの値は、SXP 接続の切断から学習した IP-SGT マッピングが削除されるまで保持する秒数を 120 ～ 64000 の範囲で指定します。

例：

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

各 SXP 接続が削除ホールド ダウン タイマーに関連付けられます。このタイマーは、リスナー側の SXP 接続が切断されたときにトリガーされます。この SXP 接続から学習した IP-SGT マッピングはすぐには削除されません。その代わりに、削除ホールド ダウン タイマーの有効期限が切れるまで保持されます。このタイマーの有効期限が切れると、マッピングが削除されます。

ステップ 7 （任意）SXPv2 以下を使用するピアへのスピーカーとして機能する場合の IPv4 サブネット拡張の深さを設定します。

cts sxp mapping network-map *maximum_hosts*

ピアが SXPv2 以下を使用する場合、ピアはサブネット バインディングへの SGT を理解できません。ASA は、個々のホスト バインディングに IPv4 サブネット バインディングを拡張できます（IPv6 バインディングは拡張されません）。このコマンドでは、サブネット バインディングから生成できるホスト バインディングの最大数が指定されます。

最大数には 0 ～ 65535 を指定できます。デフォルトは 0 で、サブネット バインディングがホスト バインディングに拡張されないことを意味します。

SXP 接続のピアの追加

SXP 接続のピアを追加するには、次の手順を実行します。

手順

SXP ピアへの SXP 接続を設定します。

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **none**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

例：

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

SXP 接続は IP アドレスごとに設定されます。単一デバイスのペアは複数の SXP 接続に対応できます。

peer_ip_address 引数は、SXP ピアの IPv4 または IPv6 アドレスです。ピア IP アドレスは、ASA 発信インターフェイスからアクセスできる必要があります。

source_ip_address 引数は、SXP 接続のローカル IPv4 または IPv6 アドレスです。送信元 IP アドレスは ASA 発信インターフェイスと同じである必要があります。そうでなければ、接続が失敗します。

SXP 接続の送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。

SXP 接続に認証キーを使用するかどうかを指定します。

- **default**：SXP 接続用に設定されたデフォルト パスワードを使用します。
- **none**：SXP 接続にパスワードを使用しません。

SXP 接続のモードを指定します。

- **local**：ローカル SXP デバイスを使用します。
- **peer**：ピア SXP デバイスを使用します。

SXP 接続で、ASA が送信者または受信者のいずれとして機能するかを指定します。

- **speaker**：ASA は IP-SGT マッピングをアップストリーム デバイスに転送できます。
- **listener**：ASA はダウンストリーム デバイスから IP-SGT マッピングを受信できます。

次に、ASA で SXP ピアを設定する例を示します。

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default
mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default
mode peer speaker
```

環境データの更新

ASA は、ISE からセキュリティ グループ タグ（SGT）名テーブルなどの環境データをダウンロードします。ASA で次のタスクを完了すると、ASA は、ISE から取得した環境データを自動的にリフレッシュします。

- ISE と通信するように AAA サーバーを設定します。
- ISE から PAC ファイルをインポートします。

- Cisco TrustSec 環境データを取得するために ASA で使用する AAA サーバー グループを識別します。

通常、ISE からの環境データを手動でリフレッシュする必要はありません。ただし、セキュリティ グループが ISE で変更されることがあります。ASA セキュリティ グループ テーブルのデータをリフレッシュするまで、これらの変更は ASA に反映されません。そのため、ASA のデータをリフレッシュして、ISE でのセキュリティ グループの変更が確実に ASA に反映されるようにします。

（注） メンテナンス時間中に ISE のポリシー設定および ASA での手動データ リフレッシュをスケジュールすることを推奨します。このようにポリシー設定の変更を処理すると、セキュリティ グループ名が解決される可能性が最大化され、セキュリティ ポリシーが ASA で即時にアクティブ化されます。

環境データを更新するには、次の手順を実行します。

手順

ISE からの環境データを更新し、設定されたデフォルト値に調整タイマーをリセットします。

cts refresh environment-data

例：

```
ciscoasa(config)# cts refresh environment-data
```

セキュリティ ポリシーの設定

Cisco TrustSec ポリシーは、多くの ASA 機能に組み込むことができます。拡張 ACL を使用する機能（この章でサポート対象外としてリストされている機能を除く）で Cisco TrustSec を使用できます。拡張 ACL に、従来のネットワークベースのパラメータとともにセキュリティ グループ引数を追加できます。

- 拡張 ACL を設定するには、セキュリティ グループ ベースの照合（Cisco TrustSec）に使用する拡張 ACE の追加 （47 ページ） を参照してください。
- ACL で使用できるセキュリティ グループ オブジェクト グループを設定する方法については、セキュリティ グループ オブジェクト グループの設定 （25 ページ）を参照してください。

たとえば、アクセス ルールは、ネットワーク情報を使用してインターフェイスのトラフィックを許可または拒否します。Cisco TrustSec では、セキュリティ グループに基づいてアクセスを

制御できます。たとえば、sample_securitygroup1 10.0.0.0 255.0.0.0 のアクセス ルールを作成できます。これは、セキュリティ グループがサブネット 10.0.0.0/8 上のどの IP アドレスを持っていてもよいことを意味します。

セキュリティ グループの名前（サーバー、ユーザー、管理対象外デバイスなど）、ユーザー ベース属性、および従来の IP アドレスベースのオブジェクト（IP アドレス、Active Directory オブジェクト、および FQDN）の組み合わせに基づいてセキュリティ ポリシーを設定できます。セキュリティ グループ メンバーシップはロールを超えて拡張し、デバイスと場所属性を含めることができます。また、セキュリティ グループ メンバーシップは、ユーザー グループ メンバーシップに依存しません。

次に、ローカルで定義されたセキュリティ オブジェクト グループを使用する ACL を作成する例を示します。

```
object-group security objgrp-it-admin
   security-group name it-admin-sg-name
   security-group tag 1
object-group security objgrp-hr-admin
   security-group name hr-admin-sg-name  // single sg_name
   group-object it-admin     // locally defined object-group as nested object
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
object-group security objgrp-hr-network
security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

前の例で設定した ACL をアクティブにするには、アクセス グループまたはモジュラ ポリシー フレームワークを設定します。

その他の例：

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53

!match src hr-admin-sg-name from host 10.1.1.1 to dst any
access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any

!match src tag 22 from any network to dst hr-servers-sg-name any network
access-list idfw-acl permit ip security-group tag 22 any security-group
name hr-servers-sg-name any

!match src user mary from any host to dst hr-servers-sg-name any network
access-list idfw-acl permit ip user CSCO\mary any security-group
name hr-servers-sg-name any

!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
access-list idfw-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers any

!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24
! to dst objgrp-hr-servers any network
access-list idfw-acl permit ip user CSCO\Jack object-group-security
objgrp-hr-network 10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

!match src user Tom from security-group mktg any google.com
object network net-google
fqdn google.com
```

```
access-list sgacl permit ip sec name mktg any object net-google

! If user Tom or object_group security objgrp-hr-admin needs to be matched,
! multiple ACEs can be defined as follows:
access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin
    10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any
```

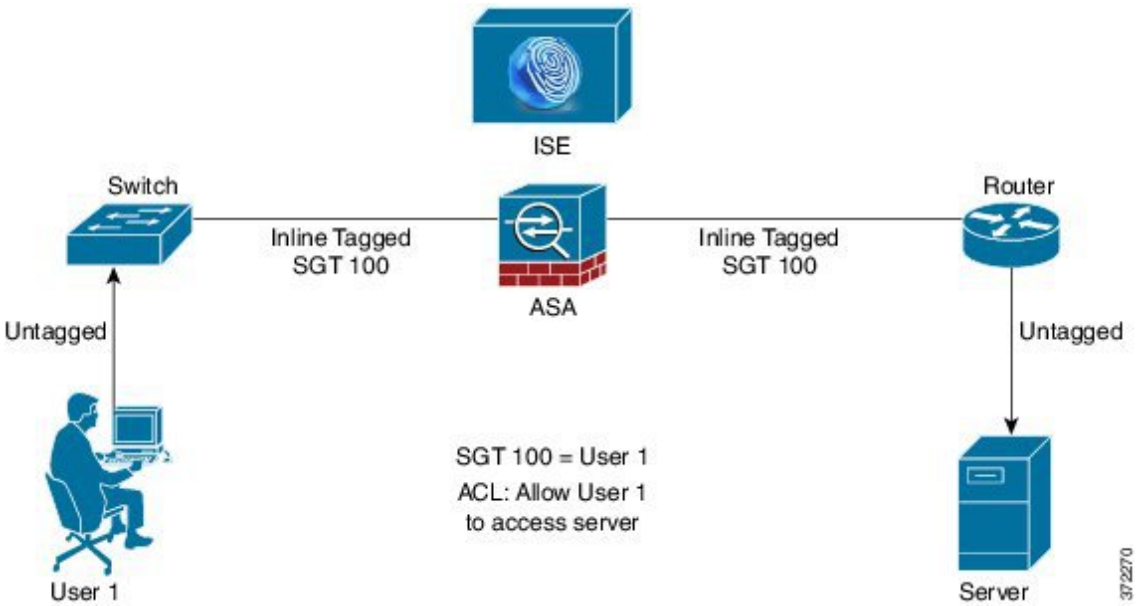
レイヤ 2 セキュリティ グループのタギング インポジションの設定

Cisco TrustSec は、各ネットワーク ユーザーおよびリソースの特定と認証を行い、セキュリティ グループ タグ（SGT）と呼ばれる 16 ビットの番号を割り当てます。この ID は、ネットワーク ホップ間で順番に伝搬されます。これにより、ASA、スイッチ、ルータなどの任意の中間デバイスで、この ID タグに基づいてポリシーを適用できます。

SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。ASA は、インターフェイスごとの手動設定に基づいて、発信パケットにセキュリティ グループ タグを挿入し、着信パケットのセキュリティ グループ タグを処理します。この機能を使用することで、ネットワーク デバイス間におけるエンドポイント ID の伝搬をインラインかつホップバイホップで実行できます。また、各ホップ間でシームレスなレイヤ 2 SGT インポジションを実現できます。

次の図 に、レイヤ 2 SGT インポジションの一般的な例を示します。

図 *5:* レイヤ *2 SGT* インポジション



使用シナリオ

次の表で、この機能を設定した場合の入力トラフィックの予期される動作について説明します。

表 *3*：入力トラフィック

インターフェイス コンフィギュレーション	タグ付きの受信パケット	タグのない受信パケット
コマンドが発行されない。	パケットがドロップされる。	SGT 値が IP-SGT マネージャから取得される。
cts manual コマンドが発行される。	SGT 値が IP-SGT マネージャから取得される。	SGT 値が IP-SGT マネージャから取得される。
cts manual コマンドと **policy static sgt** *sgt_number* コマンドが両方とも発行される。	SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。	SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。
cts manual コマンドと **policy static sgt** *sgt_number* **trusted** コマンドが両方とも発行される。	SGT 値がパケットのインライン SGT から取得される。	SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。

（注） IP-SGT マネージャと一致する IP-SGT マッピングが存在しない場合、予約されている SGT 値（「不明」を表す「0x0」）が使用されます。

次の表で、この機能を設定した場合の出力トラフィックの予期される動作について説明します。

表 *4*：出力トラフィック

インターフェイス コンフィギュレーション	送信パケットのタグの有無
コマンドが発行されない。	タグなし
cts manual コマンドが発行される。	タグ付き
cts manual コマンドと propagate sgt コマンドが両方とも発行される。	タグ付き
cts manual コマンドと no propagate sgt コマンドが両方とも発行される。	タグなし

次の表で、この機能を設定した場合の to-the-box トラフィックと from-the-box トラフィックの予期される動作について説明します。

表 *5 : to-the-box* トラフィックと *from-the-box* トラフィック

インターフェイス コンフィギュレーション	受信パケットのタグの有無
to-the-box トラフィック用の入力インターフェイスで、コマンドが発行されない。	パケットがドロップされる。
to-the-box トラフィック用の入力インターフェイスで、cts manual コマンドが発行される。	パケットは受け入れられるが、ポリシーの適用や SGT の伝搬は行われない。
cts manual コマンドが発行されない。または、from-the-box トラフィック用の出力インターフェイスで、**cts manual** コマンドと **no propagate sgt** コマンドが両方とも発行される。	タグなしパケットは送信されるが、ポリシーの適用は行われない。SGT 値が IP-SGT マネージャから取得される。
cts manual コマンドが発行される。または、from-the-box トラフィック用の出力インターフェイスで、cts manual コマンドと propagate sgt コマンドが両方とも発行される。	タグ付きパケットが送信される。SGT 値が IP-SGT マネージャから取得される。

（注） IP-SGT マネージャと一致する IP-SGT マッピングが存在しない場合、予約されている SGT 値（「不明」を表す「0x0」）が使用されます。

インターフェイスでのセキュリティ グループ タグの設定

インターフェイスでセキュリティ グループ タグを設定するには、次の手順を実行します。

手順

ステップ 1 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

ステップ 2 レイヤ 2 SGT インポジションをイネーブルにし、CTS 手動インターフェイス コンフィギュレーション モードを開始します。

cts manual

例：

```
ciscoasa(config-if)# cts manual
```

ステップ 3 インターフェイスでのセキュリティ グループ タグの伝播をイネーブルにします。伝搬はデフォルトでイネーブルになっています。

propagate sgt

例：

```
ciscoasa(config-if-cts-manual)# propagate sgt
```

ステップ 4 手動で設定された CTS リンクにポリシーを適用します。

policy static sgt *sgt_number* [**trusted**]

例：

```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

static キーワードで、リンクの着信トラフィックに適用する SGT ポリシーを指定します。

sgt キーワードと *sgt_number* 引数には、ピアからの着信トラフィックに適用する SGT 値を指定します。有効な値の範囲は 2 ～ 65519 です。

trusted キーワードは、コマンドで SGT が指定されたインターフェイスの入力トラフィックでは、SGT を上書きしてはいけないことを示します。デフォルトは untrusted です。

次に、レイヤ 2 SGT インポジション用のインターフェイスをイネーブルにし、インターフェイスが信頼できるかどうかを定義する例を示します。

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

IP-SGT バインディングの手動設定

IP-SGT バインディングを手動で設定するには、次の手順を実行します。

手順

IP-SGT バインディングを手動で設定します。

cts role-based sgt-map {*IPv4_addr*[/*mask*] | *IPv6_addr*[/*prefix*]} **sgt** *sgt_value*

例：

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

IPv4 または IPv6 ホスト アドレスを指定できます。また、10.100.10.0/24 のようなサブネット マスクまたはプレフィックス値（IPv6 の場合）を含めることで、ネットワーク アドレスを指定することもできます。*sgt_value* は SGT 番号で、2 ～ 65519 の範囲です。

トラブルシューティングのヒント

特定のセッションが許可または拒否された理由、使用されている SGT 値（パケットの SGT 値、IP-SGT マネージャから取得した SGT 値、またはインターフェイスで設定した **policy static sgt** コマンドで取得した SGT 値）、および適用されたセキュリティ グループベースのセキュリティ ポリシーを確認するには、**packet-tracer** コマンドを使用します。

次に、**packet-tracer** コマンドの出力例を示します。この出力から、セキュリティ グループ タグと IP アドレスの対応付けがわかります。

```
ciscoasa# packet-tracer input inside tcp inline-tag 100
security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

特定の SGT 値を指定するかどうかにかかわらず、Cisco CMD パケット（EtherType 0x8909）のみをキャプチャするには、**capture** *capture-name* **type inline-tag** *tag* コマンドを使用します。

次に、SGT 値を指定した場合の **show capture** コマンドの出力例を示します。

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

Cisco TrustSec の例

次に、Cisco TrustSec を使用するように ASA を設定する方法の例を示します。

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
cts server-group cts-server-list
// Configure SXP peers
```

```
cts sxp enable
cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
security-group name hr-admin-sg-name
group-object it-admin
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
   interface gi0/1
   cts manual
   propagate sgt
   policy static sgt 100 trusted
   cts role-based sgt-map 10.1.1.100 sgt 50
```

セキュアクライアントCisco TrustSec に対する VPN のサポート

ASAは、VPNセッションのセキュリティ グループ タギングをサポートしています。外部AAAサーバーを使用するか、または、ローカル ユーザーかVPN グループ ポリシーのセキュリティ グループ タグを設定することで、セキュリティ グループ タグ（SGT）をVPNセッションに割り当てることができます。さらに、レイヤ 2 イーサネット経由で、Cisco TrustSec システムを介してこのタグを伝搬することができます。AAA サーバーが SGT を提供できない場合には、セキュリティ グループ タグをグループ ポリシーで利用したり、ローカル ユーザーが利用したりすることができます。

次は、VPN ユーザーに SGT を割り当てるための一般的なプロセスです。

1. ユーザーは、ISE サーバーを含む AAA サーバー グループを使用しているリモート アクセス VPN に接続します。
2. ASA が ISE に AAA 情報を要求します。この情報に SGT が含まれている場合があります。ASA は、ユーザーのトンネル トラフィックに対する IP アドレスの割り当ても行います。
3. ASA が AAA 情報を使用してユーザーを認証し、トンネルを作成します。
4. ASA が AAA 情報から取得した SGT と割り当て済みの IP アドレスを使用して、レイヤ 2 ヘッダー内に SGT を追加します。
5. SGT を含むパケットが Cisco TrustSec ネットワーク内の次のピア デバイスに渡されます。

AAAサーバーの属性に、VPNユーザーに割り当てるためのSGTが含まれていない場合、ASAはグループ ポリシーの SGT を使用します。グループ ポリシーに SGT が含まれていない場合は、タグ 0x0 が割り当てられます。

（注） また、ISE 認可変更（CoA）を使用してポリシーの適用に ISE を使用することもできます。ポリシーの適用を設定する方法については、VPN の設定ガイドを参照してください。

リモート アクセス VPN グループ ポリシーおよびローカル ユーザーへの SGT の追加

リモート アクセス VPN グループ ポリシーまたはローカル ユーザー データベースで定義されたユーザーの VPN ポリシーで SGT 属性を設定するには、次の手順を実行します。

グループ ポリシーまたはローカル ユーザー用のデフォルト SGT はありません。

手順

ステップ 1 リモート アクセス VPN グループ ポリシーで SGT を設定するには、次の手順を実行します。

a) グループ ポリシー コンフィギュレーション モードを開始します。

group-policy *name*

例：

```
ciscoasa(config)# group policy Grpolicy1
```

b) グループ ポリシー用の SGT を設定します。

security-group-tag {**none** | **value** *sgt*}

value を使用してタグを設定する場合、タグは 2 ～ 65519 の範囲で指定できます。SGT を設定しない場合は **none** を指定します。

例：

```
ciscoasa(config-group-policy# security-group-tag value 101
```

ステップ 2 ローカル データベースでユーザー用の SGT を設定するには、次の手順を実行します。

a) 必要に応じて、ユーザーを作成します。

username *name* {**nopassword** | **password** *password* [**encrypted**]} [**privilege** *priv_level*]}

例：

```
ciscoasa(config)# username newuser password changeme encrypted privilege 15
```

b) ユーザー名コンフィギュレーション モードを開始します。

username *name* **attributes**

例：

```
asa3(config)# username newuser attributes
asa3(config-username)#
```

c) ユーザー用の SGT を設定します。

security-group-tag {**none** | **value** *sgt*}

value を使用してタグを設定する場合、タグは 2 ～ 65519 の範囲で指定できます。SGT を設定しない場合は **none** を指定します。

例：

```
ciscoasa(config-username)# security-group-tag value 101
```

Cisco TrustSec のモニタリング

Cisco TrustSec の監視については、次のコマンドを参照してください。

- **show running-config cts**
- **show running-config** [**all**] **cts role-based** [**sgt-map**]

  このコマンドは、ユーザー定義の IP-SGT バインディング テーブル エントリを表示します。

- **show cts sxp connections**

  このコマンドでは、マルチ コンテキスト モードが使用されると、特定のユーザー コンテキストの ASA の SXP 接続が表示されます。

- **show conn security-group**

  すべての SXP 接続のデータを表示します。

- **show cts environment-data**

  ASA のセキュリティ グループ テーブルに含まれる Cisco TrustSec 環境情報を表示します。

- **show cts sgt-map**

  制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示します。

- **show asp table cts sgt-map**

  このコマンドは、データ パスに保持されている IP アドレス セキュリティ グループのテーブル マップ データベースから IP アドレス セキュリティ グループのテーブル マップ エントリを表示します。

- **show cts pac**

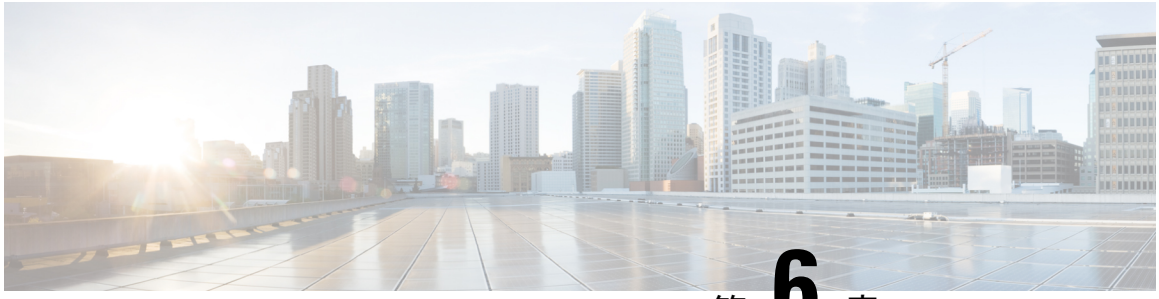
ISE から ASA にインポートされた PAC ファイルに関する情報を表示し、PAC ファイルの有効期限が切れた場合、または期限切れの 30 日以内になった場合には、警告メッセージが含まれます。

Cisco TrustSec の履歴

表 *6 : Cisco TrustSec* の履歴

機能名	プラットフォームリリース	説明
Cisco TrustSec	9.0(1)	Cisco TrustSec は、既存の ID 認識型インフラストラクチャを基盤とするアクセス コントロールです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec 機能では、実行デバイスはユーザー属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。 このリリースでは、ASA に Cisco TrustSec が統合されており、セキュリティ グループに基づいてポリシーが適用されます。Cisco TrustSec ドメイン内のアクセス ポリシーは、トポロジには依存しません。ネットワーク IP アドレスではなく、送信元および宛先のデバイスのロールに基づいています。 ASA は、セキュリティ グループに基づくその他のタイプのポリシー（アプリケーション インスペクションなど）に対しても Cisco TrustSec を活用できます。たとえば、設定するクラス マップの中に、セキュリティ グループに基づくアクセス ポリシーを入れることができます。 **access-list extended**、 **cts sxp enable**、 **cts server-group**、**cts sxp default**、**cts sxp retry period**、**cts sxp reconciliation period**、**cts sxp connection peer**、**cts import-pac**、**cts refresh environment-data**、**object-group security**、**security-group**、**show running-config cts**、**show running-config object-group**、**clear configure cts**、**clear configure object-group**、**show cts pac**、**show cts environment-data**、**show cts environment-data sg-table**、**show cts sxp connections**、**show object-group**、**show configure security-group**、**clear cts environment-data**、**debug cts,** 、 **packet-tracer** の各コマンドが導入または変更されました。

機能名	プラットフォームリリース	説明
レイヤ 2 セキュリティ グループのタグ インポジション	9.3(1)	セキュリティ グループ タギングをイーサネット タギングと組み合わせて使用して、ポリシーを適用できるようになりました。SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。 **cts manual**、**policy static sgt**、**propagate sgt**、**cts role-based sgt-map**、**show cts sgt-map**、**packet-tracer**、**capture**、**show capture**、**show asp drop**、**show asp table classify**、**show running-config all**、**clear configure all**、および **write memory** の各コマンドが導入または変更されました。
Security Exchange Protocol（SXP）バージョン 3 の Cisco TrustSec サポート	9.6(1)	ASA の Cisco Trustsec は、ホスト バインディングよりも効率的な SGT とサブネット間のバインディングを可能にする SXPv3 を実装するようになりました。 **cts sxp mapping network-map**、**cts role-based sgt-map**、**show cts sgt-map**、**show cts sxp sgt-map**、**show asp table cts sgt-map** の各コマンドが導入または変更されました。
Trustsec SXP 接続の設定可能な削除ホールド ダウン タイマー	9.8(3)	デフォルトの SXP 接続ホールド ダウン タイマーは 120 秒です。このタイマーを 120 ～ 64000 秒に設定できるようになりました。 新規/変更されたコマンド：**cts sxp delete-hold-down period**、**show cts sxp connection brief**、**show cts sxp connections**



第 6 章

Cisco Umbrella

Cisco Umbrella で定義されている FQDN ポリシーをユーザー接続に適用できるようにするため、DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。次のトピックでは、デバイスを Cisco Umbrella と統合するように Umbrella Connector を設定する方法について説明します。

- Cisco Umbrella Connector について （117 ページ）
- Cisco Umbrella Connector のライセンス要件 （119 ページ）
- Cisco Umbrella のガイドラインと制限事項 （119 ページ）
- Cisco Umbrella Connector の設定 （121 ページ）
- Umbrella Connector の例 （128 ページ）
- Umbrella Connector のモニタリング （132 ページ）
- Cisco Umbrella Connector の履歴 （135 ページ）

Cisco Umbrella Connector について

Cisco Umbrella を使用する場合、Cisco Umbrella Connector を設定して DNS クエリを Cisco Umbrella へリダイレクトできます。これにより、Cisco Umbrella で未許可もしくは疑義のあるドメイン名に対する要求を特定し、DNS ベースのセキュリティポリシーを適用することができます。

Umbrella Connector は、システムの DNS インスペクションの一部です。既存の DNS インスペクション ポリシーマップにより、DNS インスペクションの設定に基づいて要求をブロックするか、または、要求をドロップすることに決定した場合、その要求は Cisco Umbrella へ転送されません。したがって、ローカルの DNS インスペクション ポリシーと Cisco Umbrella のクラウドベースのポリシーの 2 つを保護します。

DNS ルックアップ要求を Cisco Umbrella へリダイレクトすると、Umbrella Connector は EDNS（DNS の拡張機能）レコードを追加します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。クラウドベースのポリシーでこれらの条件を使用することで、FQDN のレピュテーションだけでなくアクセスを制御することができます。また、DNSCrypt を使用して DNS 要求を暗号化し、ユーザー名と内部の IP アドレスのプライバシーを確保することもできます。

Cisco Umbrella エンタープライズ セキュリティ ポリシー

クラウド ベースの Cisco Umbrella エンタープライズ セキュリティ ポリシーでは、DNS ルックアップ要求の完全修飾ドメイン名（FQDN）のレピュテーションに基づいてアクセスを制御することができます。エンタープライズ セキュリティ ポリシーによって、次のいずれかのアクションを強制できます。

- 許可：FQDN に対するブロック ルールがなく、悪意のないサイトに属していると Cisco Umbrella が判断した場合は、サイトの実際の IP アドレスが返されます。これは、DNS ルックアップの通常の動作です。
- プロキシ：FQDN に対するブロック ルールはないが、疑わしいサイトに属していると Cisco Umbrella が判断した場合は、Umbrella インテリジェント プロキシの IP アドレスが DNS 応答で返されます。次に、プロキシで HTTP 接続を検査し、URL フィルタリングを適用します。インテリジェント プロキシが Cisco Umbrella ダッシュボード（**[Security Setting]** > **[Enable Intelligent Proxy]**）で有効になっていることを確認する必要があります。
- ブロック：FQDN が明示的にブロックされている場合、または悪意のあるサイトに属していると Cisco Umbrella が判断した場合は、ブロックされた接続の Umbrella クラウド ランディング ページの IP アドレスが DNS 応答で返されます。

Cisco Umbrella の登録

Umbrella Connector をデバイスに設定するときに、クラウドで Cisco Umbrella に登録します。登録プロセスでは、次のいずれかを特定する単一のデバイス ID が割り当てられます。

- シングル コンテキスト モードのスタンドアロン デバイス。
- シングル コンテキスト モードのハイ アベイラビリティ ペア。
- シングル コンテキスト モードのクラスタ。
- マルチコンテキスト スタンドアロン デバイスのセキュリティ コンテキスト。
- ハイ アベイラビリティ ペアのセキュリティ コンテキスト。
- クラスタのセキュリティ コンテキスト。

登録が完了すると、Cisco Umbrella ダッシュボードにデバイスの詳細が表示されます。次に、デバイスに関連付けられているポリシーを変更できます。登録中は、設定で指定するポリシーが使用されるか、デフォルトのポリシーが割り当てられます。複数のデバイスに同じ Umbrella ポリシーを割り当てることができます。ポリシーを指定する場合、受信するデバイス ID はポリシーを指定しなかった場合に取得する ID とは異なります。

Cisco Umbrella Connector のライセンス要件

Cisco Umbrella Connector を使用するには、3DES ライセンスが必要です。スマート ライセンスを使用している場合は、アカウントで輸出規制による機能限定をイネーブルにする必要があります。

Cisco Umbrella ポータルには、別のライセンス要件があります。

Cisco Umbrella のガイドラインと制限事項

コンテキスト モード

- マルチコンテキスト モードでは、コンテキストごとに Umbrella Connector を設定します。各コンテキストが異なるデバイス ID を持ち、Cisco Umbrella Connector ダッシュボードに別のデバイスとして表示されます。デバイス名は、コンテキストで設定されたホスト名にハードウェア モデルおよびコンテキスト名を追加した形式で作成されます。たとえば、CiscoASA-ASA5515-Context1 となります。

フェールオーバー

- ハイ アベイラビリティ ペアのアクティブ ユニットでは、ペアを単一ユニットとして Cisco Umbrella に登録します。両方のピアで、それぞれのシリアル番号から形成された同じデバイス ID が使用されます（*primary-serial-number_secondary-serial-number*）。マルチ コンテキスト モードでは、セキュリティ コンテキストの各ペアが単一ユニットと見なされます。ハイ アベイラビリティを設定する必要があります。ユニットでは、スタンバイ デバイスが現在障害発生状態であったとしても、Cisco Umbrella をイネーブルにする前にハイ アベイラビリティ グループを正常に作成する必要があります。これを作成しないと、登録に失敗します。

クラスタ

- クラスタ制御ユニットでは、クラスタを単一ユニットとして Cisco Umbrella に登録します。すべてのピアで同じデバイス ID を使用します。マルチ コンテキスト モードでは、クラスタ内のセキュリティ コンテキストがすべてのピアで単一ユニットと見なされます。

その他のガイドライン

- Cisco Umbrella へのリダイレクションは、通過トラフィックの DNS 要求に対してのみ実行されます。システム自体で開始する DNS 要求が Cisco Umbrella にリダイレクトされることはありません。たとえば、FQDN ベースのアクセス制御ルールが Umbrella のポリシーをベースに解決されたり、他のコマンドまたは構成設定で使用される任意の FQDN となったりすることはありません。

- Cisco Umbrella Connector は、通過トラフィックの任意の DNS 要求で動作します。ただし、ブロックおよびプロキシアクションは DNS レスポンスが HTTP/HTTPS 接続で使用される場合にのみ有効です（返される IP アドレスが Web サイト用であるため）。非 HTTP/HTTPS 接続のブロックまたはプロキシされたアドレスは、失敗するか誤った方法で完了します。たとえば、ブロックされた FQDN の ping を実行すると、Cisco Umbrella クラウドのブロックページをホストするサーバーに対して ping を実行します。

（注） Cisco Umbrella を試行して、非 HTTP/HTTPS になる可能性がある FQDN をインテリジェントに特定します。プロキシされたドメイン名の FQDN では、インテリジェントプロキシに IP アドレスを返しません。

- システムでは、Cisco Umbrella へのみ DNS/UDP トラフィックを送信します。DNS/TCP インスペクションをイネーブルにすると、システムは、Cisco Umbrella に DNS/TCP 要求を送信しません。ただし、DNS/TCP 要求によって Umbrella バイパス カウンタが増えることはありません。
- Umbrella インスペクションで DNScrypt をイネーブルにすると、システムは暗号化されたセッションに UDP/443 を使用します。DNScrypt が正しく機能するためには、Cisco Umbrella の DNS インスペクションを適用するクラス マップに UDP/53 とともに UDP/443 を含める必要があります。UDP/443 と UDP/53 はいずれも DNS のデフォルトのインスペクションクラスに含まれていますが、カスタム クラスを作成する場合は、一致するクラスに両方のポートが含まれる ACL を定義する必要があります。
- DNScrypt は、証明書の更新ハンドシェイクに対してのみ、IPv4 を使用します。ただし、DNSscrypt では、IPv4 と IPv6 の両方のトラフィックを暗号化します。
- api.umbrella.com と api.opendns.com（登録では IPv4 のみを使用）にアクセスできるインターネットへの Ipv4 ルートが必要です。また、次の DNS リゾルバへのルートも必要となるほか、アクセス ルールでこれらのホストに DNS トラフィックを許可する必要があります。これらのルートは、データ インターフェイスまたは管理インターフェイスのいずれかを通過できます。有効なルートが登録と DNS 解決の両方で機能します。システムで使用するデフォルトのサーバーを示しています。Umbrella のグローバル設定でリゾルバを設定すると他のサーバーを使用できます。
  - 208.67.220.220 （IPv4 のシステム デフォルト）
  - 208.67.222.222
  - 2620:119:53::53 （IPv6 のシステム デフォルト）
  - 2620:119:35::35
- システムは Umbrella FamilyShield サービスをサポートしていません。FamilyShield リゾルバを設定すると、予期しない結果が発生する可能性があります。

- フェールオープンにするかどうかを評価する場合、システムは、Umbrella リゾルバがダウンしているかどうか、または仲介デバイスが要求の送信後の応答待機時間に基づいて DNS 要求または応答をドロップするかどうかを考慮します。Umbrella リゾルバへのルートなしなど、他の要因は考慮されません。
- デバイスの登録を解除するには、Umbrella の設定を削除した後で Cisco Umbrella ダッシュボードからデバイスを削除します。
- FQDN ではなく IP アドレスを使用するすべての Web 要求では、Cisco Umbrella がバイパスされます。また、ローミング クライアントは、Umbrella がイネーブルになっているデバイスを通過せずに別の WAN 接続から DNS 解決を取得した場合、この DNS 解決を使用する接続で Cisco Umbrella をバイパスします。
- ユーザーに HTTP プロキシがある場合は、プロキシで DNS 解決を実行し Cisco Umbrella を通過しない可能性があります。
- NAT DNS46 および DNS64 はサポートされていません。IPv4 アドレスと IPv6 アドレスの間で DNS 要求を変換することはできません。
- EDNS レコードには、IPv4 と IPv6 の両方のホスト アドレスが含まれます。
- クライアントが HTTPS 経由で DNS を使用している場合、クラウド セキュリティ サービスでは DNS および HTTP/HTTPS トラフィックが検査されません。

Cisco Umbrella Connector の設定

クラウドで Cisco Umbrella と対話するようにデバイスを設定できます。システムは DNS ルックアップ要求を Cisco Umbrella にリダイレクトします。次に、クラウドベースのエンタープライズ セキュリティの完全修飾ドメイン名（FQDN）ポリシーを適用します。悪意のあるトラフィックまたは疑わしいトラフィックにおいては、ユーザーがサイトからブロックされるか、クラウドベースのポリシーに基づいて URL フィルタリングを実行するインテリジェント プロキシにリダイレクトされます。

次の手順では、Cisco Umbrella コネクタの設定におけるエンドツーエンドのプロセスについて説明します。

始める前に

マルチコンテキスト モードでは、Cisco Umbrella を使用する必要のある各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1 Cisco Umbrella のアカウント（https://umbrella.cisco.com）を確立します

ステップ 2 Cisco Umbrella 登録サーバーからの CA 証明書のインストール （122 ページ）。

デバイスの登録では HTTPS を使用します。これによりルート証明書をインストールするように要求されます。

ステップ 3 イネーブルになっていない場合は、DNS サーバーを設定してインターフェイス上で DNS ルックアップをイネーブルにします。

自分のサーバーを使用することも、Cisco Umbrella サーバーを設定することもできます。別のサーバーを設定する場合でも、DNS インスペクションによって Cisco Umbrella リゾルバへ自動的にリダイレクトされます。

- 208.67.220.220
- 208.67.222.222
- 2620:119:53::53
- 2620:119:35::35

例：

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220
```

ステップ 4 Umbrella Connector のグローバル設定 （123 ページ）。

ステップ 5 DNS インスペクション ポリシー マップでの Umbrella のイネーブル化 （125 ページ）。

ステップ 6 Umbrella の登録確認 （127 ページ）。

Cisco Umbrella 登録サーバーからの CA 証明書のインストール

Cisco Umbrella 登録サーバーとの間で HTTPS 接続を確立するために、ルート証明書をインポートする必要があります。システムは、デバイスを登録するときに、HTTPS 接続を使用します。Cisco Umbrella で、**[展開（Deployments）] > [構成（Configuration）] > [ルート証明書（Root Certificate）]** を選択し、証明書をダウンロードします。

始める前に

Umbrella が証明書を更新する場合は、新しい証明書をダウンロードする必要があります。ルート証明書も変更される場合があります。正しいルート証明書がアップロードされていることを確認します。

証明書を更新する場合は、Umbrella を無効化にしてから再度有効にする必要があります。これにより、システムは新しい証明書を取得し、Umbrella に正しく登録されます。

手順

ステップ 1 Cisco Umbrella 登録サーバーのトラストポイントを作成します。

crypto ca trustpoint *name*

トラストポイントには、最大 128 文字の任意の名前（ctx1 or または umbrella_server など）を使用できます。

例：

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)#
```

ステップ 2 これは、証明書を貼り付けて手動で登録することを示しています。

enrollment terminal

例：

```
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)#
```

ステップ 3 証明書をインポートします。

crypto ca authenticate *name*

この証明書で作成したトラストポイントの名前を入力します。指示に従い、base 64 でエンコードされた証明書を貼り付けます。貼り付ける証明書には、BEGIN CERTIFICATE 行および END CERTIFICATE 行を含めないでください。

```
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

Umbrella Connector のグローバル設定

Umbrella グローバル設定は、主に、Cisco Umbrella にデバイスを登録するために必要な API トークンを定義します。

グローバル設定が Umbrella を有効にするために十分ではありません。DNS インスペクション ポリシー マップでの Umbrella のイネーブル化 （125 ページ）の説明に従って、DNS インスペクション ポリシー マップでも Umbrella をイネーブルにする必要があります。

始める前に

- Cisco Umbrella ネットワーク デバイス ダッシュ ボード（https://login.umbrella.com/）にログインし、組織の従来のネットワークデバイスの API トークンを取得します。トークンは、16 進数の文字列、たとえば、AABBA59A0BDE1485C912AFE になります。従来のネットワークデバイスの API キーを Umbrella ダッシュボードから生成します。
- Cisco Umbrella 登録サーバーの証明書をインストールします。

手順

ステップ 1 Umbrella コンフィギュレーション モードを開始します。

umbrella-global

例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)#
```

ステップ 2 Cisco Umbrella への登録に必要な API トークンを設定します。

token *api-token*

例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

ステップ 3 （任意）DNS インスペクション ポリシー マップで DNScrypt をイネーブルにする場合は、必要に応じて証明書の検証に DNScrypt プロバイダーの公開キーを設定できます。キーを設定しない場合は、現在配布されているデフォルトの公開キーが検証に使用されます。

public-key *hex_key*

キーは 32 バイトの 16 進数値です。2 バイトごとにコロンで区切った ASCII の 16 進数値を入力します。キー長は 79 バイトです。このキーは Cisco Umbrella から取得します。

デフォルト キーは B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79 です。

デフォルトの公開キーの使用に戻すには、**no public-key** と入力します。設定したキーは、省略することも、コマンドの **no** バージョンに追加することもできます。

例：

```
ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

ステップ 4 （任意）アイドル タイムアウトを設定します。その時間が経過するまでサーバーからの応答がない場合、クライアントから Umbrella サーバーへの接続は削除されます。

timeout edns *hh:mm:ss*

タイムアウトは hours:minutes:seconds の形式で、0:0:0 ～ 1193:0:0 の範囲で指定できます。デフォルトは 0:02:00（2 分）です。

例：

```
ciscoasa(config-umbrella)# timeout edns 00:01:00
```

ステップ 5 （任意）Umbrella のバイパスに必要なローカル ドメイン名を設定します。

Cisco Umbrella をバイパスする必要のある DNS 要求でローカル ドメインを特定し、代わりに設定済みの DNS サーバーに直接移動することができます。たとえば、すべての内部接続が許可されることを想定して、内部 DNS サーバーで組織のドメイン名のすべての名前を解決できます。

ローカル ドメイン名を直接入力できます。必要に応じて名前を定義する正規表現を作成し、次に正規表現クラス マップを作成して次のコマンドで指定します。

local-domain-bypass {*regular_expression* | **regex class** *regex_classmap*}

例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

ステップ 6 （任意）使用する DNS 要求を解決する、デフォルト以外の Cisco Umbrella DNS サーバーのアドレスを設定します。

resolver {**ipv4** | **ipv6**} *ip_address*

コマンドを個別に入力して、デフォルト以外の Umbrella リゾルバの IPv4 および IPv6 アドレスを定義できます。

例：

```
ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222
ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

DNS インスペクション ポリシー マップでの Umbrella のイネーブル化

グローバル Umbrella 設定の構成は、デバイスの登録および DNS ルックアップ リダイレクトの有効化において十分ではありません。アクティブな DNS インスペクションの一部として Umbrella を追加する必要があります。

Umbrella を preset_dns_map DNS インスペクション ポリシーマップに追加して、グローバルにイネーブルにすることができます。

ただし、カスタマイズされた DNS インスペクションを使用して、異なるインスペクション ポリシー マップを異なるトラフィック クラスに適用する場合は、Umbrella をサービスを必要とするクラスごとにイネーブルにする必要があります。

次の手順では、Umbrella をグローバルに実装する方法について説明します。カスタマイズされた DNS ポリシー マップがある場合は、DNS インスペクション ポリシー マップの設定 （326 ページ） を参照してください。

手順

ステップ 1 preset_dns_map インスペクション ポリシーマップを編集し、パラメータ設定モードを入力します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)#
```

ステップ 2 Umbrella をイネーブルにし、必要に応じてデバイスに適用する Cisco Umbrella のポリシー名を指定します。

umbrella ［**tag** *umbrella_policy*］［**fail-open**］

タグは、Cisco Umbrella で定義されたポリシーの名前です。登録中に Cisco Umbrella によってデバイスにポリシーが割り当てられます（ポリシー名が存在する場合）。ポリシーを指定しない場合は、デフォルトの ACL が適用されます。

Umbrella DNS サーバーが使用できない場合に DNS 解決を動作させるには、**fail-open** キーワードを追加します。フェール オープンの状態で Cisco Umbrella DNS サーバーが使用できない場合は、このポリシー マップで Umbrella 自体がディセーブルになり、DNS 要求をシステム上に設定された他の DNS サーバー（存在する場合）に移動できるようになります。Umbrella DNS サーバーが再度使用可能になると、ポリシーマップはそれらの使用を再開します。このオプションが含まれていない場合、DNS 要求は到達不能の Umbrella リゾルバへ移動し続けるので、応答は取得されません。

例：

```
ciscoasa(config-pmap-p)# umbrella fail-open
```

ステップ 3 （任意）DNScrypt をイネーブルにしてデバイスと Cisco Umbrella 間の接続を暗号化します。

dnscrypt

DNScrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。DNScrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラスマップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。

例：

```
ciscoasa(config-pmap-p)# dnscrypt
```

例

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

Umbrella の登録確認

Umbrella のグローバル設定を実行し、DNS インスペクションで Umbrella をイネーブルにしたら、デバイスから Cisco Umbrella に接続して登録を行う必要があります。Cisco Umbrella にデバイス ID が指定されているかどうかを確認することで、登録が正常に完了したかどうかをチェックできます。

最初にサービス ポリシーの統計情報を確認し、Umbrella の登録回線を検出します。ここには、Cisco Umbrella によって適用されたポリシー（タグ）、接続の HTTP ステータスコード、およびデバイス ID が示されます。

HTTP ステータスは 200（成功）である必要があります。エラーコードは次を示しています：401 は API トークンが正しくないことを示し、409 はデバイスが Cisco Umbrella にすでに存在することを示しています。

Umbrella のリゾルバ回線では、リゾルバが無応答であることを示すことはできません。無応答の場合は、アクセス制御ポリシーでこれらの IP アドレスに対する DNS 通信が開いていることを確認します。これは一時的な状況の可能性もありますが、ルーティングの問題を示している場合もあります。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
        umbrella registration: mode: fail-open tag: default, status: 200 success,
device-id: 010a13b8fbdfc9aa
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
        Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
local-domain-bypass 10
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
```

```
DNScrypt: Certificate Update: completion 10, failure 1
```

また、実行コンフィギュレーション（ポリシーマップでのフィルタ処理）も確認できます。ポリシー マップの umbrella コマンドを更新して、デバイス ID を表示します。このコマンドをイネーブルにしても、デバイス ID を直接設定することはできません。次の例で、出力を編集して関連する情報を表示します。

```
ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
  umbrella device-id 010a3e5760fdd6d3
  no tcp-inspection
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
```

Umbrella Connector の例

次のトピックでは、Umbrella Connector の設定に関する例を示します。

例：グローバルDNSインスペクションポリシーでのUmbrellaのイネーブル化

次の例では、Umbrella をグローバルにイネーブルにする方法を示します。この設定では、デフォルトの公開キーを使用して DNScrypt をイネーブルにします。デフォルトの Cisco Umbrella エンタープライズ セキュリティ ポリシーを割り当てます。

（注） この例では、DigiCert グローバルルート G2 証明書を使用します。正しい証明書は時間の経過とともに変更されるため、Umbrella サイトで使用される最新のルート証明書をダウンロードしてください。ここに示す証明書は例にすぎません。

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
```

```
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUtluNJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapspUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
quit
...

Do you accept this certificate? [yes/no]: yes

...

% Certificate successfully imported
ciscoasa(config)#

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

例：カスタム インスペクション ポリシーを使用したインターフェイス上での Umbrella のイネーブル化

次に、特定のトラフィック クラスで Umbrella をイネーブルにする例を示します。Umbrella は DNS/UDP のトラフィックの内部インターフェイスでのみイネーブルになります。DNScrypt がイネーブルになっているため、トラフィック クラスに UDP/443 を追加する必要があります。「Mypolicy」（Cisco Umbrella で定義）という名前のエンタープライズ セキュリティ ポリシーが適用されます。

（注） この例では、DigiCert グローバルルート G2 証明書を使用します。正しい証明書は時間の経過とともに変更されるため、Umbrellaサイトで使用される最新のルート証明書をダウンロードしてください。ここに示す証明書は例にすぎません。

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUtluNJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapspUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
quit

...

Do you accept this certificate? [yes/no]: yes
...

% Certificate successfully imported
ciscoasa(config)#

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
ciscoasa(config-pmap-p)# dnscrypt

ciscoasa(config)# object-group service umbrella-service-object
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config-service-object-group)# service-object udp destination eq 443

ciscoasa(config)# access-list umbrella-acl extended permit
object-group umbrella-service-object any any

ciscoasa(config)# class-map dns-umbrella
ciscoasa(config-cmap)# match access-list umbrella-acl

ciscoasa(config)# policy-map inside-policy
ciscoasa(config-pmap)# class dns-umbrella
ciscoasa(config-pmap-c)# inspect dns umbrella-policy
```

```
ciscoasa(config)# service-policy inside-policy interface inside
```

例：Umbrella からの特定のホストまたはネットワークのグローバルな除外

特定のホストまたはネットワークを Umbrella で使用しないようにする必要があり、インターフェイスベースではなくグローバルを選択する場合は、グローバル DNS インスペクションを削除し、Umbrellaインスペクションを除外または含めるための個別のクラスを作成できます。

次に、192.168.1.0/24 のネットワークを Umbrella で使用しないようにグローバル インスペクション ポリシーを変更する例を示します。

始める前に

この例では、すでに Domain Name System（DNS）を有効にしており、Umbrella グローバル設定を行っていることを前提としています。

手順

ステップ 1 グローバルデフォルト DNS インスペクションを削除します。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect dns
```

ステップ 2 Umbrella を有効にする DNS ポリシーマップを作成します。

この例では、ポリシーマップの名前は umbrella-policy です。

```
ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
```

ステップ 3 除外されたトラフィックのトラフィッククラスを作成します。

次に、ACL を使用して、192.168.1.0/24 のネットワークからの UDP/53 トラフィックを識別する例を示します。

```
ciscoasa(config)# access-list Umb_Exclude permit udp 192.168.1.0 255.255.255.0 any eq
53
ciscoasa(config)# class-map Umbrella_Exclude
ciscoasa(config-cmap)# match access-list Umb_Exclude
```

ステップ 4 Umbrella を使用する必要があるホストのトラフィッククラスを作成します。

次の例では、任意の送信元からの UDP/53 トラフィックを照合します。

```
ciscoasa(config)# class-map Umbrella_Include
ciscoasa(config-cmap)# match port udp eq 53
```

ステップ 5 グローバル インスペクション ポリシーを更新し、適切な DNS ポリシーマップを使用して、トラフィック クラスの DNS インスペクションを有効にします。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)#  class Umbrella_Exclude
ciscoasa(config-pmap-c)# inspect dns
ciscoasa(config-pmap)#  class Umbrella_Include
ciscoasa(config-pmap-c)# inspect dns umbrella-policy
```

Umbrella Connector のモニタリング

ここでは、Umbrella Connector をモニターする方法について説明します。

Umbrella サービス ポリシーの統計情報のモニタリング

Umbrella をイネーブルにすると、DNS インスペクションの統計情報の概要と詳細を両方表示できます。

show service-policy inspect dns ［**detail**］

detail キーワードを使用しないと、すべての基本的な DNS インスペクション カウンタと Umbrella の設定情報が表示されます。ステータス フィールドに、システムで Cisco Umbrella への登録を試行するための HTTP ステータス コードを指定します。

リゾルバ回線は、使用中の Umbrella サーバーを示します。これらの回線によって、サーバーが**応答なし**かどうか、または現在サーバーが使用可能かどうかを判断するためにシステムでサーバーを**プローブ中**かどうかがわかります。フェール オープン モードの場合、システムで DNS 要求が許可され他の DNS サーバー（設定されている場合）に移動します。それ以外のモードの場合、Umbrella サーバーが無応答の間は DNS 要求で応答を取得できません。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
        umbrella registration: mode: fail-open tag: default, status: 200 success,
device-id: 010a13b8fbdfc9aa
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
        Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
local-domain-bypass 10
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

詳細な出力では、DNScrypt 統計情報と使用されるキーが表示されます。

```
asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: dnscrypt30000
      Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
               5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 1500, drop 0
        dns-guard, count 3
        protocol-enforcement, drop 0
        nat-rewrite, count 0
        Umbrella registration: mode: fail-open tag: default, status: 200 SUCCESS,
device-id: 010af97abf89abc3, retry 0
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
        Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6
local-domain-bypass 10
          Umbrella app-id fail, count 0
          Umbrella flow alloc fail, count 0
          Umbrella block alloc fail, count 0
          Umbrella client flow expired, count 0
          Umbrella server flow expired, count 0
          Umbrella request drop, count 0
          Umbrella response drop, count 0
        DNScrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
        DNScrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
          DNScrypt length error, count 0
          DNScrypt add padding error, count 0
          DNScrypt encryption error, count 0
          DNScrypt magic_mismatch error, count 0
          DNScrypt disabled, count 0
          DNScrypt flow error, count 0
          DNScrypt nonce error, count 0
        DNScrypt: Certificate Update: completion 1, failure 1
          DNScrypt Receive internal drop count 0
          DNScrypt Receive on wrong channel drop count 0
          DNScrypt Receive cannot queue drop count 0
          DNScrypt No memory to create channel count 0
          DNScrypt Send no output interface count 1
          DNScrypt Send open channel failed count 0
          DNScrypt Send no handle count 0
          DNScrypt Send dupb failure count 0
          DNScrypt Create cert update no memory count 0
          DNScrypt Store cert no memory count 0
          DNScrypt Certificate invalid length count 0
          DNScrypt Certificate invalid magic count 0
          DNScrypt Certificate invalid major version count 0
          DNScrypt Certificate invalid minor version count 0
          DNScrypt Certificate invalid signature count 0
          Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
          Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
          Query Magic 0x714e7a696d657555, Serial Number 1517943461,
          Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
          End Time 1549479461 (18:57:41 UTC Feb 6 2019)
          Server Public Key
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
          Client Secret Key Hash
48DD:E6D3:C058:D063:1098:C6B4:BA6F:D8A7:F0F8:0754:40B0:AFB3:CB31:2B22:A7A4:9CEE
          Client Public key
6CB9:FA4B:4273:E10A:8A67:BA66:76A3:BFF5:2FB9:5004:CD3B:B3F2:86C1:A7EC:A0B6:1A58
```

```
        NM key Hash
9182:9F42:6C01:003C:9939:7741:1734:D199:22DF:511E:E8C9:206B:D0A3:8181:CE57:8020
```

Umbrella の syslog メッセージのモニタリング

次の Umbrella 関連の syslog メッセージをモニターできます。

- 「%ASA-3-339001: DNSCRYPT certificate update failed for *number* tries.」

  Umbrellaサーバーへのルートが存在すること、および出力インターフェイスが表示され正常に機能していることを確認してください。また、DNScrypt 用に設定された公開キーが正しいことも確認してください。Cisco Umbrella から新しいキーを取得する必要が生じる場合があります。

- 「%ASA-3-339002: Umbrella device registration failed with error code *error_code*.」

  各エラー コードの内容は、次のとおりです。

  - 400：要求の形式またはコンテンツに問題があります。トークンが短すぎるか、破損している可能性があります。トークンがUmbrellaダッシュボードのトークンと一致していることを確認してください。
  - 401：API トークンが承認されていません。トークンを再設定してください。Umbrellaダッシュボードのトークンを更新する場合は、必ず新しいトークンを使用してください。
  - 409：デバイス ID が別の組織と競合しています。問題の内容について Umbrella 管理者に確認してください。
  - 500：内部サーバー エラー。問題の内容について Umbrella 管理者に確認してください。

- 「%ASA-6-339003: Umbrella device registration was successful.」
- 「%ASA-3-339004: Umbrella device registration failed due to missing token.」

  Cisco Umbrella から API トークンを取得し、Umbrella のグローバル設定で設定する必要があります。

- 「%ASA-3-339005: Umbrella device registration failed after *number* retries.」

  syslog 339002 メッセージを確認し、修正する必要のあるエラーを特定します。

- 「%ASA-3-339006: Umbrella resolver *IP_address* is reachable, resuming Umbrella redirect.」

  このメッセージは、システムが再度正常に機能していることを示します。そのため、対処は必要ありません。

- 「%ASA-3-339007: Umbrella resolver *IP_address* is unresponsive and fail-close mode used, starting probe to resolver.」

  フェール クローズ モードを使用しているため、Umbrella DNS サーバーがオンラインに戻るまで DNS 要求に対する応答を取得できません。問題が解決しない場合は、システムか

らUmbrellaサーバーへのルートが存在すること、およびアクセス制御ポリシーでサーバーへの DNS トラフィックが許可されていることを確認してください。

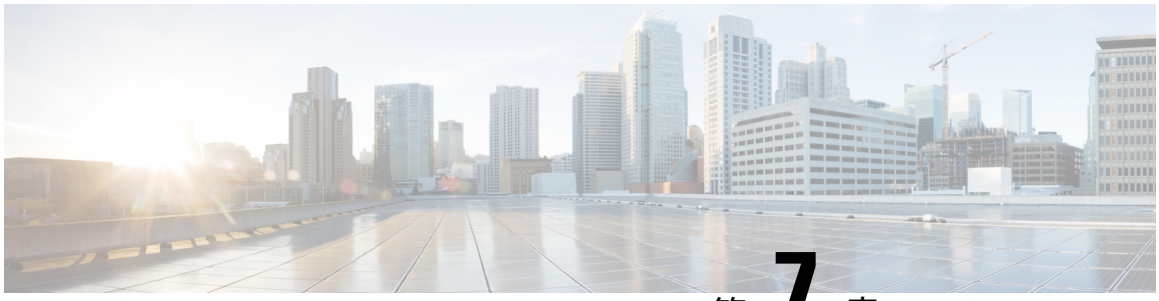
Cisco Umbrella Connector の履歴

機能名	プラットフォームリリース	説明
Cisco Umbrella サポート。	9.10(1)	Cisco Umbrella で定義されている エンタープライズ セキュリティ ポリシーをユーザー接続に適用できるように DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。FQDNに基づいて接続を許可またはブロックできます。または、疑わしいFQDNの場合はCisco Umbrellaインテリジェント プロキシにユーザーをリダイレクトして URL フィルタリングを実行できます。Umbrellaの設定は、DNSインスペクション ポリシーに含まれています。 **umbrella**、**umbrella-global**、**token**、**public-key**、**timeout edns**、**dnscrypt**、**show service-policy inspect dns detail** の各コマンドが追加または変更されました。
Cisco Umbrella の強化	9.12(1)	Cisco Umbrella をバイパスする必要があるローカル ドメイン名を特定できるようになりました。これらのドメインの DNS 要求は、Umbrellaを処理せずDNSサーバーに直接送信されます。また、DNS 要求の解決に使用する Umbrella サーバーも特定できるようになりました。さらに、Umbrellaサーバーを使用できない場合は、DNS 要求がブロックされないように、Umbrella インスペクション ポリシーをフェール オープンに定義することができます。 **local-domain-bypass**、**resolver**、**umbrella fail-open** の各コマンドが追加または変更されました。

第 II 部

仮想環境のファイアウォール サービス

- 属性ベースのアクセス制御 （139 ページ）



第 7 章

属性ベースのアクセス制御

属性は設定で使用するカスタマイズされたネットワーク オブジェクトです。Cisco ASA 設定で、VMware vCenter の管理対象 VMware ESXi 環境の 1 つ以上の仮想マシンに関連付けられるトラフィックをフィルタリングするために、属性を定義し使用できます。属性により、1 つ以上の属性を共有する仮想マシンのグループからのトラフィックにポリシーを割り当てるアクセス コントロール リスト（ACL）を定義することができます。ESXi 環境内の仮想マシンに属性を割り当て、HTTPS を使用して vCenter または 1 つの ESXi ホストに接続する、属性エージェントを設定します。エージェントは、仮想マシンのプライマリ IP アドレスに特定の属性に関連する 1 つ以上のバインディングを要求および取得します。

属性ベースのアクセス制御は、すべてのハードウェア プラットフォームと、ESXi、KVM または HyperV ハイパーバイザで動作するすべてASA 仮想のプラットフォームでサポートされます。属性は、ESXi ハイパーバイザ上で動作する仮想マシンからのみ取得できます。

- 属性ベースのネットワーク オブジェクトのガイドライン （139 ページ）
- 属性ベースのアクセス制御の設定 （140 ページ）
- 属性ベースのネットワーク オブジェクトのモニタリング （148 ページ）
- 属性ベースのアクセス制御の履歴 （149 ページ）

属性ベースのネットワークオブジェクトのガイドライン

IPv6 のガイドライン

- IPv6 アドレスは、vCenter では、ホストのクレデンシャルとしてサポートされていません。
- IPv6 は、仮想マシンのプライマリ IP アドレスが IPv6 アドレスである仮想マシンのバインドでサポートされます。

その他のガイドラインと制限事項

- マルチ コンテキスト モードはサポートされません。属性ベースのネットワーク オブジェクトは、シングルモード コンテキストでのみサポートされます。

- 属性ベースのネットワーク オブジェクトは、仮想マシンのプライマリ アドレスへのバインドのみをサポートします。単一の仮想マシン上の複数の vNIC へのバインドはサポートされません。
- 属性ベースのネットワーク オブジェクトは、アクセス グループに使用するオブジェクトにのみ設定できます。その他の機能（NAT など）のためのネットワーク オブジェクトはサポートされません。
- vCenter にプライマリ IP アドレスを報告するためには、仮想マシンが VMware ツールを実行している必要があります。属性の変更は、vCenter が仮想マシンの IP アドレスを知っている場合でないと、ASA には通知されません。これは、vCenter の制約事項です。
- 属性ベースのネットワーク オブジェクトは、Amazon Web Services（AWS）または Microsoft Azure のパブリック クラウド環境ではサポートされません。

属性ベースのアクセス制御の設定

次の手順は、VMware ESXi 環境内の管理対象の仮想マシン上で属性ベースのアクセス制御を実行するための一般的な流れを説明します。

手順

ステップ 1 管理対象の仮想マシンにカスタムの属性タイプと値を割り当てます。vCenter 仮想マシンの属性の設定 （140 ページ）を参照してください。

ステップ 2 vCenter サーバーまたは ESXi ホストに接続するための属性エージェントを設定します。VM 属性エージェントの設定 （142 ページ）を参照してください。

ステップ 3 展開スキームに必要な属性ベースのネットワーク オブジェクトを設定します。属性ベースのネットワーク オブジェクトの設定 （144 ページ）を参照してください。

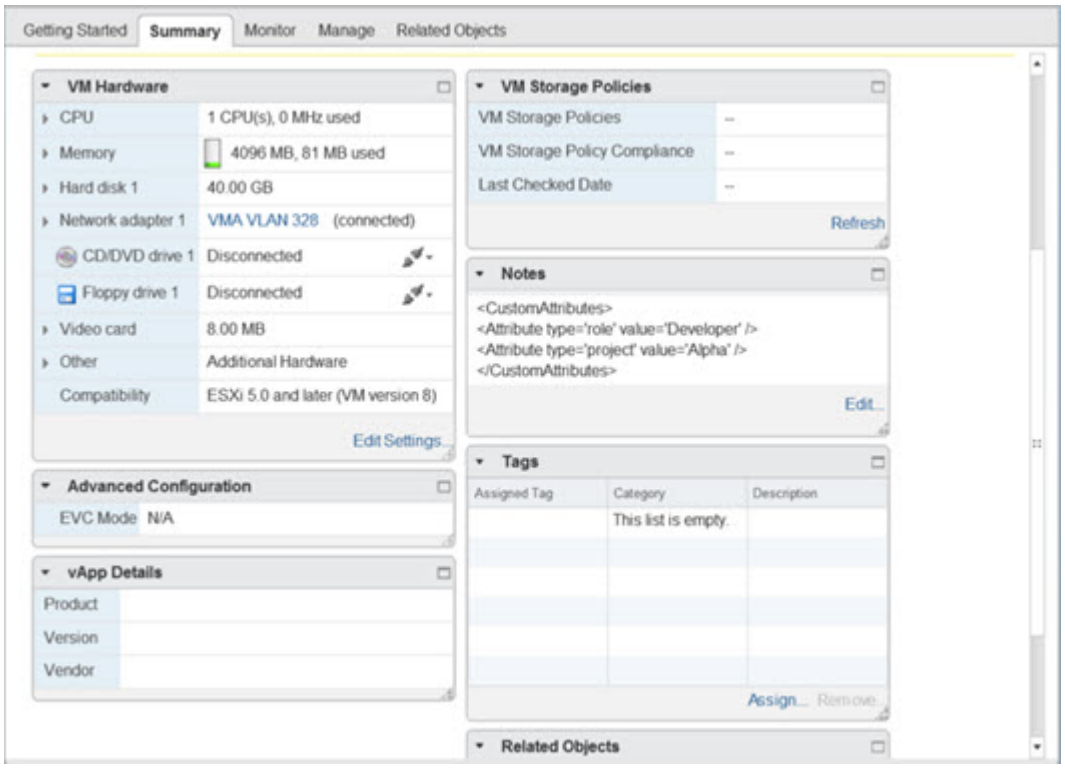
ステップ 4 アクセス コントロール リストとルールを設定します。属性ベースのネットワーク オブジェクトを使用したアクセス制御の設定 （146 ページ）を参照してください。

vCenter 仮想マシンの属性の設定

仮想マシンにカスタムの属性タイプと値を割り当て、それらの属性をネットワーク オブジェクトに関連付けます。すると、これらの属性ベースのネットワーク オブジェクトを使用して、共通のユーザー定義の特徴を持つ一連の仮想マシンに ACL を適用することができます。たとえば、開発者が構築したマシンをテストマシンから隔離したり、仮想マシンをプロジェクトおよび/または場所でグループ化したりすることができます。ASA が属性を使用して仮想マシンをモニターできるようにするには、vCenter が管理対象の仮想マシンから属性を取得できるようにする必要があります。そうするには、vCenter の仮想マシンの [Summary] ページにある [Notes] フィールドにフォーマットされたテキスト ファイルを挿入します。

[Notes] フィールドについては、次の図を参照してください。

図 *6 : vCenter* の仮想マシンの *[Summary]* タブ



カスタム属性を指定するには、適切にフォーマットした XML ファイルを仮想マシンの [Notes] フィールドにコピーします。ファイルの形式は次のとおりです。

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

上記の 2 行目を繰り返すと、単一の仮想マシンに複数の属性を定義することができます。各行には、一意の属性タイプを 1 つしか指定できないことに注意が必要です。同じ属性タイプを複数の属性値で定義すると、その都度、当該の属性タイプのバインドアップデートにより、その前の値が上書きされます。

文字列の属性値については、オブジェクト定義に関連付けられている値は、仮想マシンから vCenter に報告される値と完全に一致している必要があります。たとえば、属性値 *Build Machine* は、仮想マシンのアノテーション値である *build machine* には一致しません。この属性については、host-map にバインドが追加されることはありません。

1 つのファイルで固有の属性タイプを複数定義することができます。

手順

ステップ 1 vCenter インベントリから仮想マシンを選択します。

ステップ 2 その仮想マシンの [Summary] タブをクリックします。

ステップ 3 [Notes] フィールドで、[Edit] リンクをクリックします。

ステップ 4 [Edit Notes] ボックスにカスタム属性のテキスト ファイルを貼り付けます。テキスト ファイルは、XML テンプレートのフォーマットに従っている必要があります。

例：

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

ステップ 5 [OK] をクリックします。

例

次の例は、「role」および「project」に対してカスタム属性を定義する、仮想マシンへの適用が可能な適切にフォーマットされた XML テキスト ファイルを示します。

```
<CustomAttributes>
<Attribute type='role' value='Developer'/>
<Attribute type='project' value='Alpha'/>
</CustomAttributes>
```

VM 属性エージェントの設定

vCenter または単一の ESXi ホストと通信するため、VM の属性のエージェントを設定します。VMware 環境内の仮想マシンに属性が割り当てられると、属性エージェントは、どの属性が設定されたかを示すメッセージを vCenter に送信し、vCenter は、一致する属性タイプが設定されているすべての仮想マシンに関するバインド アップデートで応答します。

VM 属性エージェントと vCenter は、バインド アップデートの交換を次のように行います。

- エージェントが新しい属性タイプを含むリクエストを発行すると、vCenter は、その属性タイプが設定されているすべての仮想マシンに関するバインド アップデートで応答します。これ以降、属性値が追加または変更されると、vCenter のみが新しいバインドを発行します。
- モニター対象の属性が 1 つ以上の仮想マシン上で変更されると、バインド アップデート メッセージが受信されます。各バインド メッセージは、属性値を報告する仮想マシンの IP アドレスによって識別されます。

- 複数の属性が 1 つのエージェントによってモニターされている場合、1 件のバインドアップデートに各仮想マシンのすべてのモニター対象属性の現在の値が含まれます。
- エージェントによってモニターされている特定の属性が、ある仮想マシンには設定されていない場合、その仮想マシンについては、バインドには空の属性値が含まれます。
- ある仮想マシンにモニター対象の属性がまったく設定されていない場合、vCenter はバインドアップデートを送信しません。

各属性エージェントは、1 つの vCenter または ESXi ホストとだけ通信します。1 つの ASA には複数の属性エージェントを定義でき、それぞれを異なる vCenter と通信させるか、または複数の属性エージェントを同じ vCenter と通信させることができます。

手順

ステップ 1 vCenter と通信するための VM 属性エージェントを作成します。**attribute source-group** *agent-name* **type** *agent-type*

例：

```
hostname(config)# attribute source-group VMAgent type esxi
```

agent-name 引数は、VM 属性エージェントの名前を指定します。*type* 引数は、属性エージェントのタイプです。

（注） 現在、サポートされるエージェント タイプは ESXi のみです。

ステップ 2 vCenter ホスト クレデンシャルを設定します。**host** *ip-address* **username** *ESXi-username* **password** *ESXi-password*

例：

```
hostname(config-attr)# host 10.122.202.217 user admin password Cisco123
```

ステップ 3 vCenter 通信のキープアライブ設定を設定します：**keepalive retry-interval** *interval* **retry-count** *count*

例：

```
hostname(config-attr)# keepalive retry-timer 10 retry-count 3
```

デフォルトのキープアライブ タイマー値は、30 秒間隔での再試行 3 回です。

ステップ 4 VM 属性エージェント設定を確認します。**show attribute source-group** *agent-name*

例：

```
hostname(config-attr)# sh attribute source-group VMAgent

   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Inactive
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
```

[Agent State] は、ネットワーク オブジェクトを設定し、そのオブジェクトと関連付けするための属性を指定するまでアクティブになりません。

ステップ 5 属性コンフィギュレーション モードを終了します。 **exit**

例：

```
hostname(config-attr)# exit
```

属性ベースのネットワーク オブジェクトの設定

属性ベースのネットワーク オブジェクトは、VMware ESXi 環境内の 1 つ以上の仮想マシンに関連付けられている属性に応じてトラフィックをフィルタリングします。アクセス コントロール リスト（ACL）を定義すれば、1 つ以上の属性を共有する仮想マシン グループからのトラフィックにポリシーを指定できます。

たとえば、*engineering* 属性を持つマシンに対して *eng_lab* 属性を持つマシンへのアクセスを許可するアクセス ルールを設定できます。ネットワーク管理者がエンジニアリング マシンとラボ サーバーを追加・削除できる一方で、セキュリティ管理者によって管理されるセキュリティ ポリシーは、アクセス ルールを手動で更新しなくても自動的に適用され続けます。

手順

ステップ 1 オブジェクト グループの検索を有効にします。 **object-group-search access-control**

例：

```
hostname(config)# object-group-search access-control
```

属性ベースのネットワーク オブジェクトを設定するには、object-group-search を有効にする必要があります。

ステップ 2 オブジェクト名を使用して、属性ベースのネットワーク オブジェクトを作成または編集します。**object network** *object-id*

例：

```
hostname(config)# object network dev
```

ステップ 3 オブジェクトに関連付けるエージェント、属性タイプ、および属性値を指定します。**attribute** *agent-name attribute-type attribute-value*

例：

```
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

agent-name は、VM 属性エージェントを指定します。<XREF> を参照してください。設定されていない属性エージェントを使用するように属性ベースのネットワーク オブジェクトを設定した場合、クレデンシャルがなく、デフォルトのキープアライブ値を持つプレースホルダ エージェントが自動的に作成されます。このエージェントは、**host** サブコマンドを使用してホスト クレデンシャルが与えられるまで、「クレデンシャル使用不可」の状態が続きます。

また、*attribute-type* と *attribute-value* のペアは、一意の属性を定義します。*attribute-type* は任意の文字列で、**custom.** というプレフィックスが含まれている必要があります。同じ属性タイプを複数の属性値で複数回定義すると、最後に定義された値でその前の値が上書きされます。

例

次の例では、開発者グループを表し、「Developer」というロールを持つ属性ベースのネットワーク オブジェクト、*dev* を作成しています。VM 属性エージェントは vCenter と通信し、*custom.role* という属性に一致するすべての仮想マシンにバインドを返します。

```
hostname(config)# object network dev
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

次の例では、テスト グループを表し、「Automation」というロールを持つ属性ベースのネットワーク オブジェクト、*test* を作成しています。VM 属性エージェントは vCenter と通信し、*custom.role* という属性に一致するすべての仮想マシンのバインドを返します。これは、前述の例と同じ仮想マシンのリストであることに注意してください。

```
hostname(config)# object network test
hostname(config-network-object)# attribute VMAgent custom.role Automation
```

次の例では、プロジェクト グループを表し、「Alpha」というロールを持つ属性ベースのネットワーク オブジェクト、*project* を作成しています。VM 属性エージェントは vCenter と通信し、*custom.project* という属性に一致するすべての仮想マシンのバインドを返します。一部のマシンに複数の属性が重複していることに注意してください。

```
hostname(config)# object network project
```

```
hostname(config-network-object)# attribute VMAgent custom.project Alpha
```

次の例は、アクティブな状態で属性リクエストが保留中の VM 属性エージェントを示します。

```
hostname(config-attr)# show attribute source-group VMAgent

   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attribute requests pending:
       'custom.project'
       'custom.role'
```

属性ベースのネットワークオブジェクトを使用したアクセス制御の設定

属性ベースのネットワーク オブジェクトは、1つ以上の属性を共有する仮想マシンのグループからのトラフィックに対してアクセス コントロール リスト（ACL）を定義するときに使用できます。アクセス リストは、1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。ACE はアクセス リストの単一エントリで、ルールの許可または拒否（パケットの転送またはドロップ）を指定します。通常、許可または拒否ルールの適用対象は、プロトコル、送信元および宛先の IP アドレスまたはネットワークで、必要に応じて送信元および宛先ポートに適用されます。

属性ベースのネットワーク オブジェクトを使用すると、送信元または宛先の IP アドレスをこれらのオブジェクトに置き換えることができます。仮想マシンが導入、移動、または廃止されると、仮想マシン上の属性は更新されますが、割り当てられたアクセス制御ポリシーは、設定を変更しなくても効果を継続できます。

ACL に使用可能なすべてのオプションについては、ACL の設定 （40 ページ）を参照してください。

手順

ステップ 1 属性ベースのネットワーク オブジェクトを使用して、拡張 ACL エントリ（ACE）を作成および設定します。**access-list** *access_list_name* **extended** {**deny | permit**} *protocol_argument* **object** *source_object_name* **object** *dest_object_name*

例：

```
hostname(config)# access-list lab-access extended permit ip object dev object test
```

（注） ポリシーに必要なだけ繰り返します。

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- プロトコル：*protocol_argument* では、IP プロトコルを指定します。
  - *name* または *number*：プロトコルの名前または番号を指定します。**ip** を指定すると、すべてのプロトコルに適用されます。
  - **object-group** *protocol_grp_id*：**object-group protocol** コマンドを使用して作成されたプロトコル オブジェクト グループを指定します。
- 送信元オブジェクト：**object** には、**object network** コマンドを使用して作成された属性ベースのネットワーク オブジェクトを指定します。*source_object_name* には、パケットの送信元オブジェクトを指定します。
- 宛先オブジェクト：**object** には、**object network** コマンドを使用して作成された属性ベースのネットワーク オブジェクトを指定します。*dest_object_name* には、パケットの送信先オブジェクトを指定します。

ステップ 2 ACL を 1 つのインターフェイスにバインドするか、グローバルに適用します。**access-group** *access_list_name* {**in interface** *interface_name* | **global**}

例：

```
hostname(config)# access-group lab-access in interface inside
```

インターフェイス固有のアクセス グループの場合は、次の手順を実行します。

- 拡張 ACL 名を指定します。インターフェイスごとの ACL タイプごとに 1 つの **access-group** コマンドを設定できます。
- **in** キーワードによって、ACL が着信トラフィックに適用されます。
- **interface** 名を指定します。

グローバル アクセス グループの場合は、global キーワードを指定して、すべてのインターフェイスの着信方向に拡張 ACL を適用します。

例

次の例では、属性ベースの拡張 ACL をグローバルに適用する方法を示します。

```
hostname(config)# access-list lab-access extended permit ip object dev object test
hostname(config)# access-group lab-access global
hostname(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list lab-access; 1 elements; name hash: 0x62b4790b
access-list lab-access line 1 extended permit ip object dev object test (hitcnt=0)
0x64a1be76
  access-list lab-access line 1 extended permit ip object dev(2) object test(3) (hitcnt=0)
 0x64a1be76
```

属性ベースのネットワーク オブジェクトのモニタリング

属性ベースのネットワーク オブジェクトをモニターするには、次のコマンドを入力します。

- **show attribute host-map**

  指定された属性のエージェント、タイプ、および値に関する属性バインドを表示します。

- **show attribute object-map**

  object-to-attribute バインドを表示します。

- **show attribute source-group**

  設定された VM 属性エージェントが表示されます。

例

次に、host-to-attribute バインドのマップの例を示します。

```
hostname# show attribute host-map /all
IP Address-Attribute Bindings Information

         Source/Attribute                        Value
=======================================================================
VMAgent.custom.project                         'Alpha'
     10.15.28.34
     10.15.28.32
     10.15.28.31
     10.15.28.33
VMAgent.custom.role                            'Automation'
     10.15.27.133
     10.15.27.135
     10.15.27.134
VMAgent.custom.role                            'Developer'
     10.15.28.34
     10.15.28.12
```

```
     10.15.28.31
     10.15.28.13
```

次に、object-to-attribute バインドのマップの例を示します。

```
hostname# show attribute object-map /all
Network Object-Attribute Bindings Information

Object
         Source/Attribute                          Value
================================================================================
dev
     VMAgent.custom.role                           'Developer'
test
     VMAgent.custom.role                           'Automation'
project
     VMAgent.custom.project                        'Alpha'
```

次に、属性エージェントの設定例を示します。

```
hostname# show attribute source-group
   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attributes being monitored:
      'custom.role' (2)
```

属性ベースのアクセス制御の履歴

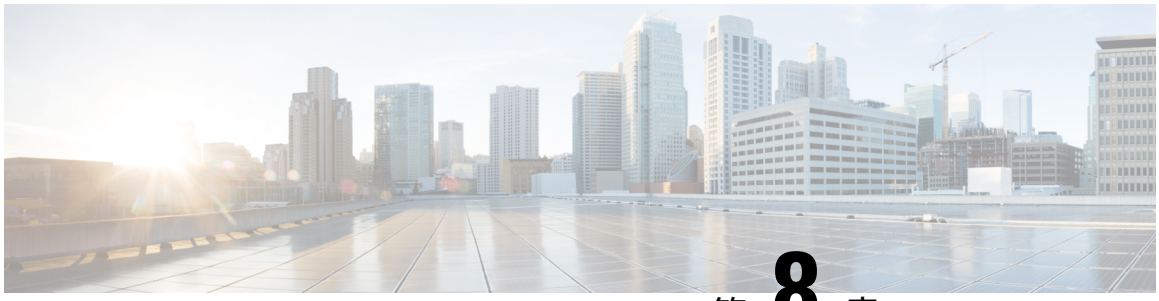
機能名	プラットフォームリリース	説明
属性ベースのネットワーク オブジェクトのサポート	9.7.(1)	現在、ネットワーク アクセスの制御には、IP アドレス、プロトコル、ポートなどの従来のネットワーク特性に加え、仮想マシンの属性も使用することができます。仮想マシンは、VMware ESXi 環境に存在している必要があります。 次のコマンドを導入しました。 **object network** *attribute* **attribute** *agent-name attribute-type attribute-value* **attribute source-group** *agent-name* **type** *agent-type* **host** *ip-address* **username** *ESXi-username* **password** *ESXi-password* **keepalive retry-interval** *interval* **retry-count** *count*

機能名	プラットフォームリリース	説明
ASA 5506-X（全モデル）、5508-X、5512-X、5516-X から VM 属性ベースのネットワーク オブジェクトのサポートを除外します。	9.10(1)	ASA 5506-X（全モデル）、5508-X、5512-X、5516-X プラットフォームでは、VM 属性ベースのオブジェクトが使用できなくなりました。

第 III 部

ネットワーク アドレス変換

- Network Address Translation（NAT） （153 ページ）
- NAT の例と参照 （221 ページ）
- アドレスとポートのマッピング（MAP） （259 ページ）



第 8 章

Network Address Translation（NAT）

ここでは、ネットワーク アドレス変換（NAT）とその設定方法について説明します。

- NAT の機能 （153 ページ）
- NAT の基本 （154 ページ）
- NAT のガイドライン （160 ページ）
- ダイナミック NAT （170 ページ）
- ダイナミック PAT （178 ページ）
- スタティック NAT （193 ページ）
- アイデンティティ NAT （205 ページ）
- NAT のモニタリング （210 ページ）
- NAT の履歴 （211 ページ）

NAT の機能

NAT では、プライベート IP アドレスをパブリック IP アドレスに置き換えることにより、プライベート IP ネットワークがインターネットに接続できるようにします。NAT は、ネットワーク全体に対して1つのパブリックアドレスだけを外部に最小限にアドバタイズすることでパブリックアドレスを節約します。

プライベート IP アドレスの範囲

IP ネットワーク内のほとんどのデバイスには、プライベート IP アドレスが割り当てられます。このようなデバイスは、パブリック IPv4 アドレスが不足しているため、企業ネットワーク外にルーティングできません。RFC 1918 では、外部にアドバタイズされないプライベート IP アドレス範囲が定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP アドレスを合法的でルーティング可能なパブリックアドレスに変換し、プライベート IP ネットワークがインターネットにアクセスできるようにすることです。このアプローチでは、ネットワーク全体に対して単一のパブリックアドレスのみをアドバタイズするように NAT を設定できるため、パブリック IP アドレスが節約されます。

NAT の他の機能には、次のおりです。

- セキュリティ：内部 IP アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティングソリューション：重複する IP アドレスを競合なく処理します。
- 柔軟性：外部から見えるパブリックアドレスに影響を与えずに、内部 IP アドレッシング方式を変更できます。
- IPv4 と IPv6 間の変換（ルーテッドモードのみ）：IPv4 と IPv6 間の変換をサポートし、異なるネットワークタイプ間の相互運用を可能にします。

（注） NAT はオプションです。特定の通信に NAT が設定されていない場合、その通信は変換されませんが、通常のセキュリティポリシーの対象になります。

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけでなく、デバイスに接続されている任意のネットワークに変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピングアドレス/ホスト/ネットワーク/インターフェイス：マッピングアドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。

（注） アドレスの変換中、デバイス インターフェイスに設定された IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、双方向に接続を開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。
- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

NAT タイプ

NAT は、次の方法を使用して実装できます。

- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけが通信を開始できます。ダイナミック NAT （170 ページ）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。ダイナミック PAT （178 ページ）を参照してください。
- スタティック NAT：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向に通信を開始できます。スタティック NAT （193 ページ）を参照してください。
- アイデンティティ NAT：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。アイデンティティ NAT （205 ページ） を参照してください。

ネットワークオブジェクト NAT および twice NAT

Network Object NAT および *twice NAT* という 2 種類の方法でアドレス変換を実装できます。

twice NAT が提供する追加機能を必要としない場合は、Network Object NAT を使用することをお勧めします。Network Object NAT は設定が容易で、Voice over IP（VoIP）などのアプリケーションでは信頼性が高い場合があります。（VoIP では、ルールで使用されているオブジェクトのいずれにも属さない間接アドレスの変換が失敗することがあります）。

ネットワークオブジェクト NAT

ネットワーク オブジェクトのパラメータとして設定されているすべてのNATルールは、*Network Object NAT* ルールと見なされます。これは、ネットワーク オブジェクトに NAT を設定するための迅速かつ簡単な方法です。しかし、グループ オブジェクトに対してこれらのルールを作成することはできません。

ネットワークオブジェクトを設定すると、そのオブジェクトのマッピングアドレスをインラインアドレスとして、または別のネットワークオブジェクトやネットワーク オブジェクト グループとして識別できるようになります。

パケットがインターフェイスに入ると、送信元IPアドレスと宛先IPアドレスの両方がNetwork ObjectNATルールと照合されます。個別の照合が行われる場合、パケット内の送信元アドレスと宛先アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないので、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、twice NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

twice NAT

twice NAT では、1 つのルールで送信元アドレスと宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポートアドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnetサーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

ネットワークオブジェクト NAT と twice NAT の比較

自動 NAT と手動 NAT の主な違いは、次のとおりです。

- 実アドレスの定義方法。
  - ネットワーク オブジェクト NAT：ネットワーク オブジェクトのパラメータとして NATを定義します。ネットワーク オブジェクトは、IPホスト、範囲、またはサブネットの名前を指定するため、実際の IP アドレスではなく、NAT コンフィギュレーショ

ン内のオブジェクトを使用できます。ネットワーク オブジェクトの IP アドレスは、実アドレスとして機能します。この方法では、設定の他の部分ですでに使用されているものであっても、ネットワーク オブジェクトに簡単に NAT を追加できます。

- twice NAT：実際のアドレスとマッピングアドレスの両方のネットワークオブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT 設定のパラメータとなります。実際のアドレスのネットワーク オブジェクト グループを使用できることは、twice NAT がよりスケーラブルであることを意味します。

- 送信元および宛先 NAT の実装方法。
  - ネットワークオブジェクト NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような 2 つのルールを 1 つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
  - twice NAT：1 つのルールにより送信元と宛先の両方が変換されます。1 つのパケットは 1 つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは、1 つの twice NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるため、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、送信元 A/宛先 A のペアには、送信元 A/宛先 B のペアとは異なる変換を適用できます。

- NAT ルールの順序。
  - ネットワークオブジェクト NAT：NAT テーブルで自動的に順序付けされます。
  - twice NAT：NAT テーブルで手動で順序付けします（Network Object NAT ルールの前または後）。

NAT ルールの順序

ネットワークオブジェクト NAT および twice NAT ルールは、3 つのセクションに分割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

（注） セクション 0 もあり、このセクションには、システムが使用するために作成される NAT ルールが含まれています。これらのルールは、他のすべてのルールよりも優先されます。これらのルールはシステムで自動的に作成され、必要に応じて xlate がクリアされます。セクション 0 では、ルールの追加、編集、または変更はできません。

表 *7: NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	twice NAT	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、twice NAT ルールはセクション 1 に追加されます。 「固有のルールを前に」とは、次のことを意味します。 • 静的ルールは動的ルールの前に配置する必要があります。 • 宛先変換を含むルールは、送信元変換のみのルールの前に配置する必要があります。 送信元アドレスまたは宛先アドレスに基づいて複数のルールが適用される可能性がある重複するルールを排除できない場合は、これらの推奨事項に従うように特に注意してください。 上記の推奨事項に従わない場合は、マッピングされたアドレスが正しいNATルールに一致するように正確なルートが設定されていることを確認します。
セクション 2	ネットワークオブジェクト NAT	セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。 **1.** スタティックルール **2.** ダイナミックルール **各ルール タイプでは、次の順序ガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 3	twice NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）
- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 192.168.1.0/24（ダイナミック）

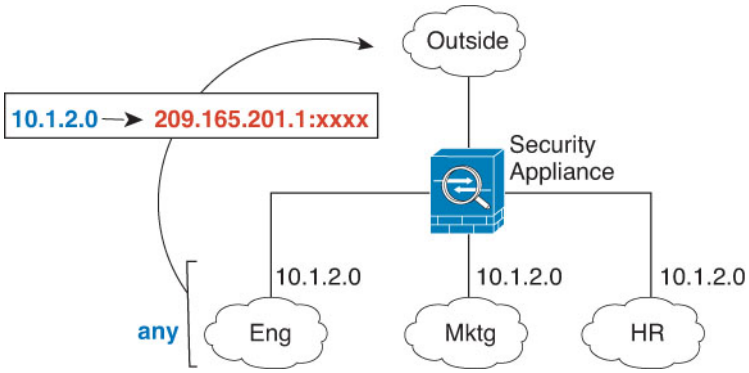
NAT インターフェイス

ブリッジ グループ メンバー インターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用されるNATルールを設定したり、特定の実際のインターフェイスとマッピング インターフェイスを識別したりできます。実際のアドレスに任意のインターフェイスを指定し、マッピングインターフェイスに特定のインターフェイスを指定することもでき、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベートアドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバルプールに変換する場合、実際のアドレスに

任意のインターフェイスを指定し、マッピング アドレスには outside インターフェイスを指定します。

図 7: 任意のインターフェイスの指定



ただし、「任意」のインターフェイスの概念は、ブリッジ グループ メンバー インターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジ グループ メンバー インターフェイスが除外されます。そのため、ブリッジ グループ メンバーに NAT を適用するには、メンバー インターフェイスを指定する必要があります。この結果、1 つのインターフェイスのみが異なる同様のルールが多数作成されることになります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできず、メンバー インターフェイスにのみ NAT を設定できます。

NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

NAT のファイアウォール モードのガイドライン

NAT は、ルーテッド モードとトランスペアレント ファイアウォール モードでサポートされています。

ただし、ブリッジ グループ メンバーのインターフェイス（ブリッジ グループ仮想インターフェイスの一部であるインターフェイス、BVI）での NAT 設定には次の制限があります。

- ブリッジ グループのメンバーに NAT を設定するには、メンバー インターフェイスを指定します。NAT をブリッジ グループ インターフェイス（BVI）自体に設定することはできません。
- ブリッジ グループ メンバーのインターフェイス間で NAT を実行するときには、実際のおよびマッピングされたアドレスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。
- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジ グループ メンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。

- 送信元インターフェイスと宛先インターフェイスが同じブリッジグループのメンバーである場合、IPv4 ネットワークと IPv6 ネットワーク（NAT64/46）同士を変換することはできません。スタティック NAT/PAT 44/66、ダイナミック NAT44/66、およびダイナミック PAT44 のみが許可されている方法であり、ダイナミック PAT66 はサポートされません。ただし、異なるブリッジ グループのメンバー同士、またはブリッジ グループのメンバー（送信元）と標準ルーテッド インターフェイス（宛先）の間では NAT64/46 を行うことができます。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 標準のルーテッド モードのインターフェイスの場合は、IPv4 と IPv6 との間でも変換できます。
- 同じブリッジ グループのメンバーであるインターフェイスでは、IPv4 と IPv6 の間の変換はできません。2 つの IPv6 ネットワーク間または 2 つの IPv4 ネットワーク間でのみ変換できます。この制限は、インターフェイスが異なるブリッジグループのメンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- 同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT（NAT66）は使用できません。この制限は、インターフェイスが異なるブリッジグループのメンバーである場合、またはブリッジグループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

IPv6 NAT のベストプラクティス

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます （twice NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向

にできます（twice NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目 IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。

- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

NAT のその他のガイドライン

- NAT ルールは、デバイスを通過する通信にのみ適用され、RADIUS 認証など、デバイスによって開始される通信には適用されません。
- ブリッジ グループのメンバーであるインターフェイスの場合は、メンバー インターフェイス用の NAT ルールを記述します。ブリッジ仮想インターフェイス（BVI）自体に対する NAT ルールは記述できません。
- サイト間 VPN で使用される仮想トンネルインターフェイス（VTI）の NAT ルールは作成できません。VTI の送信元インターフェイスのルールを作成すると、NAT は VPN トンネルに適用されません。VTI でトンネリングされた VPN トラフィックに適用される NAT ルールを作成するには、インターフェイスとして [any] を使用する必要があります。インターフェイス名を明示的に指定することはできません。
- （ネットワークオブジェクト NAT のみ）。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。たとえば、**オブジェクトネットワーク obj-10.10.10.1-01**、**オブジェクトネットワーク obj-10.10.10.1-02** などです。
- インターフェイスで VPN が定義されている場合、そのインターフェイスの着信 ESP トラフィックには NAT ルールは適用されません。システムは、確立済みの VPN トンネルに対してのみ ESP トラフィックを許可し、既存のトンネルに関連付けられていないトラフィックはドロップされます。この制約は、ESP および UDP のポート 500 と 4500 に適用されます。
- ダイナミック PAT を適用するデバイスの背後のデバイス（VPN UDP ポート 500 と 4500 は実際に使用されるポートではない）でサイト間 VPN を定義した場合、PAT デバイスの背後にあるデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンダはセキュリティ アソシエーション（SA）を開始できません。

- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションを使用できるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

  既存の接続（VPN トンネルなど）に適用する新しい NAT ルールを作成する場合は、**clear conn** を使用して接続を終了する必要があります。その後、接続を再確立しようとすると、NAT ルールが適用され、接続が正しく NAT 変換されます。

（注） ダイナミック NAT または PAT ルールを削除し、削除したルールに含まれるアドレスと重複するマッピングアドレスを含む新しいルールを追加すると、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** または **clear conn** コマンドを使用してクリアされるまで、新しいルールは使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- SCTP トラフィックを変換する場合は、スタティック ネットワーク オブジェクト NAT のみを使用します。ダイナミック NAT/PAT は許可されません。スタティック Twice NAT を設定できますが、SCTP アソシエーションの宛先部分のトポロジが不明であるため、そのような設定は推奨されません。
- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを含めることはできません。オブジェクト グループには、1 つのタイプのアドレスのみを含める必要があります。
- （twice NATのみ）。NAT ルールで送信元アドレスとして **any** を使用する場合、「any」通信の定義（IPv4 と IPv6）はルールによって異なります。ASA がパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、ASA は、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。"any" から "any" へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピング インターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- 同じマッピングオブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、次のアドレスを含めることはできません。
  - マッピング インターフェイスの IP アドレス。ルールに「any」インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッドモードのみ）の場合は、インターフェイスアドレスの代わりにインターフェイス名を指定します。

- フェイルオーバー インターフェイスの IP アドレス。
- （トランスペアレントモード。）管理 IP アドレス。
- （ダイナミック NAT。）VPN が有効な場合は、スタンバイ インターフェイスの IP アドレス。
- 既存の VPN プールのアドレス。

- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT ルールの送信元アドレスとリモートアクセス VPN アドレスプールの重複アドレスは使用できません。
- NAT や PAT に伴うアプリケーション検査の制限については、デフォルト インスペクションと NAT に関する制限事項 （300 ページ）を参照してください。
- アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。詳細については、NAT パケットのルーティング （233 ページ）を参照してください。
- **arp permit-nonconnected** コマンドを有効にすると、マッピングされたアドレスが接続されているサブネットの一部ではなく、しかも、マッピングされているインターフェイスを NAT ルールに指定しなかった（つまり、「any」インターフェイスを指定した）場合に、システムは ARP 要求に応答しません。この問題を解決するには、マッピングされたインターフェイスを指定します。
- ルールで宛先インターフェイスを指定すると、ルーティングテーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。
- NFS サーバーへの接続に使用される Sun RPC トラフィックで PAT を使用する場合、PAT の対象となるポートが 1024 よりも大きいと、NFS サーバーが接続を拒否する可能性があることに注意してください。NFS サーバーのデフォルト設定では、1024 よりも大きいポートからの接続は拒否されます。エラーメッセージは、通常「Permission Denied（権限が拒否されました）」です。下位のポートが利用できない場合に「フラット範囲」オプションを使用して大きなポート番号を使用すると、1024 よりも大きいポートのマッピングが発生する可能性があります（特にフラット範囲に下位のポートを含めるオプションを選択していない場合）。PAT プールのポート範囲に予約済みポート（1 ー 1023）を含めるオプションを選択しない場合、1024 よりも大きいポートのマッピングが発生します。この問題を回避するには、すべてのポート番号を許可するように NFS サーバーの構成を変更します。
- NAT は、通過トラフィックにのみ適用されます。システムによって生成された通信は、NAT の対象外です。
- NAT のトランザクション コミット モデルを使用すると、システムのパフォーマンスと信頼性を向上させることができます。詳細については、一般的な操作設定ガイドの基本設定

の章を参照してください。**asp rule-engine transactional-commit nat** コマンドを使用します。

- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- 単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。
- Protocol Independent Multicast（PIM）レジスタの内部ペイロードで NAT を使用することはできません。
- （twice NAT）デュアル ISP インターフェイス セットアップ（ルーティング設定でサービス レベル アグリーメントを使用するプライマリインターフェイスとバックアップインターフェイス）の NAT ルールを作成する場合は、ルールで宛先基準を指定しないでください。プライマリインターフェイスのルールがバックアップインターフェイスのルールよりも前にあることを確認してください。これにより、デバイスは、プライマリ ISP が利用できない場合に、現在のルーティング状態に基づいて正しい NAT 宛先インターフェイスを選択できます。宛先オブジェクトを指定すると、NAT ルールは、指定しない場合には重複するルールのプライマリインターフェイスを常に選択します。
- インターフェイスに定義された NAT ルールと一致しないトラフィックについて ASP ドロップ理由 nat-no-xlate-to-pat-pool が示される場合は、影響を受けるトラフィックのアイデンティティ NAT ルールを設定して、トラフィックが変換されずに通過できるようにします。
- GRE トンネルエンドポイントの NAT を設定する場合は、エンドポイントでキープアライブを無効にする必要があります。無効にしないと、トンネルを確立できません。エンドポイントは、キープアライブを元のアドレスに送信します。
- DHCP と BOOTP はポート UDP/67 ～ 68 を共有します。BOOTP は廃止されているため、DHCP も実行している場合、BOOTP ポートの NAT ルールを作成するとポート割り当ての問題が発生する可能性があります。ネットワークセグメント間で DHCP 要求を送信する場合は、代わりに DHCP リレーを使用することを検討してください。
- まれに、既存の変換（xlate）を使用した戻り通信（サーバからクライアント）が、[接続イベント（Connection Events）] に新しいフローとして記録されることがあります。これは、クライアントが接続をすでに終了しており、サーバーが別のパケットを送信すると、接続の終了と xlate の削除の間の短い間隔でデバイスに到達します（多くの場合、アプリケーションの動作または TCP スタックのクリーンアップが原因）。デバイスは接続を削除した後にのみ xlate を削除するため、xlate がまだ存在している間にサーバーパケットが届く可能性があります。有効な接続エントリが見つからない場合、デバイスは一致するアクセス コントロール ポリシーの規則に基づいて別の接続イベントをログに記録します。

マッピング アドレス オブジェクトのネットワーク オブジェクト NAT のガイドライン

ダイナミック NAT の場合は、マッピングされたアドレスに対してオブジェクトまたはグループを使用する必要があります。他のタイプの NAT の場合は、オブジェクトまたはグループを作成することも、インライン アドレスを使用することもできます。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。**object network** コマンドと **object-group network** コマンドを使用してオブジェクトを作成します。

マッピング アドレスのオブジェクトを作成する場合は、次のガイドラインを考慮してください。

- 1 つのネットワーク オブジェクト グループには、IPv4 アドレスと IPv6 アドレスのいずれか一方のオブジェクトやインライン アドレスを入れることができます。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- 拒否されるマッピング IP アドレスについては、NAT のその他のガイドライン （162 ページ）を参照してください。
- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- ダイナミック NAT：
  - インライン アドレスは使用できません。ネットワーク オブジェクトまたはグループを設定する必要があります。
  - オブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
  - マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。オブジェクトにホストアドレスが1つしか含まれていない場合は、それが PAT に使用されます。
- ダイナミック PAT（隠蔽）：
  - オブジェクトを使用する代わりに、任意でインラインホストアドレスを設定するか、またはインターフェイス アドレスを指定できます。
  - オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを含めることはできません。オブジェクトは、1 つのホスト、または範囲（PAT プールの場合）を定義する必要があります。グループ（PAT プールの場合）には、複数のホストと範囲を含めることができます。
- スタティック NAT またはポート変換を使用するスタティック NAT：

- オブジェクトを使用する代わりに、インライン アドレスを設定するか、またはインターフェイス アドレスを指定できます（ポート変換を使用するスタティック NAT の場合）。
- オブジェクトを使用する場合は、オブジェクトまたはグループにホスト、範囲、またはサブネットを入れることができます。

- アイデンティティ NAT
  - オブジェクトを使用する代わりに、インライン アドレスを設定できます。
  - オブジェクトを使用する場合は、オブジェクトは、変換する実際のアドレスと一致する必要があります。

実際のアドレス オブジェクトおよびマッピング アドレス オブジェクトの Twice NAT のガイドライン

NAT ルールごとに、次に関するネットワーク オブジェクトまたはグループを 4 つまで設定します。

- 送信元の実際のアドレス
- 送信元のマッピング アドレス
- 宛先の実際のアドレス
- 宛先のマッピング アドレス

すべてのトラフィックを表す any キーワード インライン、または一部のタイプの NAT の場合はインターフェイス アドレスを表す interface キーワードを指定しない場合は、オブジェクトが必要です。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。**object network** コマンドと **object-group network** コマンドを使用してオブジェクトを作成します。

Twice NAT のオブジェクトを作成する場合は、次のガイドラインを考慮してください。

- 1 つのネットワーク オブジェクト グループには、IPv4 アドレスと IPv6 アドレスのいずれか一方のオブジェクトやインライン アドレスを入れることができます。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- 拒否されるマッピング IP アドレスについては、NAT のその他のガイドライン （162 ページ）を参照してください。
- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- 送信元ダイナミック NAT：

- 通常は、実際のアドレスの大きいグループが小さいグループにマッピングされるように設定します。
- マッピングされたオブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
- マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。オブジェクトにホストアドレスが 1 つしか含まれていない場合は、それが PAT に使用されます。

- 送信元ダイナミック PAT（隠蔽）：
  - オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを含めることはできません。オブジェクトは、1 つのホスト、または範囲（PAT プールの場合）を定義する必要があります。グループ（PAT プールの場合）には、複数のホストと範囲を含めることができます。

- 送信元スタティック NAT またはポート変換を設定したスタティック NAT：
  - マッピングされたオブジェクトまたはグループには、ホスト、範囲、またはサブネットを含めることができます。
  - スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。

- 送信元アイデンティティ NAT
  - 実際のオブジェクトとマッピングされたオブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。

- 宛先スタティック NAT またはポート変換を設定したスタティック NAT（宛先の変換は常にスタティックです）：
  - Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、ネットワークオブジェクト NAT と twice NAT の比較 （156 ページ）を参照してください。
  - アイデンティティ NAT では、実際のオブジェクトとマッピングされたオブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。

- スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。
- ポート変換（ルーテッド モードのみ）が設定されたスタティック インターフェイス NAT では、マッピング アドレスのネットワーク オブジェクト/グループではなく、interface キーワードを指定できます。
- www.example.com などの完全修飾ドメイン名を、翻訳された （マッピングされた）宛先として使用できます。詳細については、FQDN 接続先のガイドライン （169 ページ） を参照してください。

FQDN 接続先のガイドライン

IP アドレスの代わりに完全修飾ドメイン名（FQDN）ネットワークオブジェクトを使用して、twice NAT ルールに変換済み（マッピング）宛先を指定できます。たとえば、www.example.com Web サーバーを宛先とするトラフィックに基づいてルールを作成できます。

FQDN を使用すると、システムは DNS 解決を取得し、返されたアドレスに基づいて NAT ルールを書き込みます。複数の DNS サーバーグループを使用している場合は、フィルタドメインが優先され、フィルタに基づいて適切なグループからアドレスが要求されます。DNS サーバーから複数のアドレスを取得する場合、使用されるアドレスは次の情報に基づきます。

- 指定したインターフェイスと同じサブネット上にアドレスがある場合は、そのアドレスが使用されます。同じサブネットに存在しない場合は、最初に返されたアドレスが使用されます。
- 変換後の送信元と変換後の宛先の IP タイプは一致している必要があります。たとえば、変換後の送信元アドレスが IPv6 の場合、FQDN オブジェクトはアドレスタイプとして IPv6 を指定する必要があります。変換後の送信元が IPv4 の場合、FQDN オブジェクトはアドレスタイプとして IPv4 を指定する必要があります。

手動 NAT 宛先に使用されるネットワークグループに FQDN オブジェクトを含めることはできません。NAT では、1 つの宛先ホストだけがこのタイプの NAT ルールに適しているため、FQDN オブジェクトは単独で使用する必要があります。

FQDN を IP アドレスに解決できない場合、DNS 解決が取得されるまでルールは機能しません。

実際のポートおよびマッピング ポートのサービス オブジェクトの Twice NAT のガイドライン

必要に応じて、次のサービス オブジェクトを設定できます。

- **送信元の実際のポート（スタティックのみ）**または**宛先の実際のポート**
- **送信元のマッピング ポート（スタティックのみ）**または**宛先のマッピング ポート**

object service コマンドを使用してオブジェクトを作成します。

Twice NAT のオブジェクトを作成する場合は、次のガイドラインを考慮してください。

- NAT は、TCP、UDP、および SCTP のみをサポートします。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（たとえば両方とも TCP にします）。SCTP ポートの仕様を含むスタティック Twice NAT ルールを設定できますが、SCTP アソシエーションの宛先部分のトポロジが不明であるため、これは推奨されません。SCTP に対して代わりにスタティック オブジェクト NAT を使用します。
- 「not equal（等しくない）」（**neq**）演算子はサポートされていません。
- アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。
- 送信元ダイナミック NAT：送信元ダイナミック NAT では、ポート変換はサポートされません。
- 送信元ダイナミック PAT（隠蔽）：送信元ダイナミック PAT では、ポート変換はサポートされません。
- 送信元スタティック NAT、ポート変換を設定したスタティック NAT、またはアイデンティティ NAT：サービス オブジェクトには、送信元ポートと宛先ポートの両方を含めることができます。ただし、両方のサービス オブジェクトに、送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバーなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。
- 宛先スタティック NAT またはポート変換を設定したスタティック NAT（宛先の変換は常にスタティックです）：非スタティックな送信元 NAT では、宛先でのみポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。

ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

ダイナミック NAT について

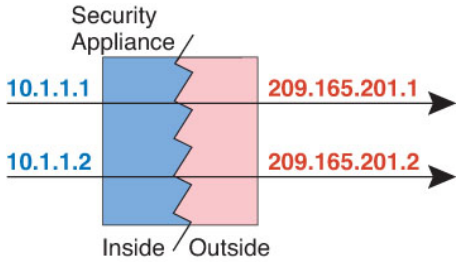
ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している

間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

（注） 変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスルールのセキュリティに依存できます。リモートホストからの接続が成功すると、接続のアイドルタイマーがリセットされます。

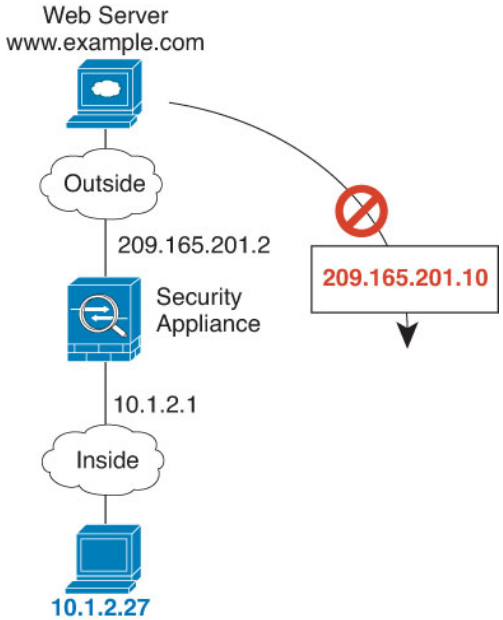
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答通信が許可されます。

図 *8 :* ダイナミック *NAT*



次の図に、マッピングアドレスへの接続開始を試みているリモートホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。

図 *9 :* マッピング アドレスへの接続開始を試みているリモート ホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  PAT では、1 つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

- マッピングされたプールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、オープン スタンダードではないアプリケーションでも機能しません。

ダイナミック ネットワーク オブジェクト NAT の設定

この項では、ダイナミック NAT のネットワーク オブジェクト NAT を設定する方法について説明します。

手順

ステップ 1 マッピング アドレスにホストまたは範囲のネットワーク オブジェクト（**object network** コマンド）、またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。

- オブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
- マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。オブジェクトにホストアドレスが 1 つしか含まれていない場合は、それが PAT に使用されます。

ステップ 2 NAT を設定するネットワーク オブジェクトを作成または編集します。**object network** *obj_name*

例：

```
hostname(config)# object network my-host-obj1
```

ステップ 3 （正しいアドレスがあるオブジェクトを編集する場合はスキップする）変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host** {*IPv4_address*|*IPv6_address*}：単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask*|*IPv6_address/IPv6_prefix*}：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **range** *start_address end_address*：アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例：

```
hostname(config-network-object)# host 10.2.2.2
```

ステップ 4 オブジェクト IP アドレスの**ダイナミック NAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。

nat [**(***real_ifc***,***mapped_ifc***)**] **dynamic** *mapped_obj* [**interface** [**ipv6**]] [**dns**]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。
- マッピング IP アドレス：マッピング IP アドレスが含まれるネットワーク オブジェクトまたはネットワーク オブジェクト グループを指定します。
- インターフェイス PAT のフォールバック：（任意）**interface** キーワードは、インターフェイス PAT のフォール バックをイネーブルにします。マッピング IP アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジ グループ メンバーのときは、**interface** を指定できません）
- DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「NAT を使用した DNS クエリと応答の書き換え （250 ページ）」を参照してください。

例：

```
hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface
```

例

次の例では、外部アドレス 10.2.2.1 ～ 10.2.2.10 の範囲の背後に 192.168.2.0 ネットワークを隠すダイナミック NAT を設定します。

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

次の例では、ダイナミック PAT バックアップを設定したダイナミック NAT を設定します。ネットワーク 10.76.11.0 内のホストは、まず nat-range1 プール（10.10.10.10 ～ 10.10.10.20）にマッピングされます。nat-range1 プール内のすべてのアドレスが割り当てられたら、pat-ip1 アドレス（10.10.10.21）を使用してダイナミック PAT が実行されます。万一、PAT 変換もすべて使用されてしまった場合は、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20

hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

次の例では、ダイナミック NAT とダイナミック PAT バックアップを使用して IPv6 ホストを IPv4 に変換するように設定します。内部ネットワーク 2001:DB8::/96 上のホストは最初に、IPv4_NAT_RANGE プール（209.165.201.30 ～ 209.165.201.1）にマッピングされます。IPv4_NAT_RANGE プール内のすべてのアドレスが割り当てられた後は、IPv4_PAT アドレス（209.165.201.31）を使用してダイナミック PAT が実行されます。PAT 変換もすべて使用されてしまった場合は、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31
```

```
hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

ダイナミック Twice NAT の設定

この項では、ダイナミック NAT の Twice NAT を設定する方法について説明します。

手順

ステップ 1 送信元の実際のアドレス、送信元のマッピング アドレス、宛先の実際のアドレス、および宛先のマッピング アドレスに、ホストまたは範囲のネットワーク オブジェクト（**object network** コマンド）、またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。宛先のマッピング アドレスに FQDN ネットワーク オブジェクトを使用することもできます。

- すべての送信元トラフィックを変換する場合、送信元の実際のアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **any** キーワードを指定できます。
- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを作成する場合は、次のガイドラインを考慮してください。

- 通常は、実際のアドレスの大きいグループが小さいグループにマッピングされるように設定します。
- オブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
- マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。オブジェクトにホストアドレスが 1 つしか含まれていない場合は、それが PAT に使用されます。

ステップ 2 （任意）宛先の実際のポートおよび宛先のマッピング ポートにサービス オブジェクトを作成します。

ダイナミック NAT の場合、宛先でポート変換のみを実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。

ステップ 3 ダイナミック **NAT** を設定します。

nat [**(***real_ifc***,***mapped_ifc***)**] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real_obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。
- セクションおよび行：（任意）デフォルトでは、NAT 規則は、NAT テーブルのセクション 1 の末尾に追加されます（NAT ルールの順序 （157 ページ）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。
- 送信元アドレス：
  - 実際のアドレス：ネットワーク オブジェクト、グループ、または **any** キーワードを指定します。
  - マッピング アドレス：異なるネットワーク オブジェクトまたはグループを指定します。必要に応じて、次のフォールバック方式を設定できます。
    - インターフェイス PAT のフォール バック：（任意）**interface** キーワードは、インターフェイス PAT のフォールバックをイネーブルにします。マッピング IP アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジ グループ メンバーになっているときは、**interface** を指定できません）
- 宛先アドレス（任意）：
  - マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合は、必ず **service** キーワードも設定します。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック NAT （194 ページ）」を参照してください。

- 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

- 宛先ポート：（任意）マッピングされたサービス オブジェクトおよび実際のサービス オブジェクトとともに、**service** キーワードを指定します。アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用します。
- DNS：（任意、送信元にのみ適用されるルール）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。**宛先**アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「NAT を使用した DNS クエリと応答の書き換え （250 ページ）」を参照してください。
- 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。
- 非アクティブ：（任意）コマンドを削除する必要なくこの規則を非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。
- 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例：

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL
destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC
```

例

次に、209.165.201.1/27 ネットワークのサーバーおよび 203.0.113.0/24 ネットワークのサーバーにアクセスする場合の内部ネットワーク 10.1.1.0/24 のダイナミック NAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
```

```
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2
```

次に、IPv4 209.165.201.1/27 ネットワークのサーバーおよび 203.0.113.0/24 ネットワークのサーバーにアクセスする場合の IPv6 内部ネットワーク 2001:DB8:AAAA::/96 のダイナミック NAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2
```

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図は、ダイナミック PAT の一般的なシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答通信が許可されます。マッピングアドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 *10* : ダイナミック *PAT*

変換が継続している間、アクセス ルールで許可されていれば、宛先ネットワーク上のリモート ホストは変換済みホストへの接続を開始できます。実際のポートアドレスおよびマッピング ポートアドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も期限切れになります。マルチセッション PAT では、PAT のタイムアウト（デフォルトでは 30 秒）が使用されます。セッションごとの PAT では、xlate がただちに削除されます。

（注） インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイス、特に「any」インターフェイスに同じプールを使用すると、プールがすぐに枯渇し、新しい変換に使用できるポートがなくなります。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、ASA インターフェイスの IP アドレスを PAT アドレスとして使用できます。

同じブリッジ グループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT（NAT66）は使用できません。この制限は、インターフェイスが異なるブリッジ グループのメンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。NAT および PAT のサポートの詳細については、デフォルト インスペクションと NAT に関する制限事項 （300 ページ） を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、この通信はサーバで DoS 攻撃として解釈される可能性があります。アドレスの PAT プールを設定して、PAT アドレスのラウンドロビン割り当てを使用すると、この状況を緩和できます。

PAT プールオブジェクトのガイドライン

PAT プールのネットワーク オブジェクトを作成する場合は、次のガイドラインに従ってください。

PAT プールの場合

- ポートは、1024 ー 65535 の範囲の使用可能なポートにマッピングされます。必要に応じ、1024 番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。

  クラスタで動作する場合、アドレスごとに 512 個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当ても有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも 512 です。クラスターユニットの制限（クラスターのサイズ）を変更する場合は、xlate をクリアするか、デバイスを再起動して、PAT プールをクラスターユニットに適切に再割り当てできるようにしてください。

- PAT プールに対してブロック割り当てを有効にする場合、ポートブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号（1 ～ 1023）を必要とするときは、機能しない可能性があります。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。

- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT が指定される場合は、もう一方のルールでも拡張 PAT が指定される必要があります。

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します。使用可能なポートがない場合、接続が妨げられる可能性があります。この問題を回避するには、ラウンドロビンオプションを使用します。

- パフォーマンスを最大にするには、PAT プール内の IP アドレスの数を 10,000 に制限します。

PAT プールの拡張 PAT の場合

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションの完全な一覧については、デフォルトインスペクションと NAT に関する制限事項 （300 ページ）を参照してください。

- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合、PAT プールのアドレスを、ポート トランスレーション ルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーション ルールを持つスタティック NAT は作成できません。

- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。

- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。
- クラスタ内のユニットで拡張 PAT を使用することはできません。
- 拡張 PAT は、デバイスでのメモリ使用率が増加します。

PAT プールのラウンド ロビン方式の場合

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。ただし、この「粘着性」は、フェールオーバーが発生すると失われます。デバイスがフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- PAT プール ルール/ラウンド ロビン ルールとインターフェイス PAT ルールが同じインターフェイス上で混在していると、IPアドレスの「粘着性」も影響を受けます。指定したインターフェイスで PAT プールまたはインターフェイス PAT のいずれかを選択します。競合する PAT ルールは作成しないでください。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時NATプールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

ダイナミック ネットワーク オブジェクト PAT の設定

この項では、ダイナミック PAT のネットワーク オブジェクト NAT を設定する方法について説明します。

手順

ステップ 1 （任意）マッピング アドレスにホストまたは範囲のネットワーク オブジェクト（**object network** コマンド）、またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。

- オブジェクトを使用する代わりに、任意でインライン ホスト アドレスを設定するか、またはインターフェイス アドレスを指定できます。
- オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを入れることはできません。オブジェクトは、1 つのホスト、または範囲（PAT プールの場合）を定義する必要があります。グループ（PAT プールの場合）には、複数のホストと範囲を入れることができます。

ステップ 2 NAT を設定するネットワーク オブジェクトを作成または編集します。**object network** *obj_name*

例：

```
hostname(config)# object network my-host-obj1
```

ステップ 3 （正しいアドレスがあるオブジェクトを編集する場合はスキップする）変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host** {*IPv4_address* | *IPv6_address*}：単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address / IPv6_prefix*}：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **range** *start_address end_address*：アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例：

```
hostname(config-network-object)# range 10.1.1.1 10.1.1.90
```

ステップ 4 オブジェクト IP アドレスの**ダイナミック PAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。

nat [(*real_ifc*,*mapped_ifc*)] **dynamic** {*mapped_inline_host_ip* | *mapped_obj* | **pat-pool** *mapped-obj* [**round-robin**] [**extended**] [**include-reserve**] [**block-allocation**] | **interface** [**ipv6**]} [**interface** [**ipv6**]]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。
- マッピング IP アドレス：マッピング IP アドレスを次のものとして指定できます。
  - *mapped_inline_host_ip*：インライン ホスト アドレス。
  - *mapped_obj*：ホスト アドレスとして定義されるネットワーク オブジェクト。
  - **pat-pool** *mapped-obj*：複数のアドレスを含むネットワーク オブジェクトまたはグループ。
  - **interface** [**ipv6**]：マッピングされたインターフェイスの IP アドレスがマッピング アドレスとして使用されます。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジ グループ メ

ンバーのときは、**interface** を指定できません）このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。

- PAT プールについて、次のオプションの 1 つ以上を指定できます。
  - **round-robin**：PAT プールのラウンドロビンアドレス割り当てをイネーブルにします。ラウンドロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。
  - **extended**：拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。
  - **include-reserve**：アドレス変換に使用できるポートの範囲に予約済みポート（1 ー 1023）を含めます。このオプションを指定しない場合、アドレスは 1024 ー 65535 の範囲内のポートのみに変換されます。
  - **block-allocation**：ポートブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に 1 つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ～ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては **round-robin** と互換性がありますが、**extended** オプションを使用することはできません。また、インターフェイス PAT のフォールバックを使用することもできません。
- インターフェイス PAT のフォール バック：（任意）**interface** [**ipv6**] キーワードは、プライマリ PAT アドレスの後に入力されたときにインターフェイス PAT のフォールバックをイネーブルにします。プライマリ PAT アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジグループ メンバーのときは、**interface** を指定できません）

例：

```
hostname(config-network-object)# nat (any,outside) dynamic interface
```

例

次の例では、アドレス 10.2.2.2 の背後に 192.168.2.0 ネットワークを隠すダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

次の例では、外部インターフェイスアドレスの背後に192.168.2.0ネットワークを隠蔽するダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

次の例では、ダイナミック PAT と PAT プールを使用して内部 IPv6 ネットワークを外部 IPv4 ネットワークに変換するように設定します。

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

ダイナミック Twice PAT の設定

この項では、ダイナミック PAT の Twice NAT を設定する方法について説明します。

手順

ステップ 1 送信元の実際のアドレス、送信元のマッピング アドレス、宛先の実際のアドレス、および宛先のマッピング アドレスに、ホストまたは範囲のネットワーク オブジェクト（**object network** コマンド）、またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。宛先のマッピング アドレスに FQDN ネットワーク オブジェクトを使用することもできます。

- すべての送信元トラフィックを変換する場合、送信元の実際のアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **any** キーワードを指定できます。
- インターフェイス アドレスをマッピング アドレスとして使用する場合は、送信元のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを含めることはできません。オブジェクトは、1 つのホスト、または範囲（PAT プールの場合）を定義する必要があります。グループ（PAT プールの場合）には、複数のホストと範囲を含めることができます。

ステップ 2 （任意）宛先の実際のポートおよび宛先のマッピング ポートにサービス オブジェクトを作成します。

ダイナミック NAT の場合、宛先でポート変換のみを実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。

ステップ 3 **ダイナミック PAT** を設定します。

nat [(*real_ifc*,*mapped_ifc*)] [*line* | **after-auto** [*line*]] **source dynamic** {*real-obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]] | **pat-pool** *mapped-obj* [**round-robin**] [**extended**] [**include-reserve**] [**block-allocation**] [**interface** [**ipv6**]] | **interface** [**ipv6**]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**unidirectional**] [**inactive**] [**description** *description*]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。

- セクションおよび行：（任意）デフォルトでは、NAT 規則は、NAT テーブルのセクション 1 の末尾に追加されます（NAT ルールの順序 （157 ページ）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。

- 送信元アドレス：

  - 実際のアドレス：ネットワーク オブジェクト、グループ、または **any** キーワードを指定します。実際のインターフェイスからマッピングされたインターフェイスへのすべてのトラフィックを変換する場合、**any** キーワードを使用します。

  - マッピング アドレス：次のいずれかを設定します。

    - ネットワーク オブジェクト：ホスト アドレスを含むネットワーク オブジェクト。

    - **pat-pool** *mapped-obj*：複数のアドレスを含むネットワーク オブジェクトまたはグループ。

- **interface** [**ipv6**]：（ルーテッドモードのみ。）マッピング インターフェイスの IP アドレスがマッピング アドレス（インターフェイス PAT）として使用されます。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジ グループ メンバーのときは、**interface** を指定できません）PAT プールまたはネットワーク オブジェクトでこのキーワードを指定すると、インターフェイス PAT のフォールバックが有効になります。PAT IP アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。

PAT プールについて、次のオプションの 1 つ以上を指定できます。

- **round-robin**：PAT プールのラウンドロビン アドレス割り当てをイネーブルにします。ラウンド ロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。
- **extended**：拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。
- **include-reserve**：アドレス変換に使用できるポートの範囲に予約済みポート（1ー1023）を含めます。このオプションを指定しない場合、アドレスは 1024ー65535 の範囲内のポートのみに変換されます。
- **block-allocation**：ポート ブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に 1 つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ～ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては **round-robin** と互換性がありますが、**extended** オプションを使用することはできません。また、インターフェイス PAT のフォールバックを使用することもできません。

- 宛先アドレス（任意）：
  - マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換を設定したスタティック インターフェイス NAT に限り（非ブリッジ グループのメンバ インターフェイスのみ）、**interface** キーワードを指定します。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する

場合は、必ず **service** キーワードも設定します。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック NAT （194 ページ）」を参照してください。

- 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

- 宛先ポート：（任意）マッピングされたサービス オブジェクトおよび実際のサービス オブジェクトとともに、**service** キーワードを指定します。アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用します。
- 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。
- 非アクティブ：（任意）コマンドを削除する必要なくこのルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。
- 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例：

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet interface
destination static Server1 Server1
description Interface PAT for inside addresses when going to server 1
```

例

次に、外部 Telnet サーバー 209.165.201.23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、203.0.113.0/24 ネットワーク上のサーバーへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface
```

```
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

次に、外部 IPv6 Telnet サーバー 2001:DB8::23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、2001:DB8:AAAA::/96 ネットワーク上のサーバーへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

ポート ブロック割り当てによる PAT の設定

キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ブロックのポートを使用する最後の xlate が削除されると、ブロックが解放されます。

ポート ブロックを割り当てる主な理由は、ロギングの縮小です。ポート ブロックの割り当てが記録され、接続が記録されますが、ポートブロック内で作成された xlate は記録されません。一方、ログ分析はより困難になります。

ポートのブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。TCP、UDP、および ICMP 接続用の個別のブロックがあり、これらのブロックは重複する場合があります。そのため、アプリケーションが小さいポート番号（1 ～ 1023）を必要とするときは、機能しない可能性があります。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。低いポート番号を使用するアプリケーションに対してブロック割り当てを使用しない個別の NAT ルールを作成できます。Twice NAT の場合は、ルールが確実にブロック割り当てルールの前に来るようにします。

始める前に

NAT ルールの使用上の注意：

- **round-robin** キーワードは含めることはできますが、**extended**、**include-reserve**、または **interface**（インターフェイス PAT フォールバック用）を含めることはできません。その他の送信元/宛先のアドレスとポート情報も許可されます。
- 既存のルールを置き換える場合は、NAT を変更するすべてのケースと同様、置き換えるルールに関連する xlate をクリアする必要があります。これは、新しいルールを有効にするために必要です。それらを明示的にクリアするか、または単にタイムアウトになるまで待ちます。ただし、クラスターで動作する場合、ユニットがブロックを正しく配布できるようにクラスターをリロードする必要があります。

（注） 通常の PAT ルールとブロック割り当て PAT ルールを切り替える場合、オブジェクト NAT では、まずルールを削除してから xlate をクリアする必要があります。その後、新しいオブジェクト NAT ルールを作成できます。そうしないと、**show asp drop** 出力に pat-port-block-state-mismatch ドロップが表示されます。

- 制御ノードになるデバイスに PAT プールを使用する既存の NAT ポリシーがある間にクラスターを形成すると、PAT ポートブロック配布が正しく初期化されないことがあります。制御ノードはポートブロックを所有または分散せず、**show nat pool cluster summary** コマンドはすべてのクラスターノードですべてのポートブロックを *RESERVED* と表示する場合があります。
  - クラスターを形成する前に、制御ノードになるデバイスから PAT プールを使用する既存の NAT ポリシーを削除します。クラスターの形成が完了したら、NAT ポリシーを再設定して展開します。
  - クラスターがすでに形成されており、すべてのポートブロックが *RESERVED* と表示されている場合は、影響を受ける NAT ポリシーを削除してから変更を展開します。その後、ポリシーを再作成して展開します。**show nat pool cluster summary** コマンドを使用して、ポートブロックがクラスターノード全体に正しく分散されていることを確認します。
- 特定の PAT プールに対し、そのプールを使用するすべてのルールに対してブロック割り当てを指定する（または指定しない）必要があります。1 つのルールにブロックを割り当てることはできず、別のルールに割り当てることもできません。重複する PAT プールもまたロック割り当て設定を混在させることはできません。また、ポート変換ルールを含むスタティック NAT とプールを重複させることはできません。

手順

ステップ 1 （オプション）ブロック割り当てサイズを設定します。これは各ブロックのポート数です。

xlate block-allocation size *value*

範囲は 32 ～ 4096 です。デフォルトは 512 です。デフォルト値に戻すには、no 形式を使用します。

デフォルトを使用しない場合は、選択したサイズが 64,512 に均等に分割していることを確認します（1024 ～ 65535 の範囲のポート数）。確認を怠ると、使用できないポートが混入します。たとえば、100 を指定すると、12 個の未使用ポートがあります。

ステップ 2 （任意）ホストごとに割り当てることができる最大ブロック数を設定します。

xlate block-allocation maximum-per-host *number*

制限はプロトコルごとに設定されるので、制限「4」は、ホストごとの上限が 4 つの UDP ブロック、4 つの TCP ブロック、および 4 つの ICMP ブロックであることを意味します。指定できる値の範囲は 1 ～ 8 で、デフォルトは 4 です。デフォルト値に戻すには、no 形式を使用します。

ステップ 3 （オプション）暫定 syslog の生成をイネーブルにします。

xlate block-allocation pba-interim-logging *seconds*

デフォルトでは、ポート ブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ロギングをイネーブルにすると、指定した間隔で次のメッセージが生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポート ブロックをレポートします（プロトコル（ICMP、TCP、UDP）、送信元および宛先インターフェイス、IP アドレス、ポート ブロックを含む）。間隔は 21600 ～ 604800 秒（6 時間から 7 日間）を指定することができます。

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

例：

```
ciscoasa(config)# xlate block-allocation pba-interim-logging 21600
```

ステップ 4 PAT プールのブロック割り当てを使用する NAT ルールを追加します。

- **オブジェクト PAT。**

  nat [(*real_ifc*,*mapped_ifc*)] **dynamic pat-pool** *mapped-obj* **block-allocation**

  例：

```
object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_host
   host 10.111.10.15
object network src_host
   nat (inside,outside) dynamic
```

```
pat-pool mapped-pat-pool block-allocation
```

- **Twice PAT。**

  nat [(*real_ifc*,*mapped_ifc*)] [*line* | **after-auto** [*line*]] **source dynamic** *real_obj* **pat-pool***mapped-obj* **block-allocation**

  例：

```
object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_network
   subnet 10.100.10.0 255.255.255.0
nat (inside,outside) 1 source dynamic src_network
pat-pool mapped-pat-pool block-allocation
```

Per-Session PAT または Multi-Session PATの設定

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。

Per-session PAT によって PAT の拡張性が向上し、クラスタリングの場合に各メンバーユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、制御ユニットに転送して制御ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。

HTTP や HTTPS などの「ヒットエンドラン」トラフィックの場合、Per-Session PAT は、1 つのアドレスによってサポートされる接続率を大幅に増やすことができます。Per-Session PAT を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-Session PAT を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。

Multi-Session PAT のメリットを活用できるトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。ただし、これらのプロトコルで使用する UDP ポートにセッション単位の PAT も使用する場合は、それらに許可ルールを作成する必要があります。

始める前に

デフォルトでは、次のルールがインストールされます。

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
```

```
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次のものを追加します。

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

手順

Per-session PAT の許可または拒否ルールを作成します。このルールはデフォルト ルールの上に置かれますが、他の手動作成されたルールよりは下です。ルールは必ず、適用する順序で作成してください。

xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip* [*operator dest_port*]

変換元と変換先の IP アドレスについては、次のように設定できます。

- **host** *ip_address*：IPv4 または IPv6 ホスト アドレスを指定します。
- *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
- *ipv6-address/prefix-length*：IPv6 ネットワーク アドレスとプレフィックスを指定します。
- **any4** および **any6**：**any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。

operator では、変換元または変換先で使用されるポート番号の条件を指定します。デフォルトでは、すべてのポートです。使用できる演算子は、次のとおりです。

- **lt**：より小さい
- **gt**：より大きい
- **eq**：等しい
- **neq**：等しくない

- **range**：値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します（例：**range 100 200**）。

例

次の例では、H.323 トラフィックのための拒否ルールを作成します。このトラフィックには Multi-Session PAT が使用されるようにするためです。

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

次に、SIP UDP ポートにセッション単位の PAT を許可することで、クラスタのメンバ間での SIP の分散を有効にする例を示します。SIP TCP ポートではセッション単位の PAT がデフォルトであるため、デフォルトのルールを変更した場合を除き、TCP にルールは必要ありません。

```
hostname(config)# xlate per-session permit udp any4 any4 eq sip
```

スタティック NAT

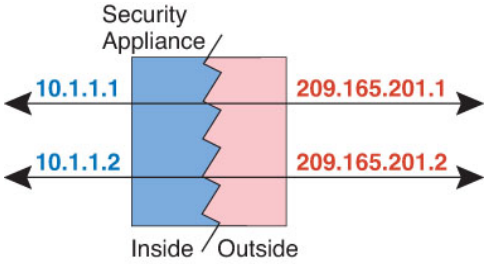
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じであるため、スタティック NAT では、双方向の接続（ホストへの接続とホストから接続の両方）を開始できます（接続を許可するアクセス ルールが存在する場合）。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するため、双方向の開始はサポートされません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブであるため、実際のホストとリモート ホストの両方が接続を開始できます。

図 *11* : スタティック *NAT*



（注） 必要に応じて、双方向をディセーブルにできます。

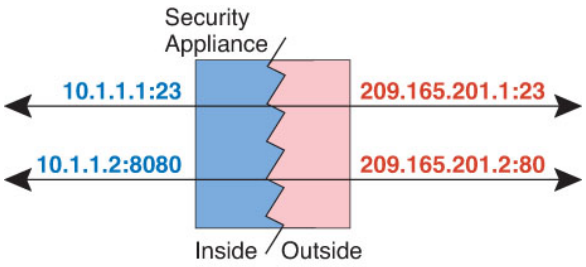
ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルおよびポートとマッピングされたプロトコルおよびポートを指定できます。

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IP アドレスは別の値にマッピングされています。この変換は常にアクティブであるため、変換されたホストとリモート ホストの両方が接続を開始できます。

図 *12* : ポート変換を設定したスタティック *NAT* の一般的なシナリオ



ポート変換ルールを設定したスタティック NAT は、指定されたポートの宛先 IP アドレスのみにアクセスを制限します。NAT ルール対象外の別のポートで宛先 IP アドレスにアクセスしようとすると、接続がブロックされます。さらに、twice NAT の場合、NAT ルールの送信元 IP アドレスと一致しないトラフィックが宛先 IP アドレスと一致する場合、宛先ポートに関係なくドロップされます。したがって、宛先 IP アドレスに対して許可される他のすべてのトラフィックに追加ルールを追加する必要があります。たとえば、ポートを指定せずに IP アドレスにスタティック NAT ルールを設定し、ポート変換ルールの後ろにそれを配置できます。

（注） セカンダリチャネルのアプリケーションインスペクションが必要なアプリケーション（FTP、VoIP など）については、NAT が自動的にセカンダリポートを変換します。

次に、ポート変換を設定したスタティック NAT のその他の使用例の一部を示します。

アイデンティティポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する 3 つの個別のサーバ（FTP、HTTP、SMTP など）がある場合は、それらのサービスにアクセスするための単一の IP アドレスを外部ユーザに提供できます。その後、アイデンティティ ポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバーの正しい IP アドレスにマッピングできます。サーバーは標準のポート（それぞれ 21、80、および 25）を使用しているため、ポートを変更する必要はありません。この例の設定方法については、FTP、HTTP、およびSMTPの単一アドレス（ポート変換を設定したスタティックNAT）（225ページ）を参照してください。

標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、ウェルノウンポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

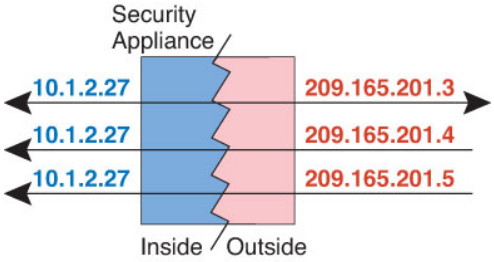
スタティック NAT は、実際のアドレスをインターフェイスアドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

一対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし、場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります（1 対多）。1 対多のスタティック NAT を設定する場合、実際のホストが通信を開始すると、常に最初のマッピングアドレスが使用されます。しかし、ホストに向けて開始された通信の場合、任意のマッピングアドレスへの通信を開始でき、1 つの実際のアドレスには変換されません。

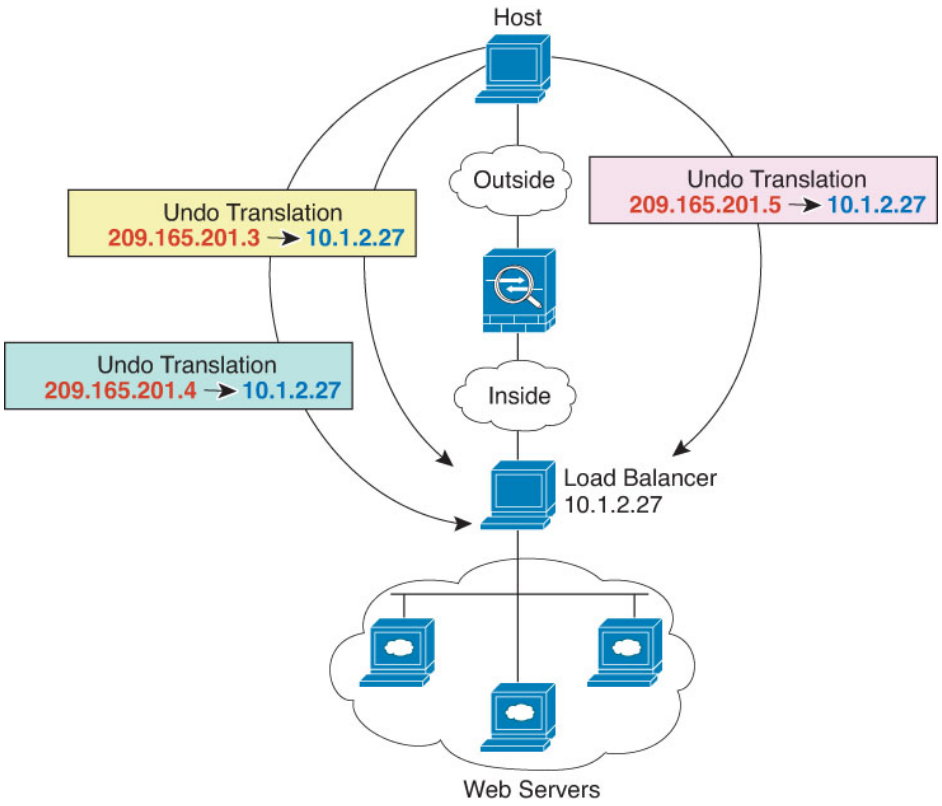
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 *13 :* 一対多のスタティック *NAT*



たとえば、10.1.2.27 にロードバランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。この例の設定方法については、複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロードバランサ （224 ページ）を参照してください。

図 *14 : 1* 対多のスタティック *NAT* の例



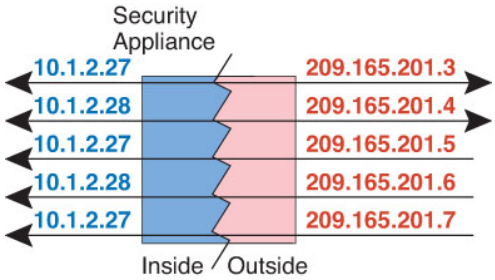
他のマッピングシナリオ（非推奨）

NAT には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多マッピングだけを使用することをお勧めします。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は1対多と同じです。ただし、設定が複雑になり、実際のマッピングがひと目で明らかにならない可能性があるため、必要とする実際の各アドレスに対して1対多の設定を作成することをお勧めします。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピングアドレスに順番にマッピングされます（Aは1、Bは2、Cは3）。すべての実際のアドレスがマッピングされたら、次のマッピングアドレスが最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（Aは4、Bは5、Cは6）。この結果、実際の各アドレスに対して複数のマッピングアドレスが存在することになります。1対多の設定のように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 *15*：少対多のスタティック *NAT*

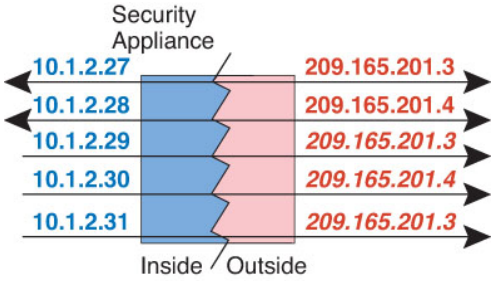


多対少または多対1の設定では、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足する前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピング プールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の5つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注） 多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じIPアドレスに変換されると、アドレスの競合がある（5つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 *16 :* 多対少のスタティック *NAT*



このようにスタティック ルールを使用するのではなく、双方向の開始を必要とするトラフィックに 1 対 1 のルールを作成し、残りのアドレスにダイナミック ルールを作成することをお勧めします。

スタティック ネットワーク オブジェクト NAT またはポート変換を設定したスタティック NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してスタティック NAT ルールを設定する方法について説明します。

手順

ステップ 1 （任意）マッピング アドレスにネットワーク オブジェクト（**object network** コマンド）またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。

- オブジェクトを使用する代わりに、インライン アドレスを設定するか、またはインターフェイス アドレスを指定できます（ポート変換を使用するスタティック NAT の場合）。
- オブジェクトを使用する場合は、オブジェクトまたはグループにホスト、範囲、またはサブネットを入れることができます。

ステップ 2 NAT を設定するネットワーク オブジェクトを作成または編集します。**object network** *obj_name*

例：

```
hostname(config)# object network my-host-obj1
```

ステップ 3 （正しいアドレスがあるオブジェクトを編集する場合はスキップする）変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host** {*IPv4_address*|*IPv6_address*}：単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask*|*IPv6_address/IPv6_prefix*}：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6

の場合、2001:DB8:0:CD30::/60のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

- **range** *start_address end_address*：アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例：

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

ステップ 4 オブジェクト IP アドレスの**スタティック NAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。

nat[(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_host_ip* | *mapped_obj* |**interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp** | **sctp**} *real_port mapped_port*] [**no-proxy-arp**]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。

- マッピング IP アドレス：マッピング IP アドレスを次のいずれかとして指定できます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。スタティック NAT （193 ページ）を参照してください。

  - *mapped_inline_host_ip*：インライン ホスト IP アドレス。これにより、ホストオブジェクトに 1 対 1 のマッピングが提供されます。サブネットオブジェクトの場合は、インラインホストアドレスに対して同じネットマスクが使用され、マッピングされたインラインホストのサブネット内のアドレスに対して 1 対 1 の変換が行われます。範囲オブジェクトの場合は、マッピングされたアドレスには、範囲オブジェクトにある同じ数のホストが含まれ、それらはマッピングされたホストアドレスから始まります。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲として定義され、172.20.1.1 をマッピング アドレスとして指定する場合、マッピング範囲には、172.20.1.1 ～ 172.20.1.6 が含まれます。NAT46 または NAT66 変換では、IPv6 ネットワーク アドレスを指定できます。

  - *mapped_obj*：既存のネットワーク オブジェクトまたはグループ。IP アドレスの範囲に 1 対 1 のマッピングを行うには、同じ数のアドレスを含む範囲を含むオブジェクトを選択します。

  - **interface**：（ポート変換を設定したスタティック NAT のみ）マッピング インターフェイスの IP アドレスがマッピング アドレスとして使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc*

に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジ グループ メンバーのときは、**interface** を指定できません）このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。**service** キーワードも必ず設定します

- ネットツーネット：（任意）NAT 46 の場合、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に、というように変換されます。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。
- DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「NAT を使用した DNS クエリと応答の書き換え （250 ページ）」を参照してください。
- ポート変換：（ポート変換を設定したスタティック NAT のみ）希望するプロトコル キーワードと実際のポートおよびマッピング ポートとともに **service** を指定します。ポート番号または予約済みポートの名前（**http** など）のいずれかを入力できます。
- プロキシ ARP なし：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。プロキシ ARP のディセーブル化が必要となる可能性がある状況については、マッピング アドレスとルーティング （233 ページ）を参照してください。

例：

```
hostname(config-network-object)#
nat (inside,outside) static MAPPED_IPS service tcp 80 8080
```

例

次の例では、内部にある実際のホスト 10.1.1.1 の、DNS リライトがイネーブルに設定された外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

次の例では、内部にある実際のホスト 10.1.1.1 の、マッピングされたオブジェクトを使用する外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
```

```
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

次の例では、10.1.1.1 の TCP ポート 21 の、外部インターフェイスのポート 2121 への、ポート変換を設定したスタティック NAT を設定します。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21
2121
```

次の例では、内部 IPv4 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

次の例では、内部 IPv6 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

スタティック Twice NAT またはポート変換を設定したスタティック NAT の設定

この項では、Twice NAT を使用してスタティック NAT ルールを設定する方法について説明します。

手順

ステップ 1 送信元の実際のアドレス、送信元のマッピング アドレス、宛先の実際のアドレス、および宛先のマッピング アドレスに、ホストまたは範囲のネットワーク オブジェクト（**object network** コマンド）、またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。宛先のマッピング アドレスに FQDN ネットワーク オブジェクトを使用することもできます。

- ポート変換を設定した送信元のスタティック インターフェイス NAT のみを設定する場合は、送信元のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。
- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを作成する場合は、次のガイドラインを考慮してください。

- マッピングされたオブジェクトまたはグループには、ホスト、範囲、またはサブネットを含めることができます。
- スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT （193 ページ）」を参照してください。

ステップ 2 （オプション）次のサービス オブジェクトを作成します。

- 送信元または宛先の実際のポート
- 送信元または宛先のマッピング ポート

サービス オブジェクトには、送信元ポートと宛先ポートの両方を含めることができますが、両方のサービス オブジェクトに送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバーなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。

ステップ 3 **スタティック NAT** を設定します。

nat [**(***real_ifc***,***mapped_ifc***)**] [*line* | {**after-object** [*line*]}] **source static** *real_ob* [*mapped_obj* | **interface** [**ipv6**]] [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | **no-proxy-arp**] [**inactive**] [**description** *desc*]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。
- セクションおよび行：（任意）デフォルトでは、NAT 規則は、NAT テーブルのセクション 1 の末尾に追加されます（NAT ルールの順序 （157 ページ）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。
- 送信元アドレス：
  - 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT に使用される **any** キーワードを使用しないでください。
  - マッピング アドレス：異なるネットワーク オブジェクトまたはグループを指定します。ポート変換を設定したスタティック インターフェイス NAT に限り、**interface** キーワードを指定できます。**ipv6** を指定すると、インターフェイスの IPv6 アドレス

が使用されます。**interface** を指定する場合、**service** キーワードも設定します（この場合、サービス オブジェクトは送信元ポートだけを含む必要があります）。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジ グループ メンバーのときは、**interface** を指定できません）詳細については、「ポート変換を設定したスタティック NAT （194 ページ）」を参照してください。

- 宛先アドレス（任意）：
  - マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービス オブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジ グループ メンバーのときは、**interface** を指定できません）
  - 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

- ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービス オブジェクトの順序は、**service** *real_obj mapped_obj* です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービス オブジェクトの順序は、**service** *mapped_obj real_obj* です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2 つめのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合は、実際のポートとマッピング ポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービス オブジェクトを使用するだけです。

- ネットツーネット：（任意）NAT 46 の場合、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に、というように変換されます。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。

- DNS：（任意、送信元にのみ適用されるルール）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。**宛先** アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「NAT を使用した DNS クエリと応答の書き換え （250 ページ）」を参照してください。

- 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。
- プロキシ ARP なし：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング （233 ページ）」を参照してください。
- 非アクティブ：（任意）コマンドを削除する必要なくこの規則を非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。
- 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例：

```
hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped
destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC
```

例

次に、ポート変換を使用するスタティック インターフェイス NAT の使用例を示します。外部にあるホストが、宛先ポート 65000 ～ 65004 を指定して外部インターフェイス IP アドレスに接続することにより、内部にある FTP サーバーにアクセスします。トラフィックは、192.168.10.100:6500 ～ 65004 の内部 FTP サーバーに変換されません。コマンドで指定した送信元アドレスとポートを変換するため、サービス オブジェクトには送信元ポート範囲（宛先ポートではなく）を指定することに注意してください。宛先ポートは「any」です。スタティック NAT は双方向であるため、「送信元」および「宛先」を使用して一次的にコマンドキーワードを扱うものであり、パケット内の実際の送信元および実際の宛先のアドレスとポートは、パケットを送信するホストによって異なります。この例では、外部から内部への接続が発生しているため、FTP サーバーの「送信元」アドレスとポートは、実際には発信元パケット内では宛先アドレスとポートになります。

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface
service FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

次に、IPv6 ネットワークへのアクセス時のある IPv6 から別の IPv6 へのスタティック変換、および IPv4 ネットワークへのアクセス時の IPv4 PAT プールへのダイナミック PAT 変換の例を示します。

```
hostname(config)# object network INSIDE_NW
```

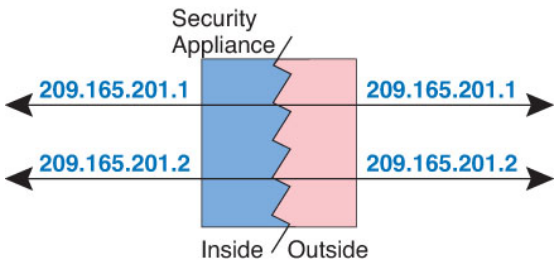
```
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254

hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW
destination static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

アイデンティティ NAT

NAT 設定では、IP アドレスを自身に変換する必要がある場合があります。たとえば、すべてのネットワークに NAT を適用する広範なルールを作成し、1 つのネットワークを NAT から除外したい場合、スタティック NAT ルールを作成してそのネットワークを自身に変換することができます。アイデンティティ NAT は、クライアント トラフィックを NAT から除外する必要のあるリモート アクセス VPN の場合に必須です。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 *17*：アイデンティティ *NAT*



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ ネットワーク オブジェクト NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。

手順

ステップ 1 （任意）マッピング アドレスにネットワーク オブジェクト（**object network** コマンド）またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。

- オブジェクトを使用する代わりに、インライン アドレスを設定できます。
- オブジェクトを使用する場合は、オブジェクトは、変換する実際のアドレスと一致する必要があります。

ステップ 2 NAT を設定するネットワーク オブジェクトを作成または編集します。**object network** *obj_name*

各オブジェクトのコンテンツが同一である必要がある場合でも、オブジェクトはマッピング アドレスに使用する内容とは異なるオブジェクトにする必要があります。

例：

```
hostname(config)# object network my-host-obj1
```

ステップ 3 （正しいアドレスがあるオブジェクトを編集する場合はスキップする）変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host** {*IPv4_address*|*IPv6_address*}：単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask*|*IPv6_address/IPv6_prefix*}：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **range** *start_address end_address*：アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例：

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

ステップ 4 オブジェクト IP アドレスの**アイデンティティ NAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。

nat [**(***real_ifc***,***mapped_ifc***)**] **static** {*mapped_inline_host_ip*|*mapped_obj*} [**no-proxy-arp**] [**route-lookup**]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使

用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。

- マッピング IP アドレス：マッピング アドレスと実際のアドレスの両方に同じ IP アドレスを設定するようにしてください。次のいずれかを使用します。
  - *mapped_inline_host_ip*：インライン ホスト IP アドレス。ホストオブジェクトの場合は、同じアドレスを指定します。範囲オブジェクトの場合は、実際の範囲における最初のアドレスを指定します（範囲内の同じ数のアドレスが使用されます）。サブネットオブジェクトの場合は、実際のサブネット内にある任意のアドレスを指定します（サブネット内のすべてのアドレスが使用されます）。
  - *mapped_obj*：実際のオブジェクトと同じアドレスを含むネットワーク オブジェクトまたはグループ。
- プロキシ ARP なし：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。プロキシ ARP のディセーブル化が必要となる可能性がある状況については、マッピング アドレスとルーティング（233 ページ）を参照してください。
- ルート ルックアップ：（ルーテッド モードのみ、インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「出力インターフェイスの決定 （236 ページ）」を参照してください。

例：

```
hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS
```

例

次の例では、インラインのマッピング アドレスを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

次の例では、ネットワーク オブジェクトを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
```

```
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

アイデンティティ Twice NAT の設定

この項では、Twice NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。

手順

ステップ 1 送信元の実際のアドレス（通常、送信元のマッピングアドレスに同じオブジェクトを使用）、宛先の実際のアドレス、および宛先のマッピングアドレスに、ホストまたは範囲のネットワーク オブジェクト（**object network** コマンド）、またはネットワーク オブジェクト グループ（**object-group network** コマンド）を作成します。宛先のマッピング アドレスに FQDN ネットワーク オブジェクトを使用することもできます。

- すべてのアドレスに対してアイデンティティ NAT を実行する場合は、送信元の実際のアドレスのオブジェクトの作成をスキップして、代わりに、**nat** コマンドで **any any** キーワードを使用します。
- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを作成する場合は、次のガイドラインを考慮してください。

- マッピングされたオブジェクトまたはグループには、ホスト、範囲、またはサブネットを含めることができます。
- 実際のオブジェクトとマッピングされた送信元オブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。

ステップ 2 （任意）次のサービス オブジェクトを作成します。

- 送信元または宛先の実際のポート
- 送信元または宛先のマッピング ポート

サービス オブジェクトには、送信元ポートと宛先ポートの両方を含めることができますが、両方のサービス オブジェクトに送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバーなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。

ステップ 3 **アイデンティティ NAT** を設定します。

nat [**(***real_ifc*,*mapped_ifc***)**] [*line* | {**after-object** [*line*]}] **source static** {*nw_obj nw_obj* | **any any**} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**no-proxy-arp**] [**route-lookup**] [**inactive**] [**description** *desc*]

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジ グループ メンバーのインターフェイスに必要）実際のインターフェイス（*real_ifc*）およびマッピング インターフェイス（*mapped_ifc*）を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、（any,outside）のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバ インターフェイスには適用されません。

- セクションおよび行：（任意）デフォルトでは、NAT 規則は、NAT テーブルのセクション 1 の末尾に追加されます（NAT ルールの順序 （157 ページ）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。

- 送信元アドレス：実際のアドレスとマッピング アドレスの両方にネットワーク オブジェクト、グループ、または **any** キーワードを指定します。

- 宛先アドレス（任意）：

  - マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービス オブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。（実際のインターフェイスがブリッジ グループ メンバーである場合、**interface** を指定することはできません）

  - 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

- ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービス オブジェクトの順序は、**service** *real_obj mapped_obj* です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービス オブジェクトの順序は、**service** *mapped_obj real_obj* です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2 つめのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合は、実際のポートとマッピング ポートの両方（コン

フィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービス オブジェクトを使用するだけです。

- プロキシ ARP なし：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング （233 ページ）」を参照してください。
- ルート ルックアップ：（任意、ルーテッド モードのみ、インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「出力インターフェイスの決定 （236 ページ）」を参照してください。
- 非アクティブ：（任意）コマンドを削除する必要なくこの規則を非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。
- 説明：（オプション）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例：

```
hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet
destination static Server1 Server1
```

NAT のモニタリング

NAT をモニターするには、次のコマンドを使用します。

- **show nat**

  各 NAT ルールのヒットを含む NAT の統計情報を表示します。

- **show nat pool**

  割り当てられたアドレスとホスト、および割り当て回数を含む、NAT プールの統計情報を表示します。

- **show running-config nat**

  NAT コンフィギュレーションを表示します。**show running-config object** を使用してオブジェクト NAT ルールを表示することはできません。修飾子を指定せずに show running-config コマンドを使用すると、NAT ルールが含まれるオブジェクトが 2 回表示されます。最初に基本アドレス設定とともに、その後、設定で NAT ルールとともにオブジェクトが表示されます。完全なオブジェクトは、アドレスと NAT ルールとともにユニットとして表示されません。

- **show xlate**

  現在の NAT セッション情報を表示します。

NAT の履歴

機能名	プラットフォームリリース	説明
ネットワーク オブジェクト NAT	8.3(1)	ネットワーク オブジェクトの IP アドレスの NAT を設定します。 **nat**（オブジェクトネットワーク コンフィギュレーション モード）、**show nat**、**show xlate**、**show nat pool** コマンドが導入または変更されました。
Twice NAT	8.3(1)	Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。 **nat**、**show nat**、**show xlate**、**show nat pool** コマンドが変更または導入されました。

機能名	プラットフォームリリース	説明
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。 8.3 よりも前の設定の場合、8.4(2) 以降への NAT 免除ルール（**nat 0 access-list** コマンド）の移行には、プロキシ ARP をディセーブルにするキーワード **no-proxy-arp** およびルート ルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 8.4(1) への移行に使用された **unidirectional** キーワードは、移行に使用されなくなりました。8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。**unidirectional** キーワードは削除されました。 nat static [no-proxy-arp] [route-lookup] コマンドが変更されました。

機能名	プラットフォームリリース	説明
PAT プールおよびラウンド ロビン アドレス割り当て	8.4(2)/8.5(1)	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。また、オプションで、PAT アドレスのすべてのポートを使用してからプール内の次のアドレスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネーブルにすることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。 **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] コマンドおよび **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] コマンドが変更されました。
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 変更されたコマンドはありません。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。
PAT プールの PAT ポートのフラットな範囲	8.4(3)	使用できる場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートには、小さい PAT プールのみがあります。 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを使用するときに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。 **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] コマンドおよび **nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] コマンドが変更されました。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。

機能名	プラットフォームリリース	説明
PAT プールの拡張 PAT	8.4(3)	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。 **nat dynamic** [**pat-pool** *mapped_object* [**extended**]] コマンドおよび **nat source dynamic** [**pat-pool** *mapped_object* [**extended**]] コマンドが変更されました。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。

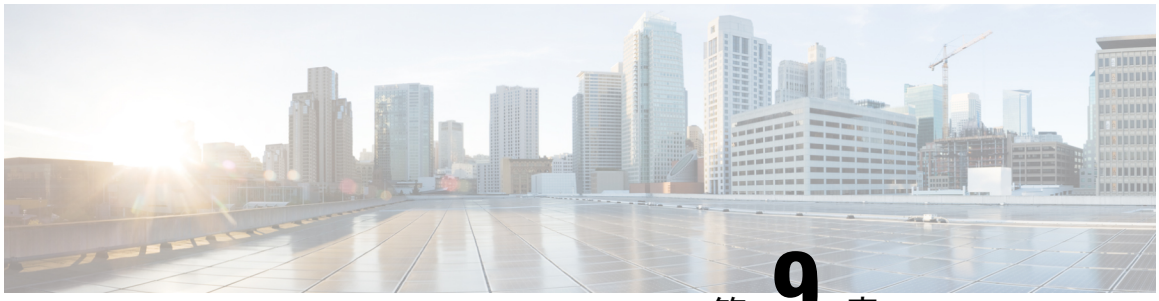
機能名	プラットフォームリリース	説明
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバーおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPNセッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは**show nat** コマンドを使用して表示できます。 ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。 • Cisco IPsec および セキュアクライアント のみがサポートされます。 • NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。 • ロードバランシングはサポートされません（ルーティングの問題のため）。 • ローミング（パブリック IP 変更）はサポートされません。 **nat-assigned-to-public-ip** *interface* コマンド（トンネル グループ一般属性コンフィギュレーション モード）が導入されました。

機能名	プラットフォームリリース	説明
IPv6 用の NAT のサポート	9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。 **nat** (global and object network configuration modes)、**show nat**、 **show nat pool**, **show xlate** の各コマンドが変更されました。
逆引き DNS ルックアップ用の NAT のサポート	9.0(1)	NAT ルールがイネーブルにされた DNS インスペクションを使用する IPv4 NAT、IPv6 NAT、および NAT64 を使用する場合、NAT は逆引き DNS ルックアップ用の DNS PTR レコードの変換をサポートするようになりました。
Per-Session PAT	9.0(1)	Per-session PAT 機能によって PAT の拡張性が向上し、クラスタリングの場合に各メンバーユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、制御ユニットに転送して制御ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンドノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえばHTTPやHTTPS の場合は、Per-session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよびUDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。 **xlate per-session**、**show nat pool** の各コマンドが導入されました。

機能名	プラットフォームリリース	説明
NAT ルール エンジンのトランザクション コミット モデル	9.3(1)	イネーブルの場合、NAT ルールの更新はルール コンパイルの完了後に適用され、ルール照合のパフォーマンスに影響を及ぼすことはありません。 **asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit** の各コマンドに **nat** キーワードが追加されました。 [Configuration] > [Device Management] > [Advanced] > [Rule Engine] 画面に NAT が追加されました。
キャリア グレード NAT の拡張	9.5(1)	キャリア グレードまたは大規模 PAT では、NAT で 1 度に 1 つのポート変換を割り当てるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。 **xlate block-allocation size** および **xlate block-allocation maximum-per-host** コマンドが追加されました。**block-allocation** キーワードが **nat** コマンドに追加されました。
SCTP に対する NAT サポート	9.5(2)	スタティック ネットワーク オブジェクト NAT ルールに SCTP ポートを指定できるようになりました。スタティック Twice NAT での SCTP の使用は推奨されません。ダイナミック NAT/PAT は SCTP をサポートしていません。 **nat static** コマンドが変更されました（オブジェクト）。
NAT のポート ブロック割り当てに対する暫定ログ	9.12(1)	NAT のポートブロックの割り当てを有効にすると、ポートブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ログの記録を有効にすると、指定した間隔でメッセージ 305017 が生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポート ブロックをレポートします（プロトコル（ICMP、TCP、UDP）、送信元および宛先インターフェイス、IP アドレス、ポート ブロックを含む）。 **xlate block-allocation pba-interim-logging** *seconds* コマンドが追加されました。

機能名	プラットフォームリリース	説明
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの **flat** オプションがデフォルトで有効になり、設定できなくなりました。	9.15(1)	PAT アドレスがクラスタのメンバーに配布される方法が変更されます。以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。制御ユニットは各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じPATアドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1023 ー 65535 を使用できるようになりました。以前は、**flat** オプションを PAT プールルールに含めることで、フラットな範囲をオプションで使用できました。**flat** キーワードはサポートされなくなりました。PAT プールは常にフラットになります。**include-reserve** キーワードは、以前は **flat** のサブキーワードでしたが、PAT プール構成内の独立したキーワードになりました。このオプションを使用すると、PAT プール内に 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（**block-allocation** PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。 新規/変更されたコマンド：**nat**、**show nat pool**

機能名	プラットフォームリリース	説明
システム定義の NAT ルールの新しいセクション 0。	9.16(1)	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。
変換後（マップ後）の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの Twice NAT サポート。	9.17(1)	www.example.com を指定する FQDN ネットワークオブジェクトを、Twice NAT ルールの変換後（マップ後）の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。



第 9 章

NAT の例と参照

次のトピックでは、NAT を設定する例を示し、さらに高度な設定およびトラブルシューティングに関する情報について説明します。

- ネットワーク オブジェクト NAT の例 （221 ページ）
- Twice NAT の例 （227 ページ）
- ルーテッドモードとトランスペアレントモードの NAT （230 ページ）
- NAT パケットのルーティング （233 ページ）
- VPN の NAT （237 ページ）
- IPv6 ネットワークの変換 （244 ページ）
- NAT を使用した DNS クエリと応答の書き換え （250 ページ）

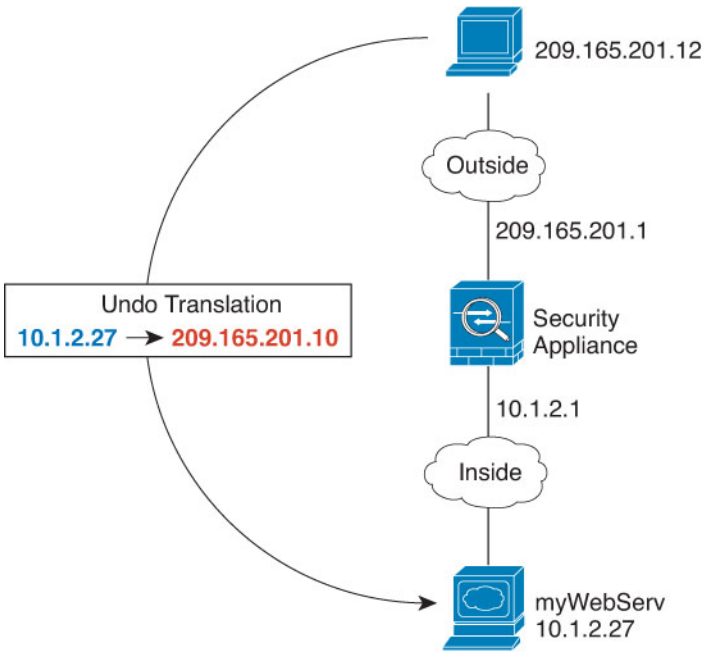
ネットワーク オブジェクト NAT の例

次に、ネットワーク オブジェクト NATの設定例を示します。

内部 Web サーバーへのアクセスの提供（スタティック NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるため、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバーへのトラフィックをホストが開始できるようにするために必要です。

図 *18 :* 内部 *Web* サーバーのスタティック *NAT*



手順

ステップ 1 内部 Web サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

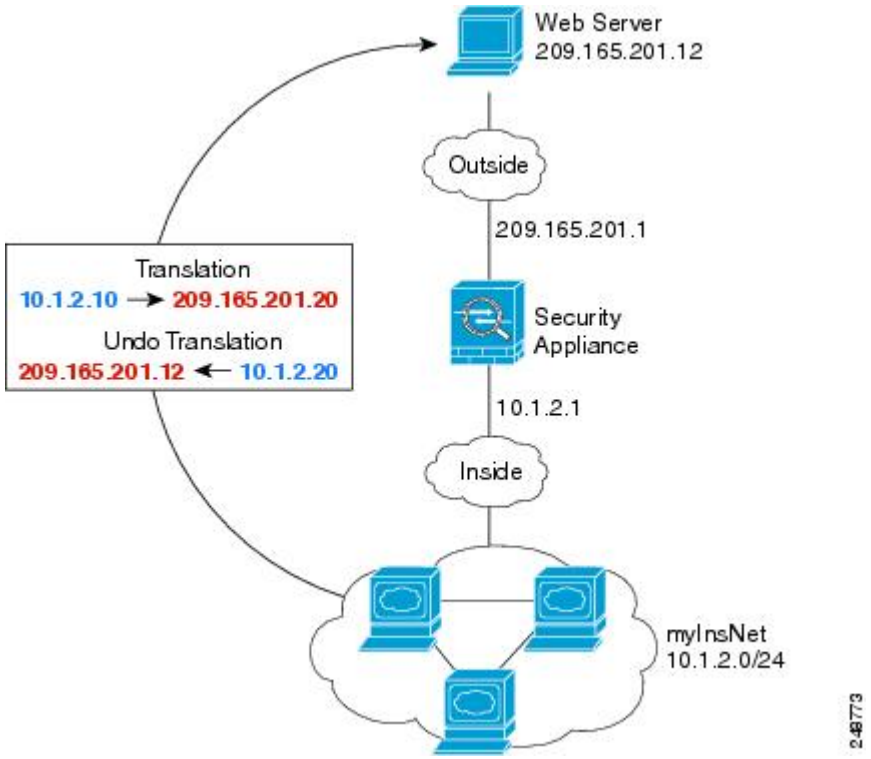
ステップ 2 オブジェクトのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

内部ホストの NAT（ダイナミック NAT）および外部 Web サーバーの NAT（スタティック NAT）

次の例では、プライベート ネットワーク上の内部ユーザーが外部にアクセスする場合、このユーザーにダイナミック NAT を設定します。また、内部ユーザーが外部 Web サーバーに接続する場合、この Web サーバーのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます。

図 *19* : 内部のダイナミック *NAT*、外部 *Web* サーバーのスタティック *NAT*



手順

ステップ 1 内部アドレスに変換するダイナミック NAT プールのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

ステップ 2 内部ネットワークのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 3 ダイナミック NAT プール オブジェクトを使用して内部ネットワークのダイナミック NAT をイネーブルにします。

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

ステップ 4 外部 Web サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 209.165.201.12
```

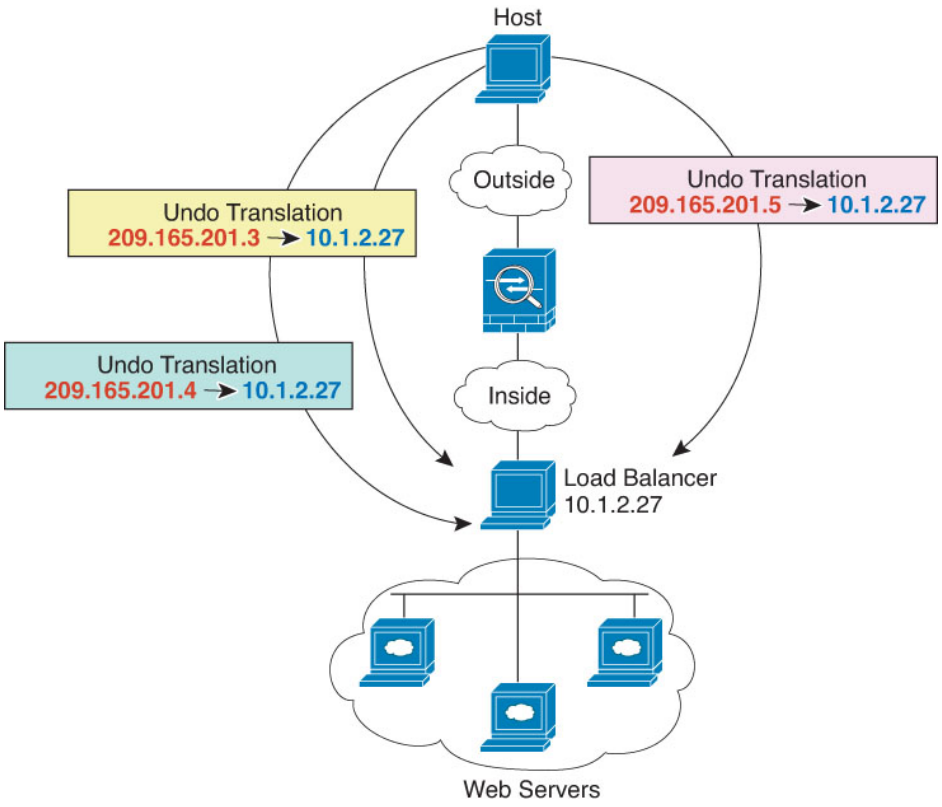
ステップ 5 Web サーバーのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ

次の例は、複数の IP アドレスに変換される内部ロード バランサを示します。外部ホストがいずれかのマッピング IP アドレスにアクセスすると、このアドレスは単一のロード バランサ アドレスに逆変換されます。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 *20 :* 内部ロード バランサに対する *1* 対多のスタティック *NAT*



手順

ステップ 1 ロードバランサをマッピングするアドレスに対し、ネットワーク オブジェクトを作成します。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

ステップ 2 ロード バランサに対するネットワーク オブジェクトを作成します。

```
hostname(config)# object network myLBHost
hostname(config-network-object)# host 10.1.2.27
```

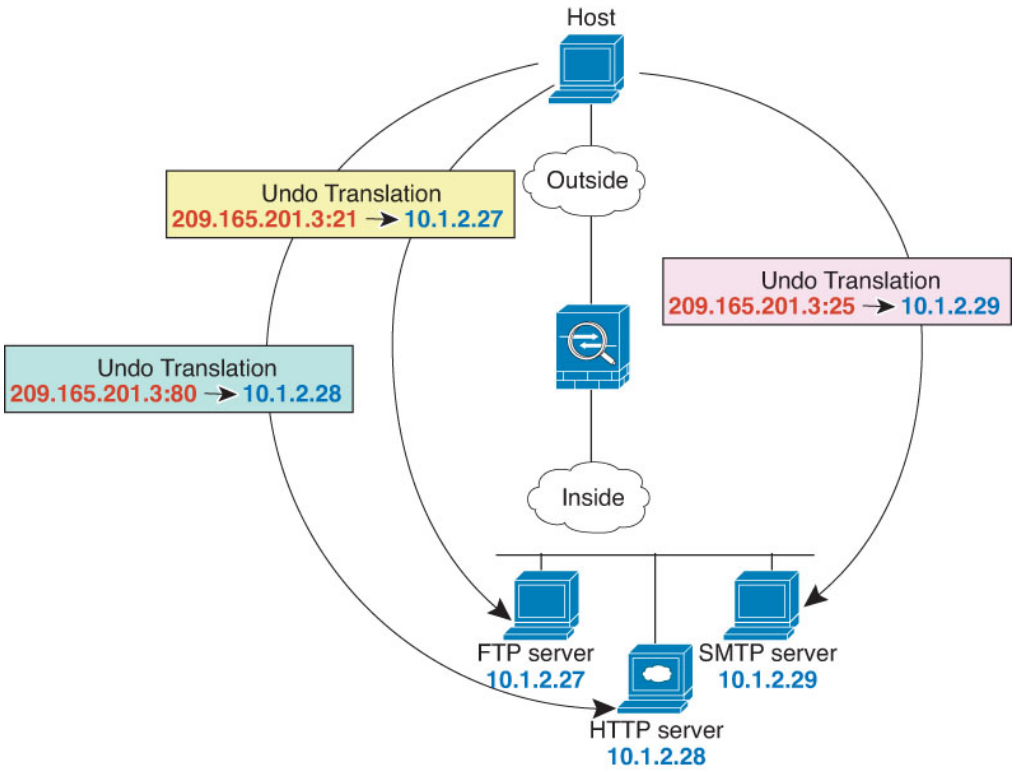
ステップ 3 範囲オブジェクトを適用するロードバランサのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザーが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバーは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用できます。

図 *21* : ポート変換を設定したスタティック *NAT*



手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成して、ポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
ftp ftp
```

ステップ 2 HTTP サーバーのネットワーク オブジェクトを作成して、ポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

```
hostname(config)# object network HTTP_SERVER
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
http http
```

ステップ 3 SMTP サーバーのネットワーク オブジェクトを作成して、ポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

```
hostname(config)# object network SMTP_SERVER
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
smtp smtp
```

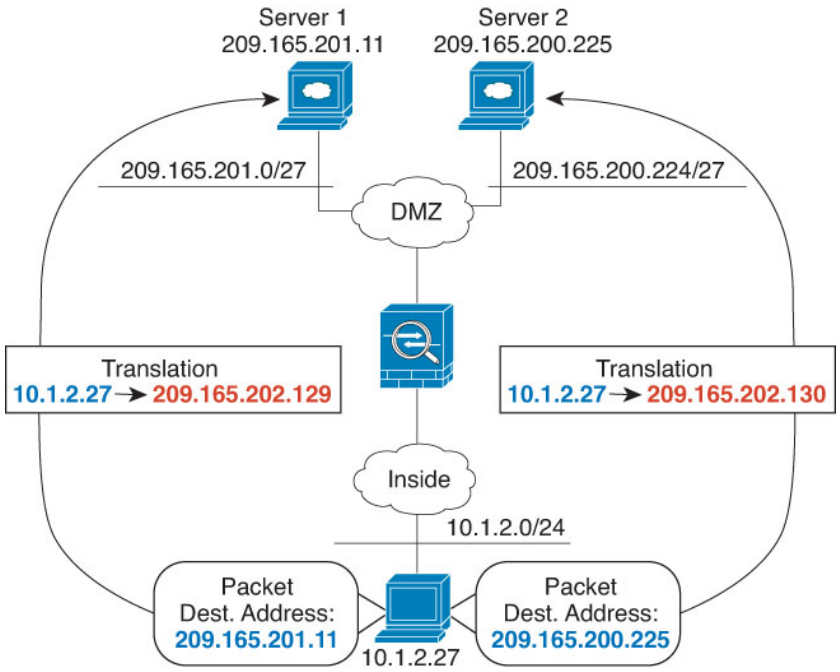
Twice NAT の例

ここでは、次の設定例を示します。

宛先に応じて異なる変換（ダイナミック Twice PAT）

次の図に、2 台の異なるサーバーにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 *22 :* 異なる宛先アドレスを使用する *Twice NAT*



手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを追加します。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

ステップ 3 PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4 最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

宛先アドレスは変換しないため、実際の宛先アドレスとマッピング宛先アドレスの両方に同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。

ステップ 5 DMZ ネットワーク 2 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

ステップ 6 PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

ステップ 7 2 つめの Twice NAT ルールを設定します。

例：

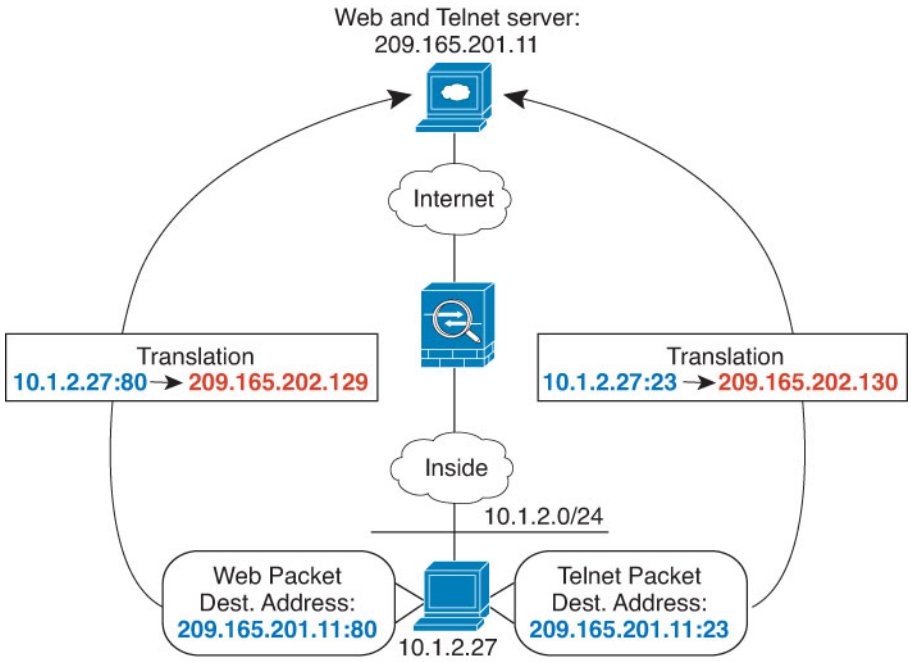
```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT）

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバーにアクセスすると、実際のアドレスは 209.165.202.129:

ポートに変換されます。ホストが Web サービスを求めて同じサーバーにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 *23 :* 異なる宛先ポートを使用する *Twice NAT*



手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを追加します。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 2 Telnet/Web サーバーのネットワーク オブジェクトを追加します。

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

ステップ 3 Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4 Telnet のサービス オブジェクトを追加します。

```
hostname(config)# object service TelnetObj
```

```
hostname(config-network-object)# service tcp destination eq telnet
```

ステップ 5 最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

宛先アドレスまたはポートを変換しないため、実際の宛先アドレスとマッピング宛先アドレスに同じアドレスを指定し、実際のサービスとマッピング サービスに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。

ステップ 6 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

ステップ 7 HTTP のサービス オブジェクトを追加します。

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

ステップ 8 2 つめの Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

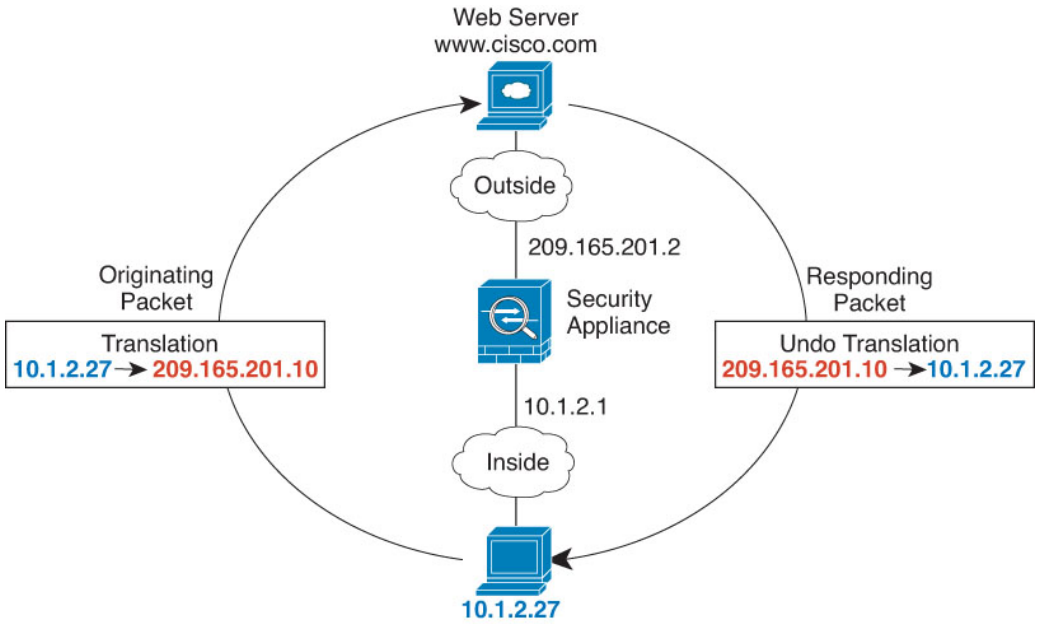
ルーテッドモードとトランスペアレントモードの NAT

NAT は、ルーテッド モードおよびトランスペアレント ファイアウォール モードの両方に設定できます。次の項では、各ファイアウォールモードの一般的な使用方法について説明します。

ルーテッドモードの NAT

次の図は、内部にプライベートネットワークを持つ、ルーテッドモードの一般的な NAT の例を示しています。

図 *24 : NAT* の例：ルーテッドモード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピング アドレス 209.165.201.10 に変換されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.10 に応答を送信し、ASA がそのパケットを受信します。これは、ASA がプロキシ ARP を実行してパケットを要求するためです。
3. ASA はその後、パケットをホストに送信する前に、マッピング アドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

トランスペアレントモードまたはブリッジグループ内の NAT

NAT をトランスペアレント モードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータが必要なくなります。これによりルーテッド モードでブリッジ グループ内で同様の機能を実行できます。

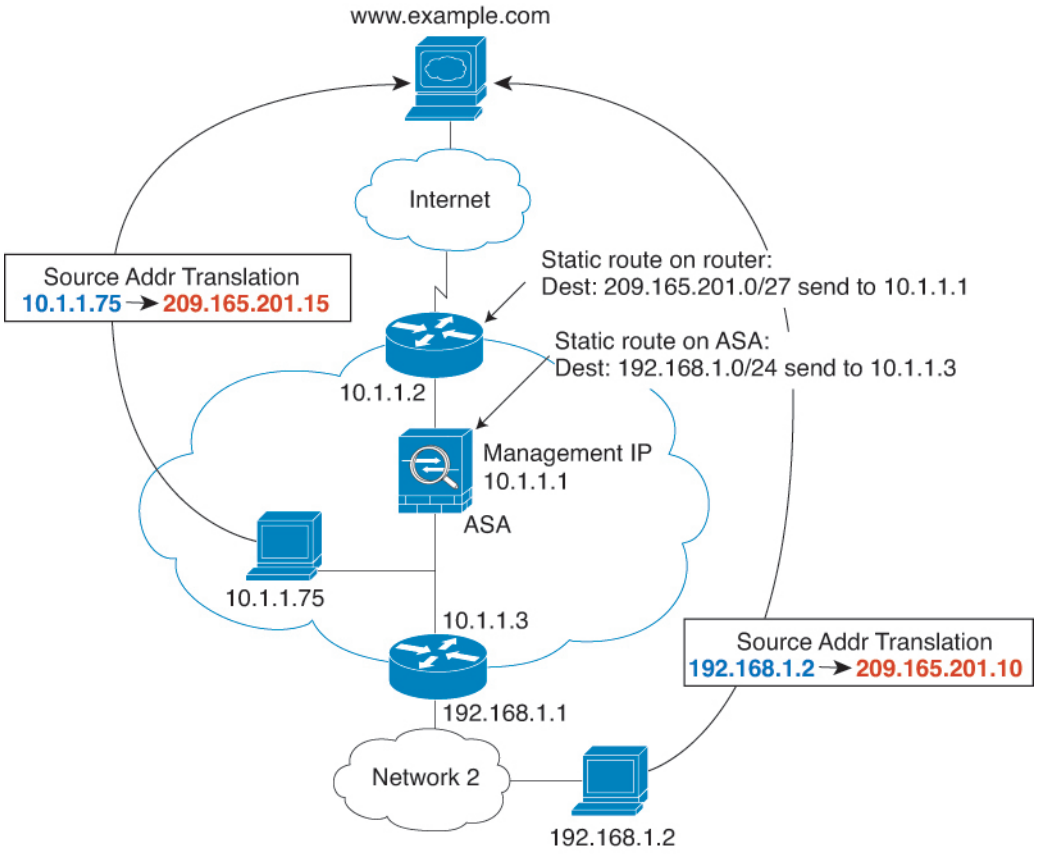
トランスペアレント モードまたは同じブリッジ グループのメンバー間のルーテッド モードの NAT には、以下の要件および制限があります。

- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジ グループ メンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- ARP インスペクションはサポートされていません。また、何らかの理由で、一方のASAのホストがもう一方のASAのホストに ARP 要求を送信し、開始ホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされる場合、実際のアドレスは ARP 要求で可視のままになります。

- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレントモードの一般的な NAT のシナリオを示します。このシナリオのトランスペアレント ファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 *25 : NAT* の例：トランスペアレント モード



1. 内部ホスト 10.1.1.75 が Web サーバーにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピング アドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.15 に応答を送信し、ASA がそのパケットを受信します。これは、アップストリーム ルータには、ASA の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。
3. その後、ASAはマッピング アドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.1.75 に戻します。実際のアドレスは直接接続されているため、ASAはそのアドレスを直接ホストに送信します。

4. ホスト 192.168.1.2 の場合も、リターン トラフィックを除き、同じプロセスが発生します。ASA はルーティング テーブルでルートを検索し、192.168.1.0/24 の ASA スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。

NAT パケットのルーティング

ASA は、マッピング アドレスに送信されるパケットの宛先である必要があります。ASA は、マッピングアドレス宛てに送信されるすべての受信パケットの出力インターフェイスを決定する必要もあります。この項では、ASA が NAT を使用してパケットの受信および送信を処理する方法について説明します。

マッピング アドレスとルーティング

実際のアドレスをマッピングアドレスに変換する場合は、選択したマッピングアドレスによって、マッピング アドレスのルーティング（必要な場合）を設定する方法が決定されます。

マッピング IP アドレスに関するその他のガイドラインについては、NAT のその他のガイドライン （162 ページ）を参照してください。

次のトピックでは、マッピング アドレスのタイプについて説明します。

マッピングインターフェイスと同じネットワーク上のアドレス

接続先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用した場合、ASA はプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することによって、マッピングアドレスを宛先とする通信を代行受信します。この方法では、ASAがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるため、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピングインターフェイスの IP アドレスも使用できます。

（注） マッピング インターフェイスを任意のインターフェイスとして設定し、マッピング インターフェイスの 1 つとして同じネットワーク上のマッピング アドレスを指定すると、そのマッピング アドレスの ARP 要求を別のインターフェイスで受信する場合、入力インターフェイスでそのネットワークの ARP エントリを手動で設定し、その MAC アドレスを指定する必要があります。通常、マッピングインターフェイスに任意のインターフェイスを指定して、マッピングアドレスの固有のネットワークを使用すると、この状況は発生しません。**arp** コマンドを使用して、ARP を設定します。

一意のネットワーク上のアドレス

宛先（マッピング）インターフェイスのネットワーク上で使用可能な数より多くのアドレスが必要な場合は、別のサブネット上でアドレスを指定できます。アップストリームルータには、ASA を指しているマッピング アドレスのスタティック ルートが必要です。

また、ルーテッド モードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピング アドレスの ASA にスタティック ルートを設定し、ルーティング プロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク（10.1.1.0/24）には NAT を使用して、マッピング IP アドレス 209.165.201.5 を使用する場合、209.165.201.5 255.255.255.255（ホスト アドレス）に対して、10.1.1.99 ゲートウェイへのスタティック ルートを設定し、これを再配布できます。

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

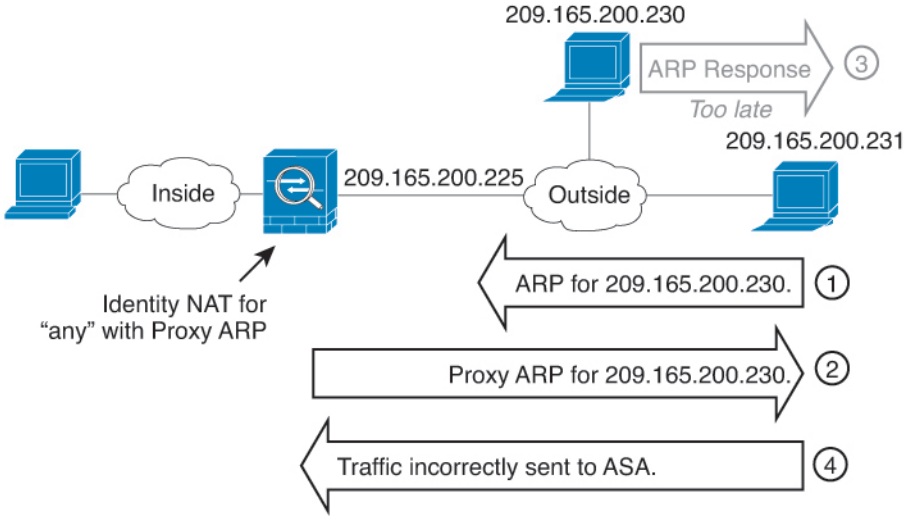
トランスペアレントモードの場合、実際のホストが直接接続されているのであれば、ASA をポイントするようにアップストリームルータのスタティックルートを設定し、ブリッジグループの IP アドレスを指定します。トランスペアレント モードのリモート ホストの場合は、上流に位置するルータのスタティック ルートで、代わりに下流ルータの IP アドレスを指定できます。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。必要に応じて標準スタティック NAT のプロキシ ARP を無効にできます。その場合は、アップストリーム ルータに適切なルートがあることを確認する必要があります。

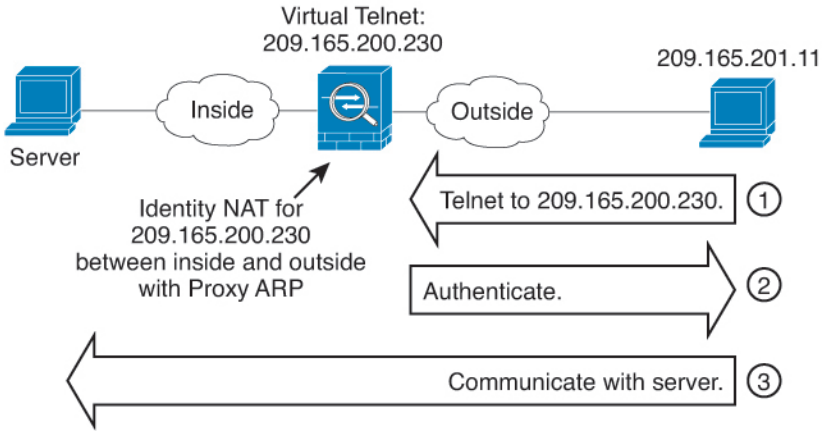
アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。たとえば、「任意」の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP を有効のままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（「任意」のアドレスと一致する）NAT ルールと一致します。このとき、実際には ASA 向けのパケットでない場合でも、ASA はこのアドレスの ARP をプロキシします（この問題は、twice NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に ASA の ARP 応答を受信した場合、トラフィックは誤って ASA に送信されます。

図 *26* : アイデンティティ *NAT* に関するプロキシ *ARP* の問題



まれに、アイデンティティ NAT に対してプロキシ ARP が必要になります（仮想 Telnet など）。AAA をネットワーク アクセスに使用すると、ホストは、その他のトラフィックが通過する前に、Telnet などのサービスを使用して ASA に対して認証する必要があります。必要なログインを提供するために、ASA に仮想 Telnet サーバを設定できます。外部から仮想 Telnet アドレスにアクセスする場合は、プロキシ ARP 機能専用アドレスのアイデンティティ NAT ルールを設定する必要があります。仮想 Telnet の内部プロセスにより、プロキシ ARP では ASA は NAT ルールに応じて送信元インターフェイスからトラフィックを送信するのではなく、仮想 Telnet アドレス宛てのトラフィックを保持できます（次の図を参照してください）。

図 *27* : プロキシ *ARP* と仮想 *Telnet*



リモート ネットワークのトランスペアレント モードのルーティング要件

トランスペアレント モードで NAT を使用する場合、一部のタイプのトラフィックには、スタティック ルートが必要になります。詳細については、一般的な操作の設定ガイドを参照してください。

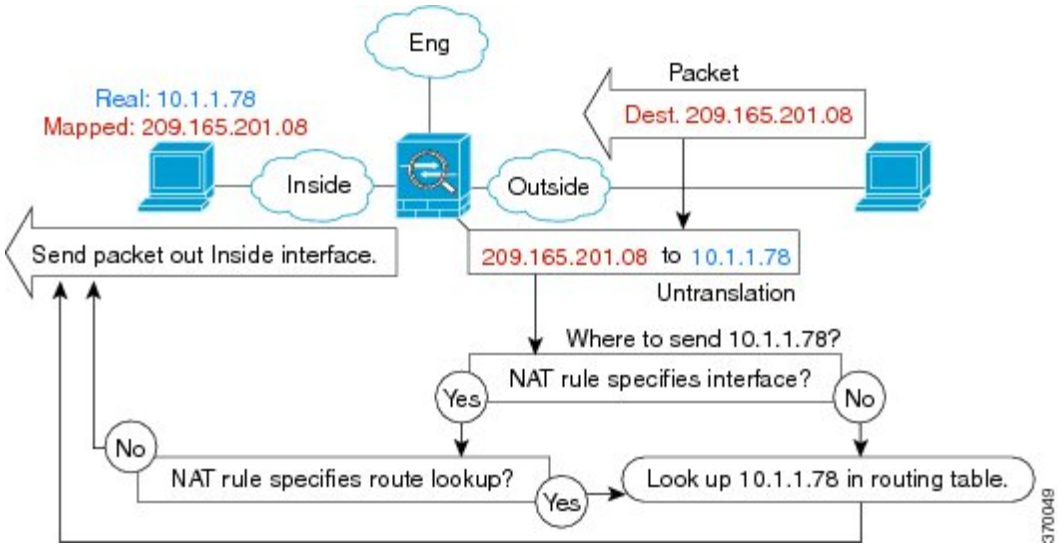
出力インターフェイスの決定

NAT を使用していて、ASA がマッピング アドレスのトラフィックを受信する場合、ASA は NAT ルールに従って宛先アドレスを逆変換し、実際のアドレスにパケットを送信します。ASA は、次の方法でパケットの出力インターフェイスを決定します。

- トランスペアレント モードまたはルーテッドモードのブリッジグループ インターフェイス：ASA は NAT ルールを使用して実際のアドレスの出力インターフェイスを決定します。NAT ルールの一部として送信元、宛先のブリッジグループ メンバー インターフェイスを指定する必要があります。
- ルーテッドモードの通常インターフェイス：ASA は、次のいずれかの方法で出力インターフェイスを決定します。
  - NAT ルールでインターフェイスを設定する：ASA は NAT ルールを使用して出力インターフェイスを決定します。ただし、代わりにオプションとして常にルート ルックアップを使用することもできます。一部のシナリオでは、ルート ルックアップの上書きが必要になる場合があります。
  - NAT ルールでインターフェイスを設定しない：ASA はルート ルックアップを使用して出力インターフェイスを決定します。

次の図に、ルーテッドモードでの出力インターフェイスの選択方法を示します。ほとんどの場合、ルート ルックアップは NAT ルールのインターフェイスと同じです。ただし、一部の構成では、2 つの方法が異なる場合があります。

図 *28 : NAT* によるルーテッド モードでの出力インターフェイスの選択



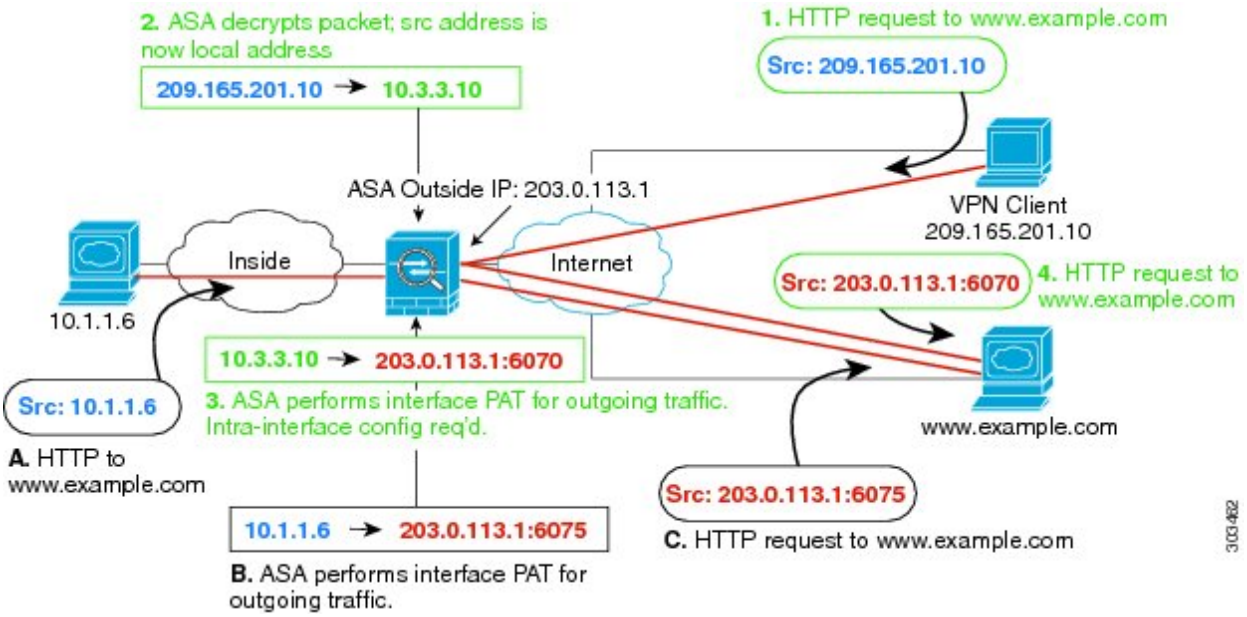
VPN の NAT

次のトピックでは、さまざまなタイプの VPN を用いた NAT の使用例について説明します。

NAT とリモート アクセス VPN

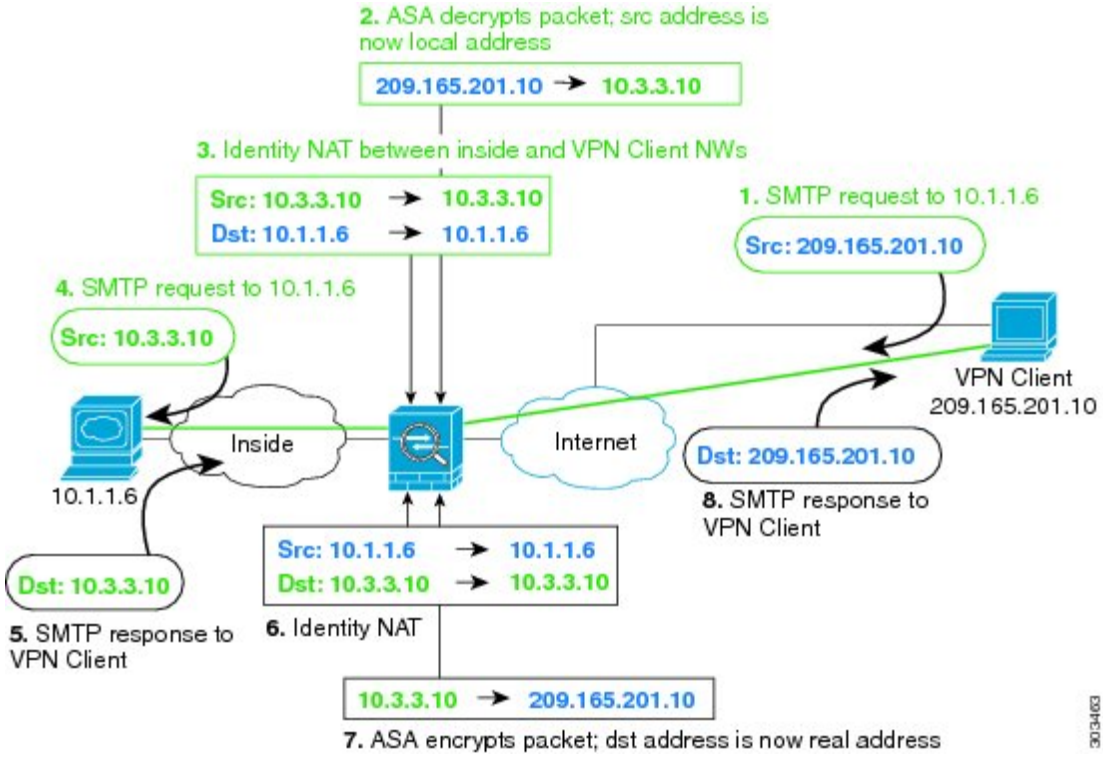
次の図に、内部サーバー（10.1.1.6）とインターネットにアクセスする VPN クライアント（209.165.201.10）の両方を示します。VPN クライアント用のスプリット トンネリング（指定したトラフィックのみが VPN トンネル上でやりとりされる）を設定しない限り、インターネット バインドされた VPN トラフィックも ASA を経由する必要があります。VPN トラフィックが ASA に渡されると、ASA はパケットを復号化し、得られたパケットには送信元として VPN クライアント ローカル アドレス（10.3.3.10）が含まれています。内部ネットワークと VPN クライアント ローカル ネットワークの両方で、インターネットにアクセスするために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。VPN トラフィックが、入ってきたインターフェイスと同じインターフェイスから出て行けるようにするには、インターフェイス内通信（別名「ヘアピン ネットワーキング」）をイネーブルにする必要があります。

図 *29* : インターネット宛 *VPN* トラフィックのインターフェイス *PAT*（インターフェイス内）



次の図に、内部のメール サーバーにアクセスする VPN クライアントを示します。ASA は、内部ネットワークと外部ネットワークの間のトラフィックが、インターネットアクセス用に設定したインターフェイス PAT ルールに一致することを期待するので、VPN クライアント（10.3.3.10）から SMTP サーバー（10.1.1.6）へのトラフィックは、リバース パス障害が原因で廃棄されます。10.3.3.10 から 10.1.1.6 へのトラフィックは、NAT ルールに一致しませんが、10.1.1.6 から 10.3.3.10 へのリターン トラフィックは、送信トラフィックのインターフェイス PAT ルールに一致する必要があります。順方向および逆方向のフローが一致しないため、ASA は受信時にパケットをドロップします。この障害を回避するには、それらのネットワーク間のアイデンティティ NAT ルールを使用して、インターフェイス PAT ルールから VPN クライアント内部のトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 *30 : VPN* クライアントのアイデンティティ *NAT*



上記のネットワークのための次のサンプル NAT の設定を参照してください。

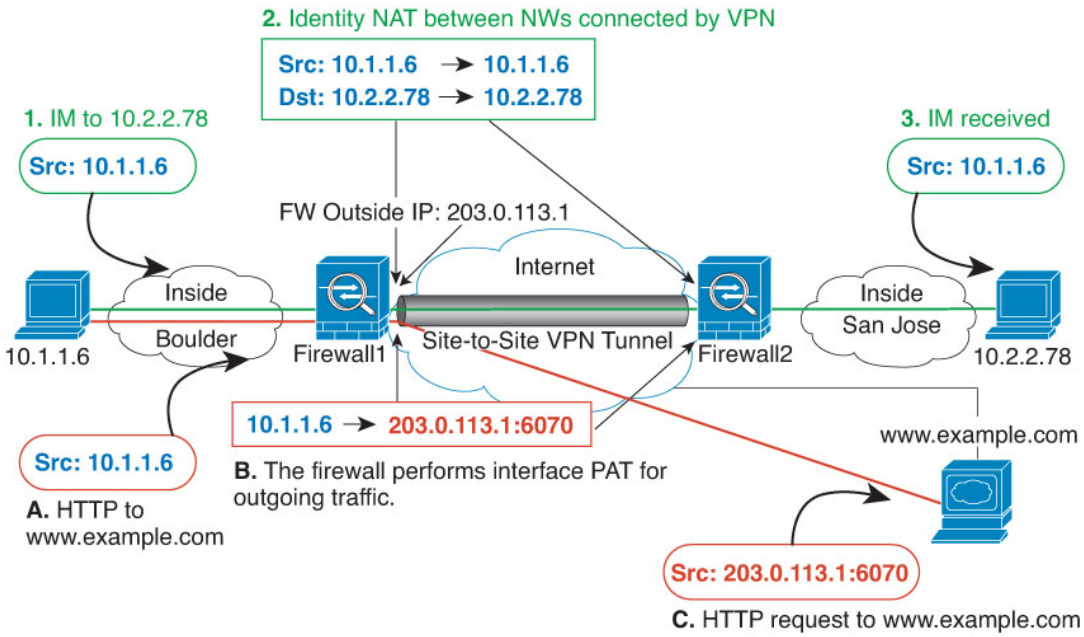
```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local
vpn_local
```

NAT およびサイト間 VPN

次の図に、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて（たとえばボールダーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用していま

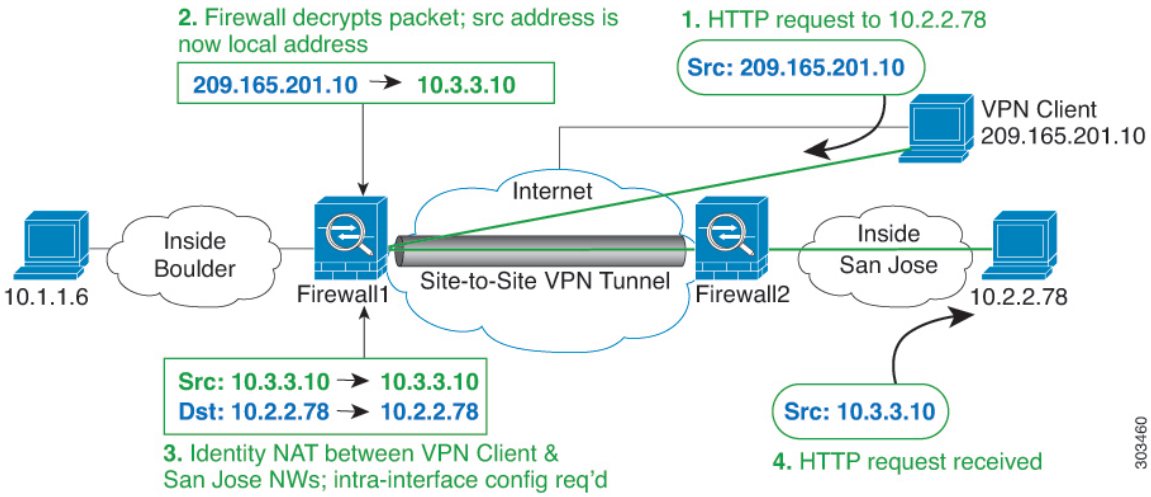
す。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 *31* : サイトツーサイト *VPN* のためのインターフェイス *PAT* およびアイデンティティ *NAT*



次の図に、Firewall1（ボールダー）に接続する VPN クライアントと、Firewall1 と Firewall2（サンノゼ）間のサイトツーサイト トンネル上でアクセス可能なサーバー（10.2.2.78）に対する Telnet 要求を示します。これはヘアピン接続であるため、VPN クライアントからの非スプリットトンネルのインターネット宛トラフィックにも必要な、インターフェイス内通信を有効化する必要があります。発信 NAT ルールからこのトラフィックを除外するため、VPN に接続された各ネットワーク間で行うのと同様に、VPN クライアントとボールダーおよびサンノゼのネットワーク間でアイデンティティ NAT を設定する必要もあります。

図 *32* : サイトツーサイト *VPN* への *VPN* クライアント アクセス



2 番目の例の Firewall1（ボールダー）については、次の NAT の設定例を参照してください。

```
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local
destination static sanjose_inside sanjose_inside
```

Firewall2（サンノゼ）については、次の NAT の設定例を参照してください。

```
! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
```

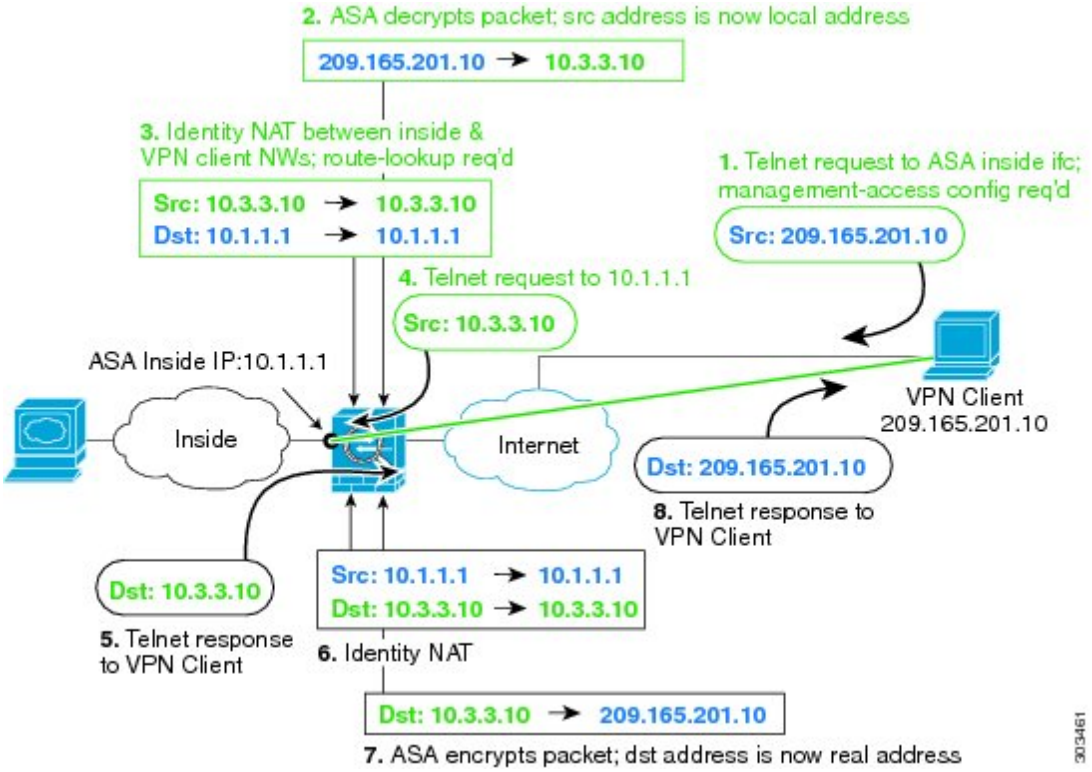
```
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static boulder_inside boulder_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static vpn_local vpn_local
```

NAT および VPN 管理アクセス

VPN を使用する場合、ASA を開始したインターフェイス以外のインターフェイスへの管理アクセスを許可することができます（**management-access** コマンドを参照）。たとえば、外部インターフェイスから ASA を開始する場合、管理アクセス機能では、ASDM、SSH、Telnet、または SNMP を使用して内部インターフェイスに接続することが可能です。または、内部インターフェイスに ping を実行できます。

次の図に、ASA の内部インターフェイスに Telnet 接続する VPN クライアントを示します。管理アクセス インターフェイスを使用し、NAT とリモート アクセス VPN （237 ページ）またはNAT およびサイト間 VPN （239 ページ）に従ってアイデンティティ NAT を設定する場合、ルート ルックアップ オプションを使用して NAT を設定する必要があります。ルート ルックアップがない場合、ASA は、ルーティング テーブルの内容に関係なく、NAT コマンドで指定されたインターフェイスからトラフィックを送信します。次の例では、出力インターフェイスは内部インターフェイスです。ASA で、内部ネットワークに管理トラフィックを送信しません。これは、内部インターフェイスの IP アドレスには戻りません。ルート ルックアップ オプションを使用すると、ASA は、内部ネットワークの代わりに内部インターフェイスの IP アドレスに直接トラフィックを送信できます。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルートルックアップオプションがあっても正しい出力インターフェイス（内部）になるため、通常のトラフィック フローは影響を受けません。ルートルックアップオプションの詳細については、出力インターフェイスの決定 （236 ページ）を参照してください。

図 *33 : VPN* 管理アクセス



上記のネットワークのための次のサンプル NAT の設定を参照してください。

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Enable management access on inside ifc:
management-access inside

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local
destination static inside_nw inside_nw route-lookup
```

NAT と VPN のトラブルシューティング

VPN を使用した NAT の問題をトラブルシューティングするためには、次の監視ツールを参照してください。

- パケット トレーサ：正しく使用した場合、パケット トレーサは、パケットが該当している NAT ルールを表示します。
- **show nat detail**：特定の NAT ルールのヒット カウントおよび変換解除されたトラフィックを表示します。
- **show conn all**：ボックス トラフィックとの間の接続を含むアクティブ接続を表示します。

動作に関係のない設定と動作するための設定をよく理解するには、次の手順を実行します。

1. アイデンティティ NAT を使用しない VPN を設定します。
2. **show nat detail** と **show conn all** を入力します。
3. アイデンティティ NAT の設定を追加します。
4. **show nat detail** と **show conn all** を繰り返します。

IPv6 ネットワークの変換

IPv6 専用ネットワークと IPv4 専用ネットワークの間でトラフィックを通過させる必要がある場合、NAT を使用してアドレス タイプを変換する必要があります。2 つの IPv6 ネットワークの場合でも、外部ネットワークから内部アドレスを隠す必要がある場合があります。

IPv6 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4（およびその反対）に変換します。2 つのポリシーを定義する必要があります。1 つは IPv6 から IPv4 への変換用、もう 1 つは IPv4 から IPv6 への変換用です。これは、1 つの twice NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS応答をリライトする必要があります。宛先を指定するときに twice NAT ルールで DNS リライトを有効にすることができないため、2 つの Network Object NAT ルールを作成することがより適切なソリューションです。

（注） NAT46 がサポートするのは、スタティック マッピングのみです。

- NAT66：IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

（注） NAT64 および NAT 46 は、標準的なルーテッド インターフェイスでのみ使用できます。NAT66 は、ルーテッド インターフェイスとブリッジ グループ メンバー インターフェイスの両方で使用できます。

NAT64/46：IPv6 アドレスの IPv4 への変換

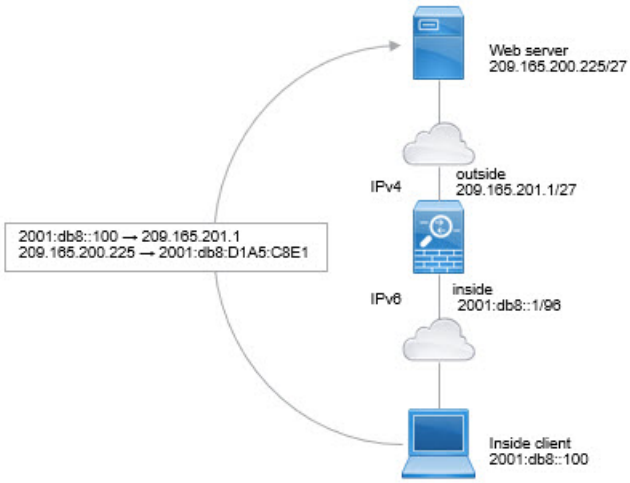
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。2 つのアドレス プール（IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレス プールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレス プール）を定義する必要があります。

- NAT64 ルール用の IPv4 アドレス プールは通常は小さく、一般的に IPv6 クライアント アドレスを使用して 1 対 1 のマッピングを設定するにはアドレスが足りない場合があります。ダイナミック PAT は、ダイナミック NAT やスタティック NAT と比べると、多数の IPv6 クライアント アドレスがある場合でも、比較的簡単に対応できます。
- NAT 46 ルールの IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数と等しいか、それより多くなります。これによって、各 IPv4 アドレスを別の IPv6 アドレスにマッピングできます。NAT 46 はスタティック マッピングのみをサポートするため、ダイナミック PAT を使用することはできません。

送信元 IPv6 ネットワークと宛先 IPv4 ネットワークの 2 つのポリシーを定義する必要があります。これは、1 つの twice NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに twice NAT ルールで DNS リライトを有効にすることができないため、2 つの Network Object NAT ルールを作成することがより適切なソリューションです。

NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット

次に、内部 IPv6 専用ネットワークがある場合に、インターネットに送信される通信を IPv4 に変換する簡単な例を示します。この例では、DNS 変換が不要なため、1 つの twice NAT ルールで NAT64 と NAT46 の両方の変換を実行できると想定しています。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、

2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。

手順

ステップ 1 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
```

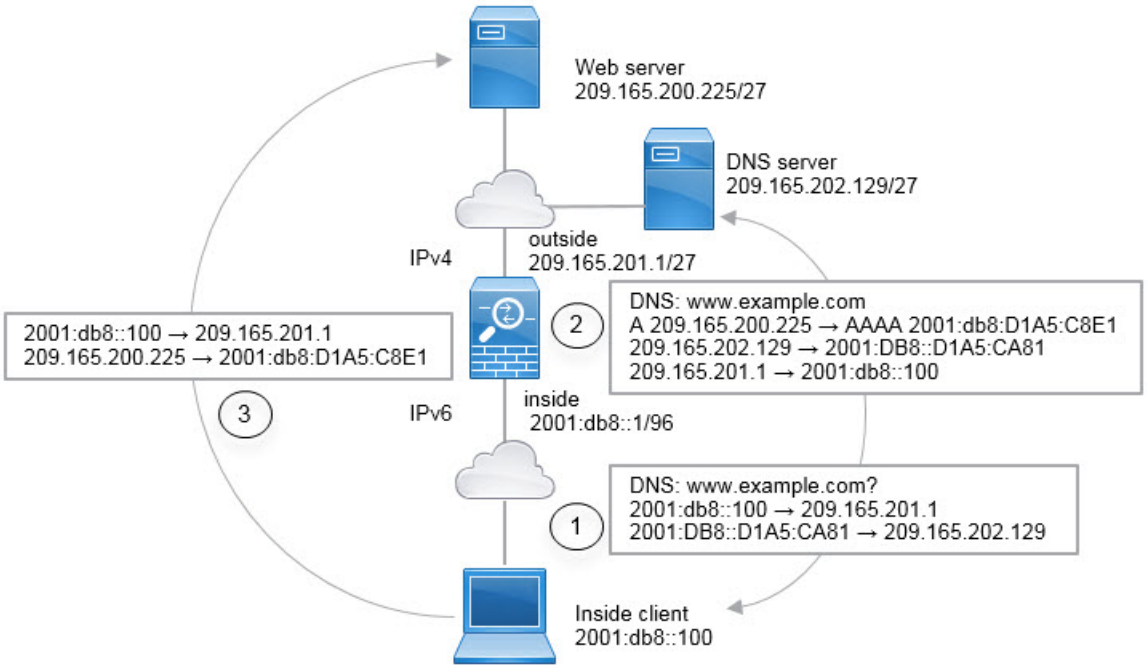
ステップ 2 IPv6 ネットワークを IPv4 に変換して再び戻すための Twice NAT ルールを作成します。

```
hostname(config)# nat (inside,outside) source dynamic inside_v6 interface
destination static inside_v6 any
```

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。逆に、内部インターフェイスに入る外部ネットワークの IPv4 アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。

NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク

次の図は、内部の IPv6 専用ネットワークが存在し、内部ユーザーが必要とするいくつかの IPv4 専用サービスが外部のインターネット上に存在する一般的な例です。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。NAT46 ルールで DNS の書き換えを有効にすると、外部 DNS サーバーからの応答を A（IPv4）レコードから AAAA（IPv6）レコードに変換でき、アドレスが IPv4 から IPv6 に変換されます。

次は、内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとしている場合の Web 要求の一般的なシーケンスです。

1. クライアントのコンピュータが 2001:DB8::D1A5:CA81 にある DNS サーバーに DNS 要求を送信します。NAT ルールにより、DNS 要求の送信元と宛先が次のように変換されます。
   - 2001:DB8::100 を 209.165.201.1 上の一意のポートに変換（NAT64 インターフェイス PAT ルール）。
   - 2001:DB8::D1A5:CA81 を 209.165.202.129 に変換（NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 に相当します）。
2. DNS サーバーが、www.example.com が 209.165.200.225 であることを示す A レコードに応答します。DNS の書き換えが有効になっている NAT46 ルールにより、A レコードが IPv6 の同等の AAAA レコードに変換されて、AAAA レコードの 209.165.200.225 が 2001:db8:D1A5:C8E1 に変換されます。なお、DNS 応答の送信元アドレスと宛先アドレスは変換されません。
   - 209.165.202.129 を 2001:DB8::D1A5:CA81 に変換
   - 209.165.201.1 を 2001:db8::100 に変換
3. これで、IPv6 クライアントが Web サーバーの IP アドレスを取得し、www.example.com（2001:db8:D1A5:C8E1）に HTTP 要求を送信できます。（D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します）。HTTP 要求の送信元と宛先が変換されます。
   - 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換（NAT64 インターフェイス PAT ルール）。
   - 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換（NAT46 ルール）。

次の手順では、この例の設定方法について説明します。

手順

ステップ 1 内部 IPv6 ネットワーク用のネットワーク オブジェクトを作成し、NAT64 ルールを追加します。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface
```

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスへのトラフィックは、外部インターフェイスの IPv4 アドレスを使用した NAT64 PAT 変換を取得します。

ステップ 2 外部 IPv4 ネットワーク用に変換された IPv6 ネットワークのネットワーク オブジェクトを作成し、NAT46 ルールを追加します。

```
hostname(config)# object network outside_v4_any
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat(outside,inside) static 2001:db8::/96 dns
```

このルールを使用すると、内部インターフェイスに届く外部ネットワークのすべての IPv4 アドレスが、組み込みの IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答が A（IPv4）レコードから AAAA（IPv6）レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

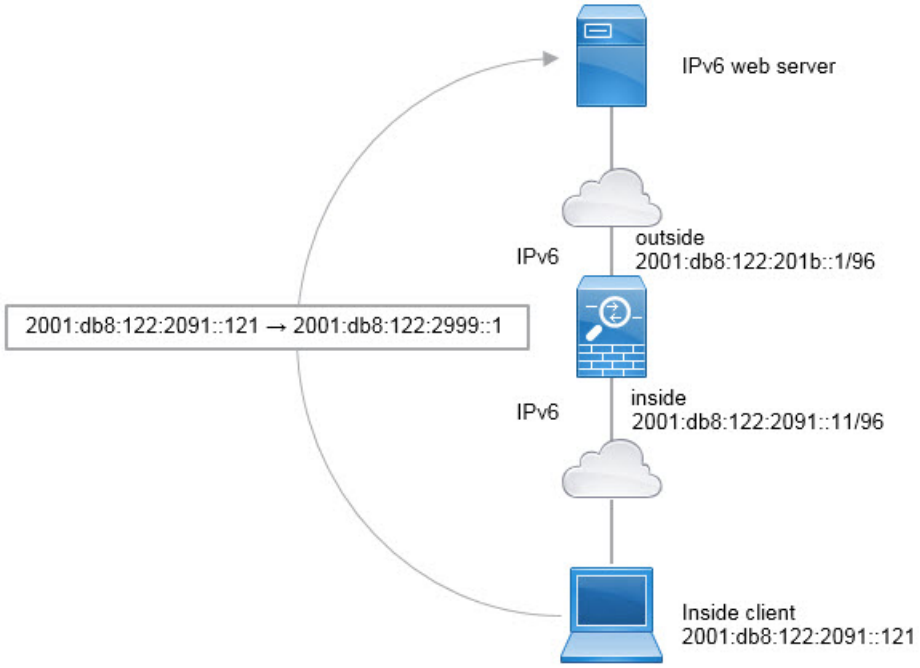
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

異なるアドレス タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。これらのルールは、Network Object NATを使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、twice NAT のみを使用してスタティック NAT ルールを単方向にできます。

NAT66 の例：ネットワーク間のスタティック変換

Network Object NATを使用して、IPv6 アドレスプール間のスタティック変換を設定できます。次の例では、2001:db8:122:2091::/96 ネットワークの内部アドレスを 2001:db8:122:2999::/96 ネットワークの外部アドレスに変換する方法について説明します。



手順

内部 IPv6 ネットワークのネットワーク オブジェクトを作成し、スタティック NAT のルールを追加します。

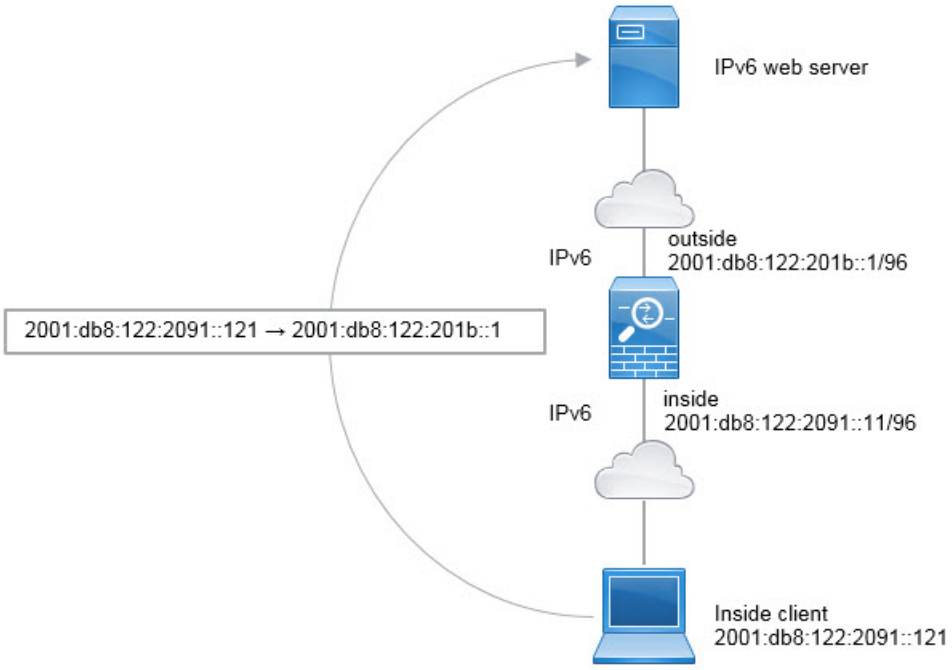
```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) static 2001:db8:122:2999::/96
```

このルールにより、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスへのすべてのトラフィックは、2001:db8:122:2999::/96 ネットワークのアドレスへのスタティック NAT66 変換を取得します。

NAT66 の例：シンプルな IPv6 インターフェイス PAT

NAT66 を実装するための簡単なアプローチは、外部インターフェイスの IPv6 アドレス上の異なるポートに内部アドレスを動的に割り当てる方法です。

NAT66 のインターフェイス PAT ルールを設定すると、そのインターフェイスに設定されているすべてのグローバル アドレスが PAT のマッピングに使用されます。インターフェイスのリンクローカル アドレスまたはサイトローカル アドレスは、PAT には使用されません。



手順

内部 IPv6 ネットワークのネットワーク オブジェクトを作成し、ダイナミック PAT ルールを追加します。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface ipv6
```

このルールでは、内部インターフェイスの 2001:db8:122:2091::/96 subnet サブネットから外部インターフェイスへのトラフィックは、外部インターフェイス用に設定された IPv6 グローバル アドレスのいずれかへの NAT66 PAT 変換を取得します。

NAT を使用した DNS クエリと応答の書き換え

DNS の書き換えは、DNS 応答で返される IP アドレスが NAT 設定と一致するアドレスに置き換えられるように、DNS 応答を変更するプロセスです。これは、DNS レコード内の元のアドレスではなく、変換されたアドレスをリクエスト送信者に返す必要がある場合に使用されます。この機能は DNS 改ざんとも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスを書き換えます（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコー

ド）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へ書き換えられます。逆に、任意のインターフェイスからマッピン インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。この機能は、NAT44、NAT66、 NAT46、および NAT64 と連動します。

以下に、NAT ルールで DNS の書き換えを設定する必要が生じる主な状況を示します。

- ルールは NAT64 または NAT46 であり、DNS サーバは外部ネットワークにあります。DNS A レコード（IPv4 用）と AAAA レコード（IPv6 用）を変換するために DNS の書き換えが必要です。
- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

DNS の書き換えには次の制限事項があります。

- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS の書き換えは PAT には適用されません。
- twice NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- DNS クエリと応答を書き換えるには、NAT ルールに対して有効な DNS NAT の書き換えを用いた DNS アプリケーション インスペクションを有効にする必要があります。デフォルトでは、有効にされた DNS NAT の書き換えによる DNS インスペクションはグローバルに適用されるため、インスペクション設定を変更する必要はありません。
- 実際には、DNS の書き換えは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、書き換えが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS の書き換えによって、DNS ダイナミック アップデートのメッセージ（オペレーション コード 5）は書き換えられません。

次のトピックで、NAT ルールの DNS の書き換え例を示します。

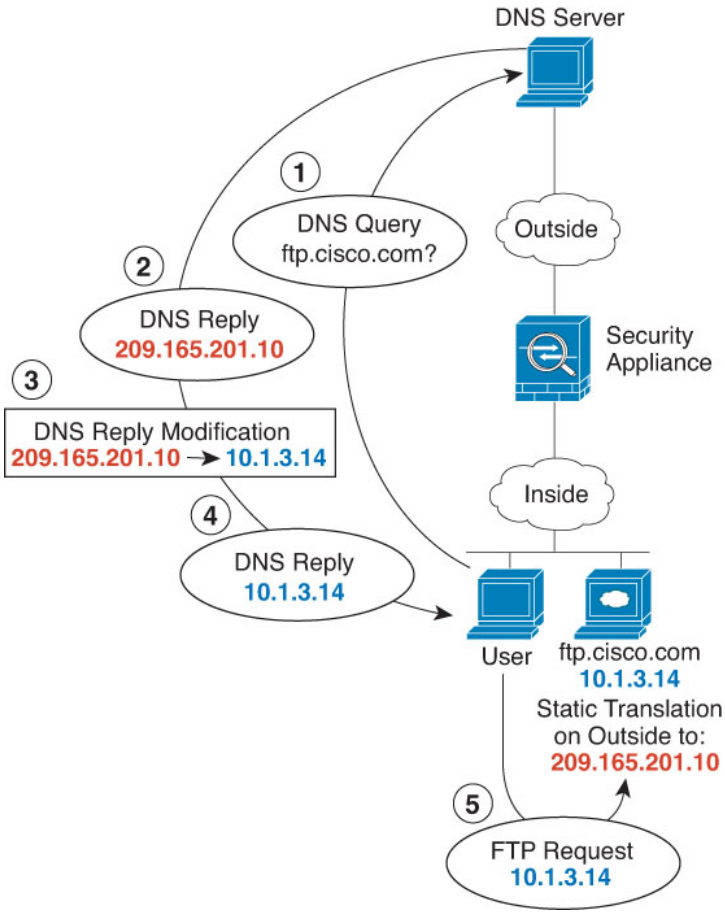
DNS 応答修正：外部の DNS サーバー

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）

を、外部ネットワーク上で確認できるマッピング アドレス（209.165.201.10）にスタティックに変換するように NAT を設定します。

この場合、このスタティック ルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して ftp.cisco.com にアクセスできる内部ユーザーは、マッピング アドレスではなく実際のアドレスを DNS サーバーから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバーはマッピング アドレス（209.165.201.10）を応答します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.3.14
```

ステップ 2 DNS 修正を設定したスタティック NAT を設定します。

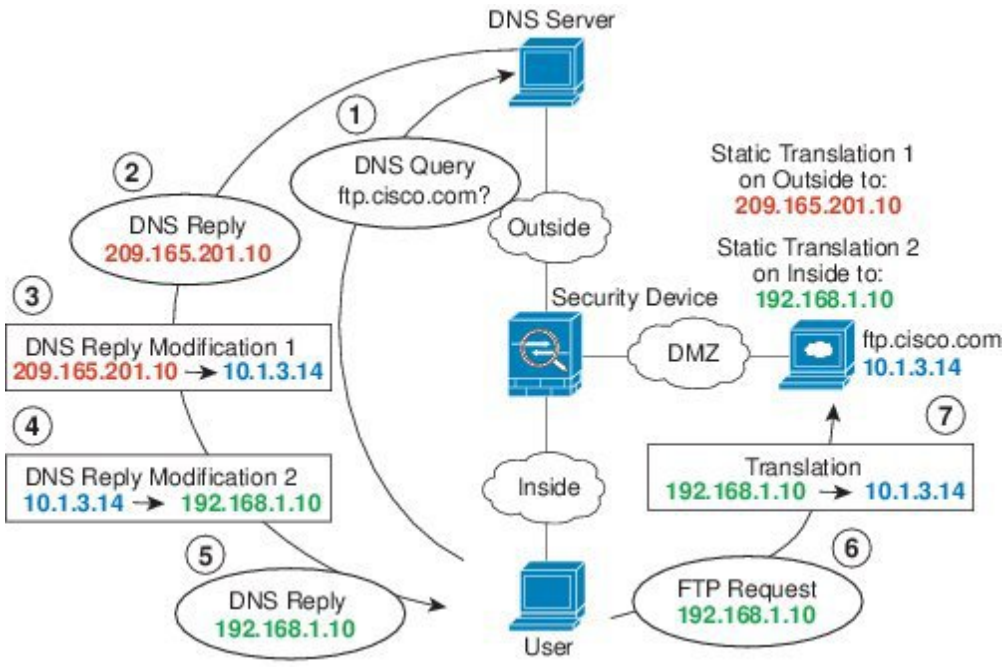
```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

DNS応答修正：別々のネットワーク上のDNSサーバー、ホスト、およびサーバー

次の図に、外部 DNS サーバーから DMZ ネットワークにある ftp.cisco.com の IP アドレスを要求する内部ネットワークのユーザーを示します。DNS サーバーは、ユーザーが DMZ ネットワーク上に存在しない場合でも、外部と DMZ 間のスタティック ルールに従って応答でマッピング アドレス（209.165.201.10）を示します。ASA は、DNS 応答内のアドレスを 10.1.3.14 に変換します。

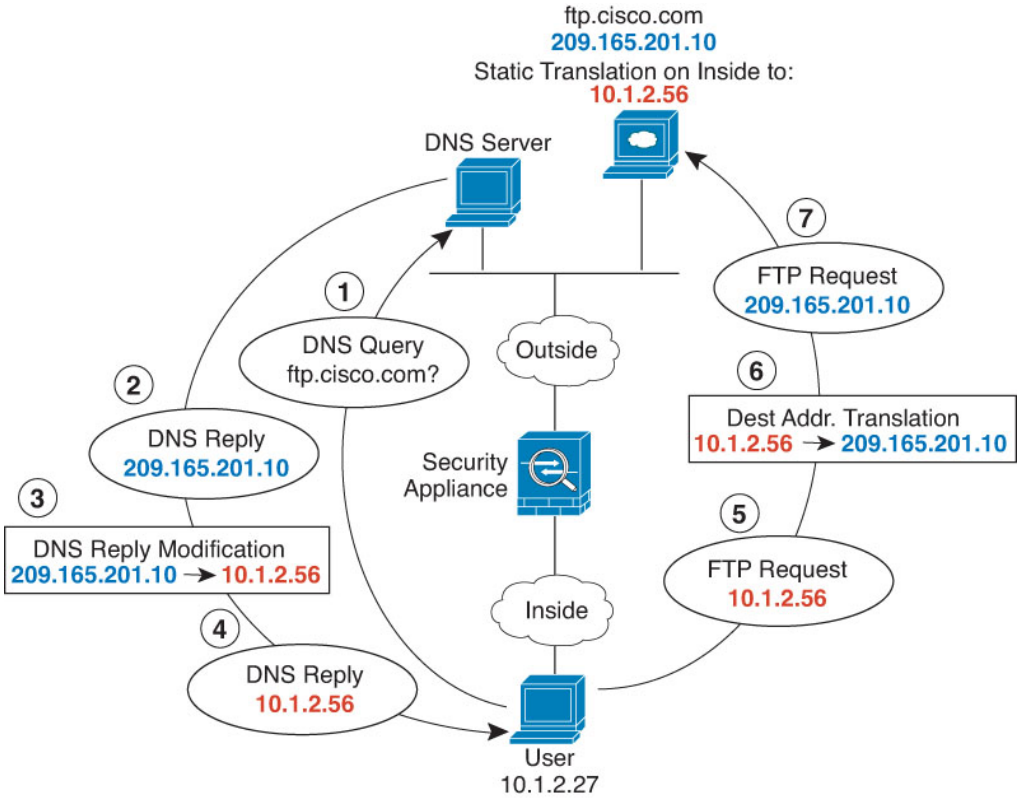
ユーザーが実際のアドレスを使用して ftp.cisco.com にアクセスする必要がある場合、これ以上の設定は必要ありません。内部と DMZ 間にもスタティック ルールがある場合は、このルールに対して DNS 応答修正もイネーブルにする必要があります。DNS 応答は、2 回変更されます。この場合、ASA は内部と DMZ 間のスタティック ルールに従ってもう一度 DNS 応答内のアドレスを 192.168.1.10 に変換します。

図 *34 : DNS* 応答修正：別々のネットワーク上の *DNS* サーバー、ホスト、およびサーバー



DNS 応答修正：ホスト ネットワーク上の DNS サーバー

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部ユーザーが ftp.cisco.com のアドレスを DNS サーバーに要求すると、DNS サーバーは実際のアドレス（209.165.20.10）を応答します。内部ユーザに ftp.cisco.com のマッピング アドレス（10.1.2.56）を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。



手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.201.10
```

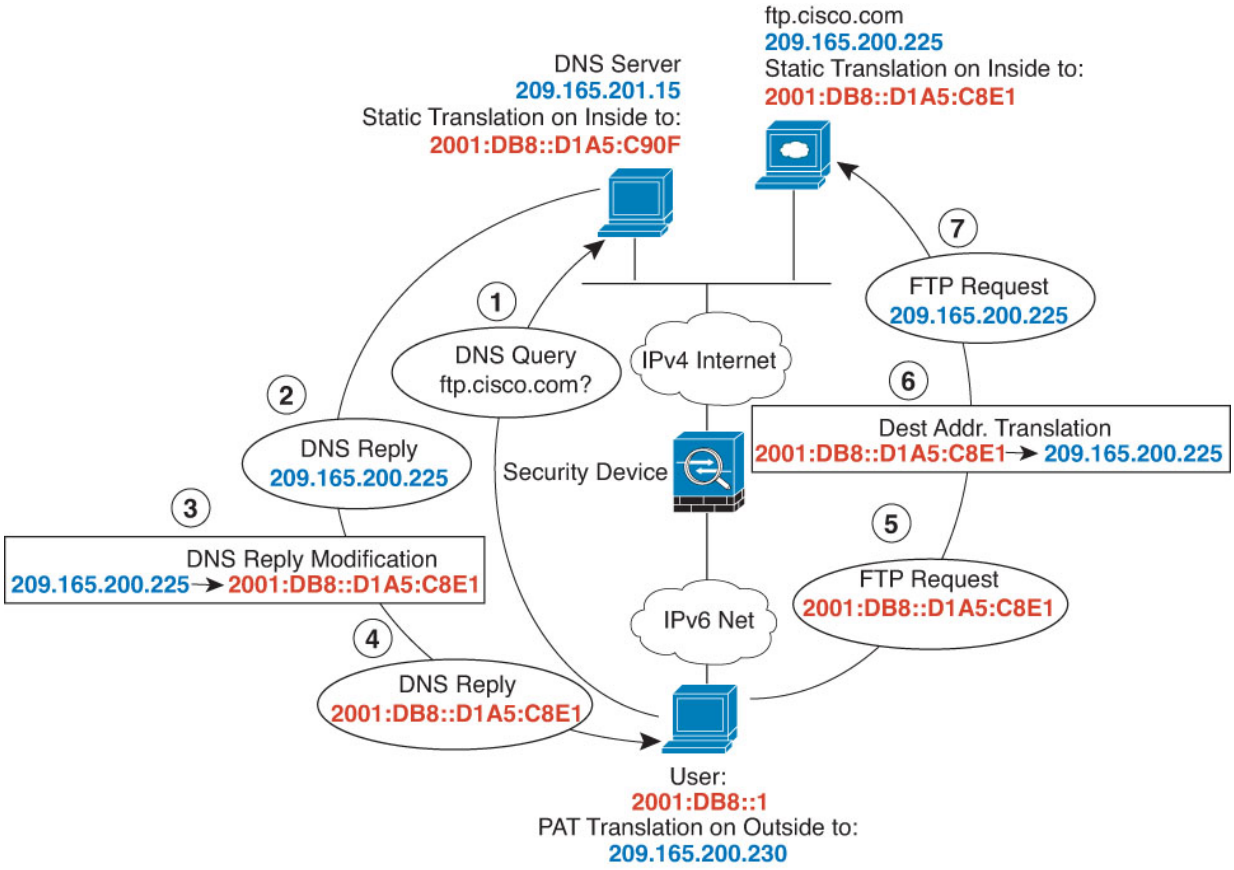
ステップ 2 DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

DNS64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザーが ftp.cisco.com のアドレスを DNS サーバーに要求すると、DNS サーバーは実際のアドレス（209.165.200.225）を応答します。

内部ユーザーに ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1：D1A5:C8E1 は IPv6 の 209.165.200.225 に相当）を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。この例には、DNS サーバーのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成して DNS 修正を設定したスタティック NAT を設定します。これは 1 対 1 変換であるため、NAT 46 の **net-to-net** オプションを含めます。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
```

```
net-to-net dns
```

ステップ 2 DNS サーバーのネットワーク オブジェクトを作成して、スタティック NAT を設定します。NAT 46 の **net-to-net** オプションを含めます。

```
hostname(config)# object network DNS_SERVER
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

ステップ 3 内部 IPv6 ネットワークを変換するための IPv4 PAT プールを設定します。

例：

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 209.165.200.230 209.165.200.235
```

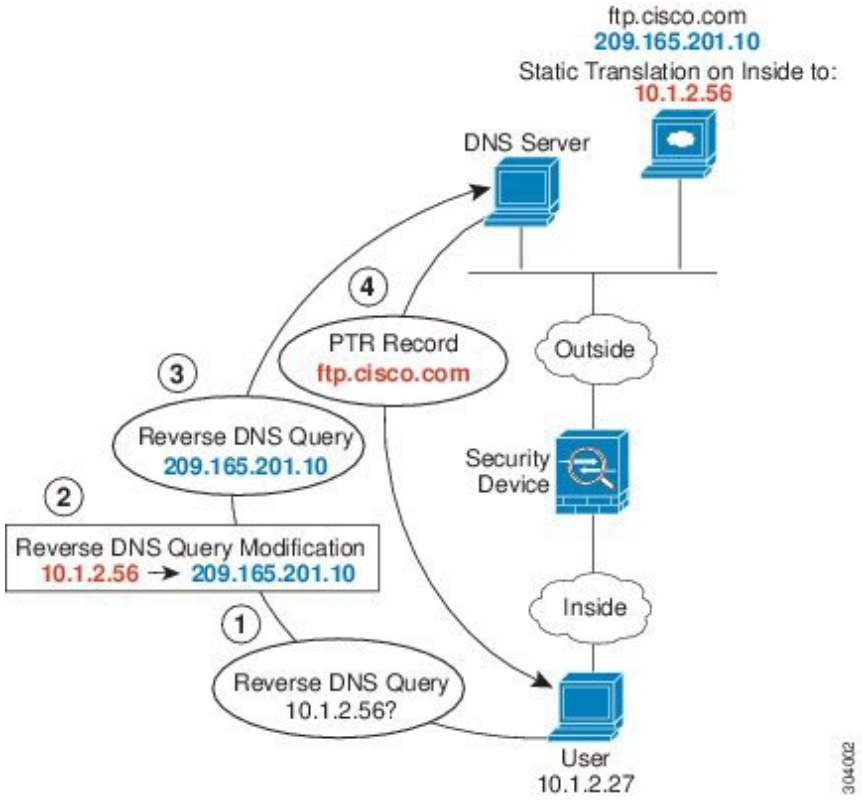
ステップ 4 内部 IPv6 ネットワークのネットワーク オブジェクトを作成して、PAT プールを設定したダイナミック NAT を設定します。

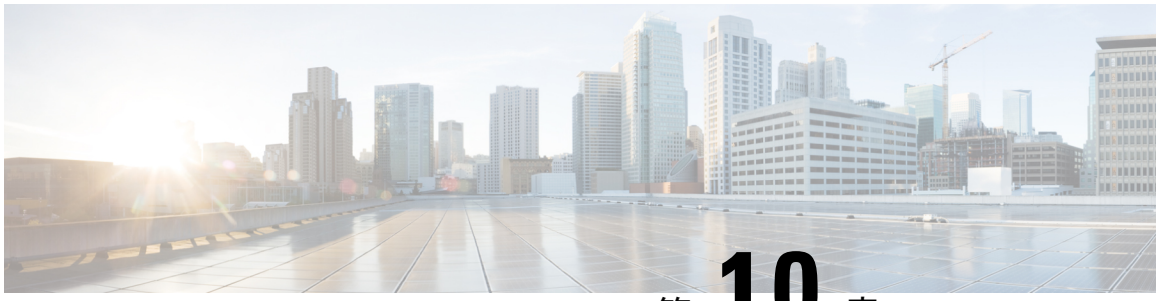
```
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

PTR の変更、ホスト ネットワークの DNS サーバー

次の図に、外部の FTP サーバーと DNS サーバーを示します。ASA には、外部サーバー用のスタティック変換があります。この場合、内部のユーザーが 10.1.2.56 の逆引き DNS ルックアップを実行する場合、ASA は実際のアドレスを使用して逆引き DNS クエリーを変更し、DNS サーバーはサーバー名、ftp.cisco.com を使用して応答します。

図 *35 : PTR* の変更、ホスト ネットワークの *DNS* サーバー





第 10 章

アドレスとポートのマッピング（MAP）

アドレスとポートのマッピング（MAP）は、IPv4 アドレスを IPv6 に変換するためのキャリアグレードの機能であるため、サービスプロバイダーエッジで IPv4 に変換される前にサービスプロバイダーの IPv6 ネットワーク経由でトラフィックを送信できます。

- アドレスとポートのマッピング（MAP）について （259 ページ）
- アドレスとポートのマッピング（MAP）に関するガイドライン （261 ページ）
- MAP-T ドメインの設定 （262 ページ）
- MAP のモニタリング （264 ページ）
- MAP の履歴 （266 ページ）

アドレスとポートのマッピング（MAP）について

アドレスとポートのマッピング (MAP) は、主にサービスプロバイダー (SP) ネットワークで使用する機能です。サービス プロバイダーは、IPv6 専用ネットワーク、MAP ドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリック インターネット上の IPv4 専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。

MAP ドメイン内のサービスプロバイダーの場合、NAT46 を介した MAP の利点は、サブスクライバの IPv4 アドレスに対する IPv6 アドレスの代替（および SP ネットワークエッジでの IPv4 への変換）がステートレスであることです。これにより、NAT46 と比較して SP ネットワーク内の効率が向上します。

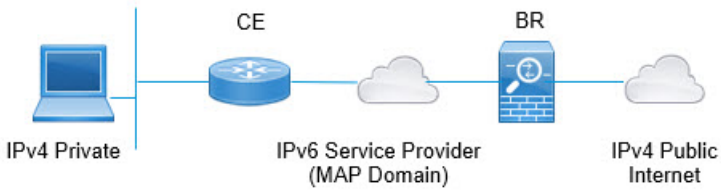
MAP 変換（MAP-T）と MAP カプセル化（MAP-E）という 2 つのマップ技術があります。ASA は MAP-T をサポートしています。MAP-E はサポートされていません。

変換によるアドレスとポートのマッピング（MAP-T）について

MAP-T では、まず、サブスクライバの IPv4 アドレスがサーバープロバイダー（SP）のパブリック IPv4 アドレスに変換されます。これは、1 対 1 のアドレスマッピングである場合も、プレフィックスまたは共有アドレスへのマッピングである場合もあります。次に、その IPv4 アドレスが MAP ドメイン内の IPv6 アドレスに変換され、パケットが SP IPv6 ネットワークを介して送信されます。ネットワークエッジで、SP の境界リレーが、パケットをパブリック IPv4

ネットワークにルーティングする前にIPv6アドレスをSPのIPv4アドレスに変換し直します。パブリック IPv4 ネットワークからサブスクライバに着信するトラフィックに対しては、まったく逆の処理が実行されます。

図 *36 : MAP-T* ネットワーク



MAP-T を使用すると、SP ネットワークを IPv6 専用アーキテクチャに移行しながら、サブスクライバは IPv4 を引き続き使用して IPv4 専用インターネットまたは SP ネットワーク外の他のサイトと通信できます。

MAP-T は NAT64 変換と同様に動作しますが、IPv4 アドレスが埋め込まれた IPv6 アドレスを使用する代わりに、ポート番号も埋め込むエンコーディングスキームを使用します。したがって、MAP-T では、デバイスが使用するポート範囲を制限できます。

MAP-T システムには、以下が含まれます。

- **カスタマーエッジ（CE）デバイス**：CE は、ホームゲートウェイ（ワイヤレスルータ、ルータ付きケーブルモデムなど）です。CE は IPv4/IPv6 変換およびネイティブ IPv6 転送を提供します。これには、WAN 側のプロバイダー向け IPv6 アドレス指定インターフェイス、およびプライベート IPv4 アドレッシングを使用してアドレス指定される 1 つ以上の LAN 側インターフェイスがあります。IPv4 から IPv6 へのパケットの変換およびその逆の変換を行うために CE で使用する 1 つ以上の MAP ドメインを設定します。
- **境界リレー（BR）デバイス**：ASA を境界リレーとしてインストールします。BR は、IPv4/IPv6 変換をサポートする、MAP ドメインのエッジにあるプロバイダー側コンポーネントです。BR には、IPv6 対応インターフェイスが少なくとも 1 つ、および IPv4 ネットワークに接続された IPv4 インターフェイスが 1 つあります。IPv4 から IPv6 へのパケットの変換およびその逆の変換を行うために BR で使用する 1 つ以上の MAP ドメインを設定します。同じ MAP ドメインルールを使用して CE と BR を設定する必要があります。
- **MAP ドメイン**：MAP ドメインは、MAP-T CE デバイスのセットと MAP-T BR デバイスのセットをグループ化するメカニズムです。ドメインは、そのドメインに割り当てられた BR デバイスと CE デバイスの間で共有されるパラメータのセットです。BR デバイスと CE デバイスのそれぞれに対して、同じパラメータを含む同じドメインを設定します。

アドレスとポートのマッピング（MAP）に関するガイドライン

ファイアウォール モードのガイドライン

MAP はルーテッドモードでのみ設定できます。トランスペアレント モードはサポートされていません。

その他のガイドライン

- ASA はメッシュモードでのパケット転送には関与しません。したがって、MAP ドメインで転送マッピングルール（FMR）を設定することはできません。
- MAP は、トンネル化された VPN トラフィック、マルチキャストトラフィック、エニーキャストトラフィックをサポートしません。
- 特定の接続で NAT と MAP の両方を使用することはできません。NAT ルールと MAP ルールが重複していないことを確認してください。ルールが重複している場合は、予期しない結果になります。
- 次のインスペクションは、MAP 変換をサポートしていません。これらのインスペクションの対象となるパケットは変換されません。
  - CTIQBE
  - DCERPC
  - [Diameter]
  - WINS 経由の名前解決
  - GTP
  - H.323、H.225、H.245、RAS
  - ILS（LDAP）
  - インスタント メッセージ
  - IP オプション（RFC 791、2113）
  - IPSec Pass Through
  - LISP
  - M3UA
  - MGCP
  - MMP
  - NetBIOS

- PPTP
- RADIUS アカウンティング
- RSH
- RTSP
- SIP
- SKINNY
- SMTP および ESMTP
- SNMP
- SQL*Net
- STUN
- Sun RPC
- TFTP
- WAAS
- XDMCP
- アクティブ FTP

MAP-T ドメインの設定

MAP-T を設定するには、1 つまたは複数のドメインを作成します。カスタマーエッジ（CE）およびボーダーリレー（BR）デバイスで MAP-T を設定する場合は、各ドメインに参加するデバイスごとに同じパラメータを使用するようにしてください。

最大 25 個の MAP-T ドメインを設定できます。マルチコンテキストモードでは、コンテキストごとに最大 25 のドメインを設定できます。

手順

ステップ 1 MAP ドメインを作成（または編集）します。

map-domain *name*

name は 48 文字以下の英数字文字列です。また、名前には、ピリオド（.）、スラッシュ（/）、およびコロン（:）の特殊文字を含めることもできます。

例：

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)#
```

ステップ 2 デフォルトマッピングルールを設定します。

default-mapping-rule *ipv6_prefix/prefix_length*

RFC 6052 に従って IPv4 宛先アドレスを埋め込むために使用する IPv6 プレフィックスを指定します。通常のプレフィックスの長さは 64 ですが、使用可能な値は 32、40、48、56、64、または 96 です。埋め込み IPv4 アドレスの後の任意の末尾ビットは 0 に設定されます。

ボーダーリレー（BR）デバイスはこのルールを使用し、MAP ドメイン外のすべての IPv4 アドレスを、MAP ドメイン内で動作する IPv6 アドレスに変換します。

例：

```
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
```

ステップ 3 基本マッピングルールを設定します。

カスタマーエッジ（CE）デバイスは、基本マッピングルールを使用して、専用 IPv4 アドレッシングまたは共有アドレスとポート セットの割り当てを決定します。CE デバイスは最初に、システムの IPv4 アドレスをプールのプレフィックスおよびポート範囲内の IPv4 アドレスおよびポート（NAT44 を使用）に変換し、次にルールの IPv6 プレフィックスによって定義されたプール内の IPv6 アドレスに、新しい IPv4 アドレスを変換します。その後、パケットはサービスプロバイダーの IPv6 専用ネットワークを介してボーダーリレー（BR）デバイスに送信されるようになります。

a) 基本マッピング ルール コンフィギュレーション モードに切り替えます。

basic-mapping-rule

b) IPv4 プレフィックスを設定します。

ipv4-prefix *ipv4_network_address netmask*

IPv4 プレフィックスは、カスタマーエッジ（CE）デバイスの IPv4 アドレス プールを定義します。CE デバイスは、最初に IPv4 アドレスを、IPv4 プレフィックスによって定義されたプール内のアドレス（およびポート番号）に変換します。次に、MAP は、デフォルトのマッピング ルールのプレフィックスを使用して、この新しいアドレスを IPv6 アドレスに変換します。

ネットワーク アドレスとサブネット マスク（たとえば、192.168.3.0 255.255.255.0）を指定します。異なる MAP ドメインで同じ IPv4 プレフィックスを使用することはできません。

c) IPv6 プレフィックスを設定します。

ipv6-prefix *ipv6_prefix/prefix_length*

IPv6 プレフィックスは、CE デバイスの IPv6 アドレスのアドレスプールを定義します。MAP は、このプレフィックスを持つ宛先アドレスと、デフォルトのマッピングルールで定義されている IPv6 プレフィックスを持つ送信元アドレスを持つパケットが、適切なポート範囲内にある場合にのみ、IPv6 パケットを IPv4 に戻します。他のアドレスから CE デバイスに送信されるすべての IPv6 パケットは、MAP を変換せずに IPv6 トラフィックとして処理されるだけです。MAP の送信元/宛先プールからのパケットは、範囲外のポートでは単にドロップされます。

IPv6 プレフィックスおよびプレフィックス長（通常は 64）を指定しますが、8 未満を指定することはできません。異なる MAP ドメインで同じ IPv6 プレフィックスを使用することはできません。

d) 開始ポートを設定します。

start-port *number*

変換されたアドレスのポートプールに表示される最初のポート。指定するポートは 1 ～ 32768 の範囲内とし、2 の累乗にする必要があります（1、2、4、8 など）。既知のポートを除外する場合は、1024 以降から開始します。

e) ポート比率を設定します。これにより、ポートプール内のポート数が決まります。

share-ratio *number*

プール内に存在する必要があるポートの数を指定します。ポート数は 1～65536 の範囲内とし、2 の累乗にする必要があります（1、2、4、8 など）。

例：

```
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

例

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

MAP のモニタリング

次のトピックでは、MAP の構成およびアクティビティをモニタリングする方法について説明します。

MAP ドメイン構成の確認

マップドメインとそのステータスを表示して、構成が正しいことを確認できます。

show map-domain コマンドによって MAP 構成が表示されます（**show running-config map-domain** コマンドと同様）が、同時にドメイン構成が有効かどうかも示されます。次の例には、2 つの

ドメイン（1 と 2）があります。この出力では、MAP ドメイン 2 が不完全なためにアクティブではないことが説明されています。

```
MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
    Rule EA-bit length 12

MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64

Warning: map-domain 2 configuration is incomplete and not in effect.
```

MAP syslog メッセージのモニタリング

syslog を有効にすると、次の syslog メッセージで MAP の動作をモニタリングできます。

- 305018: MAP translation from *interface name:source IP address/source port-destination IP address/destination port* to *interface name:translated source IP address/translated source port-translated destination IP address/translated destination port*

  新しい MAP 変換が行われました。このメッセージには、変換前と変換後の送信元および宛先が表示されます。

- 305019: MAP node address *IP address/port* has inconsistent Port Set ID encoding

  パケットのアドレスは MAP の基本的なマッピングルールに一致しますが（つまり、変換されることを意味します)、アドレス内でエンコードされたポートセット ID には（RFC7599 との）一貫性がありません。これは、このパケットの発信元である MAP ノードにソフトウェア障害がある可能性が高いことを意味します。

- 305020: MAP node with address *IP address* is not allowed to use port *port*

  パケットには、MAP の基本的なマッピングルール（つまり、変換されることを意味する）に一致するアドレスがありますが、関連するポートは、そのアドレスに割り当てられた範囲内にありません。これは、このパケットの発信元である MAP ノードの設定に誤りがある可能性が高いことを意味します。

MAP の履歴

機能名	プラットフォームリリース	説明
アドレスとポート変換のマッピング（MAP-T）	9.13(1)	アドレスとポートのマッピング (MAP) は、主にサービスプロバイダー(SP)ネットワークで使用する機能です。サービスプロバイダーは、IPv6専用ネットワーク、MAPドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリックインターネット上のIPv4専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。 次のコマンドが導入または変更されました。**basic-mapping-rule**、**default-mapping-rule**、**ipv4-prefix**、**ipv6-prefix**、**map-domain**、**share-ratio**、**show map-domain**、**start-port**。

第 IV 部

サービス ポリシーとアプリケーション インスペクション

- サービス ポリシー （269 ページ）
- アプリケーション レイヤ プロトコル インスペクションの準備 （295 ページ）
- 基本インターネット プロトコルのインスペクション （321 ページ）
- 音声とビデオのプロトコルのインスペクション （371 ページ）
- モバイル ネットワークのインスペクション （401 ページ）

第 11 章

サービス ポリシー

モジュラ ポリシー フレームワークを使用したサービス ポリシーにより、一貫性のある柔軟な方法で ASA の機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。サービス ポリシーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

- サービス ポリシーについて （269 ページ）
- サービス ポリシーのガイドライン （277 ページ）
- サービス ポリシーのデフォルト （279 ページ）
- サービス ポリシーの設定 （280 ページ）
- サービス ポリシーのモニタリング （289 ページ）
- サービス ポリシー（モジュラ ポリシー フレームワーク）の例 （289 ページ）
- サービス ポリシーの履歴 （292 ページ）

サービス ポリシーについて

次の各トピックでは、サービス ポリシーの仕組みについて説明します。

サービス ポリシーのコンポーネント

サービス ポリシーのポイントは、許可しているトラフィックに高度なサービスを適用することです。アクセス ルールによって許可されるトラフィックにサービス ポリシーを適用し、サービス モジュールへのリダイレクトやアプリケーション インスペクションの適用などの特別な処理を実行できます。

次のタイプのサービス ポリシーを使用できます。

- すべてのインターフェイスに適用される 1 つのグローバル ポリシー。
- インターフェイスごとに適用される 1 つのサービス ポリシー。このポリシーは、デバイスを通過するトラフィックを対象とするクラスと、ASA インターフェイスに向けられた（イ

ンターフェイスを通過するのではない）管理トラフィックを対象とするクラスの組み合わせである場合があります。

各サービス ポリシーは、次の要素で構成されます。

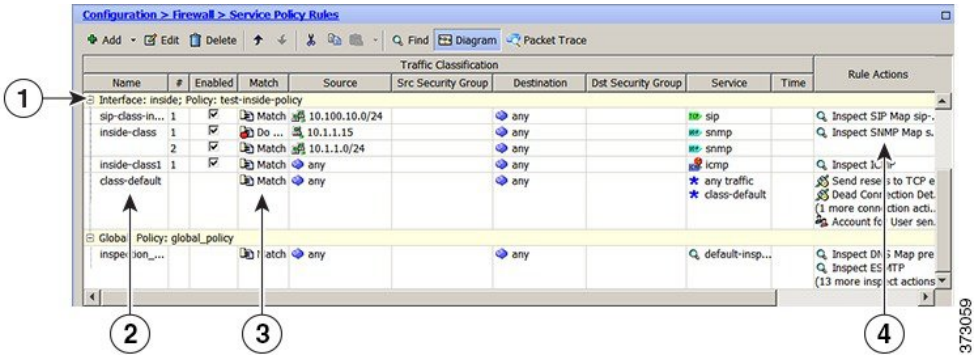
1. サービス ポリシー マップ。これはルールの順序セットであり、**service-policy** コマンドで命名されます。ASDM では、ポリシー マップは [Service Policy Rules] ページにフォルダとして表示されます。

2. ルール。各ルールは、サービス ポリシー内の、**class** コマンドと **class** に関連するコマンド群で構成されます。ASDM では、各ルールは個別の行に表示され、ルールの名前はクラス名です。

   class コマンドは、ルールのトラフィック照合基準を定義します。

   inspect や set connection timeout などの class 関連のコマンドは、一致するトラフィックに適用するサービスと制約を定義します。inspect コマンドは、検査対象トラフィックに適用するアクションを定義するインスペクション ポリシー マップを指す場合があります。インスペクション ポリシー マップとサービス ポリシー マップは同じではないことに注意してください。

次の例では、サービス ポリシーが CLI と ASDM でどのように表示されるかを比較します。図の吹き出しと CLI の行は 1 対 1 で対応しないことに注意してください。



次の CLI は、上の図に示すルールによって生成されます。

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
```

```
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

サービス ポリシーで設定される機能

次の表に、サービス ポリシーを使用して設定する機能を示します。

表 *8*：サービス ポリシーで設定される機能

機能	通過トラフィック用か	管理トラフィック用か	次を参照してください。
アプリケーション インスペクション（複数タイプ）	RADIUS アカウンティングを除くすべて	**RADIUS アカウンティング**のみ	• アプリケーション レイヤ プロトコル インスペクションの準備 （295 ページ）。 • 基本インターネット プロトコルのインスペクション （321 ページ）。 • 音声とビデオのプロトコルのインスペクション （371 ページ）。 • モバイル ネットワークのインスペクション （401 ページ）。
NetFlow セキュア イベント ロギングのフィルタリング	**対応**	**対応**	NetFlow 実装ガイドを参照してください。
QoS 入出力ポリシング	**対応**	非対応	QoS （499 ページ）。
QoS 標準プライオリティ キュー	**対応**	非対応	QoS （499 ページ）。
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	**対応**	**対応**	接続設定 （459 ページ）。
TCP の正規化	**対応**	非対応	接続設定 （459 ページ）。
TCP ステート バイパス	**対応**	非対応	接続設定 （459 ページ）。
アイデンティティ ファイアウォールのユーザー統計情報	**対応**	**対応**	コマンド リファレンスの user-statistics コマンドを参照してください。

機能の方向性

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラスマップと一致した場合に、ポリシーマップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。

（注） グローバル ポリシーを使用する場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS プライオリティ キューなど単方向に適用される機能の場合は、ポリシー マップを適用するインターフェイスに出入りする（機能によって異なります）トラフィックだけが影響を受けます。各機能の方向については、次の表を参照してください。

表 *9*：機能の方向性

機能	単一インターフェイスでの方向	グローバルでの方向
アプリケーション インスペクション（複数タイプ）	双方向	入力
NetFlow セキュア イベント ロギングのフィルタリング	該当なし	入力
QoS 入力ポリシング	入力	入力
QoS 出力ポリシング	出力	出力
QoS 標準プライオリティ キュー	出力	出力
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	双方向	入力
TCP の正規化	双方向	入力
TCP ステート バイパス	双方向	入力
アイデンティティ ファイアウォールのユーザー統計情報	双方向	入力

サービス ポリシー内の機能照合

パケットは、次のルールに従って特定のインターフェイスのポリシー マップのクラス マップに一致します。

1. パケットは、各機能タイプのポリシー マップ ルールで、1 つのクラス マップにだけ一致します。
2. パケットが機能タイプのクラス マップに一致した場合、ASA は、その機能タイプの後続のクラス マップとは照合しません。
3. ただし、パケットが別の機能タイプの後続のクラス マップと一致した場合、ASA は、後続のクラスマップのアクションも適用します（サポートされている場合）。サポートされていない組み合わせの詳細については、特定の機能アクションの非互換性 （275 ページ）を参照してください。

（注） アプリケーション インスペクションには、複数のインスペクション タイプが含まれ、ほとんどのタイプは相互に排他的です。組み合わせ可能なインスペクションの場合、各インスペクションは個々の機能と見なされます。

パケット照合の例

次に例を示します。

- パケットが接続制限値のクラス マップ と一致し、アプリケーション インスペクションのクラス マップ とも一致した場合、両方のクラス マップ アクションが適用されます。
- パケットが HTTP インスペクションで 1 つのクラス マップと一致し、HTTP インスペクションを含む別のクラス マップ とも一致した場合、2 番目のクラス マップ のアクションは適用されません。
- パケットが FTP インスペクションで 1 つのクラスマップ と一致し、HTTP インスペクションを含む別のクラス マップ とも一致した場合、HTTP および FTP インスペクションは組み合わせることができないため、2 番目のクラスマップのアクションは適用されません。
- パケットが HTTP インスペクションで 1 つのクラス マップ と一致し、さらに IPv6 インスペクションを含む別のクラス マップ とも一致した場合、IPv6 インスペクションは他のタイプのインスペクションと組み合わせることができるため、両方のアクションが適用されます。

複数の機能アクションが適用される順序

ポリシー マップの各種のアクションが実行される順序は、ポリシー マップ 中に出現する順序とは無関係です。

アクションは次の順序で実行されます。

1. QoS 入力ポリシング
2. TCP の正規化、TCP と UDP の接続制限値とタイムアウト、TCP シーケンス番号のランダム化、および TCP ステート バイパス

（注） ASA がプロキシサービス（AAA など）を実行したり、TCP ペイロード（FTP インスペクションなど）を変更したりするときは、TCP ノーマライザはデュアルモードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

3. 他のインスペクションと組み合わせることができるアプリケーション インスペクション：
   1. IPv6

2. IP オプション
3. WAAS

4. 他のインスペクションと組み合わせることができないアプリケーション インスペクション：詳細については、「特定の機能アクションの非互換性 （275 ページ）」を参照してください。
5. QoS 出力ポリシング
6. QoS 標準プライオリティ キュー

（注） NetFlow セキュア イベント ロギングのフィルタリングとアイデンティティ ファイアウォールのユーザー統計情報は順番に依存しません。

特定の機能アクションの非互換性

一部の機能は同じトラフィックに対して相互に互換性がありません。次のリストには、すべての非互換性が含まれていない場合があります。各機能の互換性については、機能に関する章または項を参照してください。

- QoS プライオリティ キューイングと QoS ポリシングは同じトラフィックの集合に対して設定できません。
- ほとんどのインスペクションは別のインスペクションと組み合わせられないため、同じトラフィックに複数のインスペクションを設定しても、ASA は 1 つのインスペクションだけを適用します。例外は、複数の機能アクションが適用される順序 （274 ページ）に記載されています。

（注） デフォルト グローバル ポリシーで使用される **match default-inspection-traffic** コマンドは、デフォルト ポートをすべてのインスペクションと照合する特別な CLI ショートカットです。ポリシーマップで使用すると、このクラスマップでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

誤った設定例は、同じポリシー マップに複数のインスペクションを設定しても、default-inspection-traffic ショートカットを使用しないことです。最初の例では、ポート 21 宛てのトラフィックが、FTP インスペクションと HTTP インスペクションの両方に誤って設定されています。2 番目の例では、ポート 80 宛てのトラフィックが、FTP インスペクションと HTTP

インスペクションの両方に誤って設定されています。どちらの誤った設定例の場合も、FTPインスペクションだけが適用されています。これは、適用されたインスペクションの順序では、FTP が HTTP よりも先になるためです。

例 1：**FTP パケットの誤設定（HTTP インスペクションも設定されている）**

```
class-map ftp
   match port tcp eq 21
class-map http
   match port tcp eq 21 [it should be 80]
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

例 2：**HTTP パケットの誤設定（FTP インスペクションも設定されている）**

```
class-map ftp
   match port tcp eq 80 [it should be 21]
class-map http
   match port tcp eq 80
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

複数のサービス ポリシーの機能照合

TCP および UDP トラフィック（およびステートフル ICMP インスペクションがイネーブルの場合は ICMP）の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。トラフィックが、1 つのインターフェイスのポリシーで定義されている機能に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。最初のポリシーのみが使用されます。

たとえば、HTTP トラフィックが、HTTP トラフィックを検査する内部インターフェイスのポリシーと一致するときに、HTTP インスペクション用の外部インターフェイスに別のポリシーがある場合、そのトラフィックが外部インターフェイスの出力側でも検査されることはありません。同様に、その接続のリターン トラフィックが外部インターフェイスの入力ポリシーによって検査されたり、内部インターフェイスの出力ポリシーによって検査されたりすることもありません。

ステートフル ICMP インスペクションをイネーブルにしない場合の ICMP のように、フローとして扱われないトラフィックの場合は、リターン トラフィックを戻り側のインターフェイスの別のポリシー マップと照合できます。

サービス ポリシーのガイドライン

インスペクションのガイドライン

アプリケーション インスペクションのサービス ポリシーに関する詳細なガイドラインを提供する単独のトピックがあります。アプリケーション インスペクションのガイドライン （298 ページ）を参照してください。

IPv6 のガイドライン

IPv6 は次の機能でサポートされています。

- 複数の、しかしすべてではないプロトコルに対するアプリケーション インスペクション。詳細については、アプリケーション インスペクションのガイドライン （298 ページ）を参照してください。
- NetFlow セキュア イベント ロギングのフィルタリング
- SCTP ステート バイパス
- TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化
- TCP の正規化
- TCP ステート バイパス
- アイデンティティ ファイアウォールのユーザー統計情報

クラスマップ（トラフィック クラス）のガイドライン

すべてのタイプのクラスマップ（トラフィック クラス）の最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- レイヤ 3/4 クラスマップ（通過トラフィックと管理トラフィック向け）。
- インスペクション クラス マップ
- 正規表現クラス マップ
- **match** インスペクション ポリシー マップ下で直接使用されるコマンド

この制限には、すべてのタイプのデフォルト クラス マップも含まれ、ユーザー設定のクラス マップを約 235 に制限します。

ポリシー マップのガイドライン

ポリシー マップを使用する場合は、次のガイドラインを参考にしてください。

- 各インターフェイスには、ポリシーマップを1つだけ割り当てることができますローエンドのファイアウォールの場合、設定で最大 64 個のポリシーマップを作成できます。より強力なファイアウォールの場合、最大で 128 個まで作成できます。

  各インターフェイスには、ポリシー マップを 1 つだけ割り当てることができますCisco Secure Firewall 3100 のようなローエンドのファイアウォールの場合、設定では最大 64 個のポリシーマップを作成できます。Firepower 4100 など、より強力なファイアウォールでは、最大で 128 個まで作成できます。

- 同一のポリシー マップを複数のインターフェイスに適用できます。
- 1 つのレイヤ 3/4 ポリシー マップで最大 63 のレイヤ 3/4 クラス マップを識別できます。
- クラスマップごとに、1つ以上の機能タイプから複数のアクションを割り当てることができます（サポートされている場合）。特定の機能アクションの非互換性（275 ページ）を参照してください。

サービス ポリシーのガイドライン

- 入力インターフェイスのインターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、FTP インスペクションのグローバル ポリシーと、TCP 正規化のインターフェイス ポリシーがある場合、FTP インスペクションと TCP 正規化の両方がインターフェイスに適用されます。これに対し、FTP インスペクションのグローバル ポリシーと、FTP インスペクションの入力インターフェイス ポリシーがある場合は、入力インターフェイス ポリシーの FTP インスペクションだけがそのインターフェイスに適用されます。入力またはグローバル ポリシーが機能を実装していない場合は、機能を指定する出力インターフェイスのインターフェイス サービス ポリシーが適用されます。
- 適用できるグローバル ポリシーは 1 つだけです。たとえば、機能セット 1 が含まれたグローバル ポリシーと、機能セット 2 が含まれた別のグローバル ポリシーを作成できません。すべての機能は 1 つのポリシーに含める必要があります。
- コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての新しい接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。show コマンドの出力には、古い接続に関するデータは含まれません。

  たとえば、インターフェイスから QoS サービス ポリシーを削除し、変更したバージョンを追加した場合、**show service-policy** コマンドには、新しいサービス ポリシーに一致する新しい接続に関連付けられた QoS カウンタだけが表示されます。古いポリシーの既存の接続はコマンド出力には表示されなくなります。

  すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** または **clear local-host** コマンドを使用します。

サービス ポリシーのデフォルト

次の各トピックでは、サービス ポリシーとモジュラ ポリシー フレームワークのデフォルト設定について説明します。

デフォルトのサービス ポリシー設定

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは1つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。（特定の機能では、グローバル ポリシーはインターフェイス ポリシーより優先されます）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- DNS
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- SIP
- NetBios
- TFTP
- IP オプション

デフォルトのクラス マップ（トラフィック クラス）

設定には、ASA が default-inspection-traffic Default Inspection Trafficというデフォルト グローバル ポリシーで使用するデフォルトのレイヤ 3/4 クラス マップ（トラフィック クラス）が含まれます。このクラス マップは、デフォルトのインスペクション トラフィックを照合します。

デフォルト グローバル ポリシーで使用されるこのクラスは、デフォルト ポートをすべてのインスペクションと照合する特別なショートカットです。

ポリシーで使用すると、このクラスでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

```
class-map inspection_default
 match default-inspection-traffic
```

デフォルト コンフィギュレーションにある別のクラス マップは、class-default と呼ばれ、すべてのトラフィックと一致します。このクラス マップは、すべてのレイヤ 3/4 ポリシー マップの最後に示され、原則的に、他のすべてのトラフィックでどのようなアクションも実行しないように ASA に通知します。class-default クラス（ASDM の任意の通信クラス）を使用する場合は、TCP シーケンスのランダム化、TTL デクリメント、またはその他のオプション属性の変更を有効にするなど、より広範な目的で使用してください。インスペクションには使用しないでください。使用すると、通信の中断が発生する可能性があります。一部の機能は class-default でしか使用できません。

```
class-map class-default
 match any
```

サービス ポリシーの設定

モジュラ ポリシー フレームワークを使用してサービス ポリシーを設定するには、次の手順を実行します。

手順

ステップ 1 トラフィックの特定（レイヤ 3/4 クラス マップ） （282 ページ） の説明に従って、レイヤ 3/4 クラス マップを作成して、操作対象のトラフィックを特定します。

たとえば、ASA を通過するすべてのトラフィックでアクションを実行したり、10.1.1.0/24 から任意の宛先アドレスまでのトラフィックで特定のアクションだけを実行したりできます。

ステップ 2 必要に応じて、あるインスペクション トラフィックで追加のアクションを実行します。

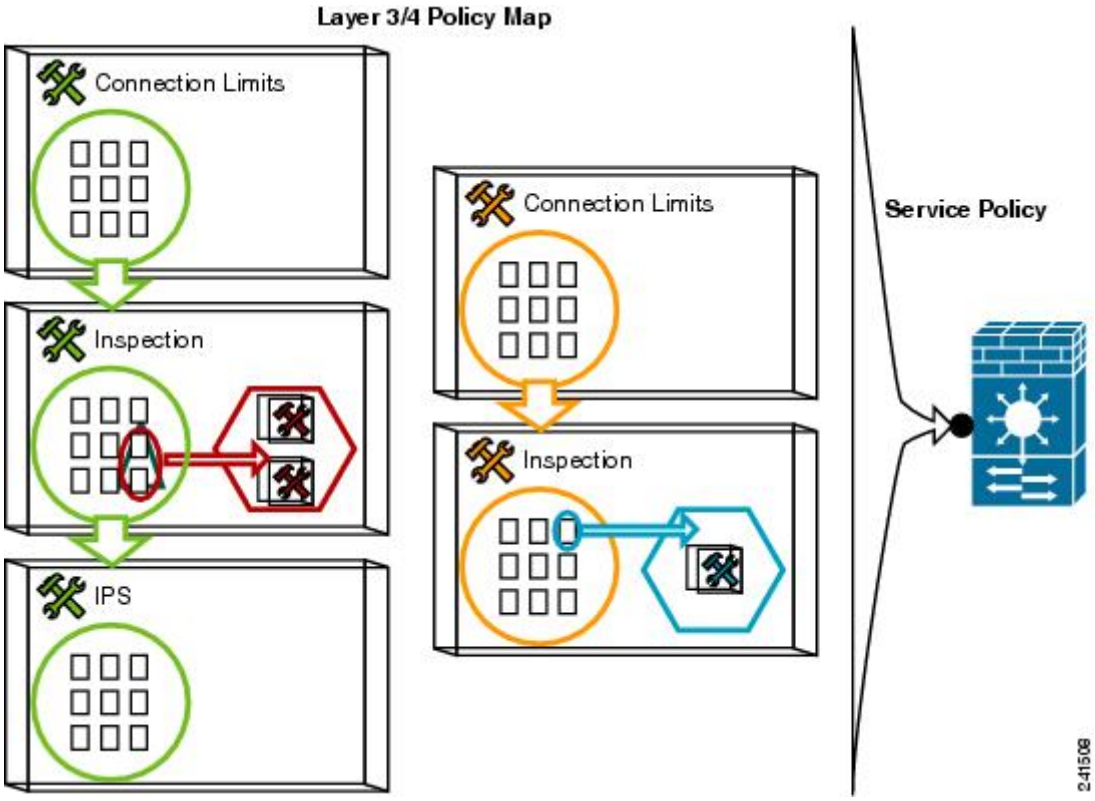
実行するアクションの 1 つがアプリケーション インスペクションで、一部のインスペクション トラフィックで追加のアクションを実行する場合、インスペクション ポリシー マップを作成します。インスペクション ポリシー マップはトラフィックを特定し、そのトラフィックで何をするかを指定します。

たとえば、本文の長さが 1000 バイトを上回るすべての HTTP 要求をドロップできます。

match コマンドでトラフィックを直接特定する独立したインスペクション ポリシー マップを作成したり、再利用のために、またはより複雑な照合のためにインスペクション クラス マップを作成したりできます。たとえば、正規表現または正規表現のグループ（正規表現クラス マップ）を使用して検査対象のパケット内のテキストを照合し、より限定された基準に基づいてアクションの対象を設定できます。たとえば、「example.com」というテキストが含まれた URL を持つすべての HTTP 要求をドロップできます。

アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

ステップ 3 アクションの定義（レイヤ 3/4 ポリシー マップ） （286 ページ）の説明に従って、レイヤ 3/4 ポリシーマップを作成して、各レイヤ 3/4 クラスマップで実行するアクションを定義します。



ステップ 4 インターフェイス（サービス ポリシー）へのアクションの適用 （288 ページ）の説明に従って、ポリシーマップを適用するインターフェイスを決定するか、ポリシーマップをグローバルに適用します。

トラフィックの特定（レイヤ 3/4 クラス マップ）

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。1 つのレイヤ 3/4 ポリシー マップに複数のレイヤ 3/4 クラス マップを作成できます。

通過トラフィック用のレイヤ 3/4 クラス マップの作成

レイヤ 3/4 クラス マップでは、プロトコル、ポート、IP アドレス、およびレイヤ 3 またはレイヤ 4 の他の属性に基づいてトラフィックを照合します。

ヒント トラフィック インスペクションは、アプリケーション トラフィックが発生するポートだけで行うことをお勧めします。**match any** などを使用してすべてのトラフィックを検査すると、ASA のパフォーマンスに影響が出る場合があります。

手順

ステップ 1 レイヤ 3/4 クラス マップを作成します。**class-map** *class_map_name*

class_map_name は、最大 40 文字の文字列です。

「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラスマップですでに使用されている名前は再度使用できません。CLI はクラスマップ コンフィギュレーション モードに移行します。

例：

```
hostname(config)# class-map all_udp
```

ステップ 2 （任意）説明をクラス マップに追加します。

description *string*

例：

```
hostname(config-cmap)# description All UDP traffic
```

ステップ 3 次のいずれかのコマンドを使用してトラフィックを照合します。特に指定がない場合、クラスマップに含めることができる **match** コマンドは 1 つだけです。

- **match any**：すべてのトラフィックを照合します。

  ```
  hostname(config-cmap)# match any
  ```

- **match access-list** *access_list_name*：拡張アクセス リストで指定されているトラフィックを照合します。

  ```
  hostname(config-cmap)# match access-list udp
  ```

- **match port** {**tcp** | **udp** | **sctp**} {**eq** *port_num* | **range** *port_num port_num*}：指定されたプロトコルに対し、宛先ポート（単一のポートまたは連続する範囲のポート）を照合します。複数の非連続ポートを使用するアプリケーションに対しては、match access-list コマンドを使用して、各ポートと一致する ACE を定義します。

  ```
  hostname(config-cmap)# match tcp eq 80
  ```

- **match default-inspection-traffic**：インスペクション用のデフォルト トラフィックを照合します（ASA が検査可能なすべてのアプリケーションによって使用されるデフォルトの TCP および UDP ポート）。

  ```
  hostname(config-cmap)# match default-inspection-traffic
  ```

デフォルト グローバル ポリシーで使用されるこのコマンドは、ポリシー マップで使用されると、トラフィックの宛先ポートに基づいて各パケットに正しいインスペクションを適用する特別な CLI ショートカットです。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラスマップに複数のインスペクションを設定できます（他のインスペクションとともに設定可能な WAAS インスペクションを除きます。アクションの組み合わせの詳細については、特定の機能アクションの非互換性（275 ページ）を参照してください）。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

デフォルト ポートのリストについては、デフォルト インスペクションと NAT に関する制限事項（300 ページ）を参照してください。**match default-inspection-traffic** コマンドにポートが含まれているすべてのアプリケーションが、ポリシーマップでデフォルトでイネーブルになっているわけではありません。

match access-list コマンドを **match default-inspection-traffic** コマンドとともに指定すると、一致するトラフィックを絞り込むことができます。**match default-inspection-traffic** コマンドによって照合するポートとプロトコルが指定されるため、ACL のポートとプロトコルはすべて無視されます。

- **match dscp** *value1* [*value2*] [...] [*value8*]：IP ヘッダーの DSCP 値（最大 8 個の DSCP 値）と照合します。

```
hostname(config-cmap)# match dscp af43 cs1 ef
```

- **match precedence** *value1* [*value2*] [*value3*] [*value4*]：IP ヘッダーの TOS バイトによって表される、最大 4 つの Precedence 値を照合します。Precedence 値は 0 ～ 7 に指定できます。

```
hostname(config-cmap)# match precedence 1 4
```

- **match rtp** *starting_port range*：RTP トラフィックを照合します。*starting_port* には、2000 ～ 65534 の間の偶数の UDP 宛先ポートを指定します。*range* には、*starting_port* よりも上の追加 UDP ポートの数を 0 ～ 16383 で指定します。

```
hostname(config-cmap)# match rtp 4004 100
```

- **match tunnel-group** *name*：QoS を適用する VPN トンネル グループ トラフィックを照合します。

  トラフィック照合を調整するために、**match** コマンドをもう 1 つ指定できます。上記のコマンドのいずれかを指定できますが、**match any**、**match access-list**、および **match default-inspection-traffic** コマンドは指定できません。または、match flow ip destination-address コマンドを入力して、各 IP アドレス宛てのトンネル グループのフローを照合することもできます。

```
hostname(config-cmap)# match tunnel-group group1
```

```
hostname(config-cmap)# match flow ip destination-address
```

例

次に **class-map** コマンドの例を示します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

管理トラフィック用のレイヤ 3/4 クラス マップの作成

ASAへの管理トラフィックに対して、この種類のトラフィックに特有のアクションの実行が必要になる場合があります。管理クラス マップを指定して、ACL または TCP や UDP のポートと照合できます。ポリシー マップの管理クラス マップで設定可能なアクションのタイプは、管理トラフィック専用です。

手順

ステップ 1 管理クラス マップを作成します。**class-map type management** *class_map_name*

class_map_name は、最大 40 文字の文字列です。

「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラスマップですでに使用されている名前は再度使用できません。CLI はクラスマップ コンフィギュレーション モードに移行します。

例：

```
hostname(config)# class-map management all_udp
```

ステップ 2 （任意）説明をクラス マップに追加します。

description *string*

例：

```
hostname(config-cmap)# description All UDP traffic
```

ステップ 3 次のいずれかのコマンドを使用してトラフィックを照合します。

- **match access-list** *access_list_name*：拡張アクセス リストで指定されているトラフィックを照合します。

```
hostname(config-cmap)# match access-list udp
```

- **match port** {**tcp** | **udp** | **sctp**} {**eq** *port_num* | **range** *port_num port_num*}：指定されたプロトコルに対し、宛先ポート（単一のポートまたは連続する範囲のポート）を照合します。複数の非連続ポートを使用するアプリケーションに対しては、match access-list コマンドを使用して、各ポートと一致する ACE を定義します。

```
hostname(config-cmap)# match tcp eq 80
```

アクションの定義（レイヤ 3/4 ポリシー マップ）

トラフィックを識別するレイヤ 3/4 クラス マップを設定したら、レイヤ 3/4 ポリシー マップを使用してそれらのクラスにアクションを関連付けます。

ヒント ポリシー マップの最大数は 64 ですが、各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

手順

ステップ 1 ポリシー マップを追加します。**policy-map** *policy_map_name*

policy_map_name は、最大 40 文字のポリシー マップ名です。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシーマップですでに使用されている名前は再度使用できません。CLI はポリシー マップ コンフィギュレーション モードに入ります。

例：

```
hostname(config)# policy-map global_policy
```

ステップ 2 以前に設定したレイヤ 3/4 クラス マップを指定します。**class** *class_map_name*

class_map_name には、クラス マップの名前を指定します。

クラス マップを追加するには、トラフィックの特定（レイヤ 3/4 クラス マップ） （282 ページ）を参照してください。

例：

```
hostname(config-pmap)# class all_http
```

ステップ 3 このクラス マップに、1 つ以上のアクションを指定します。

サービス ポリシーで設定される機能 （271 ページ）を参照してください。

（注） クラス マップに **match default-inspection-traffic** コマンドがない場合、そのクラスに最大 1 つの **inspect** コマンドを設定できます。

ステップ 4 このポリシー マップに含めるクラス マップごとに、この手順を繰り返します。

例

接続ポリシーの **policy-map** コマンドの例を次に示します。このコマンドは、Web サーバー 10.1.1.1 への接続許可数を制限します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout idle 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラス マップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラス マップと照合されないことを示しています。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout idle 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout idle 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout idle 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、ASA はこの照合を行いません。

インターフェイス（サービス ポリシー）へのアクションの適用

レイヤ 3/4 ポリシー マップをアクティブにするには、1 つ以上のインターフェイスに適用するサービス ポリシー、またはすべてのインターフェイスにグローバルに適用するサービス ポリシーを作成します。次のコマンドを使用します。

service-policy *policy_map_name* {**global** | **interface** *interface_name*} [**fail-close**]

それぞれの説明は次のとおりです。

- *policy_map_name* は、ポリシー マップの名前です。
- **global** は、特定のポリシーを持たないすべてのインターフェイスに適用するサービス ポリシーを作成します。

  適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するグローバル ポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがトラフィックにグローバルに適用されます。デフォルト サービス ポリシーには、**service-policy global_policy global** コマンドが含まれます。

- **interface** *interface_name* は、インターフェイスにポリシー マップを関連付けてサービス ポリシーを作成します。
- **fail-close** は、IPv6 トラフィックをサポートしないアプリケーション インスペクションによってドロップされた IPv6 トラフィックの syslog（767001）を生成します。デフォルトでは、syslog が生成されません。

例

たとえば、次のコマンドは、外部インターフェイスで inbound_policy ポリシー マップをイネーブルにします。

```
hostname(config)# service-policy inbound_policy interface outside
```

次のコマンドは、デフォルト グローバル ポリシーをディセーブルにし、新しいポリシー new_global_policy をイネーブルにします。

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

サービス ポリシーのモニタリング

サービス ポリシーをモニターするには、次のコマンドを入力します。

- **show service-policy**

  サービス ポリシーの統計情報を表示します。

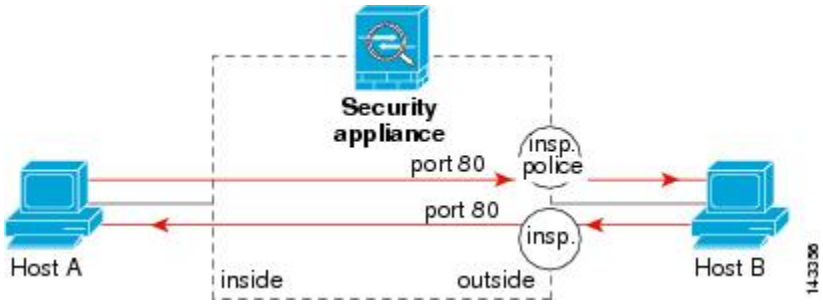
サービスポリシー（モジュラポリシーフレームワーク）の例

このセクションでは、モジュラ ポリシー フレームワークの例をいくつか示します。

HTTP トラフィックへのインスペクションと QoS ポリシングの適用

この例では、外部インターフェイスを通過して ASA を出入りするすべての HTTP 接続（ポート 80 の TCP トラフィック）が HTTP インスペクション対象として分類されます。外部インターフェイスを出るすべての HTTP トラフィックがポリシング対象として分類されます。

図 *37* : *HTTP* インスペクションと *QoS* ポリシング



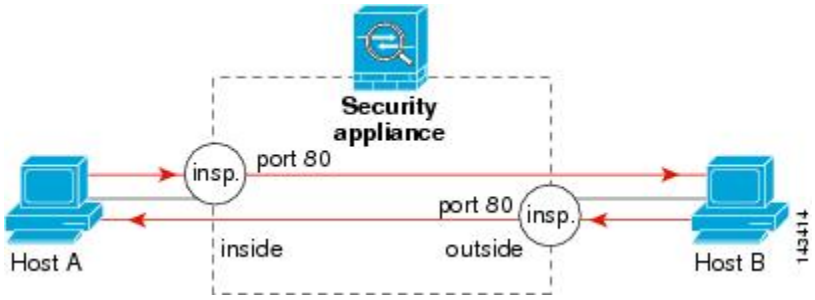
この例について、次のコマンドを参照してください。

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside
```

HTTP トラフィックへのインスペクションのグローバルな適用

この例では、任意のインターフェイスを通過して ASA に入るすべての HTTP 接続（ポート 80 の TCP トラフィック）が HTTP インスペクション対象として分類されます。このポリシーはグローバルポリシーなので、インスペクションが発生するのは各インターフェイスにトラフィックが入ったときだけです。

図 *38* : グローバル *HTTP* インスペクション



この例について、次のコマンドを参照してください。

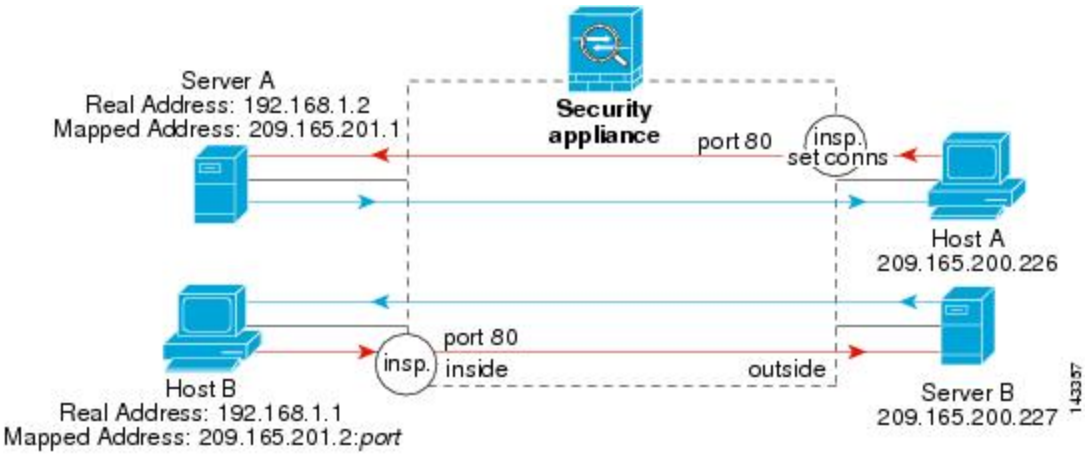
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global
```

特定のサーバーへの HTTP トラフィックに対するインスペクションと接続制限値の適用

この例では、外部インターフェイスを通過してASAに入るサーバーA宛てのHTTP接続（ポート 80 の TCP トラフィック）が HTTP インスペクションおよび最大接続数制限値の対象として分類されます。サーバー A から発信されたホスト A への接続は、クラスマップの ACL と一致しないので、影響を受けません。

内部インターフェイスを通じて ASA に入るサーバー B 宛てのすべての HTTP 接続は、HTTP インスペクション対象として分類されます。サーバーBから発信されたホストBへの接続は、クラスマップの ACL と一致しないので、影響を受けません。

図 *39* : 特定のサーバーに対する *HTTP* インスペクションと接続制限値



この例について、次のコマンドを参照してください。

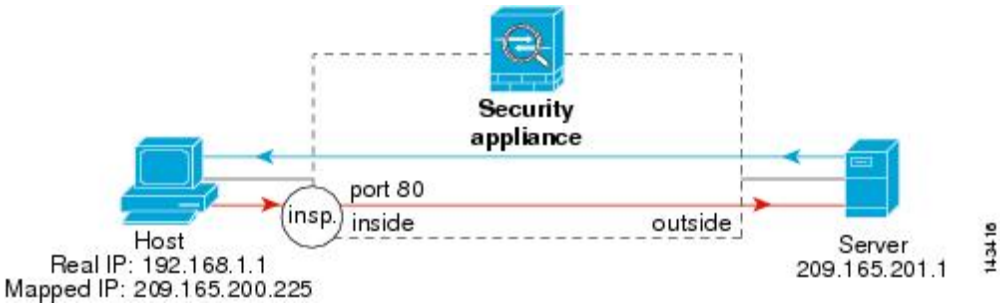
```
hostname(config)# object network obj-192.168.1.2
hostname(config-network-object)# host 192.168.1.2
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1
hostname(config)# object network obj-192.168.1.0
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 eq
80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
```

```
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

NAT による HTTP トラフィックへのインスペクションの適用

この例では、ネットワーク内のホストに 2 つのアドレスがあります。1 つは、実際の IP アドレスの 192.168.1.1 です。もう 1 つは、外部ネットワークで使用するマッピング IP アドレスの 209.165.200.225 です。クラス マップの ACL の実際の IP アドレスを使用する必要があります。outside インターフェイスに適用する場合にも、実際のアドレスを使用します。

図 *40 : NAT* による *HTTP* インスペクション



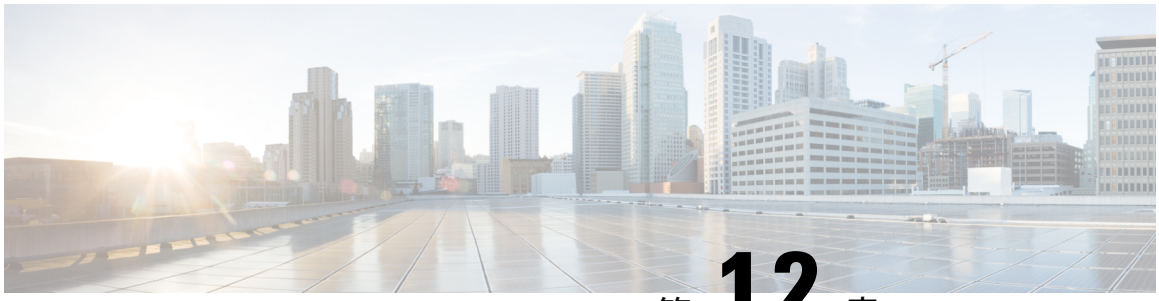
この例について、次のコマンドを参照してください。

```
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1,outside) static 209.165.200.225

hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 any eq
80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client

hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```

サービス ポリシーの履歴

機能名	リリース	説明
モジュラ ポリシー フレームワーク	7.0(1)	モジュラ ポリシー フレームワークが導入されました。

機能名	リリース	説明
RADIUSアカウンティング トラフィックで使用する管理クラス マップ	7.2(1)	RADIUSアカウンティング トラフィックで使用する管理クラス マップが導入されました。**class-map type management** コマンドおよび**inspect radius-accounting** コマンドが導入されました。
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラスマップに一致させることができます。以前は、**match all** だけが使用可能でした。



第 12 章

アプリケーション レイヤ プロトコル インスペクションの準備

次のトピックで、アプリケーション レイヤ プロトコル インスペクションを設定する方法について説明します。

- アプリケーション レイヤ プロトコル インスペクション （295 ページ）
- アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）
- 正規表現の設定 （313 ページ）
- インスペクション ポリシーのモニタリング （317 ページ）
- アプリケーション インスペクションの履歴 （319 ページ）

アプリケーション レイヤ プロトコル インスペクション

インスペクション エンジンは、ユーザーのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、ASA で詳細なパケット インスペクションを行う必要があります。そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。ASA では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。

次のトピックで、アプリケーション インスペクションについて詳しく説明します。

アプリケーション プロトコル インスペクションを使用するタイミング

ユーザーが接続を確立すると、ASA は ACL と照合してパケットをチェックし、アドレス変換を作成し、高速パスでのセッション用にエントリを作成して、後続のパケットが時間のかかるチェックをバイパスできるようにします。ただし、高速パスは予測可能なポート番号に基づいており、パケット内部のアドレス変換を実行しません。

多くのプロトコルは、セカンダリの TCP ポートまたは UDP ポートを開きます。既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエーションされます。

パケットに IP アドレスを埋め込むアプリケーションもあります。この IP アドレスは送信元アドレスと一致する必要があり、通常、ASA を通過するときに変換されます。

これらのアプリケーションを使用する場合は、アプリケーションインスペクションをイネーブルにする必要があります。

IP アドレスを埋め込むサービスに対してアプリケーション インスペクションをイネーブルにすると、ASA は埋め込まれたアドレスを変換し、チェックサムや変換の影響を受けたその他のフィールドを更新します。

ダイナミックに割り当てられたポートを使用するサービスに対してアプリケーションインスペクションをイネーブルにすると、ASA はセッションをモニターしてダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポートでのデータ交換を許可します。

インスペクション ポリシー マップ

インスペクション ポリシー マップを使用して、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。これらのマップはオプションです。インスペクション ポリシー マップをサポートするプロトコルに関しては、マップを設定しなくてもインスペクションをイネーブルにできます。デフォルトのインスペクションアクション以外のことが必要な場合にのみ、これらのマップが必要になります。

インスペクション ポリシー マップは、次に示す要素の 1 つ以上で構成されています。インスペクション ポリシー マップで使用可能な実際のオプションは、アプリケーションに応じて決まります。

- トラフィック照合基準：アプリケーショントラフィックをそのアプリケーションに固有の基準（URL 文字列など）と照合し、その後アクションをイネーブルにできます。

  一部のトラフィック照合基準では、正規表現を使用してパケット内部のテキストを照合します。ポリシー マップを設定する前に、正規表現クラス マップ内で、正規表現を単独またはグループで作成およびテストしておいてください。

- インスペクション クラス マップ：一部のインスペクション ポリシー マップでは、インスペクション クラス マップを使用して複数のトラフィック照合基準を含めることができます。その後、インスペクション ポリシー マップ内でインスペクション クラス マップを指定し、そのクラス全体でアクションをイネーブルにします。クラスマップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、より複雑な一致基準を作成できる点と、クラス マップを再使用できる点です。ただし、異なる照合基準に対して異なるアクションを設定することはできません。

- パラメータ：パラメータは、インスペクション エンジンの動作に影響します。

次のトピックで、詳細に説明します。

使用中のインスペクション ポリシー マップの交換

サービス ポリシーのポリシー マップでインスペクションが有効になっている場合、ポリシー マップの交換は2つのステップからなるプロセスです。最初に、インスペクションを削除する必要があります。次に、新しいポリシー マップ名でそれを再度追加します。

たとえば、SIP インスペクションで sip-map1 を sip-map2 と交換するには、次のコマンド シーケンスを使用します。

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

複数のトラフィック クラスの処理方法

インスペクション ポリシー マップには、複数のインスペクション クラス マップや直接照合を指定できます。

1 つのパケットが複数の異なるクラスまたはダイレクト マッチに一致する場合、ASA がアクションを適用する順序は、インスペクション ポリシー マップにアクションが追加された順序ではなく、ASA の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザーが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。たとえば、次の match コマンドは任意の順序で入力できますが、**match request method get** コマンドが最初に照合されます。

```
match request header host length gt 100
  reset
match request method get
  log
```

アクションがパケットをドロップすると、インスペクション ポリシー マップではそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の照合基準との照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます

パケットが、同一の複数の一致基準と照合される場合は、ポリシーマップ内のそれらのコマンドの順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから2番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが行われ、ログには記録されません。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

クラス マップは、そのクラス マップ内で重要度が最低の match オプション（重要度は、内部ルールに基づきます）に基づいて、別のクラス マップまたはダイレクト マッチと同じタイプであると判断されます。クラス マップに、別のクラス マップと同じタイプの重要度が最低の

matchオプションがある場合、それらのクラスマップはポリシーマップに追加された順序で照合されます。各クラス マップの重要度が最低の照合が異なる場合、重要度が高い match オプションを持つクラスマップが最初に照合されます。たとえば、次の3つのクラスマップには、**match request-cmd**（高重要度）と **match filename**（低重要度）という2つのタイプの **match** コマンドがあります。ftp3クラスマップには両方のコマンドが含まれていますが、最低重要度のコマンドである **match filename** に従ってランク付けされています。ftp1 クラスマップには最高重要度のコマンドがあるため、ポリシー マップ内での順序に関係なく最初に照合されます。ftp3 クラス マップは ftp2 クラス マップと同じ重要度としてランク付けされており、**match filename** コマンドも含まれています。これらのクラス マップの場合、ポリシー マップ内での順序に従い、ftp3 が照合されてから ftp2 が照合されます。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

アプリケーション インスペクションのガイドライン

フェールオーバー

インスペクションが必要なマルチメディア セッションのステート情報は、ステートフル フェールオーバーのステート リンク経由では渡されません。ステート リンク経由で複製される GTP、M3UA、および SIP は例外です。ステートフル フェールオーバーを取得するために、M3UA インスペクションで厳密なアプリケーション サーバー プロセス（ASP）のステート チェックを設定する必要があります。

クラスタ

次のインスペクションはクラスタリングではサポートされていません。

- CTIQBE
- H323、H225、および RAS
- IPsec パススルー
- MGCP
- MMP
- RTSP

- SCCP（Skinny）
- WAAS

IPv6

IPv6 は次のインスペクションでサポートされています。

- Diameter
- DNS over UDP
- FTP
- GTP
- HTTP
- ICMP
- IPSec パススルー
- IPv6
- M3UA
- SCCP（Skinny）
- SCTP
- SIP
- SMTP
- VXLAN

NAT64 は次のインスペクションでサポートされています。

- DNS over UDP
- FTP
- HTTP
- ICMP
- SCTP

その他のガイドライン

- 一部のインスペクション エンジンは、PAT、NAT、外部 NAT、または同一セキュリティ インターフェイス間の NAT をサポートしません。NAT サポートの詳細については、デフォルト インスペクションと NAT に関する制限事項（300 ページ）を参照してください。
- すべてのアプリケーション インスペクションについて、ASA はアクティブな同時データ接続の数を 200 接続に制限します。たとえば、FTP クライアントが複数のセカンダリ接続を開く場合、FTP インスペクション エンジンはアクティブな接続を 200 だけ許可して 201

番目の接続からはドロップし、適応型セキュリティ アプライアンスはシステム エラー メッセージを生成します。

- 検査対象のプロトコルは高度な TCP ステート トラッキングの対象となり、これらの接続の TCP ステートは自動的には複製されません。スタンバイ装置への接続は複製されますが、TCP ステートを再確立するベスト エフォート型の試行が行われます。
- TCP接続にインスペクションが必要であるとシステムが判断した場合、システムはそれらのインスペクションの前に、パケット上でMSSおよび選択的確認応答（SACK）オプションを除き、すべての TCP オプションをクリアします。その他のオプションは、接続に適用されている TCP マップで許可されているとしてもクリアされます。
- ASA（インターフェイス）に送信される TCP/UDP トラフィックはデフォルトで検査されます。ただし、インターフェイスに送信される ICMP トラフィックは、ICMP インスペクションをイネーブルにした場合でも検査されません。したがって、ASA がバックアップ デフォルト ルートを介して到達できる送信元からエコー要求が送信された場合など、特定の状況下では、インターフェイスへの ping（エコー要求）が失敗する可能性があります。

アプリケーション インスペクションのデフォルト

次のトピックで、アプリケーション インスペクションのデフォルトの動作について説明します。

デフォルト インスペクションと NAT に関する制限事項

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。デフォルト アプリケーション インスペクション トラフィックには、各プロトコルのデフォルト ポートへのトラフィックが含まれます。適用できるグローバル ポリシーは 1 つだけであるため、グローバル ポリシーを変更する（標準以外のポートにインスペクションを適用する場合や、デフォルトで有効になっていないインスペクションを追加する場合など）には、デフォルトのポリシーを編集するか、デフォルトのポリシーを無効にして新しいポリシーを適用する必要があります。

次の表に、サポートされているすべてのインスペクション、デフォルトのクラスマップで使用されるデフォルト ポート、およびデフォルトでオンになっているインスペクション エンジン（太字）を示します。この表には、NAT に関する制限事項も含まれています。この表の見方は次のとおりです。

- デフォルト ポートに対してデフォルトで有効になっているインスペクション エンジンは太字で表記されています。
- ASAは、これらの指定された標準に準拠していますが、インスペクション対象のパケットには準拠を強制しません。たとえば、各FTPコマンドは特定の順序である必要がありますが、ASA によってその順序を強制されることはありません。

表 *10*：サポートされているアプリケーション検査エンジン

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	説明
CTIQBE	TCP/2748	拡張 PAT なし NAT64 なし。 （クラスタリング）スタティック PAT なし。	—	—
DCERPC	TCP/135	NAT64 なし。	—	—
Diameter	TCP/3868 TCP/5868（TCP/TLS 用） SCTP/3868	NAT/PAT なし。	RFC 6733	キャリアライセンスが必要です。
DNS over UDP DNS over TCP	UDP/53 UDP/443 TCP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	RFC 1123	DNS over TCP を検査するには、DNS インスペクション ポリシーマップで DNS/TCP インスペクションを有効にする必要があります。 UDP/443 は、Cisco Umbrella DNScrypt セッションのみに使用されます。
FTP	TCP/21	（クラスタリング）スタティック PAT なし。	RFC 959	—
GTP	UDP/3386（GTPv0） UDP/2123（GTPv1+）	拡張 PAT なし NAT は使用できません。	—	キャリアライセンスが必要です。
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP（RAS）1718 ～ 1719	（クラスタリング）スタティック PAT はサポートされません。 拡張 PAT なし 同一セキュリティのインターフェイス上の NAT はサポートされません。 NAT64 なし。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	説明
HTTP	TCP/80	—	RFC 2616	ActiveX と Java をストリッピングする場合の MTU 制限に注意してください。MTU が小さすぎて Java タグまたは ActiveX タグを 1 つのパケットに納められない場合は、ストリッピングが行われない可能性があります。
ICMP	ICMP	—	—	ASA インターフェイスに送信される ICMP トラフィックのインスペクションは実行されません。
ICMP ERROR	ICMP	—	—	—
ILS（LDAP）	TCP/389	拡張 PAT なし NAT64 なし。	—	—
インスタント メッセージング（IM）	クライアントにより異なる	拡張 PAT なし NAT64 なし。	RFC 3860	—
IP オプション	RSVP	NAT64 なし。	RFC 791、RFC 2113	—
IPsec Pass Through	UDP/500	PAT なし。 NAT64 なし。	—	—
IPv6	—	NAT64 なし。	RFC 2460	—
LISP	—	NAT および PAT はサポートされません。	—	—
M3UA	SCTP/2905	埋め込まれたアドレスに対する NAT または PAT はなし。	RFC 4666	キャリアライセンスが必要です。
MGCP	UDP/2427、2727	拡張 PAT なし NAT64 なし。 （クラスタリング）スタティック PAT なし。	RFC 2705bis-05	—
MMP	TCP/5443	拡張 PAT なし NAT64 なし。	—	—

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	説明
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	拡張 PAT なし NAT64 なし。	—	NetBIOS は、NBNS UDP ポート 137 および NBDS UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。
PPTP	TCP/1723	NAT64 なし。 （クラスタリング）スタティック PAT なし。	RFC 2637	—
RADIUS アカウンティング	UDP/1646	NAT64 なし。	RFC 2865	—
RSH	TCP/514	PAT なし。 NAT64 なし。 （クラスタリング）スタティック PAT なし。	Berkeley UNIX	—
rtsp	TCP/554	拡張 PAT なし NAT64 なし。 （クラスタリング）スタティック PAT なし。	RFC 2326、2327、1889	HTTP クローキングは処理しません。
SCTP	SCTP	—	RFC 4960	キャリアライセンスが必要です。 SCTP トラフィックでスタティック ネットワーク オブジェクト NAT を実行できますが（ダイナミック NAT/PAT なし）、インスペクション エンジンは NAT には使用されません。
SIP	TCP/5060 UDP/5060	同等以上または以下のセキュリティ レベルを持つインターフェイスでの NAT/PAT はサポートされません。 拡張 PAT なし NAT64 または NAT46 なし （クラスタリング）スタティック PAT なし。	RFC 2543	一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	説明
SKINNY（**SCCP**）	TCP/2000	同一セキュリティのインターフェイス上の NAT はサポートされません。 拡張 PAT なし NAT64、NAT46、または NAT66 なし （クラスタリング）スタティック PAT なし。	—	一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。
SMTP および **ESMTP**	TCP/25	NAT64 なし。	RFC 821、1123	—
SNMP	UDP/161、162 Cisco Secure Firewall Extensible Operating System（FXOS）も実行するプラットフォーム上の UDP/4161。	NAT および PAT はサポートされません。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 ～ 1908、v.3 RFC 2570 ～ 2580 FXOS プラットフォームでは、SNMP を設定すると、この検査は自動的に有効になり、無効にすることはできません。
SQL*Net	TCP/1521	拡張 PAT なし NAT64 なし。 （クラスタリング）スタティック PAT なし。	—	v.1 および v.2
STUN	TCP/3478 UDP/3478	（WebRTC）スタティック NAT/PAT44 のみ。 （Cisco Spark）スタティック NAT/PAT44 と 64、およびダイナミック NAT/PAT。	RFC 5245、5389	—
Sun RPC	TCP/111 UDP/111	拡張 PAT なし NAT64 なし。	—	—
TFTP	UDP/69	NAT64 なし。 （クラスタリング）スタティック PAT なし。	RFC 1350	ペイロード IP アドレスは変換されません。

アプリケーション	デフォルト プロトコル、ポート	NAT に関する制限事項	標準	説明
WAAS	TCP/1～65535	拡張 PAT なし NAT64 なし。	—	—
XDMCP	UDP/177	拡張 PAT なし NAT64 なし。 （クラスタリング）スタティック PAT なし。	—	—
VXLAN	UDP/4789	N/A	RFC 7348	Virtual Extensible Local Area Network。

デフォルトのインスペクション ポリシー マップ

一部のインスペクション タイプは、非表示のデフォルト ポリシー マップを使用します。たとえば、マップを指定しないで ESMTP インスペクションをイネーブルにした場合、_default_esmtp_map が使用されます。

デフォルトのインスペクションは、各インスペクション タイプについて説明しているセクションで説明されています。これらのデフォルト マップは、show running-config all policy-map コマンドを使用して表示できます。

DNS インスペクションは、明示的に設定されたデフォルト マップ preset_dns_map を使用する唯一のインスペクションです。

アプリケーション レイヤ プロトコル インスペクションの設定

サービス ポリシーにアプリケーション インスペクションを設定します。

インスペクションは、一部のアプリケーションの標準のポートとプロトコルに関しては、デフォルトですべてのインターフェイスでグローバルに有効になっています。デフォルトのインスペクションの詳細については、デフォルト インスペクションと NAT に関する制限事項（300 ページ）を参照してください。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

始める前に

一部のアプリケーションでは、インスペクション ポリシー マップを設定することでインスペクションをイネーブルにすると、特別なアクションを実行できます。この手順の後半の表に、

インスペクション ポリシー マップを使用できるプロトコルを示します。また、それらの設定手順へのポインタも記載しています。これらの拡張機能を設定する場合は、インスペクションを設定する前にマップを作成します。

手順

ステップ 1 既存のクラスマップにインスペクションを追加する場合を除き、L3/L4 クラスマップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。inspection_default クラスにのみ複数のインスペクションを設定できます。また、デフォルトのインスペクションを適用する既存のグローバル ポリシーを編集するだけの場合もあります。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。選択するクラスマップに関する詳細情報については、インスペクションの適切なトラフィック クラスの選択（312 ページ）を参照してください。

照合ステートメントについては、通過トラフィック用のレイヤ 3/4 クラス マップの作成（282 ページ）を参照してください。管理レイヤ 3/4 クラスを使用する RADIUS アカウンティング インスペクションの場合は、RADIUS アカウンティング インスペクションの設定（444 ページ）を参照してください。

ステップ 2 クラス マップ トラフィックで実行するアクションを設定するレイヤ 3/4 ポリシー マップを追加または編集します。**policy-map** *name*

例：

```
hostname(config)# policy-map global_policy
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3 インスペクションに使用する L3/L4 クラス マップを特定します。**class** *name*

例：

```
hostname(config-pmap)# class inspection_default
```

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

必要に応じて同じポリシー内に複数のクラスマップを組み合わせることができるため、照合するトラフィックに応じたクラスマップを作成することができます。ただし、トラフィックがインスペクション コマンドを含むクラス マップと一致し、その後同様にインスペクション コマンドを含む別のクラスマップとも一致した場合、最初に一致したクラスだけが使用されます。たとえば、SNMP では inspection_default クラス マップを照合します。SNMP インスペクションをイネーブルにするには、デフォルト クラスの SNMP インスペクションをイネーブルにします。SNMP を照合する他のクラスを追加しないでください。

ステップ 4 アプリケーション インスペクションをイネーブルにします。**inspect** *protocol*

protocol には、次のいずれかの値を指定します。

表 *11* : インスペクション プロトコル キーワード

キーワード	注記
ctiqbe	CTIQBE インスペクション （371 ページ）を参照してください。
dcerpc [*map_name*]	DCERPC インスペクション （322 ページ）を参照してください。 DCERPC インスペクション ポリシー マップの設定 （323 ページ）に従って DCERPC インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
diameter [*map_name*] [**tls-proxy** *proxy_name*]	Diameter インスペクション （407 ページ）を参照してください。 Diameter インスペクション ポリシー マップの設定 （419 ページ） に従って Diameter インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。 **tls-proxy** *proxy_name* には、このインスペクションに使用する TLS プロキシを指定します。TLS プロキシは、暗号化されたトラフィックのインスペクションをイネーブルにする場合にのみ必要です。

キーワード	注記
dns [*map_name*] [**dynamic-filter-snoop**]	DNS インスペクション （325 ページ）を参照してください。 DNS インスペクション ポリシー マップの設定 （326 ページ）に従って DNS インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。デフォルトの DNS インスペクション ポリシー マップの名前は「preset_dns_map」です。 **dynamic-filter-snoop** は、ボットネット トラフィック フィルタによってのみ使用される動的フィルタのスヌーピングをイネーブルにします。ボットネット トラフィック フィルタリングを使用する場合に限り、このキーワードを指定します。DNS スヌーピングは、外部 DNS 要求が送信されるインターフェイスでだけイネーブルにすることを推奨します。すべての UDP DNS トラフィック（内部 DNS サーバーへの送信トラフィックを含む）に対して DNS スヌーピングをイネーブルにすると、ASA で不要な負荷が発生します。
esmtp [*map_name*]	SMTP および拡張 SMTP インスペクション （357 ページ）を参照してください。 ESMTP インスペクション ポリシー マップの設定 （359 ページ）に従って ESMTP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
ftp [**strict** [*map_name*]]	FTP インスペクション （331 ページ）を参照してください。 **strict** キーワードを使用して、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できないようにすることで、保護されたネットワークのセキュリティを強化できます。詳細については、「厳密な FTP （332 ページ）」を参照してください。 FTP インスペクション ポリシー マップの設定 （333 ページ）に従って FTP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
gtp [*map_name*]	GTP インスペクションの概要 （401 ページ）を参照してください。 GTP インスペクション ポリシー マップの設定 （412 ページ）に従って GTP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
h323 h225 [*map_name*]	H.323 インスペクション （372 ページ）を参照してください。 H.323 インスペクション ポリシー マップの設定 （375 ページ）に従って H323 インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。

キーワード	注記
h323 ras [*map_name*]	H.323 インスペクション （372 ページ）を参照してください。 H.323 インスペクション ポリシー マップの設定 （375 ページ）に従って H323 インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
http [*map_name*]	HTTP インスペクション （337 ページ）を参照してください。 HTTP インスペクション ポリシー マップの設定 （337 ページ）に従って HTTP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
icmp	ICMP インスペクション （342 ページ）を参照してください。
icmp error	ICMP エラー インスペクション （342 ページ）を参照してください。
ils	ILS インスペクション （343 ページ）を参照してください。
im [*map_name*]	インスタント メッセージ インスペクション （344 ページ）を参照してください。 インスタント メッセージ インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
ip-options [*map_name*]	IP オプション インスペクション （347 ページ）を参照してください。 IP オプション インスペクション ポリシー マップの設定 （348 ページ）に従って IP オプション インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
ipsec-pass-thru [*map_name*]	IPsec パススルー インスペクション （350 ページ）を参照してください。 IPsec パススルー インスペクション ポリシー マップの設定 （351 ページ）に従って IPsec パススルー インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
ipv6 [*map_name*]	IPv6 インスペクション （352 ページ）を参照してください。 IPv6 インスペクション ポリシー マップの設定 （353 ページ）に従って IPv6 インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。

キーワード	注記
lisp [*map_name*]	インスペクションなどのLISPを設定する詳細については、全般設定ガイドのクラスタリングの章を参照してください。 LISP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
m3ua [*map_name*]	M3UAインスペクション（408ページ）を参照してください。 M3UA インスペクション ポリシー マップの設定（438 ページ）に従って M3UA インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
mgcp [*map_name*]	MGCPインスペクション（378ページ）を参照してください。 MGCP インスペクション ポリシー マップの設定（381 ページ）に従って MGCP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
netbios [*map_name*]	NetBIOS インスペクション（355 ページ）を参照してください。 NetBIOS インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
pptp	PPTPインスペクション（356ページ）を参照してください。
radius-accounting *map_name*	RADIUSアカウンティングインスペクションの概要（410ページ）を参照してください。 **radius-accounting** キーワードは、管理クラス マップだけで使用できます。RADIUS アカウンティング インスペクション ポリシー マップを指定する必要があります。RADIUS アカウンティング インスペクション ポリシー マップの設定（444ページ）を参照してください。
rsh	RSH インスペクション（356 ページ）を参照してください。
rtsp [*map_name*]	RTSPインスペクション（382ページ）を参照してください。 RTSPインスペクションポリシーマップの設定（384ページ）に従って RTSP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
sctp [*map_name*]	SCTPアプリケーション レイヤのインスペクション（405ページ）を参照してください。 SCTPインスペクションポリシーマップの設定（417ページ）に従って SCTP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。

キーワード	注記
sip [*map_name*] [**tls-proxy** *proxy_name*]	SIP インスペクション （386 ページ）を参照してください。 SIP インスペクション ポリシー マップの設定 （389 ページ）に従って SIP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。 **tls-proxy** *proxy_name* には、このインスペクションに使用する TLS プロキシを指定します。TLS プロキシは、暗号化されたトラフィックのインスペクションをイネーブルにする場合にのみ必要です。
skinny [*map_name*]	Skinny（SCCP）インスペクション （393 ページ）を参照してください。 Skinny（SCCP）インスペクションポリシーマップの設定 （395 ページ）に従って Skinny インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
snmp [*map_name*]	SNMP インスペクション （362 ページ）を参照してください。 SNMP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
sqlnet	「SQL*Net インスペクション （363 ページ）」を参照してください。
stun	「STUN インスペクション （397 ページ）」を参照してください。
sunrpc	Sun RPC インスペクション （363 ページ）を参照してください。 デフォルトのクラス マップには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにするには、TCP ポート 111 を照合する新しいクラス マップを作成し、クラスをポリシーに追加してから、そのクラスに **inspect sunrpc** コマンドを適用する必要があります。
tftp	TFTP インスペクション （365 ページ）を参照してください。
waas	TCP オプション 33 解析をイネーブルにします。Cisco Wide Area Application Services 製品を導入するときに使用します。
xdmcp	XDMCP インスペクション （366 ページ）を参照してください。
vxlan	VXLAN インスペクション （366 ページ）を参照してください。

（注） 別のインスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（または使用中のポリシー）を編集する場合、**no inspect** *protocol* コマンドを使用して古いインスペクションを削除し、新しいインスペクション ポリシー マップ名でインスペクションを再度追加する必要があります。

例：

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

ステップ 5 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを1つだけ適用できます。

インスペクションの適切なトラフィック クラスの選択

通過トラフィックのデフォルトのレイヤ3/4クラスマップの名前は「inspection_default」です。このクラス マップは、特殊な match コマンド（match default-inspection-traffic）を使用して、トラフィックを各アプリケーションプロトコルのデフォルトのプロトコルおよびポートと照合します。このトラフィック クラスは（インスペクションには通常使用されない **match any** とともに）、IPv6 をサポートするインスペクションについて IPv4 および IPv6 トラフィックの両方を照合します。IPv6 がイネーブルなインスペクションのリストについては、アプリケーション インスペクションのガイドライン （298 ページ）を参照してください。

match access-list コマンドを match default-inspection-traffic コマンドとともに指定すると、照合するトラフィックを特定の IP アドレスに絞り込むことができます。match default-inspection-traffic コマンドによって照合するポートが指定されるため、ACL のポートはすべて無視されます。

ヒント　トラフィック インスペクションは、アプリケーション トラフィックが発生するポートだけで行うことをお勧めします。match any などを使用してすべてのトラフィックを検査すると、ASA のパフォーマンスに影響が出る場合があります。

標準以外のポートを照合する場合は、標準以外のポート用に新しいクラスマップを作成してください。各インスペクション エンジンの標準ポートについては、デフォルト インスペクションと NAT に関する制限事項（300 ページ）を参照してください。必要に応じて同じポリシー内に複数のクラスマップを組み合わせることができるため、照合するトラフィックに応じたクラス マップを作成することができます。ただし、トラフィックがインスペクション コマンドを含むクラス マップと一致し、その後同様にインスペクション コマンドを含む別のクラス マップとも一致した場合、最初に一致したクラスだけが使用されます。たとえば、SNMP では inspection_default クラスを照合します。SNMP インスペクションをイネーブルにするには、デフォルト クラスの SNMP インスペクションをイネーブルにします。SNMP を照合する他のクラスを追加しないでください。

たとえば、デフォルトのクラスマップを使用して、インスペクションを 10.1.1.0 から 192.168.1.0 へのトラフィックに限定するには、次のコマンドを入力します。

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

次のコマンドを使用して、クラス マップ全体を表示します。

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

ポート 21 とポート 1056（標準以外のポート）の FTP トラフィックを検査するには、それらのポートを指定する ACL を作成し、新しいクラス マップに割り当てます。

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

正規表現の設定

正規表現は、テキスト文字列のパターン照合を定義します。一部のプロトコルインスペクション マップでは、正規表現を使用して、URL や特定のヘッダー フィールドのコンテンツなどの文字列に基づいてパケットを照合できます。

正規表現の作成

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、メタ文字を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して特定のアプリケーション トラフィックの内容と照合できます。たとえば、HTTP パケット内部の URL 文字列と照合できます。

始める前に

Ctrl キーを押した状態で V キーを押すと、CLI において、疑問符（?）やタブなどの特殊文字をすべてエスケープできます。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

正規表現をパケットと照合する場合のパフォーマンスへの影響については、コマンド リファレンスで regex コマンドを参照してください。一般的に、長い入力文字列と照合したり、多くの正規表現と照合しようとすると、システム パフォーマンスが低下します。

（注） 最適化のために、ASA では、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。通常、「http://」のようなダブル スラッシュが使用される文字列では、代わりに「http:/」を検索してください。

次の表に、特別な意味を持つメタ文字を示します。

表 *12 :* 正規表現のメタ文字

文字	説明	注記
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp*)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。

文字	説明	注記
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc*]	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc*]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字以外の任意の 1 文字に一致します。
[*a-c*]	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
“”	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。

文字	説明	注記
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

手順

ステップ 1 正規表現が一致すべきものと一致するかどうかをテストします。**test regex** *input_text regular_expression*

input_text 引数は、正規表現を使用して照合する、長さが最大で 201 文字の文字列です。*regular_expression* 引数の長さは、最大 100 文字です。

Ctrl+V を使用して、CLI の特殊文字をすべてエスケープします。たとえば、**test regex** コマンドの入力文字にタブを入力するには、**test regex "test[Ctrl+V Tab]" "test\t"** と入力する必要があります。

正規表現が入力テキストと一致する場合は、次のメッセージが表示されます。

```
INFO: Regular expression match succeeded.
```

正規表現が入力テキストと一致しない場合は、次のメッセージが表示されます。

```
INFO: Regular expression match failed.
```

ステップ 2 テスト後に正規表現を追加するには、次のコマンドを入力します。**regex** *name regular_expression*

name 引数の長さは、最大 40 文字です。*regular_expression* 引数の長さは、最大 100 文字です。

例

次に、インスペクション ポリシー マップで使用する 2 つの正規表現を作成する例を示します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

正規表現クラス マップの作成

正規表現クラスマップは、1つ以上の正規表現を特定します。正規表現クラスマップは、正規表現オブジェクトを集めているにすぎません。多くの場合、正規表現オブジェクトの代わりに正規表現クラス マップを使用できます。

手順

ステップ 1 正規表現クラス マップを作成します。**class-map type regex match-any** *class_map_name*

class_map_name は、最大 40 文字の文字列です。「class-default」という名前は予約されています。すべてのタイプのクラスマップで同じ名前スペースが使用されるため、別のタイプのクラス マップですでに使用されている名前は再度使用できません。

match-any キーワードにより、トラフィックが少なくとも 1 つの正規表現と一致する場合には、そのトラフィックがクラス マップと一致するように指定します。

ステップ 2 （任意）クラス マップに説明を追加します。**description** *string*

ステップ 3 正規表現ごとに次のコマンドを入力して、クラスマップに含める正規表現を特定します。**match regex** *regex_name*

例

次に、2 つの正規表現を作成し、これを正規表現クラス マップに追加する例を示します。トラフィックに文字列「example.com」または「example2.com」が含まれる場合、トラフィックはクラス マップと一致します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

インスペクション ポリシーのモニタリング

インスペクション サービス ポリシーをモニターするには、次のコマンドを入力します。構文の詳細と例については、Cisco.com のコマンド リファレンスを参照してください。

- **show service-policy inspect** *protocol*

インスペクション サービス ポリシーの統計情報を表示します。*protocol* は、**dns** などの inspect コマンドからのプロトコルです。ただし、すべてのインスペクション プロトコルでこのコマンドを使用して統計情報が表示されるわけではありません。次に例を示します。

```
asa# show service-policy inspect dns

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
asa#
```

- **show conn**

  デバイスを通過するトラフィックの現在の接続を示します。さまざまなプロトコルに関する情報を取得できるように、このコマンドにはさまざまなキーワードがあります。

- 特定の検査対象プロトコルの追加コマンドは次のとおりです。

  - **show ctiqbe**

    CTIQBEインスペクションエンジンによって割り当てられたメディア接続に関する情報を表示します。

  - **show h225**

    H.225 セッションの情報を表示します。

  - **show h245**

    スロースタートを使用しているエンドポイントによって確立されたH.245セッションの情報を表示します。

  - **show h323 ras**

    ゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの接続情報を表示します。

  - **show mgcp** {**commands** | **sessions** }

    コマンド キュー内の MGCP コマンドの数、または既存の MGCP セッションの数を表示します。

  - **show sip**

    SIP セッションの情報を表示します。

  - **show skinny**

    Skinny（SCCP）セッションに関する情報を表示します。

- **show sunrpc-server active**

  Sun RPC サービス用に開けられているピンホールを表示します。

アプリケーション インスペクションの履歴

機能名	リリース	説明
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラスマップに一致させることができます。以前は、**match all** だけが使用可能でした。

第 13 章

基本インターネット プロトコルのインスペクション

ここでは、基本インターネット プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、アプリケーション レイヤ プロトコル インスペクションの準備 （295 ページ）を参照してください。

- DCERPC インスペクション （322 ページ）
- DNS インスペクション （325 ページ）
- FTP インスペクション （331 ページ）
- HTTP インスペクション （337 ページ）
- ICMP インスペクション （342 ページ）
- ICMP エラー インスペクション （342 ページ）
- ILS インスペクション （343 ページ）
- インスタント メッセージ インスペクション （344 ページ）
- IP オプション インスペクション （347 ページ）
- IPsec パススルー インスペクション （350 ページ）
- IPv6 インスペクション （352 ページ）
- NetBIOS インスペクション （355 ページ）
- PPTP インスペクション （356 ページ）
- RSH インスペクション （356 ページ）
- SMTP および拡張 SMTP インスペクション （357 ページ）
- SNMP インスペクション （362 ページ）
- SQL*Net インスペクション （363 ページ）
- Sun RPC インスペクション （363 ページ）
- TFTP インスペクション （365 ページ）
- XDMCP インスペクション （366 ページ）
- VXLAN インスペクション （366 ページ）
- 基本的なインターネット プロトコル インスペクションの履歴 （367 ページ）

DCERPC インスペクション

デフォルトのインスペクション ポリシーでは、DCERPC インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。デフォルトのグローバルインスペクション ポリシーを編集するだけで、DCERPC インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

次の項では、DCERPC インスペクション エンジンについて説明します。

DCERPC の概要

DCERPC に基づく Microsoft リモート プロシージャ コール（MSRPC）は、Microsoft 分散クライアントおよびサーバー アプリケーションで広く使用されているプロトコルであり、ソフトウェア クライアントがサーバー上のプログラムをリモートで実行できるようにします。

通常、このプロトコルの接続では、クライアントが予約済みポート番号で接続を受け入れるエンドポイント マッパーというサーバーに、必要なサービスについてダイナミックに割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバーのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCERPC インスペクション エンジンは、EPM とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバーは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバーの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバーのポートに対して複数の接続を試みる可能性があるので、ピンホールが複数使用でき、ユーザーがそのタイムアウトを設定できるようになっています。

DCE インスペクションは、次の汎用一意識別子（UUID）とメッセージをサポートします。

- エンドポイント マッパー（EPM）UUID。すべての EPM メッセージがサポートされます。
- ISystemMapper UUID（非 EPM）。サポートされるメッセージ タイプは次のとおりです。
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- OxidResolver UUID（非EPM）。サポートされるメッセージは次のとおりです。
  - ServerAlive2 opnum5
- IP アドレスまたはポート情報を含まない任意のメッセージ（これらのメッセージでは検査の必要がないため）。

DCERPC インスペクション ポリシー マップの設定

DCERPC インスペクションの追加のパラメータを指定するには、DCERPC インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、DCERPC インスペクションをイネーブルにすると適用できます。

トラフィックの一致基準を定義するときに、クラスマップを作成するか、またはポリシーマップにmatchステートメントを直接含めることができます。クラスマップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、クラスマップを再使用できる点です。

手順

ステップ 1 （任意）DCERPC インスペクション クラス マップを作成します。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect dcerpc** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-anyキーワードは、トラフィックが少なくとも1つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI はクラス マップ コンフィギュレーション モードに移行します。

b) 次の **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **uuid** *type*：DCERPC メッセージの汎用一意識別子（UUID）を照合します。*type* は次のいずれかです。
  - **ms-rpc-epm**：Microsoft RPC EPM メッセージを照合します。
  - **ms-rpc-isystemactivator**：ISystemMapper メッセージを照合します。
  - **ms-rpc-oxidresolver**：OxidResolver メッセージを照合します。

c) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 DCERPC インスペクション ポリシー マップを作成します。**policy-map type inspect dcerpc** *policy_map_name*

policy_map_name には、ポリシーマップの名前を指定します。CLI はポリシーマップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- DCERPC クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- DCERPC クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **reset** [**log**]：パケットをドロップし、接続を閉じてサーバーまたはクライアントに TCP リセットを送信します。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。

例：

```
hostname(config)# policy-map type inspect dcerpc dcerpc-map
hostname(config-pmap)# match uuid ms-rpc-epm
hostname(config-pmap-c)# log
```

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **timeout pinhole** *hh:mm:ss*：DCERPC ピンホールのタイムアウトを設定し、2 分のグローバル システム ピンホール タイムアウトを上書きします。タイムアウトは 00:00 01 ～ 119:00:00 まで指定できます。
- **endpoint-mapper** [**epm-service-only**] [**lookup-operation** [**timeout** *hh:mm:ss*]]：エンドポイント マッパー トラフィックのオプションを設定します。**epm-service-only** キーワードを指定すると、バインド中にエンドポイント マッパー サービスを実行し、このサービスのトラフィックだけが処理されるようにします。**lookup-operation** キーワードを指定すると、エンドポイント マッパー サービスのルックアップ操作をイネーブルにします。ルックアップ操作で生成されたピンホールのタイムアウトを設定できます。

ルックアップ操作にタイムアウトが設定されていない場合は、timeout pinhole コマンドで指定した値かデフォルトの値が使用されます。

例

次の例は、DCERPCインスペクション ポリシーマップを定義し、DCERPC のピンホールのタイムアウトを設定する方法を示しています。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-map

hostname(config)# service-policy global-policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

DNS インスペクション

DNSインスペクションはデフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。ここでは、DNS アプリケーション インスペクションについて説明します。

DNS インスペクションのデフォルト

DNS インスペクションは、次のような preset_dns_map インスペクション クラス マップを使用して、デフォルトでイネーブルになっています。

- 最大 DNS メッセージ長は、512 バイトです。
- DNS over TCP インスペクションは無効です。
- 最大クライアント DNS メッセージ長は、リソース レコードに一致するように自動的に設定されます。

- DNS ガードはイネーブルになり、ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニターして DNS 応答の ID が DNS クエリの ID と一致することを確認します。
- NAT の設定に基づく DNS レコードの変換はイネーブルです。
- プロトコルの強制はイネーブルであり、DNS メッセージ形式チェックが行われます。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。

次のデフォルトの DNS インスペクション コマンドを参照してください。

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
! ...
service-policy global_policy global
```

（注） 毎秒多数のパケットが検査される場合、Cisco ASA で CPU 使用率が上昇する可能性があります。処理されるパケットの数が増えると（特にデバイスがスループットまたは接続キャパシティの最大値に近づいた場合）、CPU 使用率も上昇します。これは、Cisco ASA が毎秒多くの操作を実行する必要があり、CPU リソースの消費が増えるために発生します。

DNS インスペクション ポリシー マップの設定

デフォルトのインスペクション動作がネットワークにとって十分でない場合、DNS インスペクション ポリシー マップを作成して DNS インスペクション アクションをカスタマイズできます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、DNS インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect dns** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **header-flag** [**eq**] {*f_name* [*f_name...*] | *f_value*}：DNS フラグと一致します。*f_name* 引数は DNS フラグ名であり、**AA**（権限応答）、**QR**（クエリー）、**RA**（使用できる再帰）、**RD**（必要な再帰）、**TC**（切り捨て）のいずれかです。*f_value* 引数は、0x で始まる 16 ビットの 16 進値です（0x0 ～ 0xffff）。eq キーワードは完全一致を指定します（すべて一致）。**eq** キーワードを指定しないと、パケットは指定されているヘッダーの 1 つと一致するだけで十分です（いずれかと一致）。例：**match header-flag AA QR**

- **match** [**not**] **dns-type {eq** {*t_name* | *t_value*} | **range** *t_value1 t_value2*}：DNS タイプと一致します。*t_name* 引数は DNS タイプ名であり、次のいずれかです。**A**（IPv4 アドレス）、**AXFR**（フル ゾーン転送）、**CNAME**（正規の名前）、**IXFR**（増分ゾーン転送）、**NS**（権限ネーム サーバー）、**SOA**（権限ゾーンの開始）、**TSIG**（トランザクション署名）です。t_value 引数には、DNS タイプ フィールドの任意の値（0 ～ 65535）

を指定します。range キーワードは範囲を指定し、eq キーワードは完全一致を指定します。例：**match dns-type eq A**

- **match** [**not**] **dns-class {eq** {**in** | *c_value*} | **range** *c_value1 c_value2*}：DNS クラスと一致します。クラスは **in**（インターネットの場合）または c_value（DNS クラス フィールドの 0 ～ 65535 の任意の値）です。range キーワードは範囲を指定し、eq キーワードは完全一致を指定します。例：**match dns-class eq in**
- **match** [**not**] {**question** | **resource-record** {**answer** | **authority** | **additional**}}：DNS の質問またはリソース レコードと一致します。**question** キーワードは、DNS メッセージの問い合わせ部分を指定します。resource-record キーワードは、リソース レコードのセクション **answer**、authority、**additional** のいずれかを指定します。例：**match resource-record answer**
- **match** [**not**] **domain-name regex** {*regex_name* | **class** *class_name*}：DNS メッセージのドメイン名のリストを、指定された正規表現または正規表現クラスに対して照合します。

d) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 DNS インスペクション ポリシー マップを作成します。**policy-map type inspect dns** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- DNS クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- DNS クラスマップで説明されている **match** コマンドのいずれかを使用して、ポリシーマップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop** [**log**]：一致するすべてのパケットをドロップします。
- **drop-connection** [**log**]：パケットをドロップし、接続を閉じます。
- **mask** [**log**]：パケットの一致する部分をマスクします。このアクションは、ヘッダー フラグの照合だけで利用可能です。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。

- **enforce-tsig** [**drop**] [**log**]：メッセージに TSIG リソース レコードが存在することを強制します。TSIG リソース レコードがないパケットをドロップ、ログ記録、またはドロップしてログ記録できます。ヘッダー フラグ一致の場合、このオプションをマスク アクションと組み合わせて使用できます。それ以外の場合、このアクションと他のアクションを同時に指定することはできません。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法（297 ページ）を参照してください。

例：

```
hostname(config)# policy-map type inspect dns dns-map
hostname(config-pmap)# class dns-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match header-flag eq aa
hostname(config-pmap-c)# drop log
```

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **dnscrypt**：DNScrypt を有効にしてデバイスと Cisco Umbrella 間の接続を暗号化します。DNScrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。DNScrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラス マップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。
- **dns-guard**：DNS ガードをイネーブルにします。ASA で DNS 応答が転送されるとすぐに、ASA は DNS クエリーに関連付けられた DNS セッションを切断します。ASA はまた、メッセージ交換をモニターして DNS 応答の ID が DNS クエリの ID と一致することを確認します。
- **id-mismatch count** *number* **duration** *seconds* **action log**：DNS ID の過剰な不一致のロギングをイネーブルにします。**count** *number* **duration** *seconds* 引数は、システム メッセージ ログが送信されるようになる 1 秒間の不一致インスタンスの最大数を指定します。
- **id-randomization**：DNS クエリーの DNS 識別子をランダム化します。
- **message-length maximum** {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}}：DNS メッセージの最大長を設定します（512 ～ 65535 バイト）。クライアント メッセージ

またはサーバー メッセージの最大長も設定できます。**auto** キーワードは、リソース レコードの値に最大長を設定します。

- **nat-rewrite**：DNS レコードを NAT の設定に基づいて変換します。
- **protocol-enforcement**：DNS メッセージ形式のチェックをイネーブルにします。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。
- **tcp-inspection**：DNS over TCP トラフィックのインスペクションを有効にします。DNS/TCP ポート 53 トラフィックが、DNS インスペクションを適用するクラスの一部であることを確認します。インスペクションのデフォルト クラスには、TCP/53 が含まれています。
- **tsig enforced action** {[**drop**] [**log**]}：TSIG リソース レコードの存在を要求します。準拠していないパケットをドロップしたり（**drop**）、パケットをログに記録したり（**log**）できます。両方指定することもできます。
- **umbrella** ［**tag** *umbrella_policy*］［**fail-open**］：Cisco Umbrella をイネーブルにし、必要に応じてデバイスに適用する Cisco Umbrella のポリシー名（**tag**）を指定します。ポリシーを指定しない場合は、デフォルトの ACL が適用されます。詳細については、Cisco Umbrella （117 ページ）を参照してください。

  Umbrella DNS サーバーが使用できない場合に DNS 解決を動作させるには、**fail-open** キーワードを追加します。フェール オープンの状態で Cisco Umbrella DNS サーバーが使用できない場合は、このポリシー マップで Umbrella 自体がディセーブルになり、DNS 要求をシステム上に設定された他の DNS サーバー（存在する場合）に移動できるようになります。Umbrella DNS サーバーが再度使用可能になると、ポリシーマップはそれらの使用を再開します。このオプションが含まれていない場合、DNS 要求は到達不能の Umbrella リゾルバへ移動し続けるので、応答は取得されません。

例：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

例

次の例では、グローバル デフォルト設定で新しいインスペクション ポリシー マップを使用する方法を示します。

```
regex domain_example “example\.com”
regex domain_foo “foo\.com”

! define the domain names that the server serves
```

```
class-map type regex match-any my_domains
   match regex domain_example
   match regex domain_foo

! Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
   match not header-flag QR
   match question
   match not domain-name regex class my_domains

policy-map type inspect dns new_dns_map
    class pub_server_map
        drop log
    match header-flag RD
        mask log
    parameters
        message-length maximum client auto
        message-length maximum 512
        dns-guard
        protocol-enforcement
        nat-rewrite

policy-map global_policy
 class inspection_default
  no inspect dns preset_dns_map
  inspect dns new_dns_map
service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

FTP インスペクション

FTPインスペクションは、デフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。ここでは、FTPインスペクションエンジンについて説明します。

FTP インスペクションの概要

FTPアプリケーションインスペクションは、FTPセッションを検査し、次の4つのタスクを実行します。

- FTP データ転送のために動的なセカンダリ データ接続チャネルを準備します。これらのチャネルのポートは、PORT コマンドまたは PASV コマンドを使用してネゴシエートされます。セカンダリ チャネルは、ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト イベントへの応答で割り当てられます。
- FTP コマンド/応答シーケンスを追跡します。
- 監査証跡を生成します。

- 取得またはアップロードされたファイルごとに監査レコード303002が生成されます。
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

- 埋め込み IP アドレスを変換します。

（注） FTPインスペクションをディセーブルにすると、発信ユーザーはパッシブ モードでしか接続を開始できなくなり、着信 FTP はすべてディセーブルになります。

厳密な FTP

厳密な FTP を使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが強化されます。厳密なFTPをイネーブルにするには、**inspect ftp**コマンドに strict オプションを含めます。

厳密な FTP を使用するときは、オプションで FTP インスペクション ポリシー マップを指定して、ASA を通過することが許可されない FTP コマンドを指定できます。

厳密な FTP インスペクションでは、次の動作が強制されます。

- FTP コマンドが確認応答されてからでないと、ASA は新しいコマンドを許可しません。
- ASA は、埋め込みコマンドを送信する接続をドロップします。
- 227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

注意 厳密な FTP を使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。さらに、インスペクションをFTPポートのみに適用する必要があります（通常の FTP ポートは TCP/21 です）。非 FTP トラフィックに厳密な FTP インスペクションを適用すると、（特にHTTPトラフィックで）予期しないトラフィック損失が発生する可能性があります。

厳密な FTP インスペクションでは、各 FTP コマンドと応答のシーケンスを追跡し、次の異常なアクティビティがないかをチェックします。

- 切り捨てされたコマンド：PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド：FTP コマンドが、RFC の要求どおりに <CR><LF> 文字で終了しているかどうか確認されます。終了していない場合は、接続が閉じられます。

- RETR コマンドと STOR コマンドのサイズ：これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラーメッセージがロギングされ、接続が閉じられます。
- コマンドスプーフィング：PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバーから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV 応答コマンド（227）は、常にサーバーから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザーが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集：ASA は、TCP ストリーム編集を検出した場合に接続が閉じられます。
- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- ASA は SYST コマンドに対する FTP サーバーの応答を連続した X で置き換えて、サーバーのシステム タイプが FTP クライアントに知られないようにします。このデフォルトの動作を無効にするには、FTP マップで、**no mask-syst-reply** コマンドを使用します。

FTP インスペクション ポリシー マップの設定

厳密な FTP インスペクションには、セキュリティと制御を向上させるためのコマンド フィルタリングとセキュリティ チェック機能が用意されています。プロトコルとの適合性のインスペクションには、パケットの長さのチェック、デリミタとパケットの形式のチェック、コマンドのターミネータのチェック、およびコマンドの検証が含まれます。

また、ユーザーの値に基づいて FTP 接続をブロックできるので、FTP サイトにダウンロード用のファイルを置き、アクセスを特定のユーザーだけに制限できます。ファイルのタイプ、サーバ名、および他の属性に基づいて、FTP 接続をブロックできます。インスペクション時に FTP 接続が拒否されると、システム メッセージのログが作成されます。

FTP インスペクションで FTP サーバーがそのシステム タイプを FTP クライアントに公開することを許可し、許可する FTP コマンドを制限する場合、FTP インスペクション ポリシー マップを作成および設定します。作成したマップは、FTP インスペクションをイネーブルにすると適用できます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、FTP インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect ftp** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*}：FTP 転送のファイル名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **filetype regex** {*regex_name* | **class** *class_name*}：FTP 転送のファイル タイプを、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **request-command** *ftp_command* [*ftp_command...*]：FTP コマンドを照合します。以下の 1 つ以上です。
  - **APPE**：ファイルに追加します。
  - **CDUP**：現在の作業ディレクトリの親ディレクトリに変更します。
  - **DELE**：サーバーのファイルを削除します。

- **GET**：サーバーからファイルを取得します。
- **HELP**：ヘルプ情報を提供します。
- **MKD**：サーバーにディレクトリを作成します。
- **PUT**：ファイルをサーバーに送信します。
- **RMD**：サーバーのディレクトリを削除します。
- **RNFR**：「変更前の」ファイル名を指定します。
- **RNTO**：「変更後の」ファイル名を指定します。
- **SITE**：サーバー固有のコマンドの指定に使用されます。通常、これはリモート管理に使用されます。
- **STOU**：一義的なファイル名を使用してファイルを保存します。

- **match** [**not**] **server regex** {*regex_name* | **class** *class_name*}：FTP サーバー名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **username regex** {*regex_name* | **class** *class_name*}：FTP ユーザー名を、指定された正規表現または正規表現クラスに対して照合します。

d) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 FTPインスペクション ポリシーマップを作成します。**policy-map type inspect ftp** *policy_map_name*

policy_map_name には、ポリシーマップの名前を指定します。CLI はポリシーマップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- FTP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- FTP クラスマップで説明されている **match** コマンドのいずれかを使用して、ポリシーマップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

- **reset** [**log**]：パケットをドロップし、接続を閉じてサーバーまたはクライアントに TCP リセットを送信します。システム ログ メッセージを送信するには、**log** キーワードを追加します。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法（297 ページ）を参照してください。

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **mask-banner**：FTP サーバーから接続時バナーをマスクします。
- **mask-syst-reply**：**syst** コマンドに対する応答をマスクします。

例

ユーザー名とパスワードを送信する前に、すべての FTP ユーザーに接続時バナーが表示されます。デフォルトでは、このバナーには、ハッカーがシステムの弱点を特定するのに役立つバージョン情報が含まれます。このバナーをマスクする方法を次に示します。

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

hostname(config)# service-policy ftp-policy interface inside
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定（305 ページ）を参照してください。

HTTP インスペクション

HTTPインスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの HTTP ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで HTTP インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービスポリシーを作成することもできます。

ここでは、HTTP インスペクション エンジンについて説明します。

HTTP インスペクションの概要

HTTP インスペクション エンジンを使用して、HTTP トラフィックに関係する特定の攻撃やその他の脅威から保護します。

HTTP アプリケーション インスペクションで HTTP のヘッダーと本文をスキャンし、さまざまなデータ チェックができます。これらのチェックで、HTTP 構築、コンテンツ タイプ、トンネル プロトコル、メッセージ プロトコルなどがセキュリティ アプライアンスを通過することを防止します。

拡張 HTTP インスペクション機能はアプリケーション ファイアウォールとも呼ばれ、HTTP インスペクション ポリシーマップを設定するときに使用できます。これによって、攻撃者がネットワーク セキュリティ ポリシーに従わない HTTP メッセージを使用できないようにします。

HTTP アプリケーション インスペクションでトンネル アプリケーションと ASCII 以外の文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが Web サーバに到達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサイズ制限、URL のブロッキング、HTTP サーバ ヘッダー タイプのスプーフィングもサポートされています。

拡張 HTTP インスペクションは、すべての HTTP メッセージについて次の点を確認します。

- RFC 2616 への準拠
- RFC で定義された方式だけを使用していること
- 追加の基準への準拠

HTTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、HTTP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、HTTP インスペクションをイネーブルにすると適用できます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、HTTP インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect http** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **req-resp content-type mismatch**：HTTP 応答の content-type フィールドが対応する HTTP 要求メッセージの accept フィールドと一致しないトラフィックを照合します。
- **match** [**not**] **request args regex** {*regex_name* | **class** *class_name*}：HTTP 要求メッセージの引数で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。

- **match** [**not**] **request body** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*}：HTTP 要求メッセージの本文で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。または、要求の本文が指定した長さより長いメッセージを照合します。
- **match** [**not**] **request header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*}：HTTP 要求メッセージ ヘッダーのフィールドの内容を、指定した正規表現または正規表現クラスと照合します。フィールド名を明示的に指定することも、フィールド名を正規表現と一致させることもできます。フィールド名は次のとおりです。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。
- **match** [**not**] **request header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*}：HTTP 要求メッセージ ヘッダーの指定したフィールドの長さ、またはヘッダーのフィールドの総数を照合します。フィールド名を明示的に指定することも、フィールド名を正規表現または正規表現クラスと一致させることもできます。フィールド名は、前の項目の一覧と同じです。
- **match** [**not**] **request header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**}：HTTP 要求メッセージヘッダーの全体の長さ、ヘッダーのフィールドの総数、またはASCII以外の文字を含むヘッダーを照合します。
- **match** [**not**] **request method** {*method* | **regex** {*regex_name* | **class** *class_name*}}：HTTP 要求のメソッドを照合します。メソッドを明示的に指定することも、メソッドを正規表現または正規表現クラスと一致させることもできます。メソッドは次のとおりです。bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。
- **match** [**not**] **request uri** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*}：HTTP 要求メッセージのURIで見つかったテキストを、指定した正規表現または正規表現クラスと照合します。または、要求のURIが指定した長さより長いメッセージを照合します。
- **match** [**not**] **response body** {**active-x** | **java-applet** | **regex** {*regex_name* | **class** *class_name*}}：HTTP 応答メッセージの本文で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。または、Java アプレットおよび Active X オブジェクトをフィルタ処理のためにコメント化します。
- **match** [**not**] **response body length gt** *bytes*：本文が指定した長さより大きい HTTP 応答メッセージを照合します。

- **match** [**not**] **response header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*}：HTTP 応答メッセージ ヘッダーのフィールドの内容を、指定した正規表現または正規表現クラスと照合します。フィールド名を明示的に指定することも、フィールド名を正規表現と一致させることもできます。フィールド名は次のとおりです。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。
- **match** [**not**] **response header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*}：HTTP 応答メッセージ ヘッダーの指定したフィールドの長さ、またはヘッダーのフィールドの総数を照合します。フィールド名を明示的に指定することも、フィールド名を正規表現または正規表現クラスと一致させることもできます。フィールド名は、前の項目の一覧と同じです。
- **match** [**not**] **response header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**}：HTTP 応答メッセージ ヘッダーの全体の長さ、ヘッダーのフィールドの総数、または ASCII 以外の文字を含むヘッダーを照合します。
- **match** [**not**] **response status-line regex** {*regex_name* | **class** *class_name*}：HTTP 応答メッセージのステータス行で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。

d) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 HTTP インスペクション ポリシー マップを作成します。**policy-map type inspect http** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- HTTP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- HTTP クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop-connection** [**log**]：パケットをドロップし、接続を閉じます。

- **reset** [**log**]：パケットをドロップし、接続を閉じてサーバーまたはクライアントに TCP リセットを送信します。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法（297 ページ）を参照してください。

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **body-match-maximum** *number*：HTTP メッセージの本文照合時に検索する本文の最大文字数を設定します。デフォルト値は 200 バイトです。大きな値を指定すると、パフォーマンスに大きな影響を与えます。
- **protocol-violation action** {**drop-connection** [**log**] | **reset** [**log**] | **log**}：HTTP プロトコル違反について確認します。違反に対して実行するアクション（切断、リセット、ログ記録）、およびロギングをイネーブルまたはディセーブルにするかどうかも選択する必要があります。
- **spoof-server** *string*：サーバーのヘッダー フィールドを文字列に置き換えます。WebVPN ストリームは spoof-server コマンドの対象になりません。

例

次に、「GET」メソッドまたは「PUT」メソッドで「www\.xyz.com/.*\.asp」または「www\.xyz[0-9][0-9]\.com」にアクセスしようとしている HTTP 接続を許可し、ロギングする HTTP インスペクション ポリシー マップを定義する例を示します。それ以外の URL/メソッドの組み合わせは、サイレントに許可されます。

```
hostname(config)# regex url1 “www\.xyz.com/.*\.asp”
hostname(config)# regex url2 “www\.xyz[0-9][0-9]\.com”
hostname(config)# regex get “GET”
hostname(config)# regex put “PUT”

hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit
```

```
hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit

hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit

hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

ICMP インスペクション

ICMP インスペクション エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になります。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP が ASA を通過するのを禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンは、要求ごとに応答が 1 つだけであること、シーケンス番号が正しいことを確認します。

ただし、ASA インターフェイスに送信される ICMP トラフィックは、ICMP インスペクションをイネーブルにした場合でも検査されません。したがって、ASA がバックアップ デフォルト ルートを介して到達できる送信元からエコー要求が送信された場合など、特定の状況下では、インターフェイスへの ping（エコー要求）が失敗する可能性があります。

（注） NAT は、ICMP インスペクションを無効にしても、パケットを変換するときに ICMP インスペクションを使用します。

ICMP インスペクションをイネーブルにする方法については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

ICMP エラー インスペクション

ICMP エラー インスペクションをイネーブルにすると、ASA は NAT の設定に基づいて、ICMP エラー メッセージを送信する中間ホップ用の変換セッションを作成します。ASA は、変換後の IP アドレスでパケットを上書きします。

ディセーブルの場合、ASA は、ICMP エラー メッセージを生成する中間ノード用の変換セッションを作成しません。内部ホストと ASA の間にある中間ノードによって生成された ICMP エラーメッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが traceroute コマンドを使用して ASA の内部にある宛先までのホップをトレースする場合、これは適切ではありません。ASA が中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

（注） NAT が ICMP パケットで使用される可能性がある場合は、常に ICMP エラー インスペクションを有効にする必要があります。NAT は、ICMP インスペクションを無効にしていても ICMP パケットに対して ICMP インスペクションを自動的に実行するため、マッピングされた宛先アドレスを送信元アドレスとして使用すると、スキャナーがネットワークを検査しているように見える可能性があります。たとえば、ICMP エラーインスペクションも有効になっていない場合、ICMP タイム超過応答に埋め込まれたエコー要求パケットの宛先が変換されると、タイム超過要求の外部ヘッダーでは、変換された宛先が送信元アドレスとして使用されます。ICMP エラーインスペクションを有効にすると、タイム超過になった送信元アドレスに正しい値が設定されます。

ICMP エラーインスペクションをイネーブルにする方法については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

ILS インスペクション

Internet Locator Service（ILS）インスペクション エンジンは、LDAP を使用してディレクトリ情報を ILS サーバーと交換する Microsoft NetMeeting、SiteServer、および Active Directory の各製品に対して NAT をサポートします。LDAP データベースには IP アドレスだけが保存されるため、ILS インスペクションで PAT は使用できません。

LDAP サーバーが外部にある場合、内部ピアが外部 LDAP サーバーに登録された状態でローカルに通信できるように、検索応答に対して NAT を使用することを検討してください。NAT を使用する必要がなければ、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることを推奨します。

ILS サーバーが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバーにアクセスするためのホールが必要となります。

（注） ILS トラフィック（H225 コール シグナリング）はセカンダリ UDP チャネルだけで発生するため、TCP 接続は TCP 非アクティブ間隔の後に切断されます。デフォルトでは、この間隔は 60 分です。この値は、TCP timeout コマンドを使用して調整できます。ASDM では、これは [Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインにあります。

ILS インスペクションには、次の制限事項があります。

- 照会要求や応答はサポートされません。
- 複数のディレクトリのユーザーは統合されません。
- 複数のディレクトリに複数の ID を持っている単一のユーザーは NAT には認識されません。

ILS インスペクションをイネーブルにする方法については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

インスタント メッセージ インスペクション

インスタントメッセージ（IM）インスペクションエンジンを使用すると、IMのネットワーク使用を制御し、機密情報の漏洩、ワームの送信、および企業ネットワークへのその他の脅威を停止できます。

IM インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IM ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IM インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

IM インスペクションを実装する場合は、メッセージがパラメータに違反した場合のアクションを指定する IM インスペクション ポリシー マップを設定することもできます。次の手順では、IM インスペクション ポリシー マップについて説明します。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、IM インスペクションのクラス マップを作成します。

クラス マップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラスマップを作成します。**class-map type inspect im** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **protocol {im-yahoo | im-msn}**：特定の IM プロトコル（Yahoo または MSN）を照合します。
- **match** [**not**] **service {chat | file-transfer** | **webcam** | **voice-chat** | **conference** | **games}**：特定の IM サービスを照合します。
- **match** [**not**] **login-name regex** {*regex_name* | **class** *class_name*}：IM メッセージの送信元クライアント ログイン名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **peer-login-name regex** {*regex_name* | **class** *class_name*}：IM メッセージの宛先ピア ログイン名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **ip-address** *ip_address mask*}：IM メッセージの送信元 IP アドレスとマスクを照合します。
- **match** [**not**] **peer-ip-address** *ip_address mask*}：IM メッセージの宛先 IP アドレスとマスクを照合します。
- **match** [**not**] **version regex** {*regex_name* | **class** *class_name*}：IM メッセージのバージョンを、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*}：IM メッセージのファイル名を、指定された正規表現または正規表現クラスに対して照合します。この照合は MSN IM プロトコルに対してはサポートされません。

d) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 IM インスペクション ポリシー マップを作成します。**policy-map type inspect im** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- IM クラスマップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- IM クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

- **drop-connection** [**log**]：パケットをドロップし、接続を閉じます。
- **reset** [**log**]：パケットをドロップし、接続を閉じてサーバーまたはクライアントに TCP リセットを送信します。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法（297 ページ）を参照してください。

例

次の例は、IM インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname4 "darshant\@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\.0"
hostname(config)# regex gif_files ".*\.gif"
hostname(config)# regex exe_files ".*\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4
```

```
hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

IP オプション インスペクション

IP オプション インスペクションを設定して、パケット ヘッダーの [IP Options] フィールドのコンテンツに基づいてどの IP パケットを許可するかについて制御できます。望ましくないオプションがあるパケットをドロップしたり、オプションをクリア（してパケットを許可）したり、変更なしでパケットを許可したりできます。

IP オプションで提供される制御機能は、一部の状況では必須ですが、ほとんどの一般的な状況では不要です。具体的には、IP オプションにはタイムスタンプ、セキュリティ、および特殊なルーティングの規定が含まれています。IP オプションの使用は任意であり、このフィールドにはオプションを 0 個、1 個、またはそれ以上含めることができます。

IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml）を参照してください。

IP オプションのインスペクションはデフォルトで有効になっていますが、RSVP トラフィックに対してのみとなっています。デフォルトのマップが許可しているもの以外に追加のオプションを許可するか、またはデフォルト以外のインスペクション トラフィック クラス マップを使用することによって他のタイプのトラフィックに適用する場合にのみ、これを設定する必要があります。

（注） IP オプション インスペクションは、フラグメント化されたパケットでは動作しません。たとえば、オプションはフラグメントからクリアされません。

次の項では、IP オプション インスペクションについて説明します。

IP オプション インスペクションのデフォルト

IP オプション インスペクションは、_default_ip_options_map インスペクション ポリシー マップを使用して、RSVP トラフィックのデフォルトのみで有効になります。

- Router Alert オプションは許可されます。

  このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインスペクションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケットの配信パス上にあるルータでの比較的複雑な処理を必要とします。Router Alert オプションが含まれた RSVP パケットをドロップすると、VoIP の実装で問題が生じることがあります。

- その他のオプションを含むパケットはドロップされます。

  インスペクションによってパケットがドロップされるたびに、syslog 106012 が発行されます。メッセージではドロップの原因になったオプションが示されます。show service-policy inspect ip-options コマンドを使用して、各オプションの統計情報を表示します。

ポリシー マップのコンフィギュレーションは次のとおりです。

```
policy-map type inspect ip-options _default_ip_options_map
 description Default IP-OPTIONS policy-map
 parameters
  router-alert action allow
```

IP オプション インスペクション ポリシー マップの設定

デフォルト以外の IP オプション インスペクションを実行する場合は、IP オプション インスペクション ポリシー マップを作成して、各オプション タイプの処理方法を指定します。

手順

ステップ 1 IP オプション インスペクション ポリシー マップを作成します。**policy-map type inspect ip-options** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4 許可するオプションを特定します。

次のオプションを検査できます。いずれの場合も、**allow** アクションはそのオプションを含むパケットを変更なしで許可し、**clear** アクションはパケットを許可しますがヘッダーからそのオプションを除去します。

マップからオプションを削除するには、このコマンドの **no** 形式を使用します。パケットに他の許可されているオプションまたはクリアされたオプションが含まれている場合でも、マップで指定されていないオプションを含むパケットはすべてドロップされます。

IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml）を参照してください。

- **default action** {**allow** | **clear**}：マップに明示的に含まれていないオプションに対するデフォルト アクションを設定します。許可またはクリアのデフォルト アクションを設定しないと、許可されていないオプションを含むパケットはドロップされます。
- **basic-security action** {**allow** | **clear**}：Security（SEC）オプションを許可またはクリアします。
- **commercial-security action** {**allow** | **clear** }：Commercial Security（CIPSO）オプションを許可またはクリアします。
- **eool action** {**allow** | **clear**}：End of Options List オプションを許可またはクリアします。
- **exp-flow-control action** {**allow** | **clear**}：Experimental Flow Control（FINN）オプションを許可またはクリアします。
- **exp-measurement action** {**allow** | **clear**}：Experimental Measurement（ZSU）オプションを許可またはクリアします。
- **extended-security action** {**allow** | **clear**}：Extended Security（E-SEC）オプションを許可またはクリアします。
- **imi-traffic-descriptor action** {**allow** | **clear**}：IMI Traffic Descriptor（IMITD）オプションを許可またはクリアします。
- **nop action** {**allow** | **clear**}：No Operation オプションを許可またはクリアします。
- **quick-start action** {**allow** | **clear**}：Quick-Start（QS）オプションを許可またはクリアします。
- **record-route action** {**allow** | **clear**}：Record Route（RR）オプションを許可またはクリアします。
- **router-alert action** {**allow** | **clear**}：Router Alert（RTRALT）オプションを許可またはクリアします。
- **timestamp action** {**allow** | **clear**}：Time Stamp（TS）オプションを許可またはクリアします。

- {**0-255**} **action** {**allow** | **clear**}：オプション タイプ番号によって識別されるオプションを許可またはクリアします。番号は全オプション タイプのオクテット（コピー、クラス、およびオプション番号）で、オクテットのオプションの番号部分だけではありません。これらのオプション タイプは、実際のオプションに表示されない可能性があります。非標準オプションは、インターネット プロトコル RFC 791、http://tools.ietf.org/html/rfc791 で定義された予測されるタイプ/長さ/値の形式である必要があります。

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

IPsec パススルー インスペクション

IPsec パススルー インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IPsec ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IPsec インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

ここでは、IPsec パススルー インスペクション エンジンについて説明します。

IPsec パス スルー インスペクションの概要

Internet Protocol Security（IPsec）は、データ ストリームの各 IP パケットを認証および暗号化することによって、IP 通信をセキュリティで保護するためのプロトコル スイートです。IPsec には、セッションの開始時、およびセッション中に使用される暗号キーのネゴシエーションの開始時に、エージェント間の相互認証を確立するためのプロトコルも含まれています。IPsec を使用して、ホスト（コンピュータ ユーザーまたはサーバーなど）のペア間、セキュリティ ゲートウェイ（ルータやファイアウォールなど）のペア間、またはセキュリティ ゲートウェイとホスト間のデータ フローを保護できます。

IPsec パススルー アプリケーション インスペクションは、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）および AH（IP プロトコル 51）トラフィックを簡単に横断できます。このインスペクションは、冗長な ACL コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

ESP または AH トラフィックの制限を指定するには、IPsec パススルーのポリシー マップを設定します。クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

IPsec パススルー インスペクション ポリシー マップの設定

IPsec パススルー マップでは、IPsec パススルー アプリケーション インスペクションのデフォルト設定値を変更できます。IPsec パススルー マップを使用すると、アクセス リストを使用しなくても、特定のフローを許可できます。

コンフィギュレーションに含まれるデフォルト マップ _default_ipsec_passthru_map では、ESP 接続に対するクライアントごとの最大数は制限なしに設定され、ESP アイドル タイムアウトは 10 分に設定されます。異なる値が必要な場合、または AH 値を設定する必要がある場合にのみ、インスペクション ポリシー マップを設定する必要があります。

手順

ステップ 1 IPsec パススルー インスペクション ポリシー マップを作成します。**policy-map type inspect ipsec-pass-thru** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **esp per-client-max** *number* **timeout** *time*：ESP トンネルを許可し、クライアントごとに許可される最大接続数およびアイドル タイムアウト（hh:mm:ss の形式）を設定します。接続の数を無制限に設定するには、値を 0 に指定します。
- **ah per-client-max** *number* **timeout** *time*：AH トンネルを許可します。パラメータの意味は esp コマンドと同じです。

例

次に、ACL を使用して IKE トラフィックを識別し、IPsec Pass Thru パラメータ マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
```

```
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

IPv6 インスペクション

IPv6 インスペクションを使用すると、拡張ヘッダーに基づいて IPv6 トラフィックを選択的にログに記録したりドロップしたりできます。さらに、IPv6インスペクションでは、IPv6パケット内の拡張ヘッダーのタイプと順序が RFC 2460 に準拠しているかどうかも確認できます。

IPv6 インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。デフォルトのグローバル インスペクション ポリシーを編集して IPv6 インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

IPv6 インスペクションのデフォルト

IPv6インスペクションをイネーブルにし、インスペクションポリシーマップを指定しないと、デフォルトの IPv6 インスペクション ポリシー マップが使用され、次のアクションが実行されます。

- 既知の IPv6 拡張ヘッダーのみを許可します。準拠しないパケットはドロップされ、ログに記録されます。
- RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。準拠しないパケットはドロップされ、ログに記録されます。
- ルーティング タイプ ヘッダーを含むパケットをドロップします。

ポリシー マップのコンフィギュレーションは次のとおりです。

```
policy-map type inspect ipv6 _default_ipv6_map
 description Default IPV6 policy-map
 parameters
  verify-header type
  verify-header order
 match header routing-type range 0 255
  drop log
```

IPv6 インスペクション ポリシー マップの設定

ドロップまたはロギングする拡張ヘッダーを指定するには、またはパケットの検証をディセーブルにするには、サービス ポリシーで使用される IPv6 インスペクション ポリシー マップを作成します。

手順

ステップ 1 IPv6 インスペクション ポリシー マップを作成します。**policy-map type inspect ipv6** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 （任意）IPv6 メッセージのヘッダーに基づいてトラフィックをドロップまたはロギングします。

a) IPv6 ヘッダーに基づいてトラフィックを識別します。**match header** *type*

type は次のいずれかです。

- **ah**：IPv6 認証拡張ヘッダーと一致します。
- **count gt** *number*：IPv6 拡張ヘッダーの最大数を指定します（0 ～ 255）。
- **destination-option**：IPv6 の宛先オプション拡張ヘッダーと一致します。
- **esp**： IPv6 のカプセル化セキュリティ ペイロード（ESP）拡張ヘッダーと一致します。
- **fragment**：IPv6 のフラグメント拡張ヘッダーと一致します。
- **hop-by-hop**：IPv6 のホップバイホップ拡張ヘッダーと一致します。
- **routing-address count gt** *number*：IPv6 ルーティング ヘッダー タイプ 0 アドレスの最大数を設定します（0 ～ 255）。
- **routing-type** {**eq** | **range**} *number*：IPv6 ルーティング ヘッダー タイプと一致します（0 ～ 255）。範囲を指定するには、値をスペースで区切ります（例：**30 40**）

b) 一致したパケットに対して実行するアクションを指定します。パケットをドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。アクションを入力しない場合、パケットがログに記録されます。

- **drop** [**log**]：一致するすべてのパケットをドロップします。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。

c) ドロップまたはロギングするすべてのヘッダーを識別するまで、プロセスを繰り返します。

ステップ 4 インスペクション エンジンに影響するパラメータを設定します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **verify-header type**：既知の IPv6 拡張ヘッダーだけを許可します。
- **verify-header order**：RFC 2460 で定義されている IPv6 拡張ヘッダーの順序を適用します。

例

次の例では、ホップバイホップ、宛先オプション、ルーティング アドレス、およびルーティング タイプ 0 の各ヘッダーを含むすべての IPv6 パケットをドロップし、ログに記録するインスペクション ポリシーマップを作成します。また、ヘッダーの順序とタイプを適用します。

```
policy-map type inspect ipv6 ipv6-pm
 parameters
  verify-header type
  verify-header order
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
 match header routing-type eq 0
  drop log

policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

NetBIOS インスペクション

NetBIOS アプリケーション インスペクションでは、NetBIOS ネーム サービス（NBNS）パケットおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレスで NAT を実行します。また、プロトコル準拠チェックを行って、さまざまなフィールドの数や長さの整合性を確認します。

NETBIOSインスペクションはデフォルトでイネーブルになっています。必要に応じて、NetBIOS プロトコル違反をドロップまたはログに記録するポリシー マップを作成できます。次の手順で、NetBIOS インスペクション ポリシー マップを設定する方法について説明します。

手順

ステップ 1 NetBIOS インスペクション ポリシー マップを作成します。**policy-map type inspect netbios** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4 NetBIOS プロトコル違反に対して実行するアクションを指定します。**protocol-violation action** {**drop** [**log**] | **log**}

drop アクションはパケットをドロップします。**log** アクションを指定すると、ポリシー マップがトラフィックに一致したときにシステム ログ メッセージを送信します。

例

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop log

hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# no inspect netbios
hostname(config-pmap-c)# inspect netbios netbios_map
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

PPTP インスペクション

PPTP は、PPP トラフィックのトンネリングに使用されるプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。

具体的には、ASA は、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続および xlate は、以降のセカンダリ GRE データ トラフィックを許可するために、必要に応じて、ダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

PPTP インスペクションをイネーブルにする方法については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

RSH インスペクション

RSH インスペクションはデフォルトでイネーブルになっています。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバーへの TCP 接続を使用します。クライアントとサーバーは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

RSH インスペクションのイネーブル化の詳細については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

SMTP および拡張 SMTP インスペクション

ESMTP インスペクションでは、スパム、フィッシング、不正形式メッセージ攻撃、バッファオーバーフロー/アンダーフロー攻撃などの攻撃を検出します。また、アプリケーションセキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、送受信者およびメール中継のブロックも行います。

ESMTP インスペクションはデフォルトでイネーブルになっています。デフォルト インスペクション マップとは異なる処理が必要な場合にのみ、設定する必要があります。

ここでは、ESMTP インスペクション エンジンについて説明します。

SMTP および ESMTP インスペクションの概要

拡張 SMTP（ESMTP）アプリケーション インスペクションを使用すると、ASA を通過できる SMTP コマンドの種類を制限し、モニター機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。

ESMTP アプリケーション インスペクションは、ユーザーが使用できるコマンドとサーバーが返送するメッセージを制御し、その数を減らします。ESMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。サポートされるコマンドは次のとおりです。
  - 拡張 SMTP：AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY。
  - SMTP（RFC 821）：DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。
- SMTP コマンド応答シーケンスをモニターします。
- 監査証跡の生成：メールアドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

ESMTP インスペクションでは、次の異常なシグニチャがないかどうか、コマンドと応答のシーケンスをモニターします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メール アドレスがスキャンされます。縦棒（|）は削除され（ブランクに変更されます）、「<」および「>」はメール アドレスを定義する場合にのみ許可されます（「>」より前に「<」がある必要があります）。
- SMTP サーバーによる不意の移行

- 未知またはサポート対象外のコマンドに対し、インスペクションエンジンは、パケット内のすべての文字を X に変更し、それらは内部サーバーによって拒否されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、破棄されます。

  サポート対象外の ESMTP コマンドは ATRN、ONEX、VERB、CHUNKING で、プライベート拡張子です。

- TCP ストリーム編集
- コマンド パイプライン

（注） ESMTP インスペクションをイネーブルにする場合、次のルールに従わないと、対話型の SMTP に使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

ESMTP インスペクションのデフォルト

ESMTP インスペクションは、_default_esmtp_map インスペクション ポリシー マップを使用して、デフォルトで有効になります。

- サーバー バナーはマスクされます。ESMTP インスペクション エンジンは、文字「2」、「0」、「0」を除くサーバーの SMTP バナーの文字をアスタリスクに変更します。復帰（CR）、および改行（LF）は無視されます。
- 暗号化接続が可能ですが、検査されません。
- 送信側と受信側のアドレスの特殊文字は認識されず、アクションは実行されません。
- コマンド行の長さが 512 より大きい接続は、ドロップされてログに記録されます。
- 受信者が 100 より多い接続は、ドロップされてログに記録されます。
- 本文の長さが 998 バイトより大きいメッセージはログに記録されます。
- ヘッダー行の長さが 998 より大きい接続は、ドロップされてログに記録されます。
- MIME ファイル名が 255 文字より長いメッセージは、ドロップされてログに記録されます。
- 「others」に一致する EHLO 応答パラメータはマスクされます。

ポリシー マップのコンフィギュレーションは次のとおりです。

```
policy-map type inspect esmtp _default_esmtp_map
 description Default ESMTP policy-map
 parameters
  mask-banner
```

```
 no mail-relay
 no special-character
 allow-tls
match cmd line length gt 512
 drop-connection log
match cmd RCPT count gt 100
 drop-connection log
match body line length gt 998
 log
match header line length gt 998
 drop-connection log
match sender-address length gt 320
 drop-connection log
match MIME filename length gt 255
 drop-connection log
match ehlo-reply-parameter others
 mask
```

ESMTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、ESMTPインスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、ESMTP インスペクションをイネーブルにすると適用できます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 ESMTP インスペクション ポリシー マップを作成します。**policy-map type inspect esmtp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **body** {**length** | **line length**} **gt** *bytes*：ESMTP 本文メッセージの長さまたは行の長さが指定したバイト数より大きいメッセージと一致します。
- **match** [**not**] **cmd verb** *verb1* [*verb2...*]：メッセージ内のコマンド動詞を照合します。次のコマンドの 1 つまたは複数を指定できます。auth、data、ehlo、etrn、helo、help、mail、noop、quit、rcpt、rset、saml、soml、vrfy。

- **match** [**not**] **cmd line length gt** *bytes*：コマンド動詞の行の長さが指定したバイト数より大きいメッセージを照合します。
- **match** [**not**] **cmd rcpt count gt** *count*：受信者の数が指定した値より大きいメッセージと一致します。
- **match** [**not**] **ehlo-reply-parameter** *parameter* [*parameter2...*]：ESMTP EHLO 応答パラメータと一致します。次のパラメータの 1 つまたは複数を指定できます。8bitmime、auth、binaryname、checkpoint、dsn、etrn、others、pipelining、size、vrfy。
- **match** [**not**] **header** {**length** | **line length**} **gt** *bytes*：ESMTP ヘッダーの長さまたは行の長さが指定したバイト数より大きいメッセージと一致します。
- **match** [**not**] **header to-fields count gt** *count*：ヘッダーの To フィールドの数が指定した値より大きいメッセージと一致します。
- **match** [**not**] **invalid-recipients count gt** *number*：無効な受信者の数が指定した値より大きいメッセージと一致します。
- **match** [**not**] **mime filetype regex** {*regex_name* | **class** *class_name*}：MIME またはメディア ファイル タイプを、指定した正規表現または正規表現クラスと照合します。
- **match** [**not**] **mime filename length gt** *bytes*：ファイル名が指定したバイト数より大きいメッセージと一致します。
- **match** [**not**] **mime encoding** *type* [*type2...*]：MIME エンコーディング タイプと一致します。次のタイプの 1 つまたは複数を指定できます。7bit、8bit、base64、binary、others、quoted-printable。
- **match** [**not**] **sender-address regex** {*regex_name* | **class** *class_name*}：送信者の電子メール アドレスを、指定した正規表現または正規表現クラスと照合します。
- **match** [**not**] **sender-address length gt** *bytes*：送信者のアドレスが指定したバイト数より大きいメッセージと一致します。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop-connection** [**log**]：パケットをドロップし、接続を閉じます。
- **mask** [**log**]：パケットの一致する部分をマスクします。このアクションは、**ehlo-reply-parameter** および **cmd verb** に対してのみ使用できます。
- **reset** [**log**]：パケットをドロップし、接続を閉じてサーバーまたはクライアントに TCP リセットを送信します。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。
- **rate-limit** *message_rate*：1 秒あたりのパケット内のメッセージのレートを制限します。このオプションは、**cmd verb** のみで使用できます。唯一のアクションとして使用することも、**mask** アクションと組み合わせて使用することもできます。

ポリシー マップでは、複数の **match** コマンドを指定できます。**match** コマンドの順序については、複数のトラフィック クラスの処理方法 （297 ページ）を参照してください。

ステップ 4 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **mail-relay** *domain-name* **action** {**drop-connection** [**log**] | **log**}：メール中継のドメイン名を指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。
- **mask-banner**：ESMTP サーバーからのバナーをマスクします。
- **special-character action** {**drop-connection** [**log**] | **log**}：電子メールの送信者または受信者アドレスに特殊文字パイプ（|）、バック クォート、NUL が含まれるメッセージに対して実行するアクションを指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。
- **allow-tls** [**action log**]：インスペクションなしで ESMTP over TLS（暗号化された接続）を許可するかどうか。必要に応じて、暗号化された接続をログに記録できます。デフォルトでは、インスペクションのない TLS セッションを許可します。**no allow-tls** を指定すると、システムはセッション接続から STARTTLS インジケータを削除し、強制的にプレーンテキスト接続を行います。

例

次の例は、ESMTP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex user1 “user1@cisco.com”
hostname(config)# regex user2 “user2@cisco.com”
hostname(config)# regex user3 “user3@cisco.com”
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description “Regular expressions to filter out undesired senders”
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map
```

```
hostname(config)# service-policy outside_policy interface outside
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

SNMP インスペクション

SNMP アプリケーション インスペクションは、デバイスへのトラフィックとデバイス経由のトラフィックの両方に適用されます。このインスペクションは、ユーザーが特定の SNMP ホストに制限される SNMP v3 を設定する場合に必要です。インスペクションなしの場合、定義された v3 ユーザーは任意の許可されたホストからデバイスをポーリングできます。SNMP インスペクションはデフォルトポートではデフォルトで有効になっているため、デフォルト以外のポートを使用する場合にのみ設定する必要があります。デフォルトポートは UDP/161、162 であり（すべてのデバイスタイプ）、FXOS は UDP/161 でリッスンするため、FXOS も実行するデバイスでは UDP/4161 です。

デフォルトでは、SNMP インスペクションはポーリングを構成されたバージョンに制限します。

（注） FXOS も実行しているデバイスで SNMP を設定する場合、SNMP インスペクションは必須であり、無効にすると再度有効になります。SNMP インスペクションは、ポート UDP/4161 を含むトラフィック クラスマップで有効になります。

必要に応じて、SNMP トラフィックを特定のバージョンの SNMP に制限することもできます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。システムは、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、以下に説明するように、SNMP マップを作成して制御します。バージョンを制御する必要がない場合は、マップなしで SNMP インスペクションを有効にします。

手順

SNMP マップを作成します。

snmp-map *map_name* コマンドを使ってマップを作成して SNMP マップ 設定モードに入り、次に **deny version** *version* コマンドで拒否するバージョンを識別します。バージョンは 1、 2、 2c、 3 があります。

例：

次の例では、SNMP バージョン 1 および 2 を拒否しています。

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

SQL*Net インスペクション

SQL*Net インスペクションはデフォルトでイネーブルになっています。インスペクション エンジンは、SQL*Net バージョン 1 および 2 をサポートしていますが、形式は Transparent Network Substrate（TNS）のみです。インスペクションでは、表形式データ ストリーム（TDS）形式をサポートしていません。SQL*Net メッセージは、埋め込まれたアドレスとポートについてスキャンされ、必要に応じて NAT の書き換えが適用されます。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、構造化照会言語（SQL）の IANA ポート割り当てとは一致しません。アプリケーションが別のポートを使用する場合は、そのポートを含むトラフィック クラスに SQL*Net インスペクションを適用します。

次の場合は、SQL*Net インスペクションを無効にします。

- SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われます。SQL*Net インスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。
- 高レートの SQL 通信のインスペクションにより、CPU 使用率の許容できないスパイクが発生します。

SQL*Net インスペクションを無効にした後、 **clear conn port 1521** コマンドを使用して、インスペクションなしで接続を再構築できるようにします。

SQL*Net インスペクションをイネーブルにする方法については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

Sun RPC インスペクション

この項では、Sun RPC アプリケーション インスペクションについて説明します。

Sun RPC インスペクションの概要

Sun RPC プロトコル インスペクションはデフォルトではイネーブルです。Sun RPC サーバー テーブルを管理するだけで、ファイアウォールの通過を許可されているサービスを識別できます。ただし、NFS のピンホール化は、サーバー テーブルの設定がなくても各サーバーで実行されます。

Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバー上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス（通常は rpcbind）に照会します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバーに送信します。サーバーが応答すると、ASA はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

Sun RPC サービスの管理

Sun RPC サービス テーブルを使用して、確立された Sun RPC セッションに基づいて Sun RPC トラフィックを制御します。

手順

ステップ 1 Sun RPC サービス プロパティを設定します。

sunrpc-server *interface_name ip_address mask* **service** *service_type* **protocol** {**tcp** | **udp**} *port*[*-port*] **timeout** *hh:mm:ss*

それぞれの説明は次のとおりです。

- *interface_name*：サーバーへのトラフィックが伝送されるインターフェイス。
- *ip_address mask*：Sun RPC サーバーのアドレス。
- **service** *service_type*：特定のサービス タイプとそのサービスに使用するポート番号の間のマッピングである、サーバー上のサービス タイプ。サービス タイプ（100003 など）を判定するには、Sun RPC サーバー マシンの UNIX または Linux コマンドラインで、sunrpcinfo コマンドを使用します。
- **protocol** {**tcp** | **udp**}：サービスが TCP と UDP のどちらを使用するかを示します。
- *port*[*-port*]：サービスによって使用されるポートまたはポートの範囲。ポート範囲を指定するには、範囲の開始ポート番号と終了ポート番号をハイフンで区切ります（111-113 など）。

- **timeout** *hh:mm:ss*：Sun RPC インスペクションによって接続のために開かれたピンホールのアイドル タイムアウト。

例：

たとえば、IP アドレスが 192.168.100.2 の Sun RPC サーバーに対して 30 分のタイムアウトを作成するには、次のコマンドを入力します。この例では、Sun RPC サーバーは TCP ポート 111 を使用する内部インターフェイスにあります。

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255
service 100003 protocol tcp 111 timeout 00:30:00
```

ステップ 2 （オプション）これらのサービス用に作成されたピンホールをモニターします。

Sun RPC サービスで開かれているピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に例を示します。

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL カラムのエントリは、内部インターフェイスのクライアントまたはサーバーの IP アドレスを示します。FOREIGN カラムの値は、外部インターフェイスのクライアントまたはサーバーの IP アドレスを示します。

必要に応じ、次のコマンドを使用してこれらのサービスをクリアすることができます。 **clear sunrpc-server active**

TFTP インスペクション

TFTP インスペクションはデフォルトでイネーブルになっています。

TFTP は、RFC 1350 に記述されているように、TFTP サーバーとクライアントの間のファイルの読み書きを行うための簡易プロトコルです。

インスペクション エンジンは、TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバーの間のファイル転送を許可します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバーだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバーの間に存在できる不完全なセカンダリ チャネルは1つまでです。サーバーからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

TFTPインスペクションをイネーブルにする方法については、アプリケーション レイヤプロトコル インスペクションの設定 （305 ページ）を参照してください。

XDMCP インスペクション

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、ASA は、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、TCP ポートを許可するアクセス ルールを使用できます。または、ASA で **established** コマンドを使用できます。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、ASA が必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

XDMCP インスペクションのイネーブル化の詳細については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

VXLAN インスペクション

Virtual Extensible Local Area Network （VXLAN）インスペクションは、ASA を通過する VXLAN のカプセル化されたトラフィックで機能します。VXLAN ヘッダーフォーマットが標準に準拠し、不正な形式のパケットをドロップすることを確認します。VXLAN インスペクションは、ASA が VXLAN トンネル エンドポイント（VTEP）または VXLAN ゲートウェイとして機能するトラフィックでは行われません。これは、それらのチェックが VXLAN パケットの通常の非カプセル化の一部として行われるためです。

VXLAN パケットは通常、ポート 4789 の UDP です。このポートは、default-inspection-traffic クラスの一部であるため、inspection_default サービス ポリシー ルールに VXLAN インスペクショ

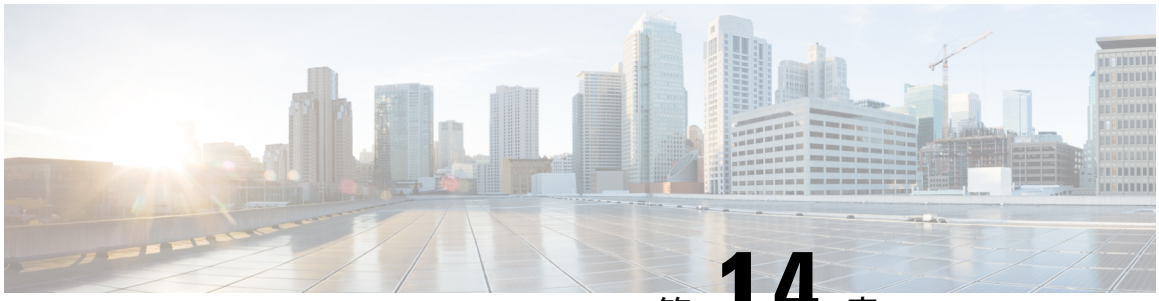
ンを追加するだけです。または、それに対してポートまたは ACL マッチングを使用してクラスを作成することもできます。

基本的なインターネットプロトコルインスペクションの履歴

機能名	リリース	機能情報
DCERPC インスペクションで ISystemMapper UUID メッセージ RemoteGetClassObject opnum3 をサポート。	9.4(1)	ASA は、リリース 8.3 で EPM 以外の DCERPC メッセージのサポートを開始し、ISystemMapper UUID メッセージ RemoteCreateInstance opnum4 をサポートしています。この変更により、RemoteGetClassObject opnum3 メッセージまでサポートが拡張されます。 変更されたコマンドはありません。
VXLAN パケット インスペクション	9.4(1)	ASA は、標準形式に準拠するために VXLAN ヘッダーを検査できます。 **inspect vxlan** コマンドが導入されました。
ESMTP インスペクションの TLS セッションでのデフォルトの動作の変更。	9.4(1)	ESMTP インスペクションのデフォルトが、検査されない、TLS セッションを許可するように変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。**no allow-tls** を含むシステムをアップグレードする場合、このコマンドは変更されません。 デフォルトの動作の変更は、古いバージョンでも行われました：8.4（7.25）、8.5（1.23）、8.6（1.16）、8.7（1.15）、9.0（4.28）、9.1（6.1）、9.2（3.2）、9.3（1.2）、9.3（2.2）。
IP オプション インスペクションの改善	9.5(1)	IP オプション インスペクションは、すべての有効な IP オプションをサポートするようになりました。まだ定義されていないオプションを含む、標準または試行的なオプションを許可、クリア、またはドロップするようにインスペクションを調整できます。また、IP オプション インスペクション マップで明示的に定義されていないオプションのデフォルトの動作を設定できます。 **basic-security**、**commercial-security**、**default**、**exp-flow-control**、**exp-measure**、**extended-security**、**imi-traffic-description**、**quick-start**、**record-route**、**timestamp**、および {**0-255**}（IP オプション タイプ番号を示します）の各コマンドが追加されました。

機能名	リリース	機能情報
DCERPC インスペクションの改善および UUID フィルタリング	9.5(2)	DCERPC インスペクションは、OxidResolver ServerAlive2 opnum5 メッセージに対して NAT をサポートするようになりました。また、DCERPC メッセージの汎用一意識別子（UUID）でフィルタリングし、特定のメッセージ タイプをリセットするかログに記録できるようになりました。UUID フィルタリング用の新しい DCERPC インスペクション クラス マップがあります。 次のコマンドが導入されました。**match** [**not**] **uuid**。次のコマンドが変更されました。**class-map type inspect**。
DNS over TCP インスペクション。	9.6(2)	DNS over TCP トラフィック（TCP/53）を検査できるようになりました。 **tcp-inspection** コマンドが追加されました。
Cisco Umbrella サポート。	9.10(1)	Cisco Umbrella で定義されている エンタープライズ セキュリティ ポリシーをユーザー接続に適用できるように DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。FQDN に基づいて接続を許可またはブロックできます。または、疑わしい FQDN の場合は Cisco Umbrella インテリジェント プロキシにユーザーをリダイレクトして URL フィルタリングを実行できます。Umbrella の設定は、DNS インスペクション ポリシーに含まれています。 **umbrella**（グローバルおよびポリシー マップ パラメータのコンフィギュレーション モード）、**token**、**public-key**、**timeout edns**、**dnscrypt**、**show service-policy inspect dns detail** の各コマンドが追加または変更されました。
Cisco Umbrella の強化	9.12(1)	Cisco Umbrella をバイパスする必要があるローカル ドメイン名を特定できるようになりました。これらのドメインの DNS 要求は、Umbrella を処理せず DNS サーバーに直接送信されます。また、DNS 要求の解決に使用する Umbrella サーバーも特定できるようになりました。さらに、Umbrella サーバーを使用できない場合は、DNS 要求がブロックされないように、Umbrella インスペクション ポリシーをフェール オープンに定義することができます。 **local-domain-bypass**、**resolver**、**umbrella fail-open** の各コマンドが追加または変更されました。

機能名	リリース	機能情報
新規インストールでは、デフォルトでXDMCPインスペクションが無効になっています。	9.15(1)	以前は、すべてのトラフィックに対してXDMCPインスペクションがデフォルトで有効になっていました。新しいシステムと再イメージ化されたシステムを含む新規インストールでは、XDMCPはデフォルトで無効になっています。このインスペクションが必要な場合は、有効にしてください。アップグレードでは、デフォルトのインスペクション設定を使用してXDMCPインスペクションを有効にしただけでも、XDMCPインスペクションの現在の設定は保持されます。



第 14 章

音声とビデオのプロトコルのインスペクション

ここでは、音声とビデオのプロトコルのアプリケーションインスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、アプリケーション レイヤ プロトコル インスペクションの準備 （295 ページ）を参照してください。

- CTIQBE インスペクション （371 ページ）
- H.323 インスペクション （372 ページ）
- MGCP インスペクション （378 ページ）
- RTSP インスペクション （382 ページ）
- SIP インスペクション （386 ページ）
- Skinny（SCCP）インスペクション （393 ページ）
- STUN インスペクション （397 ページ）
- 音声とビデオのプロトコル インスペクションの履歴 （398 ページ）

CTIQBE インスペクション

CTIQBE プロトコル インスペクションは、NAT、PAT、および双方向 NAT をサポートします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、ASA を経由してコール セットアップを行えるようになります。

TAPI と JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TSP が Cisco CallManager と通信するために使用されます。

CTIQBE インスペクションをイネーブルにする方法については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ）を参照してください。

CTIQBE インスペクションの制限事項

CTIQBE コールのステートフル フェールオーバーはサポートされていません。

次に、CTIQBEアプリケーションインスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が ASA の異なるインターフェイスに接続されている場合、これら 2 つの電話間のコールは失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT を使用しているときに Cisco CallManager の IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録するためには、TCP ポート 2748 を PAT（インターフェイス）アドレスの同一ポートに対してスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザーによる設定はできません。

H.323 インスペクション

H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、インスペクション機能のアクティベーションをカスケードできます。H.323 インスペクションは、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、HSI グループ、プロトコルのステートトラッキング、H.323 通話時間制限の適用、T.38 Fax、音声/ビデオ制御をサポートします。

H.323 検査はデフォルトではイネーブルです。デフォルト以外の処理が必要な場合にのみ設定する必要があります。

ここでは、H.323 アプリケーション インスペクションについて説明します。

H.323 インスペクションの概要

H.323 インスペクションは、Cisco CallManager などの H.323 準拠のアプリケーションをサポートします。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。ASA は、H.323 v3 機能の同一コール シグナリング チャネルでの複数コールを含めて、H.323 を Version 6 までサポートします。

H.323 インスペクションをイネーブルにした場合、ASA は、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、ASA でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

H.323 の動作

H.323 のプロトコルのコレクションは、合計で最大 2 つの TCP 接続と 4 ～ 8 つの UDP 接続を使用できます。FastConnect は 1 つの TCP 接続だけを使用し、RAS は登録、アドミッション、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントは、最初に TCP ポート 1720 を使用して、H.323 サーバーへの TCP 接続を確立し、Q.931 コール セットアップを要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニターして、H.245 ポート番号を決定します。H.323 端末が、FastConnect を使用していない場合は、ASA が H.225 メッセージのインスペクションに基づいて、H.245 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高いポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出 UDP ポート
- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

RAS シグナリング用に予約済み H.323 ポート 1719 のトラフィックを許可する必要があります。さらに、H.225 コール シグナリング用に、予約済み H.323 ポート 1720 のトラフィックを許可する必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーの使用時、ASA は、ACF メッセージと RCF メッセージのインスペクションに基づいて H.225 接続を開きます。

H.225 メッセージを検査した後、ASA は H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックも検査します。ASA を通過するすべての H.245 メッセージは、H.245 アプリケーション インスペクションを受けます。このインスペクションでは、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 インスペクションを通過するパケットが通る各 UDP 接続は H.323 接続としてマークされ、**timeout** コマンドで設定された H.323 タイムアウト値でタイムアウトします。

（注） Gatekeeper がネットワーク内にある場合は、H.323 エンドポイント間のコール セットアップをイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージはゲートキーパーとの間で送信されるため、コール側エンドポイントの IP アドレスは不明であり、ASA は送信元 IP アドレス/ポート 0/0 を通じてピンホールを開けます。デフォルトでは、このオプションは無効になっています。H.323 エンドポイント間のコール セットアップをイネーブルにするには、H.323 インスペクション ポリシー マップの作成時に、パラメータ コンフィギュレーション モードで **ras-rcf-pinholes enable** コマンドを入力します。

H.245 メッセージでの H.239 サポート

ASA は、2 つの H.323 エンドポイントの間に存在します。2 つの H.323 エンドポイントが、スプレッドシート データなどのデータ プレゼンテーションを送受信できるようにテレプレゼンテーションセッションをセットアップするとき、ASA はエンドポイント間で H.239 ネゴシエーションが成功することを保証します。

H.239 は、H.300 シリーズ エンドポイントが 1 回のコールで追加ビデオ チャネルを開くことができる機能を提供する規格です。コールで、エンドポイント（ビデオ電話など）はビデオ用チャネルとデータ プレゼンテーション用チャネルを送信します。H.239 ネゴシエーションは H.245 チャネルで発生します。

ASA が追加メディア チャネル用とメディア制御チャネル用のピンホールを開きます。エンドポイントは、オープン論理チャネル メッセージ（OLC）を使用して新しいチャネルの作成を通知します。メッセージ拡張は H.245 バージョン 13 の一部です。

テレプレゼンテーションセッションの復号化と符号化は、デフォルトでイネーブルにされています。H.239 の符号化と復号化は ASN.1 コーダによって実行されます。

H.323 インスペクションの制限事項

H.323 インスペクションは、Cisco Unified Communications Manager（CUCM）7.0 でテストおよびサポートされています。CUCM 8.0 以降ではサポートされません。H.323 インスペクションは、他のリリースや製品で機能する場合があります。

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- PAT は拡張 PAT または per-session PAT を除きサポートされます。
- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。

- 同じセキュリティ レベルのインターフェイス間の NAT ではサポートされません。
- NAT64 ではサポートされません。
- H.323 インスペクションを使用する NAT は、エンドポイントで直接実行される場合には、NAT と互換性がありません。エンドポイントで NAT を実行する場合、H.323 インスペクションは無効にしてください。

H.323 インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、H.323 インスペクション ポリシー マップを作成して H.323 インスペクションのアクションをカスタマイズできます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、H.323 インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect h323** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。**match-any** キーワードは、トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して着信側を照合します。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して発信側を照合します。
- **match** [**not**] **media-type** {**audio** | **data** | **video**}：メディア タイプを照合します。

ステップ 2 H.323 インスペクション ポリシー マップを作成します。**policy-map type inspect h323** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法 （297 ページ）を参照してください。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- H.323 クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- H.323 クラス マップで記述された **match** コマンドの 1 つを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop** [**log**]：パケットをドロップします。メディア タイプの照合の場合、**log** キーワードを含めてシステム ログ メッセージを送信できます。
- **drop-connection**：パケットをドロップし、接続を閉じます。このオプションは、着信側または発信側の照合に使用できます。
- **reset**：パケットをドロップし、接続を閉じ、サーバーとクライアントの両方またはいずれかに TCP リセットを送信します。このオプションは、着信側または発信側の照合に使用できます。

ステップ 5 インスペクションエンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **ras-rcf-pinholes enable**：H.323 エンドポイント間のコール セットアップをイネーブルにします。Gatekeeperがネットワーク内にある場合は、H.323エンドポイント間のコール セットアップをイネーブルにできます。RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くには、このオプションを使用します。これらの RRQ/RCF メッセージはゲートキーパーとの間で送信されるため、コール側エンドポイントの IP アドレスは不明であり、ASA は送信元 IP アドレス/ポート 0/0 を通じてピンホールを開けます。デフォルトでは、このオプションは無効になっています。
- **timeout users** *time*：H.323 コールの制限時間（hh: mm: ss 形式）を設定します。タイムアウトを付けない場合は、00:00:00 を指定してください。範囲は、0:0:0 ～ 1193:0:0 です。
- **call-party-number**：コール設定時に発信側の番号を強制的に送信します。
- **h245-tunnel-block action** {**drop-connection** | **log**}：H.245 トンネル ブロッキングを適用します。接続をドロップするか、単にログに記録するだけかを選択します。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの enforce-payloadtype キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **state-checking** {**h225** | **ras**}：ステート チェック検証をイネーブルにします。個別にコマンドを入力して、H.225およびRASのステート チェックをイネーブルにすることができます。
- **early-message** *message_type*：H.225 SETUP メッセージの前に指定したタイプの H.225 メッセージを許可するかどうか。H.460.18 に従って、**facility** メッセージが早く到着するように許可できます。

  H.323/H.225 を使用するときに、接続が完了前に終了するコール セットアップの問題が発生した場合、このコマンドを使用して早期メッセージを許可します。また、必ず H.323 RAS と H.225 の両方にインスペクションをイネーブルにしてください（デフォルトではどちらもイネーブルになっています）。

ステップ 6 パラメータ コンフィギュレーション モードのままで、HSI グループを設定できます。

a) HSI グループを定義し、HSI グループ コンフィギュレーション モードを開始します。
hsi-group *id*

id には、HSI グループ ID を指定します。範囲は 0 ～ 2147483647 です。

b) IP アドレスを使用して HSI を HSI グループに追加します。**hsi** *ip_address*

HSI グループあたり最大 5 つのホストを追加できます。

c) HSI グループにエンドポイントを追加します。**endpoint** *ip_address if_name*

ip_address には追加するエンドポイント、*if_name* にはエンドポイントを ASA に接続するときに使用するインターフェイスを指定します。HSI グループあたり最大 10 個のエンドポイントを追加できます。

例

次の例は、電話番号のフィルタリングを設定する方法を示しています。

```
hostname(config)# regex caller 1 “5551234567”
hostname(config)# regex caller 2 “5552345678”
hostname(config)# regex caller 3 “5553456789”

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

MGCP インスペクション

MGCP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの MGCP ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで MGCP インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

ここでは、MGCP アプリケーション インスペクションについて説明します。

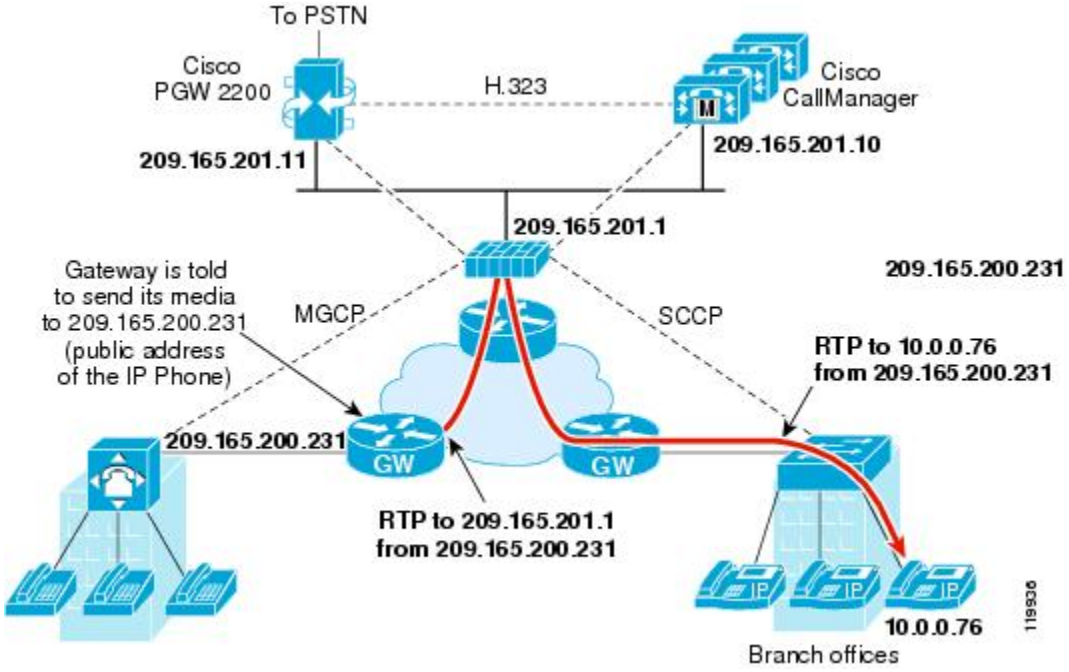
MGCP インスペクションの概要

MGCP は、メディア ゲートウェイ コントローラまたはコールエージェントと呼ばれる外部コール制御要素からメディアゲートウェイを制御するために使用されます。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブルモデムやケーブルセットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。次の図は、NAT と MGCP を使用する方法を示しています。

図 *41 : NAT* と *MGCP* の使用



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、他のマルチメディア エンドポイントとのメディア セッションを確立して制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

- 通常、ゲートウェイは UDP ポート 2427 をリッスンしてコール エージェントからのコマンドを受信します。
- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コール エージェントは UDP ポート 2727 をリッスンしてゲートウェイからコマンドを受信します。

（注） MGCP インスペクションでは、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの復元力のある IP アドレスから RTP データを送信することです。ただし、ASA は、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

MGCP インスペクション ポリシー マップの設定

ASA がピンホールを開く必要のあるコール エージェントとゲートウェイがネットワークに複数ある場合は、MGCP マップを作成します。作成した MGCP マップは、MGCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1 MGCP インスペクション ポリシー マップを作成します。**policy-map type inspect mgcp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **call-agent** *ip_address group_id*：1 つ以上のゲートウェイを管理できるコール エージェント グループを設定します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。同じ group_id を持つコール エージェントは、同じグループに属します。1 つのコール エージェントは複数のグループに所属できます。group_id オプションには、0 ～ 4294967295 の数字を指定します。ip_address オプションには、コール エージェントの IP アドレスを指定します。

（注） MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判定します。これによって、ASA を通過するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

- **gateway** *ip_address group_id*：特定のゲートウェイを管理しているコール エージェントのグループを指定します。ip_address オプションを使用して、ゲートウェイの IP アドレスを指定します。group_id オプションには 0 ～ 4294967295 の数字を指定します。この数字は、ゲートウェイを管理しているコール エージェントの group_id に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

- **command-queue** *command_limit*：MGCP コマンド キューで許容されるコマンドの最大数（1 ～ 2147483647）を設定します。デフォルトは 200 です。

例

次の例は、MGCP マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

RTSP インスペクション

RTSP インスペクションはデフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。ここでは、RTSP アプリケーション インスペクションについて説明します。

RTSP インスペクションの概要

RTSP インスペクション エンジンを使用することにより、ASA は RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV の各接続で使用されます。

（注） Cisco IP/TV では、RTSP TCP ポート 554 および 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。ASA は、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上で設定されているトランスポート モードに応じて、音声/ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

ASA は、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合、サーバーは ASA との相対位置関係で外部に存在することになるため、サーバーから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージがアウトバウンド方向である場合、ASA は、ダイナミック チャネルを開く必要はありません。

RTSP インスペクションは、PAT またはデュアル NAT をサポートしていません。また、ASA は、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

RealPlayer 設定要件

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。ASA では、サーバーからクライアントに、またはその逆に access-list コマンドを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。ASA で、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェックボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、ASA で、inspect rtsp コマンドを追加します。

RSTP インスペクションの制限事項

RSTP インスペクションには次の制限が適用されます。

- ASA は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- ASA には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- Cisco IP/TV では、メッセージの SDP 部分に対して ASA が実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバーが内部ネットワークにあるときにだけ NAT を使用できます。

RTSP インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、RTSP インスペクション ポリシー マップを作成して RTSP インスペクションのアクションをカスタマイズできます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、RTSP インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect rtsp** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。**match-any** キーワードは、トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **request-method** *method*：RTSP 要求方式を照合します。要求方式は、announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameter、teardown です。
- **match** [**not**] **url-filter regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して URL を照合します。

ステップ 2 RTSP インスペクション ポリシー マップを作成します。**policy-map type inspect rtsp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- RTSP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- RTSP クラス マップで記述された **match** コマンドの 1 つかを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop-connection** [**log**]：パケットをドロップし、接続を閉じ、任意でシステム ログ メッセージを送信します。このオプションは、URL のマッチングに使用できます。
- **log**：システム ログ メッセージを送信します。
- **rate-limit** *message_rate*：1 秒あたりのメッセージのレートを制限します。このオプションは、要求方式の照合に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法（297 ページ）を参照してください。

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **reserve-port-protect**：メディア ネゴシエーション中の予約ポートの使用を制限します。

- **url-length-limit** *bytes*：メッセージで使用できる URL の長さを 0 ～ 6000 バイトで設定します。

例

次の例は、RTSP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

SIP インスペクション

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP インスペクションはデフォルトでイネーブルになっています。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにする

ためにTLSプロキシを設定する場合にのみ設定する必要があります。ここでは、SIPインスペクションについてより詳細に説明します。

SIP インスペクションの概要

IETF で定義されている SIP により、特に 2 者間の音声会議などのコール処理セッションまたは「コール」が使用可能になります。SIP はSDP と連携して通話処理を行います。SDP は、メディア ストリーム用のポートを指定します。SIP を使用することにより、ASA はSIP VoIP ゲートウェイおよび VoIP プロキシ サーバーをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 3261
- SDP：Session Description Protocol、RFC 2327

ASA経由のSIPコールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザーデータ部分に IP アドレスを埋め込みます。ASA がサポートする SIP 要求 URI の最大長は 255 であることに注意してください。

インスタントメッセージング（IM）アプリケーションでは、SIP拡張機能（RFC 3428で定義されている）およびSIP固有のイベント通知（RFC 3265 で定義されている）も使用します。ユーザーがチャット セッション（登録/サブスクリプション）を開始した後、ユーザーが互いにチャットするときに、IM アプリケーションでは、MESSAGE/INFO 方式 202 Accept 応答を使用します。たとえば、2 人のユーザーはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定されているSIP タイムアウト値に従ってタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注） SIP インスペクションは、チャット機能のみをサポートします。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

SIP インスペクションの制限事項

SIP インスペクションは、Cisco Unified Communications Manager（CUCM）7.0、8.0、8.6、および10.5 でテストされ、サポートされています。CUCM 8.5 または 9.x. ではサポートされません。SIP インスペクションは、他のリリースや製品で機能する場合があります。

SIP 電話機が Call Manager に接続していないことを確認したら、次の CLI コマンドを使用して未処理の TCP セグメントの最大数を増やすことができます。**sysopt connection tcp-max-unprocessed-seg** *6-24*。デフォルトは 6 であるため、より大きな数値を試してください。

SIP インスペクションは、T.38 MIME インターネット ファクシミリ プロトコル （IFP） をサポートしていません。SIP インスペクションは、T.38 MIME オーディオ サブタイプを使用する SIP 招待をドロップします。このタイプを許可する必要がある場合は、SIP インスペクションを無効にして、RTP ストリームを許可するアクセス コントロール ルールを作成します。

SIP インスペクションの NAT 制限事項

- SIP インスペクションは、埋め込まれた IP アドレスに NAT を適用します。ただし、送信元と宛先両方のアドレスを変換するように NAT を設定している場合、外部アドレス（「trying」応答メッセージの SIP ヘッダー内の「from」）は書き換えられません。そのため、宛先アドレスの変換を回避するように SIP トラフィックを使用している場合は、オブジェクト NAT を使用する必要があります。
- セキュリティ レベルが同じインターフェイス、または低セキュリティ レベル（送信元）から高セキュリティ レベル（宛先）に至るインターフェイスに対しては NAT または PAT を設定しないでください。この設定はサポートされません。
- 対象となるトラフィック クラス （つまり、inspection_default 以外のトラフィック クラス）に SIP インスペクションを設定する場合は、双方向 ACL を使用し、5060 宛先ポートのみを指定するようにしてください。そうしないと、IP パケットが正しく変換されても、SIP ヘッダーの IP アドレスが変換されない NAT の問題が発生する可能性があります。
- SIP 招待の VIA ヘッダーにマッピングアドレスをハードコーディングする場合は、SIP インスペクションを有効にしないでください。静的 NAT を使用して送信元クライアントアドレスを変換し、デフォルトルートのインターフェイスがクライアントの使用する接続ルートのインターフェイスと異なる場合、問題が発生する可能性があります。

SIP インスペクションの PAT 制限事項

PAT を SIP で使用する場合、次の制限事項が適用されます。

- ASA で保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバーが外部ネットワークにある。
  - エンドポイントからプロキシ サーバーに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者/作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プ

ロトコルの制限によるものです。PAT では、変換するためにポートが必要なので、変換は失敗します。

- PAT を使用する場合は、ポートを持たない内部 IP アドレスを含む SIP ヘッダー フィールドは変換されない可能性があるため、内部 IP アドレスが外部に漏れます。この漏出を避けるには、PAT の代わりに NAT を設定します。

デフォルトの SIP インスペクション

SIP インスペクションはデフォルトでイネーブルになっており、次を含むデフォルトのインスペクション ポリシー マップを使用します。

- SIP インスタント メッセージ（IM）の拡張機能：イネーブル
- SIP トラフィック以外の SIP ポート使用：禁止。
- サーバーとエンドポイントの IP アドレスの非表示：ディセーブル
- ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
- 1 以上の宛先ホップ カウントを保証：イネーブル
- RTP 準拠：適用強制しない
- SIP 準拠：ステート チェックとヘッダー検証を実行しない

暗号化されたトラフィックのインスペクションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SIP インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、SIP インスペクション ポリシー マップを作成して SIP インスペクションのアクションをカスタマイズできます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順を実行して、SIP インスペクション クラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect sip** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-anyキーワードは、トラフィックが少なくとも1つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して、To ヘッダーで指定された着信側を照合します。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して、From ヘッダーで指定された発信側を照合します。
- **match** [**not**] **content length gt** *bytes*：SIP ヘッダーのコンテンツの長さが指定されたバイト数（0 ～ 65536）を超えているメッセージを照合します。
- **match** [**not**] **content type** {**sdp** | **regex** {*regex_name* | **class** *class_name*}：コンテンツ タイプを SDP として、または指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **im-subscriber regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して SIP IM サブスクライバを照合します。
- **match** [**not**] **message-path regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して SIP via ヘッダーを照合します。

- **match** [**not**] **request-method** *method*：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update の SIP 要求方式を照合します。
- **match** [**not**] **third-party-registration regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対してサードパーティ登録の要求者を照合します。
- **match** [**not**] **uri {sip | tel} length gt** *bytes*：指定された長さ（0 ～ 65536 バイト）を超えている、選択したタイプ（SIP または TEL）の SIP ヘッダーの URI を照合します。

d) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 SIP インスペクション ポリシー マップを作成します。**policy-map type inspect sip** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- SIP クラスマップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- SIP クラス マップで記述された **match** コマンドの 1 つを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop**：一致するすべてのパケットをドロップします。
- **drop-connection**：パケットをドロップし、接続を閉じます。
- **reset**：パケットをドロップし、接続を閉じ、サーバーとクライアントの両方またはいずれかに TCP リセットを送信します。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。
- **rate-limit** *message_rate*：メッセージのレートを制限します。レート制限は、「invite」および「register」に一致する要求方式の場合にのみ使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法（297 ページ）を参照してください。

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **im**：インスタント メッセージングをイネーブルにします。
- **ip-address-privacy**：IP アドレスのプライバシーをイネーブルにし、サーバーとエンドポイントの IP アドレスを非表示にします。
- **max-forwards-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：これにより、宛先に到達するまで 0 にすることができない Max-Forwards ヘッダーの値がチェックされます。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの enforce-payloadtype キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **software-version action** {**mask [log]** | **log**}：Server および User-Agent（エンドポイント）ヘッダー フィールドを使用するソフトウェア バージョンを識別します。SIP メッセージのソフトウェア バージョンをマスクしてオプションでロギングするか、単にロギングのみ実行することができます。
- **state-checking action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：状態遷移チェックをイネーブルにします。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **strict-header-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：RFC 3261 に従って SIP メッセージのヘッダー フィールドの厳密な検証をイネーブルにします。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **traffic-non-sip**：既知の SIP シグナリング ポートで SIP 以外のトラフィックを許可します。
- **trust-verification-server ip** *ip_address*：信頼検証サービス サーバーを指定します。信頼検証サービス サーバーは、HTTPS の確立時に Cisco Unified IP Phone がアプリケーション サーバーを認証できるようにします。最大 4 回コマンドを入力して 4 つのサーバーを指定できます。SIP インスペクションは登録された電話機ごとに各サーバーに対するピンホールを開き、電話機はどれを使用するかを決定します。CUCM サーバーで信頼検証サービス サーバーを設定します。

- **trust-verification-server port** *number*：信頼検証サービス ポートを指定します。デフォルト ポートは 2445 です。したがって、サーバーが異なるポートを使用する場合にのみ、このコマンドを使用します。使用できるポートの範囲は 1026 ～ 32768 です。
- **uri-non-sip action** {**mask [log]** | **log**}：Alert-Info および Call-Info ヘッダー フィールドにある SIP 以外の URI を識別します。SIP メッセージの情報をマスクしてオプションでロギングするか、単にロギングのみ実行することができます。

例

次の例は、SIP を使用したインスタント メッセージをディセーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

hostname(config)# service-policy global_policy global
```

次の例は、4 つの信頼検証サービス サーバーを識別する例を示します。

```
hostname(config)# policy-map type inspect sip sample_sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.1
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.2
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.3
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.4
hostname(config-pmap-p)# trust-verification-server port 2445
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

Skinny（SCCP）インスペクション

SCCP（Skinny）アプリケーション インスペクションでは、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

SCCP インスペクションはデフォルトではイネーブルです。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを設定する場合にのみ設定する必要があります。

ここでは、SCCP アプリケーション インスペクションについて説明します。

SCCP インスペクションの概要

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。

ASA は、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インスペクションは、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが ASA を通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。ASA は、TFTP サーバーの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

（注） ASA は、SCCP プロトコル バージョン 22 以前が稼働している Cisco IP Phone からのトラフィックのインスペクションをサポートします。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べて高セキュリティ インターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングはスタティックである必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリにより、セキュリティの高いインターフェイス上の Cisco CallManager は Cisco IP Phone からの登録を受け入れることができます。

Cisco IP Phone では、TFTP サーバーにアクセスして、Cisco CallManager サーバーに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバーと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、ACL を使用して UDP ポート 69 の保護された TFTP サーバーに接続する必要があります。TFTP サーバーに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバーおよび Cisco CallManager と比べてセキュリティの高いインターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするために、ACL やスタティック エントリは必要ありません。

SCCP インスペクションの制限事項

SCCP インスペクションは、Cisco Unified Communications Manager（CUCM）7.0、8.0、8.6、および 10.5 でテストされ、サポートされています。CUCM 8.5 または 9.x.ではサポートされません。SCCP インスペクションは、他のリリースや製品で機能する場合があります。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、ASA は TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。ASA は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、ASA は電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注） ASA は、コール セットアップ中のコールを除き、SCCP コールのステートフル フェールオーバーをサポートします。

デフォルトの SCCP インスペクション

SCCP インスペクションは、次のデフォルト値を使用してデフォルトでイネーブルになっています。

- 登録：適用強制しない
- メッセージの最大 ID：0x181
- プレフィックスの長さの最小値：4
- メディア タイムアウト：00:05:00
- シグナリング タイムアウト：01:00:00
- RTP 準拠：適用強制しない

Skinny（SCCP）インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、SCCP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、SCCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1 SCCP インスペクション ポリシー マップを作成します：**policy-map type inspect skinny** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 （任意）SCCP メッセージのステーション メッセージ ID フィールドに基づいてトラフィックをドロップします。

a) 0x0 ～ 0xffff の 16 進数のステーション メッセージ ID の値に基づいてトラフィックを識別します。**match** [**not**] **message-id** コマンドを使用して、単一の ID または ID の範囲を指定できます。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

match message-id {*value* | **range** *start_value end_value*}

例：

```
hostname(config-pmap)# match message-id 0x181
hostname(config-pmap)# match message-id range 0x200 0xffff
```

b) 一致したパケットに対して実行するアクションを指定します。パケットをドロップし、必要に応じてログに記録できます。**drop** [**log**]

c) ドロップするすべてのメッセージ ID を指定するまで、このプロセスを繰り返します。

ステップ 4 インスペクション エンジンに影響するパラメータを設定します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **enforce-registration**：コールを発信する前に強制的に登録を実行します。
- **message-ID max** *hex_value*：許可される最大 SCCP ステーション メッセージ ID を設定します。メッセージ ID は 16 進数で指定します。デフォルトの最大値は 0x181 です。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの enforce-payloadtype キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **sccp-prefix-len** {**max** | **min**} *length*：許可される最大または最小の SCCP プレフィックスの長さを設定します最小値と最大値の両方を設定するには、このコマンドを 2 回入力します。デフォルトの最小値は 4 で、デフォルトの最大値はありません。
- **timeout** {**media** | **signaling**} *time*：メディアおよびシグナリング接続のタイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを設定しない場合は、番号に 0 を指定

します。デフォルトのメディア タイムアウトは 5 分、デフォルトのシグナリング タイムアウトは 1 時間です。

例

次の例は、SCCP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

STUN インスペクション

RFC 5389 で定義されている Session Traversal Utilities for NAT（STUN）は、プラグインが不要になるように、ブラウザベースのリアルタイム コミュニケーション用に WebRTC クライアントによって使用されます。WebRTC クライアントは、多くの場合、クラウド STUN サーバーを使用してパブリック IP アドレスおよびポートを学習します。WebRTC は、Interactive Connectivity Establishment（ICE、RFC 5245）を使用してクライアント間の接続を確認します。これらのクライアントは、TCP やその他のプロトコルを使用することもできますが、通常、UDP を使用します。

ファイアウォールは、多くの場合、発信 UDP トラフィックをブロックするため、Cisco Spark などの WebRTC 製品が接続を完了できないことがあります。STUN インスペクションでは、STUN エンドポイント用のピンホールが開かれ、STUN と ICES の基本コンプライアンスが適用されます。これにより、両側で接続チェックが確認応答された場合にクライアントの通信が許可されます。このため、これらのアプリケーションをイネーブルにするためにアクセスルールで新しいポートを開く必要がなくなります。

デフォルトのインスペクション クラスで STUN インスペクションをイネーブルにすると、STUN トラフィックに関して TCP/UDP ポート 3478 が監視されます。このインスペクションは、IPv4 アドレスと TCP/UDP のみをサポートします。

STUN インスペクションには NAT に関するいくつかの制限があります。WebRTC トラフィックについては、スタティック NAT/PAT44 がサポートされます。Cisco Spark はピンホールを必要としないので、Spark は追加のタイプの NAT をサポートできます。また、ダイナミック NAT/PAT を含む NAT/PAT64 を Cisco Spark で使用することもできます。

ピンホールが複製されるとき、STUN インスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。STUN 要求の受信後にノードに障害が発生し、別のノードが STUN 応答を受信した場合、STUN 応答はドロップされます。

（注） STUN インスペクションでは、要求と応答を照合するためにトランザクション ID が使用されます。デバッグを使用して接続のドロップをトラブルシューティングする場合は、システムがデバッグ出力の ID の形式（エンディアンネス）を変更するため、pcap で表示される ID と直接比較されないことに注意してください。

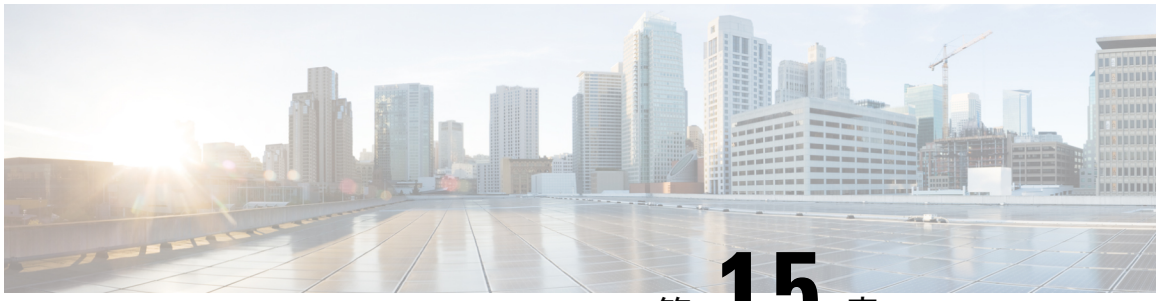
STUN インスペクションのイネーブル化の詳細については、アプリケーション レイヤ プロトコル インスペクションの設定 （305 ページ） を参照してください。

音声とビデオのプロトコル インスペクションの履歴

機能名	リリース	機能情報
SIP、SCCP、および TLS プロキシでの IPv6 のサポート	9.3(1)	SIP、SCCP、および TLS プロキシ（SIP または SCCP を使用）を使用している場合、IPv6 トラフィックを検査できるようになりました。 変更されたコマンドはありません。
SIP での信頼検証サービス、NAT66、CUCM 10.5、およびモデル 8831 電話機のサポート。	9.3(2)	SIP インスペクションで信頼検証サービス用サーバを設定できるようになりました。NAT66 も使用できます。SIP インスペクションは CUCM 10.5 でテスト済みです。 **trust-verification-server** パラメータ コマンドが追加されました。
複数のコアを搭載した ASA での SIP インスペクションのパフォーマンスが向上。	9.4(1)	複数のコアで ASA を通過する SIP シグナリングチングが複数存在する場合の SIP インスペクション パフォーマンスが向上しました。ただし、TLS、電話、または IME プロキシを使用する場合、パフォーマンスの向上は見られません。 変更されたコマンドはありません。

機能名	リリース	機能情報
ASA クラスタリングでの SIP インスペクションのサポート	9.4(1)	ASA クラスタで SIP インスペクションを設定できます。制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データ フローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 **show ssh sessions detail** コマンドが導入されました。
電話プロキシおよび UC-IME プロキシに対する SIP インスペクションのサポートが削除されました。	9.4(1)	SIP インスペクションを設定する際、電話プロキシまたは UC-IME プロキシは使用できなくなります。暗号化されたトラフィックを検査するには、TLS プロキシを使用します。 **phone-proxy**、**uc-ime** の各コマンドが削除されました。**inspect sip** コマンドから **phone-proxy** キーワードと **uc-ime** キーワードが削除されました。
H.460.18 互換性に関連する H.225 SETUP メッセージの前に着信する H.255 FACILITY メッセージに対する H.323 インスペクションのサポート。	9.6(1)	H.225 FACILITY メッセージが H.225 SETUP メッセージの前に着信する（これは、エンドポイントが H.460.18 に準拠する場合に発生する場合があります）ことを許可するように H.323 インスペクション ポリシー マップを設定できるようになりました。 次のコマンドが導入されました。**early-message**。
Session Traversal Utilities for NAT（STUN）インスペクション	9.6(2)	Cisco Spark を含む WebRTC アプリケーションの STUN トラフィックを検査できるようになりました。インスペクションでは、リターン トラフィックに必要なピンホールが開きます。 **inspect stun**、**show asp drop**、**show conn detail**、**show service-policy inspect stun** の各コマンドが追加または変更されました。
TLS プロキシでの TLSv1.2 と Cisco Unified Communications Manager 10.5.2 のサポート。	9.7(1)	暗号化 SIP 用の TLS プロキシでの TLSv1.2、または Cisco Unified Communications Manager 10.5.2 での SCCP インスペクションを使用できるようになりました。TLS プロキシは、**client cipher-suite** コマンドの一部として追加された TLSv1.2 暗号スイートをサポートします。 **client cipher-suite** コマンドが変更されました。
SCCP（Skinny）インスペクションでは、TLS プロキシが廃止されました。	9.13(1)	**tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは廃止されました。このキーワードは今後のリリースで **inspect skinny** コマンドから削除される予定です。

機能名	リリース	機能情報
SCCP（Skinny）インスペクションでは、TLS プロキシのサポートがなくなりました。	9.14(1)	**tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは削除されました。
デフォルトの SIP インスペクション ポリシーマップは、非 SIP トラフィックをドロップします。	9.16(1)	SIP インスペクションされるトラフィックでは、現在、デフォルトでは非 SIP トラフィックがドロップされます。以前のデフォルトでは、SIP のインスペクション対象ポートで非 SIP トラフィックが許可されていました。 デフォルトの SIP ポリシーマップが変更され、**no traffic-non-sip** コマンドが追加されました。



第 15 章

モバイル ネットワークのインスペクション

次の項では、LTE などのモバイル ネットワークで使用されるプロトコルに対するアプリケーション インスペクションについて説明します。これらのインスペクションには、 キャリア ライセンスが必要です。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、アプリケーション レイヤ プロトコル インスペクションの準備 （295 ページ）を参照してください。

- モバイル ネットワーク インスペクションの概要 （401 ページ）
- モバイル ネットワーク プロトコル インスペクションのライセンス （410 ページ）
- GTP インスペクションのデフォルト （411 ページ）
- モバイル ネットワーク インスペクションの設定 （412 ページ）
- モバイル ネットワーク インスペクションのモニタリング （447 ページ）
- モバイル ネットワーク インスペクションの履歴 （452 ページ）

モバイル ネットワーク インスペクションの概要

次の項では、LTE などのモバイル ネットワークで使用されるプロトコルに対応するインスペクションについて説明します。インスペクションに加えて SCTP トラフィックで利用できるサービスは他にもあります。

GTP インスペクションの概要

GPRS トンネリング プロトコルは、General Packet Radio Service（GPRS）トラフィック用に GSM、UMTS および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザー データ パケットの伝送にもトンネリング メカニズムを使用します。

サービス プロバイダー ネットワークは、GTP を使用して、エンドポイント間の GPRS バックボーンを介してマルチプロトコル パケットをトンネリングします。GTPv0-1 では、GTP は gateway GPRS support node（GGSN）と serving GPRS support node（SGSN）間のシグナリングの

ために使用されます。GTPv2 では、シグナリングは Packet Data Network Gateway（PGW）と Serving Gateway（SGW）および他のエンドポイント間で行われます。GGSN/PGW は、GPRS ワイヤレス データ ネットワークと他のネットワーク間のインターフェイスです。SGSN/SGW は、モビリティ、データ セッション管理、およびデータ圧縮を実行します。

ASA を使用して、不正なローミング パートナーに対する保護を行えます。デバイスをホームの GGSN/PGW エンドポイントと訪問した SGSN/SGW エンドポイント間に配置し、トラフィック上で GTP インスペクションを使用します。GTP インスペクションは、これらのエンドポイント間のトラフィックでのみ動作します。GTPv2 では、これは S5/S8 インターフェイスとして知られています。

GTP および関連する規格は、3GPP（第 3 世代パートナーシップ プロジェクト）によって定義されます。詳細については、http://www.3gpp.org を参照してください。

モバイル端末の場所変更の追跡

GTP インスペクションを使用すると、モバイル端末の場所の変更を追跡できます。場所の変更を追跡すると、不正なローミング請求を特定するのに役立つ場合があります。たとえば、モバイル端末が、米国のセルから欧州のセルに 30 分以内に移動するなど、ある場所から別の場所にありえない時間で移動した場合などです。

場所のロギングを有効にすると、システムは International Mobile Subscriber Identity（IMSI）ごとに新しい場所または変更された場所の syslog メッセージを生成します。

- 324010 は新しい PDP コンテキストの作成を示し、携帯電話の国コード（MCC）、モバイル ネットワーク コード（MNC）、情報要素、および必要に応じてユーザーが現在登録されているセル ID が含まれます。セル ID は、セル グローバル識別（CGI）または E-UTRAN セル グローバル識別子（ECGI）から抽出されます。
- 324011 は、IMSI が PDP コンテキストの作成中に保存されたものから移動したことを示します。メッセージには、以前および現在の MCC/MNC、情報要素、および必要に応じてセル ID が表示されます。

デフォルトでは、syslog メッセージにタイムスタンプ情報は含まれません。これらのメッセージを分析してありえないローミングを識別する場合は、タイムスタンプも有効にする必要があります。タイムスタンプ ロギングは GTP インスペクション マップに含まれません。**logging timestamp** コマンドを使用します。

場所のロギングの有効化に関する詳細については、GTP インスペクション ポリシー マップの設定 （412 ページ）を参照してください。

GTP インスペクションの制限事項

次に、GTP インスペクションに関する制限事項の一部を示します。

- GTPv2 ピギーバック メッセージはサポートされていません。これらは常にドロップされます。
- GTPv2 emergency UE attach は、IMSI（International Mobile Subscriber Identity）が含まれている場合にのみサポートされます。

- GTPインスペクションは初期のデータは検査しません。つまり、セッション要求の作成直後かつセッション応答の作成前に PGW または SGW から送信されたデータのことです。
- GTPv2 の場合、インスペクションは 3GPP 29.274 V15.5.0 までサポートされています。GTPv1 の場合、3GPP 29.060 V15.2.0 までサポートされています。GTPv0 の場合、リリース 8 までサポートしています。
- GTPインスペクションは、セカンダリ PDP コンテキストへの SGSN 間ハンドオフをサポートしていません。インスペクションは、プライマリおよびセカンダリ両方の PDP コンテキストに対しハンドオフを実行する必要があります。
- GTP インスペクションを有効にすると、GTP-in-GTP カプセル化を使用する接続は常にドロップされます。

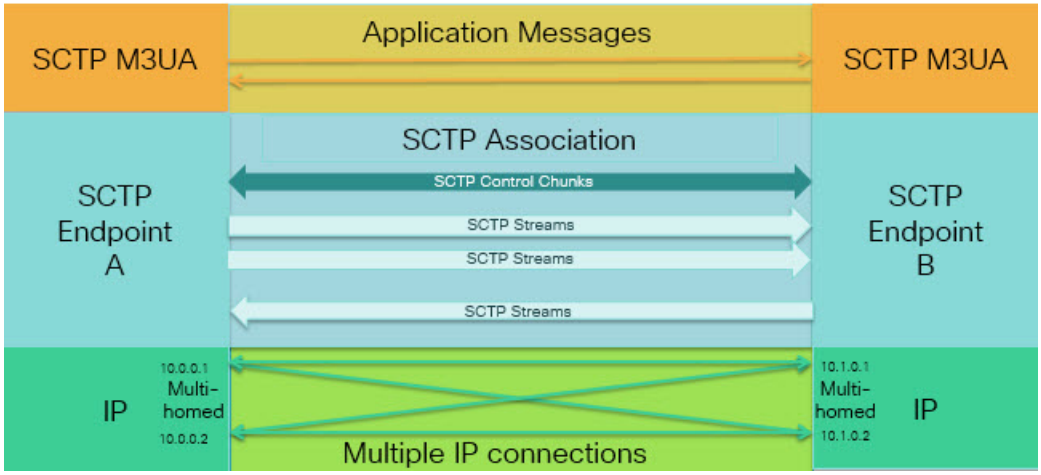
Stream Control Transmission Protocol（SCTP）インスペクションとアクセス制御

SCTP（Stream Control Transmission Protocol）は RFC 4960 で説明されています。プロトコルは IP 経由のテレフォニー シグナリング プロトコル SS7 をサポートしており、4G LTE モバイル ネットワーク アーキテクチャにおける複数のインターフェイス用の転送プロトコルでもあります。

SCTP は、TCP や UDP と同様、プロトコル スタックの IP の最上部で動作するトランスポート層プロトコルです。ただし、SCTP は、1 つ以上の送信元 IP アドレスまたは宛先 IP アドレス上の 2 つのエンド ノード間でアソシエーションと呼ばれる論理的な通信チャネルを作成します。これはマルチホーミングと呼ばれます。アソシエーションでは、各ノード（送信元と宛先）での IP アドレスのセットと、各ノードでのポートが定義されます。セット内の任意の IP アドレスは、複数の接続を形成するためにこのアソシエーションに関連付けられたデータ パケットの送信元または宛先 IP アドレスとして使用できます。各接続内では、メッセージを送信するために複数のストリームが存在する可能性があります。SCTP 内のストリームは、論理的なアプリケーション データ チャネルを表します。

次の図は、アソシエーションとそのストリームとの関係を示しています。

図 *42 : SCTP* アソシエーションとストリームの関係



ASA を通過する SCTP トラフィックがある場合、SCTP ポートに基づいてアクセスを制御し、アプリケーション層のインスペクションを実行して、接続を有効にし、オプションでペイロード プロトコル ID でフィルタリングを行い、アプリケーションを選択的にドロップ、ログに記録、またはレート制限できます。

（注） 各ノードは、最大 3 つの IP アドレスを持つことができます。上限である 3 を超えたアドレスは無視され、アソシエーションに含まれません。セカンダリ IP アドレスのピンホールは、自動的に開きます。これらを許可するアクセス制御ルールを記述する必要はありません。

ハートビートと関連付けの状態

関連付けを維持して正確なレポートを作成するために、検査エンジンは SCTP ハートビートをモニターします。システムは、接続時間をハートビート信号にリンクさせます。ハートビートが失われたか、関連付けが明示的に終了すると、デバイスは接続を閉じてイベント期間を終了します。

SCTP の関連付けとポートレポート

SCTP の検査は、フローではなく関連付けに基づいて行われます。デバイスは関連付け全体を単一のユニットとして追跡するため、個々のストリームポートはロギング出力で従来のポートフィールドにマッピングされません。そのため、接続の詳細を表示するときに、送信元ポートと宛先ポートが 0 と表示されることがあります。これは、関連付けが個々の送信元/宛先ポートのペアではなく、IP アドレスと関連付け ID によって一意に識別されるためです。

SCTP ステートフル インスペクション

TCP と同様、SCTP トラフィックは、正しく構造化されたトラフィックと RFC 4960 の限定的な適用についてレイヤ 4 で自動的に検査されます。次のプロトコル要素が検査され、適用されます。

- チャンクのタイプ、フラグ、および長さ。
- 検証タグ。
- 送信元ポートと宛先ポート。アソシエーション リダイレクト攻撃を防ぐため。
- IP アドレス。

SCTP ステートフル インスペクションは、アソシエーションの状態に基づいてパケットの受け入れまたは拒否を行います。

- 最初のアソシエーション確立のための 4 方向開閉シーケンスの検証。
- アソシエーションおよびストリーム内の TSN の転送進捗状況の確認。
- ハートビートの障害による中断チャンクを確認した場合のアソシエーションの終了。SCTP エンドポイントは、爆弾攻撃に応答して中断チャンクを送信する場合があります。

これらの強制チェックを行わない場合は、特定のトラフィック クラスの接続の設定（すべてのサービス） （486 ページ） で説明されているように、特定のトラフィック クラスに対し SCTP ステート バイパスを設定できます。

SCTP アクセス制御

SCTP トラフィックのアクセス ルールを作成できます。これらのルールは TCP/UDP ポート ベースのルールと似ており、プロトコルとして単に **sctp** を使用し、ポート番号は SCTP ポートです。SCTP 用のサービス オブジェクトまたはグループを作成するか、またはポートを直接指定できます。次の項を参照してください。

- サービス オブジェクトとサービス グループの設定 （14 ページ）
- ポートベースの照合に使用する拡張 ACE の追加 （44 ページ）

SCTP NAT

SCTP アソシエーション確立メッセージのアドレスにスタティック ネットワーク オブジェクト NAT を適用できます。スタティック Twice NAT を設定できますが、SCTP アソシエーションの宛先部分のトポロジが不明であるため、これは推奨されません。ダイナミック NAT/PAT を使用することはできません。

SCTP 用の NAT は、SCTP アプリケーション レイヤのインスペクションではなく、SCTP ステートフル インスペクションによって決まります。したがって、SCTP ステート バイパスを設定している場合は、NAT トラフィックはできません。

SCTP アプリケーション レイヤのインスペクション

SCTP アプリケーション SCTP インスペクションとフィルタリングを有効にすることにより、アクセス ルールをさらに絞り込むことができます。ペイロード プロトコル ID（PPID）に基づいて、SCTP トラフィック クラスを選択的にドロップ、ログに記録、またはレート制限することができます。

PPID でフィルタリングする場合は、次の点に注意してください。

- PPID はデータのかたまりの中にあり、特定のパケットは複数のデータ チャンクまたは 1 つの制御チャンクを持つことができます。パケットに 1 つの制御チャンクまたは複数のデータ チャンクが含まれている場合、割り当てられたアクションがドロップされてもパケットはドロップされません。
- PPID フィルタリングを使用してパケットをドロップまたはレート制限する場合は、送信機によりドロップされたパケットが再送されることに注意してください。レート制限が適用された PPID のパケットは再試行で通過する可能性がありますが、ドロップされた PPID のパケットは再びドロップされます。ネットワーク上のこのような反復的ドロップの最終成果を評価することができます。

SCTP に関する制限事項

SCTP サポートには次の制限事項が含まれます。

- 各ノードは、最大 3 つの IP アドレスを持つことができます。上限である 3 を超えたアドレスは無視され、アソシエーションに含まれません。セカンダリ IP アドレスのピンホールは、自動的に開きます。これらを許可するアクセス制御ルールを記述する必要はありません。
- 使用されないピンホールは、5 分後にタイムアウトします。
- マルチホーム エンドポイントのデュアル スタック IPv4 および IPv6 アドレスはサポートされません。
- ネットワーク オブジェクト スタティック NAT は、唯一サポートされているタイプの NAT です。また、NAT46 および NAT64 はサポートされません。
- SCTP パケットのフラグメンテーションとリアセンブリは、Diameter、M3UA、および SCTP の PPID ベースのインスペクションで処理されたトラフィックにのみ実行されます。
- SCTP で IP アドレスを動的に追加または削除するために使用される ASCONF チャンクは、サポートされません。
- IP アドレスに解決できるホスト名を指定するために使用される、INIT および INIT-ACK SCTP メッセージ内のホスト名パラメータは、サポートされません。
- ASA、またはネットワーク内の他の場所で設定されているかどうかにかかわらず、SCTP/M3UA は等コスト マルチパス ルーティング（ECMP）をサポートしません。ECMP を使用すると、復数のベストパスを介してパケットを宛先にルーティングできます。ただし、単一の宛先への SCTP/M3UA パケット応答は、送出されたときと同じインターフェイスに戻る必要があります。応答が M3UA サーバーから送信される可能性があるとしても、常に送出されたときと同じインターフェイスに戻る必要があります。この問題の症状として、SCTP INIT-ACK パケットがドロップされます。これは、**show asp drop flow sctp-chunk-init-timeout** カウンタで確認できます。

```
Flow drop:
```

```
SCTP INIT timed out (not receiving INIT ACK)(sctp-chunk-init-timeout)
```

この問題が発生した場合は、M3UA サーバーへのスタティック ルートを設定するか、またはポリシーベース ルーティングを設定して、INIT-ACK パケットが INIT パケットと同じインターフェイスを確実に通過するネットワーク設計を実装することで解決できます。

Diameter インスペクション

Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。

Diameter はトランスポート層として TCP および SCTP を使用し、TCP/TLS および SCTP/DTLS によって通信を保護します。また、オプションで、データ オブジェクトの暗号化も提供できます。Diameter の詳細については、RFC 6733 を参照してください。

Diameterアプリケーションは、課金のユーザーアクセス、サービス認証、QoS、およびレートの決定といったサービス管理タスクを実行します。Diameter アプリケーションは LTE アーキテクチャのさまざまなコントロール プレーン インターフェイスで使用されますが、ASA は、次のインターフェイスについてのみ、Diameter コマンド コードおよび属性値ペア（AVP）を検査します。

- S6a：モビリティ マネージメント エンティティ（MME）-ホーム サブスクリプション サービス（HSS）
- S9：PDN ゲートウェイ（PDG）- 3GPP AAA プロキシ/サーバー
- Rx：ポリシー/課金ルール機能（PCRF） - コール セッション制御機能（CSCF）

Diameterインスペクションでは、Diameterエンドポイント用にピンホールを開いて通信を可能にします。このインスペクションは、3GPP バージョン 12 をサポートし、RFC 6733 に準拠しています。TCP/TLS（インスペクションをイネーブルにするときに TLS を指定する場合）および SCTP には使用できますが、SCTP/DTLS には使用できません。SCTP Diameter セッションにセキュリティを提供するには IPsec を使用します。

パケットや接続のドロップまたはロギングなどの特別なアクションを適用するために、オプションで、Diameter インスペクション ポリシー マップを使用し、アプリケーション ID、コマンド コード、および AVP に基づいてトラフィックをフィルタリングできます。新規に登録された Diameter アプリケーション用のカスタム AVP を作成できます。フィルタリングにより、ネットワークで許可するトラフィックを微調整できます。

（注） 他のインターフェイス上で動作するアプリケーションに対するDiameterメッセージはデフォルトで許可され、渡されます。ただし、アプリケーション ID によってこれらのアプリケーションを破棄するための Diameter インスペクション ポリシー マップを設定できますが、これらのサポートされていないアプリケーションに対してコマンド コードまたは AVP に基づいてアクションを指定することはできません。

M3UA インスペクション

MTP3 User Adaptation（M3UA）は、SS7 Message Transfer Part 3（MTP3）レイヤと連動する IP ベース アプリケーション用のSS7ネットワークへのゲートウェイを提供するクライアント/サーバー プロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザー パート（ISUP など）を実行することが可能になります。M3UA は RFC 4666 で定義されています。

M3UA は SCTP をトランスポート層として使用します。SCTP ポート 2905 がデフォルト ポートです。

MTP3 レイヤは、ルーティングおよびノードアドレッシングなどのネットワーク機能を提供しますが、ノードの識別にポイント コードを使用します。M3UA 層は、発信ポイント コード（OPC）および宛先ポイント コード（DPC）を交換します。これは、IP が IP アドレスを使用してノードを識別する仕組みと似ています。

M3UAインスペクションは、限定されたプロトコル準拠を提供します。オプションで、厳密なアプリケーション サーバー プロセス（ASP）のステート チェックおよび選択されたメッセージの追加のメッセージの検証を実装できます。厳密なASPのステートチェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。

オプションで、ポイント コードまたはサービス インジケータ（SI）に基づいてアクセス ポリシーを適用できます。また、メッセージのクラスおよびタイプに基づいてレート制限を適用できます。

M3UA プロトコル準拠

M3UAインスペクションでは、次の限定されたプロトコルを強制できます。インスペクションは、要件を満たさないパケットをドロップしてログに記録します。

- 共通のメッセージヘッダー。インスペクションでは、共通ヘッダー内のすべてのフィールドを確認します。
  - バージョン 1 のみ。
  - メッセージの長さが正しく設定されている必要があります。
  - 予約済みの値を使用したメッセージ タイプのクラスは許可されません。

- メッセージ クラス内での無効なメッセージ ID は許可されません。

- ペイロード データ メッセージ。
  - 特定のタイプの 1 つのパラメータのみが許可されます。
  - SCTP ストリーム 0 でのデータ メッセージは許可されません。

- [Affected Point Code] フィールドは次のメッセージに含まれている必要があり、含まれていない場合、メッセージはドロップされます。利用可能な宛先（DAVA）、利用できない宛先（DUNA）、宛先の状態監査（DAUD）、シグナリング輻輳（SCON）、利用できない宛先ユーザー部（DUPU）、制限された宛先（DRST）。
- 次のメッセージについてメッセージ タグの検証を有効にすると、特定のフィールドの内容が確認および検証されます。検証で合格しなかったメッセージはドロップされます。
  - 利用できない宛先ユーザー部（DUPU）：ユーザー/理由フィールドが存在し、有効な理由およびユーザー コードのみが含まれている必要があります。
  - エラー：すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。
  - 通知：ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。

- アプリケーション サーバー プロセス（ASP）の厳密な状態検証を有効にすると、システムは M3UA セッションの ASP の状態を維持し、検証結果に基づいて ASP メッセージを許可またはドロップします。ASP の厳密な状態検証を無効にすると、すべての ASP メッセージが検査されずに転送されます。

M3UA インスペクションの制限事項

次に、M3UA インスペクションに関する制限事項の一部を示します。

- NAT は、M3UA データに埋め込まれている IP アドレスではサポートされません。
- M3UA の厳密なアプリケーション サーバー プロセス（ASP）状態の確認は、SCTP ステートフル インスペクションと依存性があります。SCTP ステート バイパスと M3UA の厳密な ASP 確認は、同じトラフィック上で実行しないでください。
- 厳密な ASP のステート チェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。

RADIUS アカウンティング インスペクションの概要

RADIUS アカウンティング インスペクションの目的は、RADIUS サーバーを使用した GPRS ネットワークの過剰請求攻撃を防ぐことです。RADIUS アカウンティング インスペクションを実行するために キャリア ライセンスは必要ありませんが、GTP インスペクションを実行し、GPRS を設定しなければ意味がありません。

GPRS ネットワークの過剰請求攻撃は、コンシューマに対して、利用していないサービスの請求を行います。この場合、悪意のある攻撃者は、サーバーへの接続をセットアップし、SGSN から IP アドレスを取得します。攻撃者がコールを終了しても、攻撃者のサーバーはパケットの送信を続けます。このパケットはGGSNによってドロップされますが、サーバーからの接続はアクティブなままです。攻撃者に割り当てられていたIPアドレスが解放され、正規ユーザーに再割り当てされるので、正規ユーザーは、攻撃者が利用するサービスの分まで請求されることになります。

RADIUSアカウンティングインスペクションは、GGSNへのトラフィックが正規のものかどうかを確認することにより、このような攻撃を防ぎます。RADIUSアカウンティングの機能を正しく設定しておくと、ASA は、RADIUS アカウンティング要求の開始メッセージと終了メッセージに含まれる Framed IP 属性との照合結果に基づいて接続を切断します。終了メッセージの Framed IP 属性の IP アドレスが一致している場合、ASA は、一致する IP アドレスを持つ送信元との接続をすべて検索します。

ASA でメッセージを検証できるように、RADIUS サーバーとの事前共有秘密キーを設定することもできます。共有秘密が設定されていない場合、ASA は、ソース IP アドレスが RADIUS メッセージを送信できるよう設定されたIPアドレスであるということだけをチェックします。

（注） GPRS をイネーブルにして RADIUS アカウンティング インスペクションを使用すると、ASA はアカウンティング要求の STOP メッセージで 3GPP-Session-Stop-Indicator をチェックして、セカンダリ PDP コンテキストを正しく処理します。具体的には、ASA では、アカウンティング要求の終了メッセージがユーザーセッションおよび関連するすべての接続を終了する前に、メッセージに 3GPP-SGSN-Address 属性が含まれる必要があります。一部のサードパーティの GGSN は、この属性をデフォルトでは送信しない場合があります。

モバイル ネットワーク プロトコル インスペクションのライセンス

次のプロトコルのインスペクションには、次の表に記載されているライセンスが必要です。

- GTP
- SCTP。
- Diameter
- M3UA

モデル	ライセンス要件
ASA 仮想 (全モデル)	キャリア ライセンス（デフォルトではイネーブル）
Cisco Secure Firewall 3100	キャリア ライセンス
Firepower 4100	キャリア ライセンス
Firepower 9300	キャリア ライセンス
他のすべてのモデル	キャリア ライセンスは他のモデルでは使用できません。これらのプロトコルは検査できません。

GTP インスペクションのデフォルト

GTP インスペクションはデフォルトではイネーブルになっていません。ただし、ユーザー自身のインスペクションマップを指定せずにイネーブルにすると、次の処理を行うデフォルトマップが使用されます。マップを設定する必要があるのは、異なる値が必要な場合のみです。

- エラーは許可されません。
- 要求の最大数は 200 です。
- トンネルの最大数は 500 です。これは、PDP コンテキスト（エンドポイント）の数に相当します。
- GTP エンドポイントのタイムアウトは 30 分です。エンドポイントには、GSN（GTPv0,1）および SGW/PGW（GTPv2）が含まれています。
- PDP コンテキストのタイムアウトは 30 分です。GTPv2 では、これはベアラ- コンテキスト タイムアウトです。
- 要求のタイムアウトは 1 分です。
- シグナリング タイムアウトは 30 分です。
- トンネリングのタイムアウトは 1 時間です。
- T3 応答タイムアウトは 20 秒です。
- 不明なメッセージ ID が許可されます。**match message v1/v2 id range** コマンドを設定して、サポートされていないコマンドや許可されていないコマンドをドロップしたり、ログに記録したりできます。未定義のメッセージやシステムでサポートされていない GTP リリースで定義されたメッセージは不明と見なされます。

モバイル ネットワーク インスペクションの設定

モバイル ネットワークで使用されるプロトコルのインスペクションはデフォルトで有効になっていません。モバイル ネットワークをサポートするには、それらを設定する必要があります。

手順

ステップ 1 （任意）GTP インスペクション ポリシー マップの設定 （412 ページ）。

ステップ 2 （オプション）SCTP インスペクション ポリシー マップの設定 （417 ページ）。

ステップ 3 （オプション）Diameter インスペクション ポリシー マップの設定 （419 ページ）。

ソフトウェアではまだサポートされていない属性値ペア（AVP）でフィルタリングする場合は、Diameter インスペクション ポリシー マップで使用するカスタム AVP を作成できます。カスタム Diameter 属性値ペア（AVP）の作成 （424 ページ）を参照してください。

ステップ 4 （任意）暗号化された Diameter TCP/TLS トラフィックを検査する場合は、次の説明に従って、必要な TLS プロキシを作成します。 暗号化された Diameter セッションの検査 （425 ページ）

ステップ 5 （任意） M3UA インスペクション ポリシー マップの設定 （438 ページ）

ステップ 6 モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ）。

ステップ 7 （オプション）RADIUS アカウンティング インスペクションの設定 （444 ページ）。

RADIUS アカウンティング インスペクションは、過剰請求攻撃から保護します。

GTP インスペクション ポリシー マップの設定

GTP トラフィックで追加のパラメーターを実行する際にデフォルト マップがニーズを満たさない場合は、GTP マップを作成し、設定します。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 GTP インスペクション ポリシー マップを作成します。**policy-map type inspect gtp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **apn regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対する Access Point Name (APN) に一致します。
- **match** [**not**] **message** {**v1** | **v2**} **id** {*message_id* | **range** *message_id_1 message_id_2*}：メッセージ ID（1 ～ 255）を照合します。1 つの ID または ID の範囲を指定できます。メッセージが GTPv0/1 用（**v1**）か GTPv2 用（**v2**）かを指定する必要があります。
- **match** [**not**] **message length min** *bytes* **max** *bytes*：UDP ペイロード（GTP ヘッダーと残りのメッセージ）の長さが最小値と最大値の間（1 ～ 65536）であるメッセージを照合します。
- **match** [**not**] **msisdn regex** {*regex_name* | **class** *class_name*}：PDP コンテキスト作成要求、セッション作成要求、およびベアラー変更応答のメッセージ内のモバイル ステーション国際サブスクライバ電話番号（MSISDN）情報要素を指定した正規表現または正規表現クラスと照合します。正規表現では、特定の MSISDN または MSISDN の範囲を最初の x 桁に基づいて識別できます。MSISDN フィルタリングは GTPv1 および GTPv2 のみでサポートされています。
- **match** [**not**] **selection-mode** *mode_value*：PDP コンテキスト作成要求内の選択モードの情報要素を照合します。選択モードでは、メッセージにアクセス ポイント名（APN）の発信元を指定しますが、次のいずれかになります。選択モードフィルタリングは、GTPv1 および GTPv2 のみでサポートされています。
  - 0：確認済み。APN はモバイル ステーションまたはネットワークによって指定されており、サブスクリプションが確認されています。
  - 1：モバイル ステーション。APN はモバイル ステーションによって指定されており、サブスクリプションは確認されていません。
  - 2：ネットワーク。APN はネットワークによって指定されており、サブスクリプションは確認されていません。
  - 3：予約済み（未使用）
- **match** [**not**] **version** {*version_id* | **range** *version_id_1 version_id_2*}：0 ～ 255 のいずれかの GTP バージョンに一致します。1 つのバージョンまたはバージョンの範囲を指定できます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop** [**log**]：一致するすべてのパケットをドロップします。システム ログ メッセージも送信するには、**log** キーワードを追加します。
- **rate-limit** *message_rate*：メッセージのレートを制限します。このオプションでは、**message id** のみ使用できます。

ポリシーマップでは、複数の **match** コマンドを指定できます。**match** コマンドの順序については、複数のトラフィック クラスの処理方法 （297 ページ）を参照してください。

ステップ 4 インスペクションエンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **anti-replay**[*window_size*]：GTP-U メッセージのスライディング ウィンドウを指定することによって、アンチリプレイをイネーブルにします。スライディング ウィンドウのサイズはメッセージの数であり、128、256、512、または 1024 になります。サイズを指定しないと、デフォルトで 512 になります。有効なメッセージが表示されると、ウィンドウは新しいシーケンス番号に移行します。シーケンス番号は 0 ～ 65535 の範囲であり、最大値に達するとラッピングされます。また、これらは PDP コンテキストごとに一意です。メッセージは、シーケンス番号がウィンドウ内であれば有効と見なされます。アンチリプレイは、ハッカーが GTP データ パケットをキャプチャし、それらをリプレイするときに発生する可能性があるセッション ハイジャックや DoS 攻撃を防ぐのに役立ちます。
- **[permit errors]**：無効な GTP パケットや別の方法で解析されるとドロップされるすべてのパケットを許可します。パケットは、ポリシーマップで定義したアクションに基づいてドロップできます。
- **request-queue** *max_requests*：キューで応答待ちができる GTP 要求数の最大値を設定します。デフォルトは 200 です。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。「Error Indication」、「Version Not Supported」および「SGSN Context Acknowledge」というメッセージは、要求と見なされないため、応答待ち要求のキューに入れられません。
- **tunnel-limit** *max_tunnels*：許可されるアクティブな GTP トンネルの最大数を設定します。これは、PDP コンテキストまたはエンドポイントの数に相当します。デフォルトは 500 です。このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。
- **timeout** {**endpoint** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *time*：指定したサービスのアイドル タイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。このコマンドは、タイムアウトごとに別々に入力します。

- **endpoint**：GTP エンドポイントが削除されるまでの非アクティブ時間の最大値。
- **pdp-context**：GTP セッションの PDP コンテキストを削除するまでの非アクティブ時間の最大値。GTPv2 では、これはベアラー コンテキストです。
- **request**：要求キューから要求が削除されるまでの非アクティブ時間の最大値。ドロップされた要求への後続の応答もドロップされます。
- **signaling**：GTP シグナリングが削除されるまでの非アクティブ時間の最大値。
- **t3-response**：接続を除去する前に応答を待機する最大時間。
- **tunnel**：GTP トンネルが切断されるまでの非アクティブ時間の最大値。

ステップ 5 パラメータ コンフィギュレーション モードになっている間に、IP パケットとアンチスプーフィングに対して GTP-U チェックを設定します。

gtp-u-header-check[**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**]]

キーワードを指定しないと、このコマンドは GTP データ パケットの内部ペイロードが有効な IP パケットであるかどうかを確認し、非 IP ヘッダーがある場合はそのパケットをドロップします。

また、**anti-spoofing** キーワードを含めると、内部ペイロードの IP ヘッダー内のモバイル ユーザー IP アドレスが GTP 制御メッセージ（セッション作成応答など）に割り当てた IP アドレスと一致しているかどうかを確認し、IP アドレスが一致しない場合は GTP-U メッセージをドロップします。このチェックでは、IPv4、IPv6、および IPv4v6 PDN タイプがサポートされています。モバイル端末が DHCP を使用してそのアドレスを取得する場合、GTPv2 でのエンドユーザーの IP アドレスは 0.0.0.0（IPv4）または *prefix*::0（IPv6）になります。その場合、システムは内部パケットで検出した最初の IP アドレスを使用してエンドユーザー IP アドレスを更新します。次のキーワードを使用して、DHCP で取得したアドレスのデフォルトの動作を変更できます。

- **gtpv2-dhcp-bypass**：0.0.0.0 または *prefix*::0 アドレスを更新しないでください。その代わりに、エンドユーザーの IP アドレスが 0.0.0.0 または *prefix*::0 の場合はパケットを許可します。IP アドレスの取得に DHCP を使用すると、このオプションはアンチスプーフィング チェックをバイパスします。
- **gtpv2-dhcp-drop**：0.0.0.0 または *prefix*::0 アドレスを更新しません。その代わりに、エンドユーザーの IP アドレスが 0.0.0.0 または *prefix*::0 の場合はすべてのパケットをドロップします。このオプションは、IP アドレスの取得に DHCP を使用するユーザーへのアクセスを防ぎます。

ステップ 6 必要に応じて、パラメータ コンフィギュレーション モードに入っている間に、IMSI プレフィックス フィルタリングを設定します。

mcc *country_code* **mnc** *network_code*

drop mcc *country_code* **mnc** *network_code*

コマンドは必要な回数入力して、ターゲットとなるすべての MCC/MNC ペアを指定できますが、ポリシーマップ内のすべてのコマンドは **mcc** または **drop mcc** である必要があります。これらのコマンドを組み合わせることはできません。

デフォルトでは、GTP インスペクションは、有効なモバイル カントリ コード（MCC）とモバイル ネットワーク コード（MNC）の組み合わせをチェックしません。IMSI プレフィックス フィルタリングを設定すると、受信パケットの IMSI の MCC と MNC が、設定された MCC と MNC の組み合わせと比較されます。次に、コマンドに基づいて次のいずれかのアクションが実行されます。

- **mcc** コマンド：一致しない場合、パケットはドロップされます。
- **drop mcc** コマンド：一致する場合、パケットはドロップされます。

モバイル カントリ コードは 0 以外の 3 桁の数字で、1 桁または 2 桁の値のプレフィックスとして 0 が追加されます。モバイル ネットワーク コードは 2 桁または 3 桁の数字です。

許可またはドロップするすべての MCC と MNC の組み合わせを追加します。デフォルトでは、ASA は MNC と MCC の組み合わせが有効であるかどうかをチェックしないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC および MNC コードの詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

ステップ 7 必要に応じて、パラメータ コンフィギュレーション モードの間に場所のロギングを有効にします。

location-logging [**cell-id**]

サブスクライバの場所をログに記録し、モバイル端末の場所の変更を追跡します。場所の変更を追跡すると、不正なローミング請求を識別するのに役立ちます。場所のログを有効にすると、システムは International Mobile Subscriber Identity（IMSI）ごとに新しい（メッセージ 324010）場所または変更された（メッセージ 324011）場所の syslog メッセージを生成します。

ユーザーが現在登録されているセル ID をログ メッセージに含める場合は、**cell-id** パラメータを指定します。セル ID は、セル グローバル識別（CGI）または E-UTRAN セル グローバル識別子（ECGI）から抽出されます。

ステップ 8 必要に応じて、パラメータ コンフィギュレーション モードに入っている間に、GSN または PGW プーリングを設定します。

permit-response to-object-group *SGSN-SGW_name* **from-object-group** *GSN-PGW_pool*

ASA が GTP インスペクションを実行する場合、デフォルトで ASA は、GTP 要求で指定されていない GSN または PGW からの GTP 応答をドロップします。これは、GSN または PGW のプール間でロードバランシングを使用して、GPRS の効率とスケーラビリティを高めているときに発生します。

GSN/PGW プーリングを設定し、ロード バランシングをサポートするために、GSN/PGW エンドポイントを指定するネットワーク オブジェクト グループを作成し、これを **from-object-group** パラメータで指定します。同様に、SGSN/SGW のためにネットワーク オブジェクト グループを作成し、**to-object-group** パラメータとして選択します。応答を行う GSN/PGW が GTP 要求の送信先 GSN/PGW と同じオブジェクト グループに属しており、応答している GSN/PGW によ

る GTP 応答の送信が許可されている先のオブジェクト グループに SGSN/SGW がある場合に、ASA で応答が許可されます。

ネットワーク オブジェクト グループは、エンドポイントをホスト アドレスまたはエンドポイントを含むサブネットから識別できます。

例：

次に、GSN/PGW プーリングの例を示します。クラス C ネットワーク全体が GSN/PGW プールとして定義されていますが、ネットワーク全体を指定する代わりに、複数の個別の IP アドレスを **network-object** コマンドで 1 つずつ指定できます。この例では、次に、プールから SGSN/SgW への応答を許可するように、GTP インスペクション マップを変更します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit-response to-object-group sgsn32
from-object-group gsnpool32
```

例

次の例は、ネットワークのトンネル数を制限する方法を示しています。

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

hostname(config)# service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ） を参照してください。

SCTP インスペクション ポリシー マップの設定

レート制限などのアプリケーション固有のペイロードプロトコル ID（PPID）に基づいて SCTP トラフィックに代替アクションを適用するには、サービス ポリシーで使用される SCTP インスペクション ポリシー マップを作成します。

（注） PPID はデータのかたまりの中にあり、特定のパケットは複数のデータ チャンクまたは 1 つの制御チャンクを持つことができます。パケットに 1 つの制御チャンクまたは複数のデータ チャンクが含まれている場合、割り当てられたアクションがドロップされてもパケットはドロップされません。たとえば、PPID 26 をドロップする SCTP インスペクション ポリシー マップを設定すると、PPID 26 データ チャンクは、Diameter PPID データ チャンクを持つパケットに結合され、そのパケットはドロップされません。

手順

ステップ 1 SCTP インスペクション ポリシー マップを作成します。**policy-map type inspect sctp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 SCTP データ チャンクの PPID に基づいて、トラフィックをドロップ、レート制限、またはログに記録します。

a) PPID に基づいてトラフィックを識別します。

match[**not**] **ppid** *ppid_1* [*ppid_2*]

ppid_1 は PPID 番号（0 ～ 4294967295）または名前です（使用可能な名前については CLI ヘルプを参照してください）。PPID の範囲を指定するには、2 番目（より大きい）の PPID、*ppid_2* を含めることができます。**match not ppid** を使用して PPID または範囲に一致しないトラフィックを特定します。

SCTP PPID の現在のリストは http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25 で確認できます。

b) 一致したパケットに対して実行するアクションを指定します。

- **drop**：一致するすべてのパケットをドロップまたはログに記録します。
- **log**：システム ログ メッセージを送信します。
- **rate-limit** *rate*：メッセージのレートを制限します。レートは、キロビット/秒（kbps）単位です。

c) 選択的に処理するすべての PPID を識別するまで、プロセスを繰り返します。

例

次の例では、未割り当ての PPID（この例の作成時点で未割り当て）をドロップし、PPID 32 ～ 40 をレート制限し、Diameter PPID をログに記録するインスペクション ポリシー マップを作成します。このサービス ポリシーは、すべての SCTP トラフィックを照合する inspection_default クラスにインスペクションを適用します。

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
  drop
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log

policy-map global_policy
 class inspection_default
  inspect sctp sctp-pmap
!
service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ） を参照してください。

Diameter インスペクション ポリシー マップの設定

さまざまな Diameter プロトコル要素でフィルタリングするための Diameter インスペクション ポリシー マップを作成できます。その後、接続を選択的にドロップまたはログに記録できます。

Diameter メッセージ フィルタリングを設定するには、これらのプロトコル要素は RFC および技術仕様で定義されているので、これらの要素について詳しい知識を持っている必要があります。たとえば、IETF には、http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml に示す登録済みアプリケーション、コマンドコード、および属性値ペアのリストがありますが、Diameterインスペクションではリストされているすべての項目をサポートしていません。技術仕様については、3GPP Web サイトを参照してください。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、Diameter インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect diameter** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **application-id** *app_id* [*app_id_2*]：アプリケーション識別子を照合します。*app_id* は Diameter アプリケーションの名前または番号（0 ～ 4294967295）です。照合する連続番号が付されたアプリケーションの範囲がある場合は、2 番目の ID を含めることができます。アプリケーションの名前または番号別に範囲を定義でき、第 1 ID および第 2 ID の間のすべての番号に適用されます。

  これらのアプリケーションは IANA に登録されます。次のコア アプリケーションがサポートされますが、他のアプリケーションもフィルタ処理できます。アプリケーション名のリストについては、CLI ヘルプを参照してください。

  - **3gpp-rx-ts29214** （16777236）
  - **3gpp-s6a** （16777251）

- **3gpp-s9** （16777267）
- **common-message** （0）。（基本 Diameter プロトコル）

- **match** [**not**] **command-code** *code* [*code_2*]：コマンド コードを照合します。*code* は Diameter コマンド コードの名前または番号（0 ～ 4294967295）です。照合する連続番号が付されたコマンド コードの範囲がある場合は、2 番目のコードを含めることができます。コマンド コードの名前または番号別に範囲を定義でき、第 1 コードおよび第 2 コードの間のすべての番号に適用されます。

  たとえば、次のコマンドは、Capability Exchange Request/Answer コマンド コードを照合します。

  ```
  match command-code cer-cea
  ```

- 属性値ペア（AVP）を照合します。

  属性によってのみ AVP を照合するには、次の手順を実行します。

  match[**not**] **avp** コード[*code_2*] [**vendor-id** *id_number*]

  属性の値に基づいて AVP を照合する場合：

  match[**not**] **avp** コード[**vendor-id** *id_number*]値

  それぞれの説明は次のとおりです。

  - *code*：属性値ペアの名前または番号（1 ～ 4294967295）。最初のコードについては、カスタム AVP、RFC または 3GPP 技術仕様に登録されている AVP、およびソフトウェアで直接サポートされている AVP の名前を指定できます。特定の範囲の AVP を照合する場合は、2 つ目のコードを番号のみで指定します。値によって AVP を照合する場合は、2 つ目のコードを指定できません。AVP 名のリストについては、CLI ヘルプを参照してください。
  - **vendor-id** *id_number*：（任意）ベンダーの ID 番号（0 ～ 4294967295）も照合します。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
  - *value*：AVP の値の部分。これは、AVP の データ タイプがサポートされている場合にのみ設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。次に、サポートされているデータ タイプの値オプションの特定の構文を示します。
    - [Diameter Identity]、[Diameter URI]、[Octet String]：これらのデータ タイプの照合には正規表現または正規表現クラス オブジェクトを使用します。

      {**regex** *regex_name* | **class** *regex_class*}
    - [Address]：照合する IPv4 または IPv6 アドレスを指定します。たとえば、10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。
    - [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。

date *year month day* **time** *hh:mm:ss* **date** *year month day* **time** *hh:mm:ss*

次に例を示します。

```
date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00
```

- [Numeric]：番号の範囲を指定します。

  range *number_1 number_2*

  有効な番号の範囲は、データ タイプによって異なります。

  - Integer32：-2147483647 ～ 2147483647
  - Integer64：-9223372036854775807 ～ 9223372036854775807
  - Unsigned32：0 ～ 4294967295
  - Unsigned64：0 ～ 18446744073709551615
  - Float32：8 桁の小数点表現
  - Float64：16 桁精度の小数点表記

d) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 Diameter インスペクション ポリシー マップを作成します。**policy-map type inspect diameter** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- Diameter クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- Diameter クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop**：一致するすべてのパケットをドロップします。
- **drop-connection**：パケットをドロップし、接続を閉じます。
- **log**：システム ログ メッセージを送信します。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法（297 ページ）を参照してください。

例：

```
hostname(config)# policy-map type inspect diameter diameter-map
hostname(config-pmap)# class diameter-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match command-code cer-cea
hostname(config-pmap-c)# log
```

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの no 形式を使用してください。

- **unsupported** {**application-id** |**command-code** |**avp**} **action log**：ロギングをサポートされていない直径要素に対してイネーブルにします。これらのオプションでは、ソフトウェアで直接サポートされていないアプリケーション ID、コマンド コード、および AVP が指定されます。デフォルトでは、ロギングなしで要素が許可されています。コマンドを 3 回入力して、すべての要素のロギングを有効にできます。
- **strict-diameter** {**state** | **session**}：Diameter プロトコルの RFC 6733 への厳密な準拠をイネーブルにします。デフォルトでは、インスペクションによって、Diameter のフレームが RFC に準拠していることが確認されます。コマンドを 2 回入力することで、**state** マシン検証または **session** 関連メッセージの検証、あるいはその両方を追加できます。

例：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# unsupported application-id action log
hostname(config-pmap-p)# unsupported command-code action log
hostname(config-pmap-p)# unsupported avp action log
hostname(config-pmap-p)# strict-diameter state
hostname(config-pmap-p)# strict-diameter session
```

例

次の例は、一部のアプリケーションをログに記録し、特定の IP アドレスをブロックする方法を示しています。

```
class-map type inspect diameter match-any log_app
```

```
  match application-id 3gpp-s6a
  match application-id 3gpp-s13

class-map type inspect diameter match-all block_ip
  match command-code cer-cea
  match avp host-ip-address 1.1.1.1

policy-map type inspect diameter diameter_map
  parameters
    unsupported application-id log
  class log_app
    log
  class block_ip
    drop-connection

policy-map global_policy
  class inspection_default
    inspect diameter diameter_map

service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクションポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ） を参照してください。

カスタム Diameter 属性値ペア（AVP）の作成

新しい属性値ペア（AVP）が定義され、登録されると、カスタム Diameter AVP を作成して、Diameterインスペクション ポリシーマップにそれらを定義し、使用することができます。RFC または AVP を定義するその他のソースから AVP の作成に必要な情報を取得します。

カスタム AVP は、AVP 照合用の Diameterインスペクション ポリシーマップまたはクラス マップで使用する場合にのみ、作成します。

手順

カスタム Diameter AVP を作成します。

diameter avp*name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

それぞれの説明は次のとおりです。

- *name*：作成しているカスタム AVP の名前（最大 32 文字）。Diameter インスペクション ポリシー マップまたはクラス マップでの match avp コマンドでこの名前を参照します。
- **code** *value*：カスタム AVP コード値（256 ～ 4294967295）。システムで定義済みのコードとベンダー ID の組み合わせを入力することはできません。
- **data-type** *type*：AVP のデータ タイプ。次のいずれかの型で AVP を定義できます。新しい AVP が別の型の場合は、その型のカスタム AVP は作成できません。

- **address**：IP アドレスの場合。
- **diameter-identity**：Diameter のアイデンティティ データ。
- **diameter-uri**：Diameter の Uniform Resource Identifier（URI）。
- **float32**：32 ビット浮動小数点。
- **float64**：64 ビット浮動小数点。
- **int32**：32 ビット整数。
- **int64**：64 ビット整数。
- **octetstring**：オクテット文字列。
- **time**：時間の値。
- **uint32**：32 ビットの符号なし整数。
- **uint64**：64 ビットの符号なし整数。

- **vendor-id** *id_number*：（任意）AVP を定義したベンダーの 0 ～ 4294967295 の ID 番号。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
- **description** *text*：（任意）AVP の説明（最大 80 文字）。スペースを含める場合は、説明を引用符で囲みます。

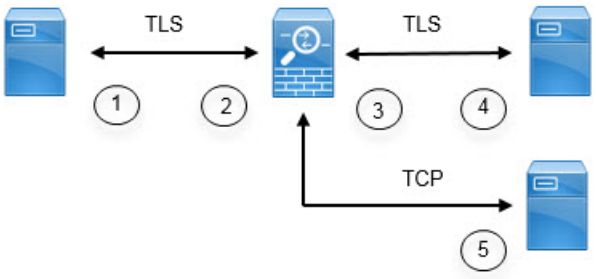
暗号化された Diameter セッションの検査

Diameter アプリケーションが TCP 上で暗号化されたデータを使用する場合、インスペクションはメッセージのフィルタリング ルールを実装するためにパケット内を確認することはできません。したがって、フィルタリング ルールを作成し、それらを暗号化された TCP トラフィックにも適用する場合は、TLS プロキシを設定する必要があります。暗号化されたトラフィックで厳密なプロトコルを適用するには、プロキシも必要です。この設定は SCTP/DTLS トラフィックには適用されません。

TLS プロキシは中間者として機能します。このプロキシは、トラフィックを復号化し、検査してから再度暗号化し、目的の宛先に送信します。したがって、接続の両側（Diameter サーバーと Diameter クライアント）は ASA を信頼する必要があり、すべての当事者が必要な証明書を保有している必要があります。TLS プロキシを実装するには、デジタル証明書を十分に理解しておく必要があります。ASA 全般設定ガイドのデジタル証明書に関する章を参照してください。

次の図は、Diameter のクライアントおよびサーバーと ASA の間の関係と、信頼を確立するための認定要件を示します。このモデルでは、Diameter クライアントは MME（モビリティ マネージメント エンティティ）であり、エンドユーザーではありません。リンクの各側の CA 証明書は、リンクの反対側の証明書の署名に使用されるものです。たとえば、ASA プロキシ TLS サーバー CA 証明書は、Diameter/TLS クライアント証明書の署名に使用されるものです。

図 *43 : Diameter TLS* インスペクション



1	Diameter TLS クライアント（MME） • クライアント ID 証明書 • ASA TLS プロキシ サーバーの ID 証明書の署名に使用される CA 証明書	2	ASA プロキシ TLS サーバー • サーバー ID 証明書 • Diameter TLS クライアントの ID 証明書の署名に使用される CA 証明書
3	ASA プロキシ TLS クライアント • クライアント ID（スタティックまたは LDC）証明書 • Diameter TLS サーバーの ID 証明書の署名に使用される CA 証明書	4	Diameter TLS サーバー（フル プロキシ） • サーバー ID 証明書 • ASA プロキシ TLS クライアントの ID 証明書の署名に使用される CA 証明書
5	Diameter TCP サーバー（TLS オフロード）	—	—

Diameter インスペクション用の TLS プロキシを設定するには、次のオプションがあります。

- フル TLS プロキシ：ASA および Diameter クライアントと ASA および Diameter サーバー間のトラフィックを暗号化します。TLS サーバーとの信頼関係を確立するには、次のオプションがあります。
  - スタティック プロキシ クライアント トラストポイントを使用します。ASA は、Diameter サーバーとの通信時に、すべての Diameter クライアントに同じ証明書を示します。Diameter サーバーにとって全クライアントが同じように見えるので、クライアントごとに差別化サービスを提供することはできません。一方、このオプションは LDC 方式よりも高速です。
  - ローカル ダイナミック証明書（LDC）を使用します。このオプションを使用すると、ASA は Diameter サーバーとの通信時に、Diameter クライアントごとに一意の証明書を示します。LDC は、公開キーと ASA からの新しい署名を除き、受信したクライアント ID 証明書からのすべてのフィールドを保持します。この方法では、Diameter サーバーでクライアント トラフィックの可視性が向上し、クライアント証明書の特性に基づいて差別化サービスを提供できるようになります。

- TLS オフロード：ASA と Diameter クライアント間のトラフィックを暗号化しますが、ASA と Diameter サーバー間でクリアテキスト接続を使用します。このオプションは、デバイス間のトラフィックが保護された場所から離れることがないと確信している場合に、Diameter サーバーが ASA と同じデータセンターにあれば実行可能です。TLS オフロードを使用すると、必要な暗号化処理量が減るので、パフォーマンスを向上させることができます。これは、オプションの中で最速です。Diameter サーバーは、クライアントの IP アドレスのみに基づいて差別化サービスを適用できます。

3 つすべてのオプションは、ASA と Diameter クライアント間の信頼関係に対して同じ設定を使用します。

（注） TLS プロキシは TLSv1.0 ～ 1.2 を使用します。TLS のバージョンと暗号スイートを設定できます。

次の項では、Diameter インスペクション用の TLS プロキシを設定する方法について説明します。

Diameter クライアントとのサーバー信頼関係の設定

ASA は、Diameter クライアントに対して TLS プロキシ サーバーとして機能します。相互信頼関係を確立するには：

- ASA のサーバー証明書への署名に使用された認証局（CA）証明書を Diameter クライアントにインポートする必要があります。これは、クライアントの CA 証明書ストアまたはクライアントが使用する他の場所に保存されている場合があります。証明書の使用の詳細については、クライアントのドキュメントを参照してください。
- ASA がクライアントを信頼できるように、Diameter TLS クライアントの証明書への署名に使用された CA 証明書をインポートする必要があります。

次の手順では、Diameter クライアントの証明書への署名に使用された CA 証明書をインポートし、ASA TLS プロキシ サーバーで使用する ID 証明書をインポートする方法について説明します。ID 証明書をインポートする代わりに、ASA で自己署名証明書を作成できます。

手順

ステップ 1 Diameter クライアントの証明書への署名に使用されている CA 証明書を ASA トラストポイントにインポートします。

この手順によって、ASA が Diameter クライアントを信頼できます。

a) Diameter クライアント用のトラストポイントを作成します。

この例では、**enrollment terminal** は、証明書を CLI に張り付けることを示しています。トラストポイントは **diameter-clients** と呼ばれます。

```
ciscoasa(config)# crypto ca trustpoint diameter-clients
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 証明書を追加します。

```
ciscoasa(config)# crypto ca authenticate diameter-clients
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

ステップ 2 証明書をインポートし、ASA プロキシ サーバーの ID 証明書およびキーペア用のトラストポイントを作成します。

この手順によって、Diameter クライアントが ASA を信頼できます。

a) pkcs12 形式で証明書をインポートします。

次の例では、**tls-proxy-server-tp** がトラストポイント名で、**“123”** が復号パス フレーズです。独自のトラストポイント名およびパス フレーズを使用します。

```
ciscoasa (config)# crypto ca import tls-proxy-server-tp pkcs12 "123"

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]

quit

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#
```

b) トラストポイントを設定します。

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-server-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

Diameter インスペクション用のスタティック クライアント証明書によるフル TLS プロキシの設定

Diameter サーバーがすべてのクライアントに対して同じ証明書を受け入れることができる場合は、Diameter サーバーと通信するときに使用する ASA 用のスタティック クライアント証明書を設定できます。

この設定では、ASA とクライアント間（Diameter クライアントとのサーバー信頼関係の設定（427 ページ） で説明されているように）、および ASA と Diameter サーバー間に相互の信頼関係を確立する必要があります。ASA と Diameter サーバーの信頼要件は次のとおりです。

- Diameter サーバーの ID 証明書への署名に使用された CA 証明書をインポートする必要があるので、ASA は、TLS ハンドシェイク中にサーバーの ID 証明書を検証できます。
- Diameter サーバーも信頼しているクライアント証明書をインポートする必要があります。Diameter サーバーがまだ証明書を信頼していない場合は、その署名に使用される CA 証明書をサーバーにインポートします。詳細については、Diameter サーバーのドキュメントを参照してください。

手順

ステップ 1 Diameter サーバーの証明書への署名に使用されている CA 証明書を ASA トラストポイントにインポートします。

この手順によって、ASA が Diameter サーバーを信頼できます。

a) Diameter サーバー用のトラストポイントを作成します。

この例では、**enrollment terminal** は、証明書を CLI に張り付けることを示しています。登録用 URL を使用して、CA との自動登録（SCEP）を指定することもできます。トラストポイントは **diameter-server** と呼ばれます。

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 証明書を追加します。

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

ステップ 2 証明書をインポートし、ASA プロキシ クライアントの ID 証明書およびキーペア用のトラストポイントを作成します。

この手順によって、Diameter サーバーが ASA を信頼できます。

a) pkcs12 形式で証明書をインポートします。

次の例では、**tls-proxy-client-tp** がトラストポイント名で、**“123”** が復号パス フレーズです。独自のトラストポイント名およびパス フレーズを使用します。

```
ciscoasa (config)# crypto ca import tls-proxy-client-tp pkcs12 "123"

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]

quit

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#
```

b) トラストポイントを設定します。

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-client-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

ステップ 3 TLS プロキシを設定します。

a) TLS プロキシに名前を付け、TLS プロキシ コンフィギュレーション モードを開始します。

tls-proxy *name*

b) ASA が Diameter クライアントとの関係においてプロキシ サーバーとして機能するときに使用されるトラストポイントを識別します。

server trust-point *trustpoint_name*

（注） テスト目的の場合、または Diameter クライアントを信頼できると確信している場合は、この手順をスキップして、TLS プロキシ コンフィギュレーションに **no server authenticate-client** コマンドを含めることができます。

c) ASA が Diameter サーバーとの関係においてプロキシ クライアントとして機能するときに使用されるトラストポイントを識別します。

client trust-point *name*

d) （任意）クライアントが使用できる暗号方式を定義します。

client cipher-suite *cipher-list*

ここで、*cipher-list* には、次の任意の組み合わせを含めることができます。

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

複数のオプションはスペースで区切ります。

TLS プロキシで使用できる暗号方式を定義しないと、プロキシ サーバーは **ssl cipher** コマンドによって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルはmediumです。つまり、NULL-SHA、DES-CBC-SHA、およびRC4-MD5を除くすべての暗号方式が使用できます。ASAで一般に使用可能なものとは異なるスイートを使用する場合にのみ、**client cipher-suite** コマンドを指定します。

ASA 上のすべての SSL クライアント接続に最小 TLS バージョンを設定する場合は、**ssl client-version** コマンドを参照してください。デフォルトは TLS v1.0 です。

e) （任意）サーバーが使用できる暗号方式を定義します。

server cipher-suite *cipher-list*

ここで、*cipher-list* には、次の任意の組み合わせを含めることができます。

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

複数のオプションはスペースで区切ります。

TLS プロキシで使用できる暗号方式を定義しないと、プロキシ サーバーは **ssl cipher** コマンドによって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルはmediumです。つまり、NULL-SHA、DES-CBC-SHA、およびRC4-MD5を除くすべての暗号方式が使用できます。ASAで一般に使用可能なものとは異なるスイートを使用する場合にのみ、**server cipher-suite** コマンドを指定します。

ASA 上のすべての SSL サーバー接続に最小 TLS バージョンを設定する場合は、**ssl server-version** コマンドを参照してください。デフォルトは TLS v1.0 です。

例：

```
ciscoasa(config)# tls-proxy diameter-tls-static-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client trust-point tls-proxy-client-tp
```

次のタスク

Diameter インスペクションで TLS プロキシを使用できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ） を参照してください。

Diameter インスペクション用のローカル ダイナミック証明書によるフル TLS プロキシの設定

Diameter サーバーでクライアントごとに一意の証明書が必要な場合は、ローカル ダイナミック証明書（LDC）を生成するように ASA を設定することができます。これらの証明書は、クライアントが接続している間存在し、その後は破棄されます。

この設定では、ASA とクライアント間（Diameter クライアントとのサーバー信頼関係の設定 （427 ページ） で説明されているように）、および ASA と Diameter サーバー間に相互の信頼関係を確立する必要があります。設定は Diameter インスペクション用のスタティック クライアント証明書によるフル TLS プロキシの設定 （429 ページ） で説明するものと同様ですが、Diameter クライアント証明書をインポートする代わりに ASA 上で LDC をセットアップする点が異なります。ASA と Diameter サーバーの信頼要件は次のとおりです。

- Diameter サーバーの ID 証明書への署名に使用された CA 証明書をインポートする必要があるので、ASA は、TLS ハンドシェイク中にサーバーの ID 証明書を検証できます。
- LDC トラストポイントを作成する必要があります。LDC サーバーの CA 証明書をエクスポートし、Diameter サーバーにインポートする必要があります。エクスポート設定は次のとおりです。証明書のインポートの詳細については、Diameter サーバーのドキュメントを参照してください。

手順

ステップ 1 Diameter サーバーの証明書への署名に使用されている CA 証明書を ASA トラストポイントにインポートします。

この手順によって、ASA が Diameter サーバーを信頼できます。

a) Diameter サーバー用のトラストポイントを作成します。

この例では、**enrollment terminal** は、証明書を CLI に張り付けることを示しています。登録用 URL を使用して、CA との自動登録（SCEP）を指定することもできます。トラストポイントは **diameter-server** と呼ばれます。

```
ciscoasa(config)# crypto ca trustpoint diameter-server
```

```
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 証明書を追加します。

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

ステップ 2 ローカル ダイナミック証明書（LDC）に署名するローカル CA を作成します。

a) トラストポイント用の RSA キーペアを作成します。

この例では、キーペア名は ldc-signer-key です。

```
ciscoasa(config)# crypto key generate rsa label ldc-signer-key
INFO: The name for the keys will be: ldc-signer-key
Keypair generation process
ciscoasa(config)#
```

b) LDC 発行元のトラストポイントを作成します。

この例では、トラストポイント名は**ldc-server** で、上記で作成されたキーペアが使用され、自己署名済みの登録が指定されます（**enrollment self**、これは必須です）。ASA の共通名はサブジェクト名として含まれています。Diameter アプリケーションにサブジェクト名に関する固有の要件があるかどうかを確認します。

proxy-ldc-issuer コマンドは、TLS プロキシのダイナミック証明書を発行するトラストポイントに、ローカル CA の役割を定義します。

```
ciscoasa(config)# crypto ca trustpoint ldc-server
ciscoasa(ca-trustpoint)# keypair ldc-signer-key
ciscoasa(ca-trustpoint)# subject-name CN=asa3
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# proxy-ldc-issuer
ciscoasa(ca-trustpoint)# exit
```

c) トラストポイントを登録します。

```
ciscoasa(config)# crypto ca enroll ldc-server
```

ステップ 3 TLS プロキシを設定します。

a) TLSプロキシに名前を付け、TLSプロキシ コンフィギュレーション モードを開始します。

tls-proxy *name*

b) ASA が Diameter クライアントとの関係においてサーバーとして機能するときに使用されるトラストポイントを識別します。

server trust-point *trustpoint_name*

（注） テスト目的の場合、またはDiameterクライアントを信頼できると確信している場合は、この手順をスキップして、TLS プロキシ コンフィギュレーションに **no server authenticate-client** コマンドを含めることができます。

c) ASAがダイナミック証明書を発行し、Diameterサーバーとの関係においてクライアントとして機能するときに使用される LDC トラストポイントを識別します。

client ldc issuer *name*

d) LDC キーペアを識別します。LDC トラストポイントで定義されている同じキーを指定します。

client ldc key-pair *name*

e) （任意）クライアントが使用できる暗号方式を定義します。

client cipher-suite *cipher-list*

ここで、*cipher-list* には、次の任意の組み合わせを含めることができます。

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

複数のオプションはスペースで区切ります。

TLS プロキシで使用できる暗号方式を定義しないと、プロキシ サーバーは **ssl cipher** コマンドによって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルはmediumです。つまり、NULL-SHA、DES-CBC-SHA、およびRC4-MD5を除くすべての暗号方式が使用できます。ASA で一般に使用可能なものとは異なるスイートを使用する場合にのみ、**client cipher-suite** コマンドを指定します。

ASA 上のすべての SSL クライアント接続に最小 TLS バージョンを設定する場合は、**ssl client-version** コマンドを参照してください。デフォルトは TLS v1.0 です。

f) （任意）サーバーが使用できる暗号方式を定義します。

server cipher-suite *cipher-list*

ここで、*cipher-list* には、次の任意の組み合わせを含めることができます。

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

複数のオプションはスペースで区切ります。

TLS プロキシで使用できる暗号方式を定義しないと、プロキシ サーバーは **ssl cipher** コマンドによって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルは medium です。つまり、NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号方式が使用できます。ASA で一般に使用可能なものとは異なるスイートを使用する場合にのみ、**server cipher-suite** コマンドを指定します。

ASA 上のすべての SSL サーバー接続に最小 TLS バージョンを設定する場合は、**ssl server-version** コマンドを参照してください。デフォルトは TLS v1.0 です。

例：

```
ciscoasa(config)# tls-proxy diameter-tls-ldc-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client ldc issuer ldc-server
ciscoasa(config-tlsp)# client ldc key-pair ldc-signer-key
```

ステップ 4 LDC CA 証明書をエクスポートし、Diameter サーバーにインポートします。

a) 証明書をエクスポートします。

次の例では、LDC トラストポイントは ldc-server です。独自の LDC トラストポイント名を指定します。

```
ciscoasa(config)# crypto ca export ldc-server identity-certificate
-----BEGIN CERTIFICATE-----
MIIDbDCCAlSgAwIBAgIQfWOQvGFpj7hCCB49+kS4CjANBgkqhkiG9w0BAQUFADAT
MREwDwYDVQQDEwhIdW5ueUJlZTAeFw0xMzA2MjUwMTE5MzJaFw00ODA2MjUwMTI5
...[data omitted]...
lJZ48NoI64RqfGC/KHUsOQ==
-----END CERTIFICATE-----
```

b) 証明書データをコピーし、ファイルに保存します。

これで、Diameter サーバーにインポートできます。手順については、Diameter サーバーのドキュメントを参照してください。データは Base64 形式であることに注意してください。

サーバーにバイナリ形式または DER 形式が必要な場合は、OpenSSL ツールを使用して形式を変換する必要があります。

次のタスク

Diameter インスペクションで TLS プロキシを使用できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ） を参照してください。

Diameter インスペクション用の TLS オフロードによる TLS プロキシの設定

ASA と Diameter サーバー間のネットワーク パスが安全であると確信している場合は、ASA とサーバー間のデータを暗号化するパフォーマンス コストを回避できます。TLS オフロードを使用すると、TLS プロキシは Diameter クライアントと ASA の間のセッションを暗号化/復号化しますが、Diameter サーバーではクリア テキストを使用します。

この設定では、ASA とクライアント間のみに相互の信頼関係を確立する必要があり、これにより設定が簡略化されます。次の手順を実行する前に、Diameter クライアントとのサーバー信頼関係の設定 （427 ページ） の手順を完了します。

手順

ステップ 1 TLS オフロードに TLS プロキシを設定します。

a) TLS プロキシに名前を付け、TLS プロキシ コンフィギュレーション モードを開始します。

tls-proxy *name*

b) ASA が Diameter クライアントとの関係においてサーバーとして機能するときに使用されるトラストポイントを識別します。

server trust-point *trustpoint_name*

（注） テスト目的の場合、または Diameter クライアントを信頼できると確信している場合は、この手順をスキップして、TLS プロキシ コンフィギュレーションに **no server authenticate-client** コマンドを含めることができます。

c) （任意）サーバーが使用できる暗号方式を定義します。

server cipher-suite *cipher-list*

ここで、*cipher-list* には、次の任意の組み合わせを含めることができます。

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**

- **des-sha1**
- **null-sha1**
- **rc4-sha1**

複数のオプションはスペースで区切ります。

TLS プロキシで使用できる暗号方式を定義しないと、プロキシ サーバーは **ssl cipher** コマンドによって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルはmediumです。つまり、NULL-SHA、DES-CBC-SHA、およびRC4-MD5を除くすべての暗号方式が使用できます。ASAで一般に使用可能なものとは異なるスイートを使用する場合にのみ、**server cipher-suite** コマンドを指定します。

ASA 上のすべての SSL サーバー接続に最小 TLS バージョンを設定する場合は、**ssl server-version** コマンドを参照してください。デフォルトは TLS v1.0 です。

d) ASA と Diameter サーバー間の通信がクリア テキストで行われることを指定します。この中では、ASA は Diameter サーバーのクライアントとして機能します。

client clear-text

例：

```
ciscoasa(config)# tls-proxy diameter-tls-offload-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client clear-text
```

ステップ 2 Diameter ポートは TCP と TLS では異なるため、Diameter サーバーからクライアントへのトラフィックに対しては、TCP ポートを TLS ポートに変換する NAT ルールを設定します。

各 Diameter サーバー用のオブジェクト NAT ルールを作成します。各ルールは以下を実行する必要があります。

- Diameter サーバー アドレスにスタティック アイデンティティ NAT を実行します。つまり、オブジェクト内の IP アドレスは、NAT ルール内の変換されたアドレスと同じである必要があります。
- 実際のポート 3868（これはデフォルトの Diameter TCP ポート番号です）を 5868（デフォルトの Diameter TLS ポート番号）に変換します。
- 送信元インターフェイスは、Diameterサーバーに接続しているものでなければならず、宛先インターフェイスは、Diameter クライアントに接続しているものでなければなりません。

次の例では、10.29.29.29 Diameter サーバーから外部インターフェイスに着信するポート 3868 上の TCP トラフィックを内部インターフェイスのポート 5868 に変換します。

```
ciscoasa(config)# object network diameter-client
ciscoasa(config-network-object)# host 10.29.29.29
ciscoasa(config-network-object)# nat (outside,inside) static 10.29.29.29
```

```
service tcp 3868 5868
```

次のタスク

Diameter インスペクションで TLS プロキシを使用できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ） を参照してください。

M3UA インスペクション ポリシー マップの設定

M3UA インスペクション ポリシー マップを使用して、ポイント コードに基づくアクセス制御を設定します。また、クラスやタイプ別にメッセージをドロップおよびレート制限できます。

デフォルトのポイント コード形式はITUです。別の形式を使用している場合は、ポリシー マップで要求される形式を指定します。

ポイント コードまたはメッセージ クラスに基づいてポリシーを適用しない場合は、M3UA ポリシー マップを設定する必要はありません。マップなしでインスペクションを有効にできます。

手順

ステップ 1 M3UA インスペクション ポリシー マップを作成します。**policy-map type inspect m3ua** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **message class** *class_id* [**id** *message_id*]：M3UA メッセージのクラスとタイプを照合します。次の表に、使用可能な値を示します。これらのメッセージの詳細については、M3UA の RFC およびドキュメンテーションを参照してください。

M3UA メッセージ クラス	メッセージ ID タイプ
0（管理メッセージ）	0 ～ 1
1（転送メッセージ）	1
2（SS7 シグナリング ネットワーク管理メッセージ）	1 ～ 6

M3UA メッセージ クラス	メッセージ ID タイプ
3（ASP 状態メンテナンス メッセージ）	1 ～ 6
4（ASP トラフィック メンテナンス メッセージ）	1 ～ 4
9（ルーティング キー管理メッセージ）	1 ～ 4

- **match** [**not**] **opc** *code*：データ メッセージ内の発信ポイント コード、つまりトラフィックの送信元を照合します。ポイント コードは *zone-region-sp* 形式で、各要素に使用可能な値は SS7 バリアントによって異なります。
  - **ITU**：ポイント コードは 3-8-3 形式の 14 ビット値です。値の範囲は、[0-7]-[0-255]-[0-7] です。
  - **ANSI**：ポイント コードは 8-8-8 形式の 24 ビット値です。値の範囲は、[0-255]-[0-255]-[0-255] です。
  - **Japan**：ポイント コードは 5-4-7 形式の 16 ビット値です。値の範囲は、[0-31]-[0-15]-[0-127] です。
  - **China**：ポイント コードは 8-8-8 形式の 24 ビット値です。値の範囲は、[0-255]-[0-255]-[0-255] です。
- **match** [**not**] **dpc** *code*：データ メッセージ内の宛先ポイント コードを照合します。ポイント コードは、**match opc** について説明しているとおり、*zone-region-sp* 形式です。
- **match** [**not**] **service-indicator** *number*：サービス インジケータ番号を照合します（0 ～ 15）。使用可能なサービス インジケータは次のとおりです。これらのサービス インジケータの詳細については、M3UA RFC およびドキュメントを参照してください。
  - 0：シグナリング ネットワーク管理メッセージ
  - 1：シグナリング ネットワーク テストおよびメンテナンス メッセージ
  - 2：シグナリング ネットワーク テストおよびメンテナンス特別メッセージ
  - 3：SCCP
  - 4：電話ユーザー部
  - 5：ISDN ユーザー部
  - 6：データ ユーザー部（コールおよび回線関連のメッセージ）
  - 7：データ ユーザー部（設備の登録およびキャンセル メッセージ）
  - 8：MTP テスト ユーザー部に予約済み
  - 9：ブロードバンド ISDN ユーザー部
  - 10：サテライト ISDN ユーザー部

- 11：予約済み
- 12：AAL タイプ 2 シグナリング
- 13：ベアラー非依存コール制御
- 14：ゲートウェイ制御プロトコル
- 15：予約済み

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop** [**log**]：一致するすべてのパケットをドロップします。任意で、システム ログ メッセージを送信します。
- **rate-limit** *message_rate*：メッセージのレートを制限します。このオプションは **match message class** でのみ使用可能です。

ポリシー マップでは、複数の **match** コマンドを指定できます。match コマンドの順序については、複数のトラフィック クラスの処理方法 （297 ページ） を参照してください。

ステップ 4 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **message-tag-validation** {**dupu** | **error** | **notify**}：特定のフィールドの内容が確認され、指定したメッセージ タイプが検証されます。検証で合格しなかったメッセージはドロップされます。検証はメッセージ タイプによって異なります。
  - 利用できない宛先ユーザー部（DUPU）：ユーザー/理由フィールドが存在し、有効な理由およびユーザー コードのみが含まれている必要があります。
  - エラー：すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。
  - 通知：ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。
- **ss7 variant** {**ITU** | **ANSI** | **JAPAN** | **CHINA**}：ネットワーク内で使用されている SS7 のバリアントを特定します。このオプションによって、ポイント コードの有効な形式が決定します。オプションを設定して M3UA ポリシーを導入した後は、ポリシーを削除しない限り変更はできません。デフォルトのバリアントは ITU です。

- **strict-asp-state**：アプリケーション サーバー プロセス（ASP）状態の検証を実行します。システムは M3UA セッションの ASP の状態を維持し、検証結果に基づいて ASP メッセージをドロップします。ASP の厳密な状態検証を無効にすると、すべての ASP メッセージが検査されずに転送されます。厳密な ASP のステート チェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。
- **timeout endpoint** *time*：M3UA エンドポイントの統計情報を削除するアイドル タイムアウトを設定します（hh:mm:ss 形式）。タイムアウトを付けない場合は、0 を指定してください。デフォルトは 30 分（0:30:00）です。
- **timeout session** *time*：厳密な ASP 状態の確認を有効にしている場合の、M3UA セッションを削除するためのアイドル タイムアウト（hh:mm:ss の形式）。タイムアウトを付けない場合は、0 を指定してください。デフォルトは 30 分（0:30:00）です。このタイムアウトを無効にすると、失効したセッションの削除を防止できます。

例

次は、M3UA ポリシー マップおよびサービス ポリシーの例です。

```
hostname(config)# policy-map type inspect m3ua m3ua-map
hostname(config-pmap)# match message class 2 id 6
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match message class 9
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match dpc 1-5-1
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# ss7 variant ITU
hostname(config-pmap-p)# timeout endpoint 00:45:00

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect m3ua m3ua-map

hostname(config)# service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （442 ページ） を参照してください。

モバイル ネットワーク インスペクションのサービス ポリシーの設定

モバイルネットワークで使用されるプロトコルのインスペクションは、デフォルトのインスペクション ポリシーでは有効になっていないので、これらのインスペクションが必要な場合は有効にする必要があります。デフォルトのグローバル インスペクション ポリシーを編集するだけで、これらのインスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1 必要な場合は、L3/L4 クラスマップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
   match parameter
```

例：

```
hostname(config)# class-map mobile_class_map
hostname(config-cmap)# match access-list mobile
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、通過トラフィック用のレイヤ 3/4 クラス マップの作成 （282 ページ） を参照してください。

ステップ 2 クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。**policy-map** *name*

例：

```
hostname(config)# policy-map global_policy
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3 インスペクションに使用する L3/L4 クラス マップを指定します。**class** *name*

例：

```
hostname(config-pmap)# class inspection_default
```

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4 インスペクションをイネーブルにします。

次のコマンドでは、インスペクション ポリシー マップはオプションです。インスペクションをカスタマイズするためにこれらのマップのいずれかを作成した場合は、適切なコマンドで名前を指定します。 Diameter では、TLS プロキシを指定して、暗号化されたメッセージのインスペクションを有効にすることもできます。

- **inspect gtp** [*map_name*]：GTP インスペクションをイネーブルにします。
- **inspect sctp**[*map_name*]：SCTP インスペクションをイネーブルにします。
- **inspect diameter** [*map_name*] [**tls-proxy** *proxy_name*]：Diameter インスペクションをイネーブルにします。

（注） Diameter インスペクション用の TLS プロキシを指定し、Diameter サーバー トラフィックに NAT ポート リダイレクションを適用した場合（たとえば、ポート 5868 から 3868 にサーバー トラフィックをリダイレクトするなど）は、グローバルに、または入力インターフェイスのみでインスペクションを設定します。出力インターフェイスにインスペクションを適用すると、NATed Diameter トラフィックはインスペクションをバイパスします。

- **inspect m3ua** [*map_name*]：M3UA インスペクションをイネーブルにします。

例：

```
hostname(config-class)# inspect gtp
hostname(config-class)# inspect sctp
hostname(config-class)# inspect diameter
hostname(config-class)# inspect m3ua
```

（注） 別のインスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（またはすべての使用中のポリシー）を編集する場合は、コマンドの **no inspect** バージョンを使用してインスペクションを削除してから、新しいインスペクション ポリシー マップの名前で再追加します。たとえば、GTP のポリシー マップを変更するには：

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

ステップ 5 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを1つだけ適用できます。

RADIUS アカウンティング インスペクションの設定

RADIUSアカウンティングインスペクションはデフォルトではイネーブルになっていません。RADIUS アカウンティング インスペクションが必要な場合は設定してください。

手順

ステップ 1 RADIUS アカウンティング インスペクション ポリシー マップの設定 （444 ページ）。
ステップ 2 RADIUS アカウンティング インスペクションのサービス ポリシーの設定 （446 ページ）。

RADIUS アカウンティング インスペクション ポリシー マップの設定

検査に必要な属性を設定する RADIUS アカウンティング インスペクション ポリシー マップを作成します。

手順

ステップ 1 RADIUS アカウンティング インスペクション ポリシー マップを作成します。**policy-map type inspect radius-accounting** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*
ステップ 3 パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4 1つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **send response**：Accounting-Request の Start および Stop メッセージを、それらのメッセージの送信元（**host** コマンド内で識別されています）へ送信するよう ASA に指示します。
- **enable gprs**：GPRS 過剰請求の保護を実装します。セカンダリ PDP コンテキストを適切に処理するため、ASA は、Accounting-Request の Stop および Disconnect メッセージの 3GPP VSA 26-10415 属性をチェックします。この属性が存在する場合、ASA は、設定インターフェイスのユーザー IP アドレスに一致するソース IP を持つすべての接続を切断します。
- **validate-attribute** *number*：Accounting-Request Start メッセージを受信する際、ユーザー アカウントのテーブルを作成する場合に使用する追加基準。これらの属性は、ASA が接続を切断するかどうかを決定する場合に役立ちます。

  検証する追加属性を指定しない場合は、Framed IP アドレス属性の IP アドレスのみに基づいて決定されます。追加属性を設定し、ASA が現在追跡されているアドレスを含むが、その他の検証する属性が異なるアカウンティング開始メッセージを受信すると、古い属性を使用して開始するすべての接続は、IP アドレスが新しいユーザーに再割り当てされたという前提で、切断されます。

  値の範囲は 1 ～ 191 で、このコマンドは複数回入力できます。属性番号および説明のリストについては、http://www.iana.org/assignments/radius-types を参照してください。
- **host** *ip_address* [**key** *secret*]：RADIUS サーバーまたは GGSN の IP アドレスです。ASA がメッセージを許可できるよう、任意で秘密キーを含めることができます。キーがない場合、IP アドレスだけがチェックされます。複数の RADIUS と GGSN のホストを識別するため、このコマンドは繰り返し実行できます。ASA は、これらのホストから RADIUS アカウンティング メッセージのコピーを受信します。
- **timeout users** *time*：ユーザーのアイドル タイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを付けない場合は、00:00:00 を指定してください。デフォルトは 1 時間です。

例

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
```

```
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

RADIUS アカウンティング インスペクションのサービス ポリシーの設定

デフォルトのインスペクション ポリシーでは、RADIUS アカウンティング インスペクションはイネーブルにされてないため、この検査が必要な場合はイネーブルにします。RADIUS アカウンティング インスペクションは ASA のトラフィック用に指示されますので、標準ルールではなく、管理インスペクション ルールとして設定してください。

手順

ステップ 1 検査を適用するトラフィックを識別するため L3/L4 マネジメント クラス マップを作成し、一致するトラフィックを識別します。

```
class-map type management name
match {port | access-list} parameter
```

例：

```
hostname(config)# class-map type management radius-class-map
hostname(config-cmap)# match port udp eq radius-acct
```

この例では、一致は radius acct UDP ポート（1646）です。ポートの範囲（**match port udp range** *number1 number2*）または **match access-list** *acl_name* と ACL を使って異なるポートを指定できます。

ステップ 2 クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。**policy-map** *name*

例：

```
hostname(config)# policy-map global_policy
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3 RADIUS アカウンティング インスペクションに使用する L3/L4 管理クラス マップを特定します。**class** *name*

例：

```
hostname(config-pmap)# class radius-class-map
```

ステップ 4 RADIUS アカウンティング インスペクションを設定します。**inspect radius-accounting**[*radius-accounting_policy_map*]

radius_accounting_policy_map はRADIUS アカウンティング インスペクション ポリシー マップの設定 （444 ページ）で作成した RADIUS アカウンティング インスペクション ポリシー マップです。

例：

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

（注） 別のインスペクション ポリシー マップを使用するために使用中のポリシーを編集する場合、**no inspect radius-accounting** コマンドで RADIUS アカウンティング インスペクションを削除してから、新しいインスペクション ポリシー マップの名前で再追加します。

ステップ 5 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを1つだけ適用できます。

モバイルネットワークインスペクションのモニタリング

ここでは、モバイル ネットワーク インスペクションをモニタリングする方法について説明します。

GTP インスペクションのモニタリング

GTP コンフィギュレーションを表示するには、特権 EXEC モードで show service-policy inspect gtp コマンドを入力します。

show service-policy inspect gtp statistics コマンドを使用して、GTP インスペクションの統計情報を表示します。次にサンプル出力を示します。

```
firewall(config)# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

show service-policy inspect gtp statistics *ip_address* コマンドに IP アドレスを入力すると、特定の GTP エンドポイントの統計情報を取得できます。

```
firewall(config)# show service-policy inspect gtp statistics 10.9.9.9
1 in use, 1 most used, timeout 0:30:00
 GTP GSN Statistics for 10.9.9.9, Idle 0:00:34, restart counter 0
  Tunnels Active                    0
  Tunnels Created                   1
  Tunnels Destroyed                 0
  Total Messages Received           1
                         Signalling Messages        Data Messages
  total received                   1                          0
  dropped                          0                          0
  forwarded                        1                          0
```

show service-policy inspect gtp pdp-context コマンドを使用して、PDP コンテキストに関する情報を表示します。GTPv2 の場合、これはベアラー コンテキストです。次に例を示します。

```
ciscoasa(config)# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146

ciscoasa(config)# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:06:14,   Timeout 3:00:00,   APN ssenoauth146

    user_name (IMSI):  50502410121507    MS address: 2005:a00::250:56ff:fe96:eec
    nsapi: 5                linked nsapi: 5
    primary pdp: Y         sgsn is Remote
```

```
    sgsn_addr_signal: 10.0.203.22    sgsn_addr_data: 10.0.203.22
    ggsn_addr_signal: 10.0.202.22    ggsn_addr_data: 10.0.202.22
    sgsn control teid:     0x00000001    sgsn data teid:        0x000003e8
    ggsn control teid:     0x000f4240    ggsn data teid:        0x001e8480
    signal_sequence:               18     state:    Ready
...
```

PDP またはベアラー コンテキストは、IMSI と NSAPI（GTPv0-1）または IMSI と EBI（GTPv2）の値の組み合わせであるトンネル ID（TID）によって識別されます。GTP トンネルは、それぞれ別個の GSN または SGW/PGW ノードにある、2 つの関連するコンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、外部パケット データ ネットワークとモバイル サブスクライバ（MS）ユーザーとの間でパケットを転送する場合に必要です。

SCTP のモニタリング

次のコマンドを使用して、SCTP をモニターできます。

- **show service-policy inspect sctp**

  SCTP インスペクションの統計情報を表示します。sctp-drop-override カウンタは、PPID がドロップ アクションに一致するたびに増加しますが、パケットには PPID が異なるデータのかたまりが含まれていたのでパケットはドロップされません。次に例を示します。

```
ciscoasa# show service-policy inspect sctp
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: sctp sctp, packet 153302, lock fail 0, drop 20665, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0, sctp-drop-override 4910
        Match ppid 30 35
           rate-limit 1000 kbps, chunk 2354, dropped 10, bytes 21408, dropped-bytes
 958
        Match: ppid 40
           drop, chunk 5849
        Match: ppid 55
           log, chunk 9546
```

- **show sctp** [**detail**]

  現在の SCTP Cookie およびアソシエーションを表示します。SCTP アソシエーションに関する詳細情報を表示するには、**detail** キーワードを追加します。詳細ビューには、マルチホーミング、複数のストリーム、およびフラグメント再構成に関する情報も表示されます。

```
ciscoasa# show sctp

AssocID: 71adeb15
Local:  192.168.107.12/50001 (ESTABLISHED)
Remote: 192.168.108.122/2905 (ESTABLISHED)
Secondary Conn List:
    192.168.108.12(192.168.108.12):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.12(192.168.108.12):2905
    192.168.108.122(192.168.108.122):2905 to 192.168.107.122(192.168.107.122):50001

    192.168.107.122(192.168.107.122):50001 to 192.168.108.122(192.168.108.122):2905
```

```
192.168.108.12(192.168.108.12):2905 to 192.168.107.12(192.168.107.12):50001
192.168.107.12(192.168.107.12):50001 to 192.168.108.12(192.168.108.12):2905
```

- **show conn protocol sctp**

  現在の SCTP 接続に関する情報を表示します。

- **show local-host** [**connection sctp** *start*[*-end*]]

  インターフェイスごとに、ASA を経由して SCTP 接続を行うホストに関する情報を表示します。特定の数または範囲の SCTP 接続を持つホストのみを表示するには、**connection sctp** キーワードを追加します。

- **show traffic**

  sysopt traffic detailed-statistics コマンドを有効にしている場合は、インターフェイスごとの SCTP 接続とインスペクションの統計情報が表示されます。

Diameter のモニタリング

次のコマンドを使用して、Diameter をモニターできます。

- **show service-policy inspect diameter**

  Diameter インスペクションの統計情報を表示します。次に例を示します。

```
ciscoasa# show service-policy inspect diameter
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: Diameter Diameter_map, packet 0, lock fail 0, drop 0, -drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
       Class-map: log_app
           Log: 5849
        Class-map: block_ip
            drop-connection: 2
```

- **show diameter**

  各 Diameter 接続のステータス情報を表示します。次に例を示します。

```
ciscoasa# show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

- **show conn detail**

  接続情報を表示します。Diameter 接続は、Q フラグを使用してマークされます。

- **show tls-proxy**

  TLS プロキシを Diameter インスペクションで使用する場合は、そのプロキシに関する情報が表示されます。

M3UA のモニタリング

次のコマンドを使用して、M3UA をモニターできます。

- **show service-policy inspect m3ua drops**

  M3UA インスペクションに対するドロップの統計情報を表示します。

- **show service-policy inspect m3ua endpoint** [*IP_address*]

  M3UA エンドポイントの統計情報を表示します。エンドポイントの IP アドレスを指定して、特定のエンドポイントに関する情報を表示できます。ハイアベイラビリティまたはクラスタ化されたシステムでは、統計情報はユニットごとに提供され、ユニット間で同期されません。次に例を示します。

```
ciscoasa# sh service-policy inspect m3ua endpoint
 M3UA Endpoint Statistics for 10.0.0.100, Idle : 0:00:06 :
                   Forwarded        Dropped          Total Received
 All Messages      21                5                 26
 DATA Messages     9                 5                 14
 M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
                   Forwarded        Dropped          Total Received
 All Messages      21                8                 29
 DATA Messages     9                 8                 17
```

- **show service-policy inspect m3ua session**

  厳密なアプリケーション サーバー プロセス（ASP）状態の確認を有効にすると、M3UA セッションに関する情報が表示されます。情報には、送信元アソシエーション ID、セッションがシングルまたはダブルいずれの交換であるか、また、クラスタの場合はクラスタ オーナーセッションとバックアップセッションのいずれであるかが含まれます。3 つ以上のユニットを持つクラスタでは、ユニットがクラスタから抜けた後に戻って来る場合、古いバックアップ セッションが表示されることがあります。これらの古いセッションは、セッション タイムアウトを無効にしていなければ、タイムアウト時に削除されます。

```
Ciscoasa# show service-policy inspect m3ua session
0 in use, 0 most used
Flags: o - cluster owner session, b - cluster backup session
       d - double exchange      , s - single exchange
AssocID: cfc59fbe in Down state, idle:0:00:05, timeout:0:01:00, bd
AssocID: dac2e123 in Active state, idle:0:00:18, timeout:0:01:00, os
```

- **show service-policy inspect m3ua table**

  分類ルールを含むランタイム M3UA インスペクション テーブルを表示します。

- **show conn detail**

接続情報を表示します。M3UA 接続は、v フラグを使用してマークされます。

モバイル ネットワーク インスペクションの履歴

機能名	リリース	機能情報
GTPv2 インスペクションと GTPv0/1 インスペクションの改善	9.5(1)	GTP インスペクションは GTPv2 を処理できるようになりました。また、すべてのバージョンの GTP インスペクションで IPv6 アドレスがサポートされるようになりました。 **match message id** コマンドが **match message** {**v1** | **v2**} **id** *message_id* に変更されました。**timeout gsn** コマンドが **timeout endpoint** に置き換えられました。**clear/show service-policy inspect gtp statistics** コマンドから **gsn** キーワードが削除され、エンドポイント ID を入力するだけでこれらの統計情報を確認またはクリアできるようになりました。**clear/show service-policy inspect gtp request** および **pdpmcb** コマンドに **version** キーワードが追加され、特定の GTP バージョンに関する情報を表示できるようになりました。
SCTP インスペクション	9.5(2)	ペイロード プロトコル ID（PPID）に基づいてアクションを適用するために、アプリケーション層インスペクションを Stream Control Transmission Protocol（SCTP）トラフィックに適用できるようになりました。 **clear conn protocol sctp**、**inspect sctp**、**match ppid**、**policy-map type inspect sctp**、**show conn protocol sctp**、**show local-host connection sctp**、**show service-policy inspect sctp** の各コマンドが追加または変更されました。
Diameter インスペクション	9.5(2)	アプリケーション層インスペクションを Diameter トラフィックに適用できるようになり、アプリケーション ID、コマンドコード、および属性値ペア（AVP）のフィルタリングに基づいてアクションを適用できるようになりました。 **class-map type inspect diameter**、**diameter**、**inspect diameter**、**match application-id**、**match avp**、**match command-code**、**policy-map type inspect diameter**、**show conn detail**、**show diameter**、**show service-policy inspect diameter**、**unsupported** の各コマンドが追加または変更されました。

機能名	リリース	機能情報
Diameter インスペクションの改善	9.6(1)	TCP/TLS トラフィック上の Diameter を検査し、厳密なプロトコル準拠チェックを適用し、クラスタ モードで SCTP 上の Diameter を検査できるようになりました。 **client clear-text**、**inspect diameter**、**strict-diameter** の各コマンドが追加または変更されました。
クラスタ モードでの SCTP ステートフル インスペクション	9.6(1)	SCTP ステートフル インスペクションがクラスタ モードで動作するようになりました。また、クラスタ モードで SCTP ステートフル インスペクション バイパスを設定することもできます。 導入または変更されたコマンドはありません。
MTP3 User Adaptation（M3UA）インスペクション。	9.6(2)	M3UA トラフィックを検査できるようになりました。また、ポイント コード、サービス インジケータ、およびメッセージのクラスとタイプに基づいてアクションを適用できるようになりました。 **clear service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**inspect m3ua**、**match dpc**、**match opc**、**match service-indicator**、**policy-map type inspect m3ua**、**show asp table classify domain inspect-m3ua**、**show conn detail**、**show service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**ss7 variant**、**timeout endpoint** の各コマンドが追加または変更されました。
SCTP マルチストリーミングの並べ替えとリアセンブル、およびフラグメンテーションのサポート。SCTP エンドポイントに複数の IP アドレスが設定された SCTP マルチホーミングのサポート。	9.7(1)	このシステムは、SCTP マルチストリーミングの並べ替え、リアセンブル、およびフラグメンテーションを完全にサポートしており、これにより SCTP トラフィックに対する Diameter および M3UA インスペクションの有効性が改善されています。このシステムは、各エンドポイントに複数の IP アドレスが設定された SCTP マルチホーミングもサポートしています。マルチホーミングでは、セカンデリ アドレスに必要なピンホールをシステムが開くので、セカンデリ アドレスを許可するためのアクセス ルールをユーザーが設定する必要はありません。SCTP エンドポイントは、それぞれ 3 つの IP アドレスに制限する必要があります。 **show sctp detail** コマンドの出力が変更されました。

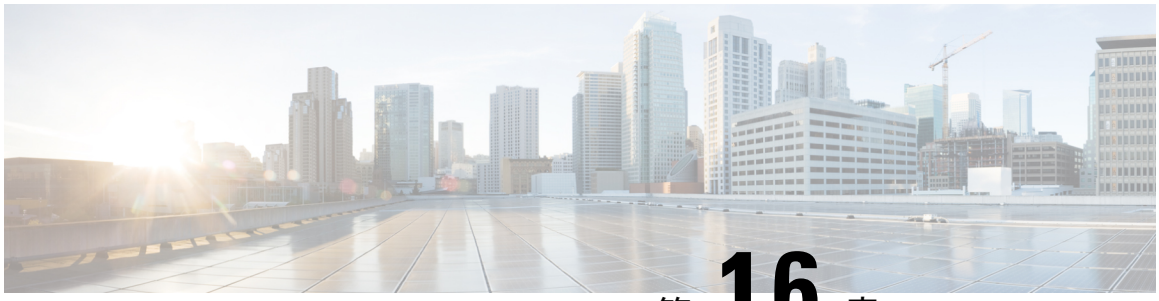
機能名	リリース	機能情報
M3UA インスペクションの改善。	9.7(1)	M3UAインスペクションは、ステートフル フェールオーバー、半分散クラスタリング、およびマルチホーミングをサポートするようになりました。また、アプリケーション サーバー プロセス（ASP）の状態の厳密な検証や、さまざまなメッセージの検証も設定できます。ASP状態の厳密な検証は、ステートフル フェールオーバーとクラスタリングに必要です。 次のコマンドが追加または変更されました。**clear service-policy inspect m3ua session** [**assocID** *id*]、**match port sctp**、**message-tag-validation**、**show service-policy inspect m3ua drop**、**show service-policy inspect m3ua endpoint**、**show service-policy inspect m3ua session**、**show service-policy inspect m3ua table**、**strict-asp-state**、**timeout session**。
TLS プロキシ サーバーの SSL 暗号スイートの設定サポート	9.8(1)	ASA が TLS プロキシ サーバーとして動作している場合は、SSL 暗号スイートを設定できるようになりました。以前は、 **ssl cipher** コマンドを使用した ASA のグローバル設定のみが可能でした。 次のコマンドが導入されました。 **server cipher-suite**
MSISDN および選択モードのフィルタリング、アンチリプレイ、およびユーザー スプーフィング保護に対する GTP インスペクションの機能拡張。	9.10(1)	モバイル ステーション国際サブスクライバ電話番号（MSISDN）または選択モードに基づいて PDP コンテキストの作成メッセージをドロップするようにGTPインスペクションを設定できるようになりました。また、アンチリプレイとユーザー スプーフィング保護も実装できます。 **anti-replay**、**gtp-u-header-check**、**match msisdn**、**match selection-mode** の各コマンドが追加されました。
GTPv1 リリース 10.12 のサポート	9.12(1)	システムで GTPv1 リリース 10.12 がサポートされるようになりました。以前は、リリース 6.1 がサポートされていました。新しいサポートでは、25 件の GTPv1 メッセージおよび 66 件の情報要素の認識が追加されています。 さらに、動作の変更もあります。不明なメッセージ ID が許可されるようになりました。以前は、不明なメッセージはドロップされ、ログに記録されていました。 追加または変更されたコマンドはありません。

機能名	リリース	機能情報
モバイル端末の場所のロギング（GTPインスペクション）。	9.13(1)	GTPインスペクションを設定すると、モバイル端末の初期の場所とそれ以降の場所の変更をログに記録できます。場所の変更を追跡すると、不正なローミング請求を識別するのに役立つ場合があります。 **location-logging** コマンドが追加されました。
GTPv2およびGTPv1リリース15がサポートされています。	9.13(1)	システムでGTPv2 3GPP 29.274 V15.5.0がサポートされるようになりました。GTPv1の場合、3GPP 29.060 V15.2.0までサポートしています。新しいサポートでは、2件のメッセージおよび53件の情報要素の認識が追加されています。 追加または変更されたコマンドはありません。
GTPインスペクションでドロップされるIMSIプレフィックスを指定する機能です。	9.16(1)	GTP インスペクションでは、許可する Mobile Country Code/Mobile Network Code（MCC/MNC）の組み合わせを識別するために、IMSI プレフィックス フィルタリングを設定できます。ドロップするMCC/MNCの組み合わせに対してIMSI フィルタリングを実行できるようになりました。これにより、望ましくない組み合わせをリストにして、デフォルトで他のすべての組み合わせを許可することができます。 **drop mcc** コマンドが追加されました。
キャリアライセンスのSecure Firewall 3100サポート	9.18(1)	キャリアライセンスは、Diameter、GTP/GPRS、SCTP検査を有効にします。 新規/変更されたコマンド： **feature carrier**

第 V 部

接続管理と脅威の検出

- 接続設定 （459 ページ）
- QoS （499 ページ）
- 脅威の検出 （513 ページ）



第 16 章

接続設定

この章では、ASA を経由する接続用、または、ASA を宛先とする管理接続用の接続を設定する方法について説明します。

- 接続の設定 （459 ページ）
- 接続の設定 （460 ページ）
- 接続のモニタリング （493 ページ）
- 接続設定の履歴 （494 ページ）

接続の設定

接続設定とは、デバイスを介した接続を管理するさまざまな機能のことを指します。

接続設定タイプ

接続設定には、次のようなタイプがあります。

- **さまざまなプロトコルのグローバルタイムアウト**：すべてのグローバルタイムアウトにデフォルト値があります。早期に接続が失われる場合にのみ、デフォルト値を変更してください。
- **トラフィック クラスごとの接続タイムアウト**：サービス ポリシーを使用して、特定のタイプのトラフィックのグローバル タイムアウトを上書きできます。すべてのトラフィック クラスのタイムアウトにデフォルト値があるため、それらの値を設定する必要はありません。
- **接続制限と TCP 代行受信**：デフォルトでは、ASA を経由する（または宛先とする）接続の数に制限はありません。サービスポリシールールを使用して、特定の通信クラスの制限を設定します。これにより、サービス妨害（DoS）攻撃からサーバーが保護されます。特に、初期接続（TCP ハンドシェイクを完了していない初期接続）に制限を設定できます。これにより、SYN フラッディング攻撃から保護されます。初期接続の制限を超えると、プロキシ接続とスロットル攻撃に対して TCP 代行受信コンポーネントがアクティブになります。

- **Dead Connection Detection（DCD; デッド接続検出）**：有効でありながらアイドル状態になることが多い永続的な接続がある場合は、DCD を有効にします。アイドルタイムアウト設定を超えると、これらの接続が閉じられることがあります。DCD では、アイドル状態ではあるものの有効な接続を特定し、アイドルタイマーをリセットすることでそれらの接続を維持します。アイドル時間を超えるたびに、DCD は接続の両側にプローブを送信して、接続が有効であることを両側で合意しているかどうかを確認します。**show service-policy** コマンドの出力には、DCD からのアクティビティ量を示すためのカウンタが含まれます。**show conn detail** コマンドを使用すると、発信側と受信側の情報およびプローブの送信頻度を取得できます。
- **TCP シーケンスのランダム化**：それぞれの TCP 接続には 2 つの ISN（初期シーケンス番号）が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバーで生成されます。デフォルトでは、ASA は、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。ランダム化により、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。ただし、TCP シーケンスのランダム化は、TCP SACK（選択的確認応答）を実質的に破棄します。クライアントが認識するシーケンス番号がサーバーが認識するものと異なるためです。必要に応じて、トラフィック クラスごとにランダム化を無効化することができます。
- **TCP 正規化**：TCP ノーマライザは、異常なパケットから保護します。一部のタイプのパケット異常をトラフィック クラスで処理する方法を設定できます。
- **TCPステートバイパス**：ネットワークで非対称ルーティングを使用するかどうかをチェックする TCP ステートをバイパスできます。
- **SCTP ステートバイパス**：Stream Control Transmission Protocol（SCTP）プロトコル検証が必要なければ、SCTP のステートフル インスペクションをバイパスできます。
- **フローのオフロード**：フローがNIC自体で切り替えられる超高速パスにオフロードされるトラフィックを識別して選択できます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。
- **IPsec フローのオフロード**：IPsec サイト間 VPN またはリモートアクセス VPN セキュリティアソシエーション（SA）の初期設定後、IPsec接続はデバイスのフィールドプログラマブルゲートアレイ（FPGA）にオフロードされるため、デバイスのパフォーマンスが向上します。この機能をサポートするプラットフォームでは、デフォルトで有効になっています。

接続の設定

接続制限、タイムアウト、TCP正規化、TCPシーケンスのランダム化、存続可能時間（TTL）のデクリメントには、ほとんどのネットワークに適切なデフォルト値があります。これらの接続の設定が必要となるのは、独自の要件があり、ネットワークに特定のタイプの設定がある場合、または早期のアイドル タイムアウトによる異常な接続切断が発生した場合のみです。

その他の接続関連機能は無効になっています。これらのサービスは、一般的なサービスとしてではなく、特定のトラフィック クラスにのみ設定します。これらの機能には次のものが含まれています：TCP 代行受信、TCP ステート バイパス、Dead Connection Detection（DCD; デッド接続検出）、SCTP ステート バイパス、フロー オフロード。

次の一般的な手順では、考えられるすべての接続の設定について説明します。必要に応じて実装する設定を選んでください。

始める前に

パケットがデバイスに入ると、ファイアウォールはまずアクセス制御ルールおよび NAT を評価して、接続エントリを作成する必要があるかどうかを判断します。接続エントリは、ネクストホップ用の ARP エントリが存在するかどうかに関係なく作成されます。このため、接続が存在しても、その接続範囲内のパケットがデバイスを通過することを意味するものではありません。アイドルタイムアウトなどの接続の設定は、不要な接続が残ってシステムリソースを占有しないようにします。

手順

ステップ 1 グローバル タイムアウトの設定（462 ページ）。これらの設定は、デバイスを通過するすべてのトラフィックに対してさまざまなプロトコルのデフォルトのアイドル タイムアウトを変更します。早期のタイムアウトによりリセットされる接続に問題がある場合は、まずグローバル タイムアウトを変更してください。

ステップ 2 SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信）（464 ページ）。この手順を使用して、TCP 代行受信を設定します。

ステップ 3 異常な TCP パケット処理のカスタマイズ（TCP マップ、TCP ノーマライザ）（467 ページ）（特定のトラフィック クラスについてデフォルトの TCP 正規化の動作を変更する場合）。

ステップ 4 非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス）（472 ページ）（このタイプのルーティング環境がある場合）。

ステップ 5 TCP シーケンスのランダム化の無効化（476 ページ）（デフォルトのランダム化が特定の接続データをスクランブルしている場合）。

ステップ 6 大規模フローのオフロード（478 ページ）（コンピューティング集約型のデータセンターのパフォーマンスを改善する必要がある場合）。

ステップ 7 特定のトラフィック クラスの接続の設定（すべてのサービス）（486 ページ）。これは、接続の設定用の汎用手順です。これらの設定は、サービス ポリシー ルールを使用して、特定のトラフィック クラスのグローバルのデフォルト値を上書きできます。これらのルールを使用して、TCP ノーマライザのカスタマイズ、TCP シーケンスのランダム化の変更、パケットの存続可能時間のデクリメント、およびその他のオプション機能の実装も行います。

ステップ 8 TCP オプションの構成（492 ページ）（他の標準的な TCP 動作をリセットまたは変更する必要がある場合）。

グローバル タイムアウトの設定

さまざまなプロトコルの接続スロットと変換スロットのグローバル アイドル タイムアウト期間を設定できます。指定したアイドル時間の間スロットが使用されなかった場合、リソースはフリー プールに戻されます。

グローバル タイムアウトを変更すると、サービス ポリシーによる特定のトラフィック フロー用に上書きできる新しいデフォルトのタイムアウトが設定されます。

特定のタイムアウトを設定できないプロトコル（GREなど）では、アイドルタイムアウトは2分です。

手順

timeout コマンドを使用して、グローバル タイムアウトを設定します。

すべてのタイムアウト値の形式は *hh*:*mm*:*ss* で、最大期間はほとんどの場合 1193:0:0 です。すべてのタイムアウトをデフォルト値にリセットするには、**clear configure timeout** コマンドを使用します。単に 1 つのタイマーをデフォルトにリセットする場合は、その設定の **timeout** コマンドをデフォルト値とともに入力します。

タイマーをディセーブルにするには、値に **0** を使用します。

次のグローバル タイムアウトを構成できます。

- **timeout conn** *hh*:*mm*:*ss*：接続を閉じるまでのアイドル時間（0:5:0 ～ 1193:0:0）。デフォルトは 1 時間（1:0:0）です。
- **timeout half-closed** *hh*:*mm*:*ss*：TCP ハーフクローズ接続を閉じるまでのアイドル時間。FIN と FIN-ACK の両方が検出された場合、接続はハーフクローズ状態と見なされます。FIN のみが検出された場合は、通常の **conn** タイムアウトが適用されます。最小値は 30 秒です。デフォルトは 10 分です。
- **timeout udp** *hh*:*mm*:*ss*：UDP 接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。
- **timeout icmp** *hh*:*mm*:*ss*：ICMP のアイドル時間（0:0:2 ～ 1193:0:0）。デフォルトは 2 秒（0:0:2）です。
- **timeout icmp-error** *hh*:*mm*:*ss*：ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間で、0:0:0 から 0:1:0 の間、または **timeout icmp** 値のいずれか低い方です。デフォルトは 0（ディセーブル）です。このタイムアウトが無効で、ICMP インスペクションを有効にすると、ASA では、エコー応答が受信されるとすぐに ICMP 接続を削除します。したがってその（すでに閉じられた）接続用に生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信できます。
- **timeout sunrpc** *hh*:*mm*:*ss*：SunRPC スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 10 分です。

- **timeout H323** *hh*:*mm*:*ss*：H.245（TCP）および H.323（UDP）メディア接続を閉じるまでのアイドル時間（0:0:0 ～ 1193:0:0）。デフォルトは 5 分（0:5:0）です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。
- **timeout h225** *hh*:*mm*:*ss*：H.225 シグナリングリ接続を閉じるまでのアイドル時間。H.225 のデフォルト タイムアウトは 1 時間（1:0:0）です。すべての呼び出しがクリアされた後に接続をすぐにクローズするには、値を 1 秒（0:0:1）にすることを推奨します。
- **timeout mgcp** *hh*:*mm*:*ss*：MGCP メディア接続を削除するまでのアイドル時間（0:0:0 ～ 1193:0:0）。デフォルトは、5 分（0:5:0）です。
- **timeout mgcp-pat** *hh*:*mm*:*ss*：MGCP PAT 変換を削除するまでの絶対間隔（0:0:0 ～ 1193:0:0）。デフォルトは 5 分（0:5:0）です。最小時間は 30 秒です。
- **timeout sctp** *hh*:*mm*:*ss*：Stream Control Transmission Protocol（SCTP）接続を閉じるまでのアイドル時間（0:1:0 ～ 1193:0:0）。デフォルトは 2 分（0:2:0）です。
- **timeout sip** *hh*:*mm*:*ss*：SIP シグナリング ポート接続を閉じるまでのアイドル時間（0:5:0 ～ 1193:0:0）。デフォルトは、30 分（0:30:0）です。
- **sip-callinit-timeout** *hh*:*mm*:*ss*：Call_Init コール状態の SIP セッションが（最初の招待メッセージの受信後）削除されるまでのアイドル時間（つまり応答を受信しなかった場合）。0:0:1～1193:0:0 の範囲で指定します。デフォルト値は 32 秒（0:00:32）です。
- **timeout sip_media** *hh*:*mm*:*ss*：SIP メディア ポート接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。SIP メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
- **timeout sip-provisional-media** *hh*:*mm*:*ss*：SIP 暫定メディア接続のタイムアウト値（0:1:0 ～ 0:30:0）。デフォルトは 2 分です。
- **timeout sip-invite** *hh*:*mm*:*ss*：暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間（0:1:0 ～ 00:30:0）。デフォルトは、3 分（0:3:0）です。
- **timeout sip-disconnect** *hh*:*mm*:*ss*：CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間（0:0:1 ～ 00:10:0）。デフォルトは 2 分（0:2:0）です。
- **timeout uath** *hh*:*mm*:*ss* {**absolute** | **inactivity**}：認証および認可キャッシュがタイムアウトし、ユーザーが次回接続時に再認証が必要となるまでの継続時間（0:0:0 ～ 1193:0:0）。デフォルトは 5 分（0:5:0）です。デフォルトのタイマーは **absolute** です。**inactivity** キーワードを入力すると、非アクティブになってから一定の期間後にタイムアウトが発生するように設定できます。uauth 継続時間は、xlate 継続時間より短く設定する必要があります。キャッシュをディセーブルにするには、0 に設定します。接続に受動 FTP を使用している場合、または Web 認証に virtual http コマンドを使用している場合は、0 を使用しないでください。

- **timeout xlate** *hh*:*mm*:*ss*：変換スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。
- **timeout pat-xlate** *hh*:*mm*:*ss*：PAT 変換スロットが解放されるまでのアイドル時間（0:0:30 ～ 0:5:0）。デフォルトは 30 秒です。前の接続がアップストリーム デバイスで引き続き開いている可能性があるため、開放された PAT ポートを使用する新しい接続をアップストリーム ルータが拒否する場合、このタイムアウトを増やすことができます。
- **timeout tcp-proxy-reassembly** *hh*:*mm*:*ss*：リアセンブリのためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウト（0:0:10 ～ 1193:0:0）。デフォルトは、1 分（0:1:0）です。
- **timeout floating-conn** *hh*:*mm*:*ss*：同じネットワークへの複数のルートが存在し、それぞれメトリックが異なる場合は、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。より良いルートを使用できるようにするには、タイムアウト値を 0:0:30 ～ 1193:0:0 の間で設定します。
- **timeout conn-holddown** *hh*:*mm*:*ss*：接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。接続ホールドダウン タイマーの目的は、ルートが発生してすぐにダウンする可能性がある場合に、ルート フラッピングの影響を減らすことです。ルートの収束がもっと早く発生するようにホールドダウン タイマーを減らすことができます。デフォルトは 15 秒です。指定できる範囲は 00:00:00 ～ 00:00:15 です。
- **timeout igp stale-route** *hh*:*mm*:*ss*：古いルートをルータの情報ベースから削除する前に保持する時間。これらのルートは OSPF などの内部ゲートウェイ プロトコル用です。デフォルトは 70 秒（00:01:10）です。指定できる範囲は 00:00:10 ～ 00:01:40 です。

SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信）

攻撃者が一連の SYN パケットをホストに送信すると、SYN フラッディング サービス妨害（DoS）攻撃が発生します。これらのパケットは通常、スプーフィングされた IP アドレスから発信されます。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、正規ユーザーからの接続要求に対してサービスを提供できなくなります。

SYN フラッディング攻撃を防ぐために初期接続数を制限できます。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

接続の初期接続しきい値を超えると、ASA はサーバーのプロキシとして動作し、その接続がターゲットホストの SYN キューに追加されないように、SYN Cookie 方式を使用してクライアント SYN 要求に対する SYN-ACK 応答を生成します。SYN クッキーは、基本的に秘密を作成するために、MSS、タイムスタンプ、およびその他の項目の数学的ハッシュから構築される SYN-ACK で返される最初のシーケンス番号です。ASA は、正しいシーケンス番号で有効な時

間ウィンドウ内にクライアントから返された ACK を受信すると、クライアントが本物であることを認証し、サーバーへの接続を許可できます。プロキシを実行するコンポーネントは、TCP 代行受信と呼ばれます。

SYN フラッド攻撃からサーバーを保護するためのエンドツーエンド プロセスでは、接続制限を設定し、TCP代行受信の統計情報をイネーブルにし、結果をモニターする必要があります。

始める前に

- 保護するサーバーの TCP SYN バックログ キューより低い初期接続制限を設定していることを確認します。これより高い初期接続制限を設定すると、有効なクライアントが、SYN 攻撃中にサーバーにアクセスできなくなります。初期接続制限に適切な値を決定するには、サーバーの容量、ネットワーク、サーバーの使用状況を入念に分析してください。
- ASA モデル上の CPU コア数によっては、同時接続および初期接続の最大数が、各コアによる接続の管理方法が原因で、設定されている数を超える場合があります。最悪の場合、ASA は最大 *n*-1 の追加接続および初期接続を許可します。ここで、*n* はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。ご使用のモデルのコア数を確認するには、**show cpu core** コマンドを入力します。

手順

ステップ 1 L3/L4 クラスマップを作成して、保護するサーバーを識別します。アクセスリスト一致を使用します。

```
class-map name
match parameter
```

例：

```
hostname(config)# access-list servers extended permit tcp any host 10.1.1.5 eq http
hostname(config)# access-list servers extended permit tcp any host 10.1.1.6 eq http
hostname(config)# class-map protected-servers
hostname(config-cmap)# match access-list servers
```

ステップ 2 クラスマップ トラフィックで実行するアクションを設定するポリシーマップを追加または編集して、クラス マップを指定します。

```
policy-map name
class name
```

例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class protected-servers
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラス マップの場合、この手順ですでに作成したクラスを指定します。

ステップ 3 初期接続制限を設定します。

- **set connection embryonic-conn-max** *n*：許可する同時 TCP 初期接続の最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。
- **set connection per-client-embryonic-max** *n*：許可する同時 TCP 初期接続のクライアントごとの最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。
- **set connection syn-cookie-mss** 初期接続数制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）（48 ～ 65535）。デフォルトは 1380 です。この設定は、**set connection embryonic-conn-max** または **per-client-embryonic-max** を設定する場合にのみ有効です。

例：

```
hostname(config-pmap-c)# set connection embryonic-conn-max 1000
hostname(config-pmap-c)# set connection per-client-embryonic-max 50
```

ステップ 4 既存のサービス ポリシー（global_policy という名前のデフォルト グローバル ポリシーなど）を編集している場合は、このステップを省略できます。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

ステップ 5 TCP 代行受信によって代行受信される攻撃の脅威検出統計情報を設定します。

threat-detection statistics tcp-intercept[**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

それぞれの説明は次のとおりです。

- **rate-interval** *minutes* は、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間隔の間に、ASA は攻撃の数を 30 回サンプリングします。

- **burst-rate** *attacks_per_sec* は、syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。
- **average-rate** *attacks_per_sec* は、syslog メッセージ生成の平均レートしきい値を、25 ～ 2147483647 の範囲で設定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。

例：

```
hostname(config)# threat-detection statistics tcp-intercept
```

ステップ 6 次のコマンドを使用して結果をモニターします。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]：攻撃を受けて保護された上位 10 サーバーを表示します。**all** キーワードは、トレースされているすべてのサーバーの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。
- **clear threat-detection statistics tcp-intercept**：TCP 代行受信の統計情報を消去します。

例：

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
 Time)>
------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

異常な TCP パケット処理のカスタマイズ（TCP マップ、TCP ノーマライザ）

TCP ノーマライザは、異常なパケットを識別します。これは、ASA による検出時に処理（パケットを許可、ドロップ、またはクリア）させることができます。TCP 正規化は、攻撃から ASA を保護するのに役立ちます。TCP 正規化は常にイネーブルになっていますが、機能の一部の動作をカスタマイズできます。

デフォルト コンフィギュレーションには、次の設定が含まれます。

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
```

```
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 18 clear
tcp-options range 20 255 clear
tcp-options md5 allow
tcp-options mss allow
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

TCP ノーマライザをカスタマイズするには、まず、TCP マップを使用して設定を定義します。次に、サービス ポリシーを使用して、選択したトラフィック クラスにマップを適用できます。

手順

ステップ 1 確認する TCP 正規化基準を指定するための TCP マップを作成します。**tcp-map** *tcp-map-name*

ステップ 2 次の 1 つ以上のコマンドを入力して TCP マップ基準を設定します。入力しないコマンドにはデフォルトが使用されます。設定を無効化するには、コマンドの **no** 形式を使用します。

- **check-retransmission**：一貫性のない TCP 再送信を防止します。このコマンドは、デフォルトでディセーブルになっています。
- **checksum-verification**：TCP チェックサムを検証し、検証に失敗したパケットをドロップします。このコマンドは、デフォルトでディセーブルになっています。
- **exceed-mss** {**allow** | **drop**}：データ長が TCP 最大セグメント サイズを超えるパケットを許可またはドロップします。デフォルトでは、パケットを許可します。
- **invalid-ack** {**allow** | **drop**}：無効な ACK を含むパケットを許可またはドロップします。デフォルトでは、パケットをドロップします（パケットが許可される WAAS 接続を除く）。次のような場合に無効な ACK が検出される可能性があります。
  - TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。
  - 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。
- **queue-limit** *pkt_num* [**timeout** *seconds*]：バッファに格納して TCP 接続の正しい順序に設定できる、異常なパケットの最大数を設定します。1 ～ 250 パケットです。デフォルト値の 0 は、この設定がディセーブルであり、トラフィックのタイプに応じたデフォルトのシステム キュー制限が使用されることを意味します。

- アプリケーション インスペクション（**inspect** コマンド）、、および TCP インスペクション再送信（TCP マップ **check-retransmission** コマンド）のための接続のキュー制限は、3 パケットです。ASA が異なるウィンドウ サイズの TCP パケットを受信した場合は、アドバタイズされた設定と一致するようにキュー制限がダイナミックに変更されます。
- 他の TCP 接続の場合は、異常なパケットはそのまま通過します。

queue-limit コマンドを 1 以上に設定した場合、すべての TCP トラフィックに対して許可される異常なパケットの数は、この設定と一致します。たとえば、アプリケーションインスペクション、および TCP check-retransmission のトラフィックの場合、TCP パケットからアドバタイズされたすべての設定が**キュー制限**設定を優先して、無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。

timeout *seconds* 引数は、異常なパケットがバッファ内に留まることができる最大時間を設定します。設定できる値は 1 ～ 20 秒です。タイムアウト期間内に正しい順序に設定されて渡されなかったパケットはドロップされます。デフォルトは 4 秒です。*pkt_num* 引数を 0 に設定した場合は、どのトラフィックのタイムアウトも変更できません。**timeout** キーワードを有効にするには、制限を 1 以上に設定する必要があります。

- **reserved-bits** {**allow** | **clear** | **drop**}：TCP ヘッダーの予約ビットに対するアクションを設定します。パケットを**許可**するか（ビットを変更せずに）、ビットを**クリア**してパケットを許可するか、またはパケットを**ドロップ**できます。
- **seq-past-window** {**allow** | **drop**}：パストウィンドウ シーケンス番号を含むパケットに対するアクションを設定します。つまり、受信した TCP パケットのシーケンス番号が、TCP 受信ウィンドウの右端より大きい場合です。**queue-limit** コマンドを 0（ディセーブル）に設定した場合にのみ、パケットを**許可**できます。デフォルトでは、パケットをドロップします。
- **synack-data** {**allow** | **drop**}：データを含む TCP SYNACK パケットを許可またはドロップします。デフォルトは、パケットのドロップです。
- **syn-data** {**allow** | **drop**}：データを含む SYN パケットを許可またはドロップします。デフォルトでは、パケットを許可します。
- **tcp-options** {**md5** |**mss** |**selective-ack** |**timestamp** |**window-scale** | **range** *lowerupper*} *action*：TCP オプションを使用してパケットのアクションを設定します。これらのオプションには**md5**、**mss**、**selective-ack**（選択的確認応答メカニズム）、**timestamp**、および**window-scale**（ウィンドウ スケール メカニズム）という名前が付いています。その他のオプションでは、**range** キーワードで数値を使用してオプションを指定します。範囲の制限は 6 ～ 7、9 ～ 18、20 ～ 255 です。数字別に単一オプションをターゲットにするには、上下の範囲に同じ数字を入力します。マップでコマンドを複数回入力することで、ポリシー全体を定義できます。TCP 接続をインスペクションする場合、設定に関係なく MSS オプションと選択的応答確認（SACK）オプションを除き、すべてのオプションがクリアされます。選択可能なアクションは、次のとおりです。

- **allow**[**multiple**]：このタイプの単一オプションを含むパケットを許可します。これは、すべての名前付きオプションのデフォルトです。オプションのインスタンスが複数含まれていてもパケットを許可する場合は、**multiple** キーワードを追加します。（**multiple** キーワードは **range** では使用できません。）
- **maximum** *limit*：**mss** のみ。最大セグメントサイズを指示された制限に設定します（68 ～ 65535）。デフォルトの TCP MSS は、**sysopt connection tcpmss** コマンドで定義されます。
- **clear**：このタイプのオプションをヘッダーから削除し、パケットを許可します。これは、すべての番号付きオプションのデフォルトです。タイムスタンプオプションを消去すると、PAWS と RTT がディセーブルになります。
- **drop**：このオプションを含むパケットをドロップします。このアクションは、**md5** および **range** でのみ使用可能です。

最初の TCP ハンドシェイク中にタイムスタンプオプションが存在する場合、TCP ノーマライザはタイムスタンプデータベースを維持します。タイムスタンプの値は、クライアントとサーバー間のタイムスタンプオプションの交換によって異なります。通信ギャップがある場合、またはサーバーが突然タイムスタンプオプションの送信を開始した場合、PAWS（ラップシーケンス番号に対する保護）チェックでエラーが発生する可能性があります。PAWS チェックが失敗すると、ASA はパケットをドロップし、最新のタイムスタンプ値を含む ACK を相手側に送信します。

- **ttl-evasion-protection**：接続の最大 TTL を最初のパケットで TTL によって決定させます。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。これによって、TTL を回避した攻撃から保護します。デフォルトでは、TTL 回避保護がイネーブルになっているため、このコマンドの **no** 形式を入力するだけです。

  たとえば、攻撃者は TTL を非常に短くしてポリシーを通過するパケットを送信できます。TTL がゼロになると、ASA とエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、ASA にとって再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。

- **urgent-flag** {**allow** | **clear**}：URG フラグを含むパケットに対するアクションを設定します。パケットを**許可**するか、フラグを**クリア**してパケットを許可できます。デフォルトでは、フラグをクリアします。

  URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈が明確にされていません。そのため、エンドシステムは緊急オフセットをさまざまな方法で処理しており、これが攻撃に対する脆弱性になることがあります。

- **window-variation** {**allow** | **drop**}：予期せずにウィンドウ サイズが変更された接続を許可またはドロップします。デフォルトでは、接続を許可します。

ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。

ステップ 3 サービス ポリシーを使用して、TCP マップをトラフィック クラスに適用します。

a) L3/L4 クラスマップを使用してトラフィック クラスを定義し、そのマップをポリシーマップに追加します。

```
class-map name
match parameter
policy-map name
class name
```

例：

```
hostname(config)# class-map normalization
hostname(config-cmap)# match any
hostname(config)# policy-map global_policy
hostname(config-pmap)# class normalization
```

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラスマップの照合ステートメントの詳細については、通過トラフィック用のレイヤ 3/4 クラス マップの作成 （282 ページ）を参照してください。

b) TCP マップを適用します：**set connection advanced-options** *tcp-map-name*

例：

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

c) 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

例

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス）

TCP ステートバイパスを使用すると、通信は ASA デバイスでステートフル インスペクション チェックをバイパスできます。

導入の考慮事項

ネットワークに非対称ルーティング環境があり、特定の接続のアウトバウンドフローとインバウンドフローが 2 つの異なる ASA デバイスを通過できる場合は、影響を受ける通信に対する TCP ステートバイパスを導入する必要があります。

ただし、TCP ステートバイパスによってネットワークのセキュリティが弱体化するため、非常に詳細に限定された通信クラスでバイパスを適用する必要があります。

非対称ルーティングの問題

非対称ルーティングの問題は、接続の戻り通信がアウトバウンド通信とは別のファイアウォールを通過する場合に発生します。この場合、パケットは高速パステーブルの既存の接続エントリと一致しないため、ドロップされます。

通信検査と高速パス動作

デフォルトでは、ASA は適応型セキュリティアルゴリズムを使用してすべての通信を検査します。ASA は、セキュリティポリシーに基づいて通信を許可するかドロップします。ASA は、各パケットの状態（新しい接続または確立された接続）を確認することにより、ファイアウォールのパフォーマンスを最大限まで高めます。新しい接続 SYN パケットをセッション管理パスに、確立された接続を高速パスに、そして詳細な検査が必要なパケットをコントロールプレーンパスに割り当てます。

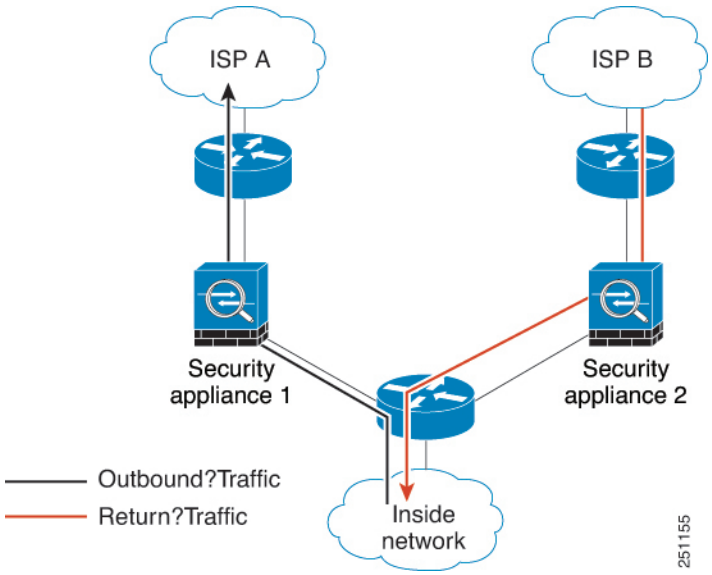
ASA は、既存の接続に一致する TCP パケットがセキュリティポリシーのあらゆる面の再検査を受けることなく高速パスを介して通過することを許可します。この機能により、パフォーマ

ンスが向上します。ただし、高速パス確立方式は、非対称ルーティングソリューションと干渉する可能性があります。この方式では SYN パケットを使用し、TCP シーケンス番号検証などのチェックを実行します。接続のアウトバウンドフローとインバウンドフローの両方が同じ ASA デバイスを通過する必要があります。

非対称ルーティングシナリオ

たとえば、ある新しい接続がセキュリティ アプライアンス 1 に到達するとします。SYNパケットはセッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続パケットがセキュリティ アプライアンス 1 を通過した場合、高速パス内のエントリに一致するのでこのパケットは送信されます。ただし、後続のパケットがセキュリティアプライアンス 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、セキュリティアプライアンス 2 はパケットをドロップします。次の図は、非対称ルーティングの例を示したもので、アウトバウンドトラフィックはインバウンドトラフィックとは異なる ASA を通過しています。

図 *44* : 非対称ルーティング



アップストリームルータに非対称ルーティングが設定されており、通信が 2 つの ASA デバイスを通過することがある場合は、特定の通信に対して TCP ステートバイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションを無効化します。この機能では、UDP 接続と同じように TCP 通信が処理されます。指定されたネットワークと一致した非 SYN パケットが ASA デバイスに入った時点で高速パスエントリが存在しない場合、高速パスで接続を確立するために、そのパケットはセッション管理パスを通過します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

TCP ステートバイパスのガイドラインと制限事項

TCP ステートバイパスでサポートされない機能

TCP ステートバイパスを使用するときは、次の機能はサポートされません。

- アプリケーションインスペクション：インスペクションでは、着信トラフィックと発信トラフィックの両方が同じ ASA を通過する必要があるため、インスペクションは TCP ステート バイパス トラフィックに適用されません。
- AAA 認証セッション：ユーザーがある ASA で認証される場合、他の ASA 経由で戻るトラフィックは、その ASA でユーザーが認証されていないため、拒否されます。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号ランダム化：ASAでは接続の状態が追跡されないため、これらの機能は適用されません。
- TCP 正規化：TCP ノーマライザはディセーブルです。

TCP ステートバイパスの NAT ガイドライン

変換セッションはデバイスごとに個別に確立されるため、TCP ステート バイパス トラフィック用に両方のデバイスでスタティック NAT を設定する必要があります。ダイナミック NAT を使用すると、デバイス 1 でのセッションに選択されるアドレスは、デバイス 2 でのセッションに選択されるアドレスとは異なります。

TCP ステート バイパスの設定

非対称ルーティング環境で TCP ステートチェックをバイパスするには、影響を受けるホストまたはネットワークのみに適用するトラフィッククラスを注意深く定義してから、サービスポリシーを使用してトラフィッククラスで TCP ステートバイパスを有効にします。バイパスによってネットワークのセキュリティが低下するため、そのアプリケーションをできるだけ制限します。

始める前に

特定の接続に 2 分間トラフィックがない場合、接続はタイムアウトします。このデフォルトは、**set connection timeout idle** コマンドを TCP ステート バイパス トラフィック クラスに使用するとオーバーライドできます。通常の TCP 接続は、デフォルトで 60 分後にタイムアウトします。

手順

ステップ 1 L3/L4 クラスマップを作成して、TCPステートバイパスを必要とするホストを識別します。アクセス リスト一致を使用して、送信元と宛先のホストを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# access-list bypass extended permit tcp host 10.1.1.1 host 10.2.2.2
hostname(config)# class-map bypass-class
hostname(config-cmap)# match access-list bypass
```

ステップ 2 クラスマップ トラフィックで実行するアクションを設定するポリシーマップを追加または編集して、クラス マップを指定します。

```
policy-map name
class name
```

例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class bypass-class
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラス マップの場合、この手順ですでに作成したクラスを指定します。

ステップ 3 クラスで TCP ステート バイパスを有効にします：**set connection advanced-options tcp-state-bypass**

ステップ 4 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

例

TCP ステート バイパスの設定例を次に示します。

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224
any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass
```

```
hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

TCP シーケンスのランダム化の無効化

各 TCP 接続には、クライアントで生成される ISN とサーバーで生成される ISN の 2 つの ISN があります。ASA は、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。ただし、TCP シーケンスのランダム化は、TCP SACK（選択的確認応答）を実質的に破棄します。クライアントが認識するシーケンス番号がサーバーが認識するものと異なるためです。

たとえば、データがスクランブルされるため、必要に応じて TCP 初期シーケンス番号ランダム化を無効化することができます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- ASA で eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- ASA で接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- ISA 3000 のハードウェア バイパスを有効にします。ISA 3000 がデータ パスの一部でなくなると、TCP 接続はドロップされます。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

手順

ステップ 1 L3/L4 クラスマップを作成して、TCP シーケンス番号をランダム化しないトラフィックを識別します。クラス マップは、TCP トラフィック用にします。TCP ポート一致を行う特定のホストを識別したり（ACL を使用して）、任意のトラフィックと照合したりすることができます。

class-map *name*

match *parameter*

例：

```
hostname(config)# access-list preserve-sq-no extended permit tcp any host 10.2.2.2
hostname(config)# class-map no-tcp-random
hostname(config-cmap)# match access-list preserve-sq-no
```

ステップ 2 クラスマップ トラフィックで実行するアクションを設定するポリシーマップを追加または編集して、クラス マップを指定します。

policy-map *name*
class *name*

例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class no-tcp-random
```

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラス マップの場合、この手順ですでに作成したクラスを指定します。

ステップ 3 クラスで TCP シーケンス番号ランダム化をディセーブルにします。

set connection random-sequence-number disable

後でオンに戻す場合は、「disable」を **enable** に置き換えます。

ステップ 4 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

大規模フローのオフロード

データセンターのサポートされているデバイス上でCisco ASAを展開する場合は、超高速パスにオフロードするトラフィックを識別して、トラフィックがNIC自身でスイッチングされるようにできます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

- ハイパフォーマンス コンピューティング（HPC）調査サイト。ここでは、ASAはストレージと高コンピューティング ステーション間で展開されます。1 つの調査サイトが NFS 経由のFTPファイル転送またはファイル同期を使用してバックアップを行うと、大量のデータ トラフィックが ASA 上のすべてのコンテキストに影響を与えます。NFS を介する FTP ファイル転送およびファイル同期のオフロードによって、他のトラフィックへの影響が軽減されます。
- 主にコンプライアンス目的で使用される High Frequency Trading（HFT）。ここでは、ASA はワークステーションと Exchange 間で展開されます。セキュリティは通常は問題にはなりませんが、遅延は大きな問題です。

オフロードされる前に、ASA は接続の確立時にアクセス ルールやインスペクションなどの通常のセキュリティ処理を最初に適用します。ASAのセッションも切断されます。ただし、一旦接続が確立されると、オフロードされる資格があれば、さらなる処理が ASA ではなく NIC で行われます。

オフロードされたフローは、基本的な TCP フラグとオプションのチェック、設定した場合にはチェックサムの確認などの、制限されたステートフルインスペクションを受信し続けます。システムは必要に応じてさらなる処理のためにファイアウォール システムへのパケットを選択的に増やすことができます。

オフロードが可能なフローを識別するには、フロー オフロード サービスを適用するサービス ポリシー ルールを作成します。一致するフローはその後、次の条件を満たす場合にオフロードされます。

- IPv4 アドレスのみ。
- TCP、UDP、GRE のみ。
- 標準または 802.1Q タグ付きイーサネット フレームのみ。
- （トランスペアレント モードのみ。）インターフェイスを 2 つだけ含むブリッジ グループのマルチキャスト フロー。

オフロードされたフローのリバース フローもオフロードされます。

フローオフロード導入の制約事項

デバイスによる制限

この機能は、以下のデバイスでサポートされています。

- Cisco Secure Firewall 3100 （静的のみ）

- Cisco Secure Firewall 4200 （静的のみ）
- Firepower 4100/9300

オフロードできないフロー

次のフロータイプをオフロードしようとしないでください。

- IPv6 アドレッシングなど、IPv4 アドレッシングを使用しないフロー。
- TCP、UDP、GRE 以外のプロトコルに対するフロー。

（注） PPTP GRE 接続はオフロードできません。

- インスペクションが必要なフロー。FTP など場合によっては、コントロール チャネルはオフロードできませんがセカンダリ データ チャネルはオフロードできます。
- デバイスで終端する IPsec および TLS/DTLS VPN 接続。
- ルーテッド モードのマルチキャスト フロー。
- 3 つ以上のインターフェイスがあるブリッジ グループに対するトランスペアレント モードのマルチキャスト フロー。
- TCP インターセプト フロー。
- TCP ステートバイパスフロー。同じトラフィックにフローオフロードと TCP ステートバイパスを設定することはできません。
- AAA カットスループロキシフロー。
- Vpath、VXLAN 関連のフロー。
- セキュリティ グループでタグ付けされたフロー。
- クラスターで非対称フローが発生した場合に備えて、別のクラスターノードから転送されるリバースフロー。
- クラスタ内の一元化されたフロー（フローのオーナーが制御ユニットでない場合）。

その他の制限事項

フローオフロードを導入する場合は、次の運用上の制約事項を考慮してください。

- フローオフロードとデッド接続検出（DCD）は互換性がありません。オフロードできる接続に DCD を設定しないでください。
- フローオフロード条件に一致する複数のフローが、ハードウェア上の同じ場所に同時にオフロードするキューに入っている場合、最初のフローのみがオフロードされます。他のフ

ローは通常どおりに処理されます。これをコリジョン（衝突）といいます。この状況の統計を表示するには、CLI で **show flow-offload flow** コマンドを使用します。

- オフロードされたフローはFXOSインターフェイスを通過しますが、それらのフローの統計は論理デバイスインターフェイスには表示されません。したがって、論理デバイスインターフェイスのカウンタとパケットレートには、オフロードされたフローは反映されません。

オフロードを無効にする条件

フローがオフロードされた後、フロー内のパケットは次の条件を満たす場合にファイアウォール オペレーティング システムに返され、さらに処理されます。

- タイムスタンプ以外の TCP オプションが含まれている。
- フラグメント化されている。
- これらは等コスト マルチパス（ECMP）ルーティングの対象であり、入力パケットは 1 つのインターフェイスから別のインターフェイスに移動する。
- ルーティングテーブルへの変更がフローに適用されます。新しいルートを決定するためにパケットがデバイスに返されます。

フロー オフロードの設定

フローオフロードを設定するには、サービスをイネーブルにしてから、オフロードする対象トラフィックを識別するサービス ポリシーを作成する必要があります。Firepower 4100/9300 の場合： 最初にサービスを有効にするときは、再起動する必要があります。

手順

ステップ 1 フロー オフロード サービスをイネーブルにします。

flow-offload enable

Firepower 4100/9300 の場合：最初にサービスを有効にするときは、再起動する必要があります。

リロードが必要な場合、ヒットレスなモード変更を行うには、クラスタまたはフェールオーバーペアに関して特に考慮すべき事柄があります。

- クラスタリング：最初に制御ノードでコマンドを入力しますが、制御ノードをすぐにリブートしないでください。代わりに、まずクラスタの各ノードをリブートしてから、制御ノードに戻ってリブートします。次に、制御ノード上でオフロードサービスポリシーを設定します。
- フェールオーバー：最初にアクティブユニット上でコマンドを入力しますが、アクティブユニットをすぐにリブートしないでください。代わりに、スタンバイ ユニットをリブート

してから、アクティブ ユニットをリブートします。次に、アクティブ ユニット上でオフロード サービス ポリシーを設定します。

マルチコンテキスト モードでは、フロー オフロードを有効または無効にすると、すべてのコンテキストのフローオフロードが有効または無効になります。コンテキストごとに異なる設定を使用することはできません。

例：

```
ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.

ciscoasa(config)# write memory
ciscoasa(config)# reload
```

ステップ 2 オフロードする対象のトラフィックを識別するサービス ポリシー ルールを作成します。

a) フロー オフロードの対象となるトラフィックを識別する L3/L4 クラス マップを作成します。アクセス リストまたはポートによる照合は最も一般的なオプションです。

```
class-map name
match parameter
```

例：

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
```

b) クラスマップ トラフィックで実行するアクションを設定するポリシーマップを追加または編集して、クラス マップを指定します。

```
policy-map name
class name
```

例：

```
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
```

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラス マップの場合、この手順ですでに作成したクラスを指定します。

c) クラスに対し、フロー オフロードをイネーブルにします。 **set connection advanced-options flow-offload**

d) 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy offload_policy interface outside
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

例

次に、10.1.1.0 255.255.255.224 サブネットからのすべての TCP トラフィックをオフロード対象として分類し、ポリシーを外部インターフェイスにアタッチする例を示します。

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
hostname(config-pmap-c)# set connection advanced-options flow-offload
hostname(config)# service-policy offload_policy interface outside
```

IPSec フローのオフロード

IPsec フローオフロードは、次のようなパフォーマンス最適化機能です。

- 初期セットアップ後にフィールドプログラマブル ゲートアレイ（FPGA）か専用のハードウェアコンポーネントに IPsec 接続をオフロードします。
- ハードウェアで事前復号、復号、事前暗号化、暗号化処理を行うことにより、デバイスのパフォーマンスを向上させます。
- サポートデバイスモデルでデフォルトで有効になっていると同時に、システムソフトウェアが内部フローセキュリティポリシーを処理できるようにします。

IPsec フローオフロードの特性

IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション（SA）の初期セットアップ後、IPsec 接続はデバイスのフィールドプログラマブル ゲートアレイ（FPGA）

にオフロードされます。このプロセスにより、デバイスのパフォーマンスが向上します。Secure Firewall 1200 シリーズでは、デバイスのパフォーマンスを向上させるために、IPsec 接続が Marvell Cryptographic Accelerator（CPT）にオフロードされます。

オフロード操作には、入出力での事前復号および復号処理が含まれます。システムソフトウェアは、内部フロー内の通信にセキュリティポリシーを適用します。

IPsec フローオフロードは、次のデバイスタイプに適用されます。

- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

IPsec フローオフロードは、デバイスの VTI ループバック インターフェイスが有効になっている場合にも使用されます。

IPsec フローオフロードの制限事項

オフロードされない IPsec フローは次のとおりです。

- IKEv1 トンネル。IKEv2 トンネルのみがオフロードされます。IKEv2 は、より強力な暗号をサポートしています。
- ボリュームベースのキー再生成が設定されているフロー。
- 圧縮が設定されているフロー。
- ポストフラグメンテーションが設定されているフロー。
- アンチリプレイ ウィンドウ サイズが 64 ビットではなく、アンチリプレイが無効になっていないフロー。
- AH 形式。ESP または NAT-T 形式のみがサポートされます。
- ファイアウォールフィルタが有効になっているフロー。
- モード：
  - トランスポートモードのフロー。トンネルモードのフローのみがオフロードされます。
  - マルチコンテキストモード。

IPsec フローオフロードの設定

IPsec フローのオフロードは、この機能をサポートするハードウェア プラットフォームではデフォルトで有効になっています。ただし、出力最適化はデフォルトでは有効になっていないため、この機能が必要な場合は構成する必要があります。

始める前に

IPsec フロー オフロードはグローバルに構成されます。選択したトラフィック フローに対して設定することはできません。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

現在の設定状態を表示するには、**show flow-offload ipsec info** コマンドを使用します。

手順

ステップ 1 IPsec フロー オフロードを有効にします。

flow-offload-ipsec

ステップ 2 出力最適化を有効にすることで、データパスを最適化して、単一トンネルフローのパフォーマンスを向上させます。

flow-offload-ipsec egress-optimization

出力最適化の構成は、フロー オフロードとは別です。ただし、出力最適化を有効にしても、IPsec フロー オフロードも有効にしないかぎり無意味です。出力最適化はデフォルトでは有効になっていません。

DTLS 暗号化アクセラレーション

ASA は、特定のファイアウォールモデルの Datagram Transport Layer Security（*DTLS*）暗号化アクセラレーションをサポートします。この機能により、 IPv4 通信と IPv6 通信両方の DTLS で暗号化および復号された通信のスループットが向上します。ASAは、遅延を改善するために、出力暗号化パケットの最適化も実行します。データパスを最適化して、単一トンネルフローのパフォーマンスを向上させます。どちらの機能もデフォルトで有効になっており、DTLS 1.2 でのみ動作します。

サポートされるモデル

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

暗号化アクセラレータの詳細

Cisco Secure Firewall 3100 および 4200 では、FPGA および Nitrox V 暗号化アクセラレータが DTLS 暗号化アクセラレーションをサポートします。

DTLS 暗号化アクセラレーション

デフォルトでは、DTLS 暗号化アクセラレーションは有効になっています。必要に応じて無効にできます。

Cisco ASA は、以下の条件下では DTLS 暗号化アクセラレーションを実行しません。

- フローが DTLS 1.0 またはパケット圧縮を使用している。
- DTLS キーが再生成されている。
- クラスタリングまたはマルチコンテキストモード。

手順

ステップ 1 デバイスで DTLS 暗号化アクセラレーションを無効にします。

no flow-offload-dtls

例：

```
ciscoasa(config)# no flow-offload-dtls
```

再び有効にするには、**flow-offload-dtls** コマンドを使用します。

ステップ 2 出力暗号化パケットの最適化を無効にし、遅延を改善します。

no flow-offload-dtls egress-optimization

例：

```
ciscoasa(config)# flow-offload-dtls egress-optimization
```

再び有効にするには、**flow-offload-dtls egress-optimization** コマンドを使用します。

DTLS 暗号化アクセラレーションのモニタリング

DTLS暗号化アクセラレーションと出力暗号化パケットの最適化を確認してモニターするには、Threat Defense デバイスで CLI コマンドを使用します。

- DTLS 暗号化アクセラレーションと出力暗号化パケットの最適化のステータスを確認するには、次のコマンドを使用します。

```
ciscoasa# show flow-offload-dtls info
  DTLS offload : Enabled
  Egress Optimization: Enabled
```

- DTLS 暗号化アクセラレーションの統計を表示するには、次のコマンドを使用します。

```
ciscoasa# show flow-offload-dtls statistics
  Packet stats of Pipe 0
  ----------------------
  Rx Packet count : 975638666
  Tx Packet count : 975638666
  Error Packet count : 0
  Drop Packet count : 0

  CAM stats of Pipe 0
  ----------------------
  Option ID Table CAM Hit Count : 1145314723
  Option ID Table CAM Miss Count : 0
  Tunnel Table CAM Hit Count : 0
  Tunnel Table CAM Miss Count : 0
  6-Tuple CAM Hit Count : 975638666
  6-Tuple CAM Miss Count : 169676057
   NOTE: The counters displayed are cumulative counters
   for all offload applications and indicates the total packets
  offloaded
```

- Secure Firewall 3100 および 4200 について、デバイスの Nitrox V 暗号化アクセラレータの統計を表示するには、次のコマンドを使用します。

```
ciscoasa# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
<snip>
[Offloaded SSL Input statistics, Pipe 0]
      Input packets: 290593023
      Input bytes: 147049729714
      Decrypted packets: 290593023
      Decrypted bytes: 147049729714
   [Offloaded SSL Output statistics, Pipe 0]
      Output packets: 254271808
      Output bytes: 136352952720
      Encrypted packets: 254271808
      Encrypted bytes: 136352952720
.
.
.
```

特定のトラフィック クラスの接続の設定（すべてのサービス）

サービス ポリシーを使用して、特定のトラフィック クラスに対してさまざまな接続の設定を行うことができます。サービス ポリシーを使用して、次の内容を実行します。

- DoS 攻撃と SYN フラッディング攻撃から保護するのに使用される接続制限と接続タイムアウトをカスタマイズします。
- アイドル状態でも有効な接続を維持するように、Dead Connection Detection（DCD; デッド接続検出）を実装します。
- TCP シーケンス番号ランダム化が不要な場合、それをディセーブルにします。
- TCP ノーマライザが異常な TCP パケットから保護する方法をカスタマイズします。

- 非対称ルーティングの対象であるトラフィックに対して TCP ステートバイパスを導入します。バイパス トラフィックはインスペクションの対象になりません。
- SCTP ステートフル インスペクションをオフにするには、Stream Control Transmission Protocol（SCTP）ステート バイパスを実装します。
- サポート対象のハードウェア プラットフォームのパフォーマンスを向上させるには、フロー オフロードを実装します。
- ASA がトレース ルート出力に表示されるように、パケットの存続可能時間（TTL）をデクリメントします。

（注） パケット存続時間（TTL）をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、トランスペアレントモードの ASA デバイスでは、パケット存続時間をデクリメントすると予期しない結果が発生する可能性があります。ASA がルーテッドモードで動作している場合は、パケット存続時間の設定をデクリメントしても OSPF のプロセスに影響を与えません。

同時に使用できない TCP ステート バイパスと TCP ノーマライザのカスタマイズを除き、特定のトラフィック クラスに対してこれらの設定の任意の組み合わせを設定できます。

ヒント この手順は、ASA を通過するトラフィックのサービス ポリシーを示します。管理（to the box）トラフィックに対して接続の最大数と初期接続の最大数を設定することもできます。

始める前に

TCP ノーマライザをカスタマイズする場合は、続行する前に必要な TCP マップを作成してください。

ここでは、**set connection** コマンド（接続制限と TCP シーケンス番号ランダム化の）と **set connection timeout** コマンドについてパラメータごとに個別に説明します。ただし、1 つの行にこれらのコマンドを入力できます。これらのコマンドを個別に入力した場合、1 つのコマンドとしてコンフィギュレーションに表示されます。

手順

ステップ 1 L3/L4 クラスマップを作成して、接続の設定をカスタマイズするトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
```

照合ステートメントについては、通過トラフィック用のレイヤ 3/4 クラス マップの作成 （282 ページ）を参照してください。

ステップ 2 クラスマップ トラフィックで実行するアクションを設定するポリシーマップを追加または編集して、クラス マップを指定します。

```
policy-map name
class name
```

例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class CONNS
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラス マップの場合、この手順ですでに作成したクラスを指定します。

ステップ 3 接続制限と TCP シーケンス番号ランダム化を設定します。（TCP 代行受信）

デフォルトでは、接続制限はありません。制限を実装すると、システムはそれらの追跡を開始する必要があります。これにより、CPU とメモリの使用率が増加し、特にクラスタでは高負荷がかかったシステムに動作上の問題が発生する可能性があります。

- **set connection conn-max** *n*：（TCP、UDP、SCTP）。クラス全体で許可される同時接続の最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。TCP 接続の場合、これは確立された接続のみに適用されます。
  - 同時接続を許可するように 2 つのサーバーが設定されている場合、接続制限数は、設定されている各サーバーに別々に適用されます。
  - 制限がクラスに適用されるため、1 つの攻撃ホストがすべての接続を使い果たし、クラスに一致する他のホストが使用できる接続がなくなる可能性があります。

- **set connection per-client-max** *n*：（TCP、UDP、SCTP）。クライアントごとに許可する同時接続の最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。この引数では、クラスに一致する各ホストに許可される同時接続最大数が制限されます。TCP 接続の場合、これには確立済み接続、ハーフオープン接続、ハーフクローズ接続が含まれています。

- **set connection embryonic-conn-max** *n*：許可される同時初期 TCP 接続の最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。0 以外の制限を設定することで、TCP 代行受信を有効にします。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。また、クライアントごとのオプションを設定して、SYN フラッディングから保護します。
- **set connection per-client-embryonic-max** *n*：クライアントごとに許可される同時初期 TCP 接続の最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。
- **set connection syn-cookie-mss** 初期接続数制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）（48 ～ 65535）。デフォルトは 1380 です。この設定は、**set connection embryonic-conn-max** または **per-client-embryonic-max** を設定する場合にのみ有効です。
- **set connection random-sequence-number** {**enable** | **disable**}：TCP シーケンス番号ランダム化をイネーブルまたはディセーブルにするかどうか。デフォルトでは、ランダム化がイネーブルになっています。

例：

```
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
```

ステップ 4 接続タイムアウトと Dead Connection Detection（DCD; デッド接続検出）を設定します。

次に説明するデフォルト値は、**timeout** コマンドを使用してこれらの動作のグローバルのデフォルト値を変更していないことを前提としています。グローバルのデフォルト値はここで説明する値を上書きします。接続がタイムアウトしないように、**0** を入力してタイマーをディセーブルにします。

- **set connection timeout embryonic** *hh*:*mm*:*ss*：TCP 初期（ハーフオープン）接続を閉じるまでのタイムアウト期間（0:0:5 ～ 1193:00:00）。デフォルト値は 0:0:30 です。
- **set connection timeout idle** *hh*:*mm*:*ss* [**reset**]：いずれかのプロトコルの確立された接続が閉じてからのアイドル タイムアウト期間（0:0:1 から 1193:0:0）。デフォルト値は 1:0:0 です。TCP トラフィックの場合、**reset** キーワードを指定すると、接続のタイムアウト時にリセット パケットが TCP エンドポイントに送信されます。

  デフォルトの **udp** アイドル タイムアウトは 2 分です。デフォルトの **icmp** アイドル タイムアウトは 2 秒です。デフォルトの **esp** および **ha** アイドル タイムアウトは 30 秒です。その他すべてのプロトコルでは、デフォルトのアイドル タイムアウトは 2 分です。
- **set connection timeout half-closed** *hh*:*mm*:*ss*：ハーフクローズ接続を閉じるまでのアイドル タイムアウト期間（9.1(1) 以前の場合は 0:5:0 ～ 1193:0:0、9.1(2) 以降の場合は 0:0:30 ～ 1193:0: 0）。デフォルト値は 0:10:0 です。ハーフクローズの接続は DCD の影響を受けません。また、ASA は、ハーフクローズ接続を切断するときにリセットを送信しません。
- **set connection timeout dcd** [*retry-interval* [*max_retries*]]：Dead Connection Detection（DCD; デッド接続検出）をイネーブルにします。アイドル接続の期限が切れる前に、ASA はエンドホストにプローブを送信して接続が有効であるかどうかを判断します。両方のホストが

応答した場合は、接続が維持されます。それ以外の場合は、接続が解放されます。トランスペアレントファイアウォールモードで動作している場合、エンドポイントにスタティック ルートを設定する必要があります。オフロードも行われる接続には DCD を設定できないため、DCD とフローオフロードのトラフィッククラスが重複しないようにしてください。発信側と受信側で送信された DCD プローブの個数を追跡するには、**show conn detail** コマンドを使用します。

retry-interval には、DCD プローブに応答がない場合に別のプローブを送信するまで待機する時間を、*hh*:*mm*:*ss* 形式で、0:0:1 から 24:0:0 の範囲で設定します。デフォルト値は 0:0:15 です。max-retries には、接続が無活動状態であると宣言するまでに失敗する DCD の連続再試行回数を設定します。最小値は 1、最大値は 255 です。デフォルトは 5 分です。

クラスタまたは高可用性構成で動作しているシステムでは、間隔を 1 分（0:1:0）未満に設定しないことを推奨します。接続をシステム間で移動する必要がある場合、必要な変更には 30 秒以上かかり、変更が行われる前に接続が削除される場合があります。

例：

```
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
```

ステップ 5 クラスに一致するパケットの存続可能時間（TTL）をデクリメントします：**set connection decrement-ttl**

このコマンド、および **icmp unreachable** コマンドは、ASA をホップの 1 つとして表示する ASA 経由の traceroute を可能とするために必要です。

例：

```
hostname(config)# class-map global-policy
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map global_policy
hostname(config-pmap)# class global-policy
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

ステップ 6 接続詳細オプションを設定します。

詳細オプションは、通常の状況では不要な特別な用途の設定です。これらのオプションは、**set connection advanced-options** コマンドを使用して設定します。

- **set connection advanced-options** *tcp_map_name*：TCP マップを適用することで、TCP ノーマライザの動作をカスタマイズします。詳細については、異常な TCP パケット処理のカスタマイズ（TCP マップ、TCP ノーマライザ） （467 ページ）を参照してください。
- **set connection advanced-options tcp-state-bypass**：TCP ステート バイパスを実装します。詳細については、非対称ルーティングの TCP ステートチェックのバイパス（TCP ステート バイパス） （472 ページ）を参照してください。

- **set connection advanced-options sctp-state-bypass**：SCTP ステート バイパスを実装して、SCTP ステートフル インスペクションを無効にします。詳細については、SCTP ステートフル インスペクション （404 ページ）を参照してください。
- **set connection advanced-options flow-offload**：（Firepower 4100/9300 シャーシ の ASA、FXOS 1.1.3 以降のみ。）フローのオフロードを実装します。フローが NIC 自体で切り替えられる超高速パスにオフロードされる適切なトラフィック。**flow-offload enable** コマンド（これはサービス ポリシーの一部ではありません）も入力する必要があります。

例：

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

ステップ 7 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを1つだけ適用できます。

例

次の例では、すべてのトラフィックに対して接続の制限値とタイムアウトを設定しています。

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

複数のパラメータを使用して **set connection** コマンドを入力するか、各パラメータを別々のコマンドとして入力できます。ASA は、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

TCP オプションの構成

各種オプションを構成して、TCP 動作のいくつかの側面を制御できます。これらの設定のデフォルト値は、ほとんどのネットワークに適しています。

手順

ステップ 1 （CLI）TCP リセット動作を構成します。

service { **resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside** }

- **resetinbound**を使用して無効にすることができます。ASA の通過を試み、アクセスリストまたはAAA設定に基づいてASAによって拒否されたすべての着信TCPセッションにTCPリセットを送信します。ASA は、アクセスリストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフルファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションをイネーブルにしなかった場合、ASA は拒否されたパケットを何も通知せずに廃棄します。インターフェイスを指定しない場合、この設定はすべてのインターフェイスに適用されます。
- **resetoutbound**を使用して無効にすることができます。ASA の通過を試み、アクセスリストまたは AAA 設定に基づいて ASA によって拒否されたすべての発信 TCP セッションに TCP リセットを送信します。ASA は、アクセスリストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションをイネーブルにしなかった場合、ASAは拒否されたパケットを何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。
- **resetoutside**を使用して無効にすることができます。最もセキュリティレベルの低いインターフェイスで終端し、アクセスリストまたはAAA設定に基づいてASAによって拒否された TCP パケットのリセットをイネーブルにします。ASA は、アクセスリストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォー

ルによって拒否されたパケットのリセットも送信します。このオプションをイネーブルにしなかった場合、ASA は拒否されたパケットを何も通知せずに廃棄します。

インターフェイス PAT では、このオプションを使用することを推奨します。このオプションを使用すると、外部 SMTP または FTP サーバーからの IDENT を ASA で終端できます。これらの接続をアクティブにリセットすることによって、30 秒のタイムアウト遅延を回避できます。

ステップ 2 通過トラフィックの最大 TCP セグメントサイズが設定した値を超えないようにし、指定したサイズ未満にならないようにするには、TCP MSS を設定します。

sysopt connection tcpmss ［ **minimum** ］ *bytes*

minimum キーワードなし。最大 TCP セグメント サイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、bytes を 0 に設定します。

minimumを使用して無効にすることができます。最大セグメントサイズを上書きし、指定したバイト（48 ～ 65535 バイト）未満にならないようにします。この機能は、デフォルトでディセーブルです（0 に設定）。

ステップ 3 TCP 接続の確立待機時間を設定します。

sysopt connection timewait

このコマンドを使用すると、各 TCP 接続において、最後の通常の TCP クローズダウンシーケンスの後に、少なくとも 15 秒の短い TIME_WAIT 状態が強制的に維持されます。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。

ステップ 4 TCP 未処理セグメントの最大数を設定します。

sysopt connection tcp-max-unprocessed-seg *segments*

TCP 未処理セグメントの最大数を 6 ～ 24 に設定します。デフォルト値は 6 です。SIP 電話機が Call Manager に接続していないことを確認したら、未処理の TCP セグメントの最大数を増やすことができます。

接続のモニタリング

次のコマンドを使用して、接続をモニターできます。

- **show conn** [**detail**]

  接続情報を表示します。詳細情報は、フラグを使用して特別な接続の特性を示します。たとえば、「b」フラグは、TCPステート バイパスの対象であるトラフィックを示します。

  detail キーワードを使用すると、デッド接続検出（DCD）プローブの情報が表示されます。この情報は、発信側と応答側で接続がプローブされた頻度を示します。たとえば、DCD 対応接続の接続詳細は次のようになります。

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show flow-offload**{**info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics**}

  全般的なステータス情報、オフロードの CPU 使用率、オフロードされたフローの数と詳細、オフロードされたフロー統計情報を含む、フローのオフロードに関する情報を示します。

- **show service-policy**

  Dead Connection Detection（DCD; デッド接続検出）の統計情報を含むサービス ポリシーの統計情報を表示します。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  攻撃を受けて保護された上位 10 サーバーを表示します。**all** キーワードは、トレースされているすべてのサーバーの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

（注） Cisco ASA 設定では、初期接続（3 ウェイ ハンドシェイク プロセスがまだ完了していない接続要求）はすぐに閉じられ、アクティブデバイスとスタンバイデバイス間で同期されません。この設計により、HA システムの効率とセキュリティが確保されます。このため、両方の Cisco ASA で接続数に違いが生じる可能性がありますが、これは予想されることです。

接続設定の履歴

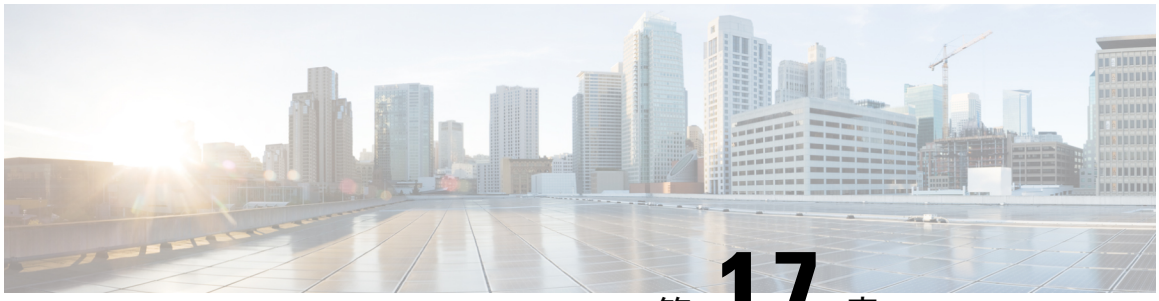
機能名	プラットフォームリリース	説明
TCP ステート バイパス	8.2(1)	この機能が導入されました。**set connection advanced-options tcp-state-bypass** コマンドが導入されました。
すべてのプロトコルの接続タイムアウト	8.2(2)	アイドル タイムアウトは、TCP だけでなく、すべてのプロトコルに適用するように変更されました。 **set connection timeout** コマンドが変更されました。

機能名	プラットフォームリリース	説明
バックアップ スタティック ルートを使用する接続のタイムアウト	8.2(5)/8.4(2)	同じネットワークへの複数のスタティック ルートが存在しており、それぞれメトリックが異なる場合は、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは0です（接続はタイムアウトしません）。この機能を使用するには、タイムアウトを新しい値に変更します。 **timeout floating-conn** コマンドが変更されました。
PAT xlate に対する設定可能なタイムアウト	8.4(3)	PAT xlate がタイムアウトし（デフォルトでは 30 秒後）、ASA が新しい変換用にポートを再使用すると、一部のアップストリーム ルータは、前の接続がアップストリーム デバイスで依然として開いている可能性があるため、この新しい接続を拒否する場合があります。PAT xlate のタイムアウトを、30 秒～ 5 分の範囲内の値に設定できるようになりました。 **timeout pat-xlate** コマンドが導入されました。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。
サービス ポリシー ルールの最大接続数の引き上げ	9.0(1)	サービス ポリシー ルールの最大接続数が 65535 から 2000000 に引き上げられました。 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、**set connection per-client-max** の各コマンドが変更されました。
ハーフ クローズ タイムアウト最小値を 30 秒に削減	9.1(2)	グローバル タイムアウトおよび接続タイムアウトの両方のハーフ クローズド タイムアウトの最小値は、より優れた DoS 保護を提供するために 5 分から 30 秒に短縮されました。 **set connection timeout half-closed**、**timeout half-closed** の各コマンドが変更されました。
ルートの収束に対する接続ホールドダウン タイムアウト。	9.4(3) 9.6(2)	接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間を設定できるようになりました。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。ルートの収束がさらに迅速に行われるようにホールドダウン タイマーを短縮することができます。ただし、ほとんどのネットワークでは、ルートのフラッピングを防止するためにデフォルトの 15 秒が適切です。 **timeout conn-holddown** コマンドが追加されました。

機能名	プラットフォームリリース	説明
SCTP アイドル タイムアウトおよび SCTP ステート バイパス	9.5(2)	SCTP 接続のアイドル タイムアウトを設定できます。また、SCTP ステート バイパスを有効にして、トラフィックのクラスで SCTP ステートフル インスペクションをオフにできます。 次のコマンドが追加または変更されました。**timeout sctp**、**set connection advanced-options sctp-state-bypass**。
Firepower 9300 上の ASA のフロー オフロード。	9.5(2.1)	ASA からオフロードされ、（Firepower 9300 上の）NIC に直接切り替えられる必要があるフローを特定できます。これにより、データセンターのより大きなデータ フローのパフォーマンスが向上します。 この機能には、FXOS 1.1.3 が必要です。 次のコマンドが追加または変更されました。**clear flow-offload**、**flow-offload enable**、**set-connection advanced-options flow-offload**、**show conn detail**、**show flow-offload**。
Firepower 4100 シリーズ 上の ASA のフロー オフロードのサポート。	9.6(1)	ASA からオフロードされ、Firepower 4100 シリーズ の NIC で直接切り替える必要があるフローを特定できます。 この機能では、FXOS 1.1.4 が必要です。 この機能には、新規のコマンドまたは ASDM 画面はありません。
トランスペアレント モードでのマルチキャスト接続のフローオフロードのサポート。	9.6(2)	トランスペアレント モードの Firepower 4100 および 9300 シリーズ デバイスで、NIC に直接切り替えられるマルチキャスト接続をオフロードできるようになりました。マルチキャスト オフロードは、インターフェイスを 2 つだけ含むブリッジ グループに使用できます。 この機能には、新規のコマンドまたは ASDM 画面はありません。

機能名	プラットフォームリリース	説明
TCP オプション処理の変更。	9.6(2)	TCP マップを設定する際にパケットの TCP ヘッダー内の TCP MSS および MD5 オプションに対するアクションを指定できるようになりました。さらに、MSS、タイムスタンプ、ウィンドウ サイズ、および選択的確認応答オプションのデフォルトの処理が変更されました。以前は、これらのオプションは、ヘッダーに特定のタイプのオプションが 2 つ以上ある場合でも許可されていました。現在は、パケットに特定のタイプのオプションが 2 つ以上含まれている場合、そのパケットはデフォルトでドロップされます。たとえば、以前は 2 つのタイムスタンプ オプションがあるパケットは許可されていましたが、現在はドロップされます。 MD5、MSS、選択的確認応答、タイムスタンプ、およびウィンドウ サイズに対し、同じタイプの複数のオプションを有効にするための TCP マップを設定できます。MD5 オプションの場合、以前のデフォルトではオプションがクリアされたのに対し、現在のデフォルトでは許可されます。また、MD5 オプションを含むパケットをドロップすることもできます。MSS オプションの場合は、TCP マップで最大セグメント サイズを設定できます（トラフィック クラスごとに）。他のすべての TCP オプションのデフォルトに変更はありません。これらはクリアされます。 次のコマンドが変更されました。**timeout igp stale-route**。
内部ゲートウェイ プロトコルの古いルートのタイムアウト	9.7(1)	OSPF などの内部ゲートウェイ プロトコルの古いルートを削除するためのタイムアウトを設定できるようになりました。 **timeout igp stale-route** コマンドが追加されました。
ICMP エラーのグローバル タイムアウト	9.8(1)	ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間を設定できるようになりました。このタイムアウトが無効（デフォルト）で、ICMP インスペクションが有効に設定されている場合、ASA はエコー応答を受信するとすぐに ICMP 接続を削除します。したがって、終了しているその接続に対して生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信することが可能になります。 次のコマンドが追加されました。 **timeout icmp-error**
TCP ステート バイパスのデフォルトのアイドル タイムアウト	9.10(1)	TCP ステート バイパス接続のデフォルトのアイドル タイムアウトは 1 時間ではなく、2 分になりました。

機能名	プラットフォームリリース	説明
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	9.13(1)	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新しい/変更されたコマンド：**show conn**（出力のみ）
初期接続の最大セグメントサイズ（MSS）を設定します。	9.16(1)	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 追加または変更されたコマンド：**set connection syn-cookie-mss**。
SIP Call Init のアイドル グローバル タイムアウトの設定	9.16(x)	Call_Init コール状態の SIP セッションが（最初の招待メッセージの受信後）削除されるまでのアイドル時間（つまり応答を受信しなかった場合）を、0:0:1 ～ 1193:0:0 の範囲で設定できます。デフォルト値は 32 秒（0:00:32）です。
IPsec フローがオフロードされます。	9.18(1)	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブル ゲートアレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 次のコマンドが追加されました。**clear flow-offload-ipsec**、**flow-offload-ipsec**、**show flow-offload-ipsec**
DTLS 暗号化アクセラレーション	9.22(1)	Cisco Secure Firewall 4200 および 3100 シリーズは、DTLS 暗号化アクセラレーションをサポートします。ハードウェアはDTLS 暗号化と復号化を実行し、DTLS 暗号化トラフィックと DTLS 復号化トラフィックのスループットを向上させます。ハードウェアは、遅延を改善するために、出力暗号化パケットの最適化も実行します。 新規/変更されたコマンド：**flow-offload-dtls**、**flow-offload-dtls egress-optimization**



第 17 章

QoS

衛星接続を使用した長距離電話では、会話が、短い間ですが認識できる程度に割り込みされ、不定期に中断されることがあります。このような中断は、ネットワークで送信されるパケットが到着する間隔の時間で、遅延と呼ばれます。音声やビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。Quality of Service（QoS）機能を使用すると、重要なトラフィックのプライオリティを高くし、帯域幅の過剰な使用を防ぎ、ネットワーク ボトルネックを管理してパケットのドロップを防止できます。

ここでは、QoS ポリシーの適用方法について説明します。

- QoS について （499 ページ）
- QoS のガイドライン （501 ページ）
- QoS の設定 （502 ページ）
- QoS のモニター （508 ページ）
- プライオリティ キューイングとポリシングの設定例 （510 ページ）
- QoS の履歴 （512 ページ）

QoS について

常に変化するネットワーク環境では、QoS は 1 回限りの構成ではなく、ネットワーク設計の継続的で不可欠な要素であることを考慮する必要があります。

この項では、ASA で使用できる QoS 機能について説明します。

サポートされている QoS 機能

ASA は、次の QoS の機能をサポートしています。

- ポリシング：分類されたフローがネットワーク帯域幅を大量に使用するのを防ぐため、クラスごとの最大使用帯域幅を制限できます。詳細については、「ポリシング （500 ページ）」を参照してください。
- プライオリティ キューイング：Voice over IP（VoIP）のような遅延を許されない重要なトラフィックについて、トラフィックを低遅延キューイング（LLQ）に指定することで、常

に他のトラフィックより先に送信できます。プライオリティ キューイング （501 ページ）を参照してください。

トークン バケットとは

トークン バケットは、フロー内のデータを規制するデバイス（トラフィック ポリサーなど）の管理に使用されます。トークン バケット自体には、廃棄ポリシーまたはプライオリティ ポリシーはありません。むしろ、トークンバケットは、フローによって規制機能が過剰に働く場合に、トークンを廃棄し、送信キューの管理の問題はフローに任せます。

トークン バケットは、転送レートの正式な定義です。トークン バケットには、バースト サイズ、平均レート、時間間隔という 3 つのコンポーネントがあります。平均レートは通常 1 秒間のビット数で表されますが、次のような関係によって、任意の 2 つの値を 3 番目の値から求めることができます。

平均レート = バースト サイズ / 時間間隔

これらの用語の定義は次のとおりです。

- 平均レート：認定情報レート（CIR）とも呼ばれ、単位時間に送信または転送できるデータ量の平均値を指定します。
- バースト サイズ：認定バースト（Bc）サイズとも呼ばれ、スケジューリングに関する問題を発生させることなく単位時間内に送信できるトラフィックの量を、バーストあたりのバイト数で指定します。
- 時間間隔：測定間隔とも呼ばれ、バーストごとの時間を秒単位で指定します。

トークンバケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。バケット自体には指定された容量があります。バケットがいっぱいになると、新しく到着するトークンは廃棄されます。各トークンは、送信元が一定の数のビットをネットワークに送信するための権限です。パケットを送信するため、規制機能はパケットサイズに等しい数のトークンをバケットから削除する必要があります。

パケットを送信するための十分なトークンがバケットにない場合、パケットは、パケットが廃棄されるか、ダウン状態とマークされるまで待機します。バケットがすでにトークンで満たされている場合、着信トークンはオーバーフローし、以降のパケットには使用できません。したがって、いつでも、送信元がネットワークに送信できる最大のバーストは、バケットのサイズにほぼ比例します。

ポリシング

ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1 つのトラフィック クラスが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、ASA は超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

プライオリティ キューイング

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。プライオリティ キューイングでは、インターフェイスで LLQ プライオリティ キューが使用されます（インターフェイスのプライオリティ キューの設定（504 ページ）を参照してください）。一方、他のトラフィックはすべて「ベストエフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これはテール ドロップと呼ばれます。キューがいっぱいになることを避けるには、キューのバッファ サイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

QoS 機能の相互作用のしくみ

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。次のことを設定できます。

プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

DSCP（DiffServ）の保存

DSCP（DiffServ）のマーキングは、ASA を通過するすべてのトラフィックで維持されます。ASA は、分類されたトラフィックをローカルにマーク/再マークすることはありません。たとえば、すべてのパケットの完全優先転送（EF）DSCP ビットを受け取り、「プライオリティ」処理が必要かどうかを判断し、ASA にそれらのパケットを LLQ に入れさせることができます。

QoS のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドラインと制限事項

- QoS は単方向に適用されます。ポリシー マップを適用するインターフェイスに出入りする（QoS 機能によって異なります）トラフィックだけが影響を受けます。
- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- プライオリティキューイングの場合、プライオリティキューは物理インターフェイス用に設定する必要があります。
- ポリシングでは、to-the-box トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。

QoS の設定

ASA に QoS を実装するには、次の手順を使用します。

手順

ステップ 1 プライオリティ キューのキューおよび TX リング制限の決定 （502 ページ）。
ステップ 2 インターフェイスのプライオリティ キューの設定 （504 ページ）。
ステップ 3 プライオリティ キューイングとポリシング用のサービス ルールの設定 （506 ページ）。

プライオリティ キューのキューおよび TX リング制限の決定

プライオリティ キューおよび TX リング制限を決定するには、次のワークシートを使用します。

キュー制限のワークシート

次のワークシートは、プライオリティ キューのサイズを計算する方法を示しています。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（テール ドロップと呼ばれます）。キューがいっぱいになることを避けるには、インターフェイスのプライオリティ キューの設定 （504ページ）に従ってキューのバッファ サイズを調節します。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 平均パケットサイズ：この値は、コーデックまたはサンプリングサイズから決定します。たとえば、VoIP over VPN の場合は、160 バイトなどを使用します。使用するサイズがわからない場合は、256 バイトにすることをお勧めします。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP の場合の推奨される最大遅延は 200 ミリ秒です。使用する遅延がわからない場合は、500 ミリ秒にすることをお勧めします。

表 *13*：キュー制限のワークシート

1	_____ アウトバウンド帯域幅（*Mbps* または *Kbps*）	Mbps	×	**125**	=	_____ バイト数/ミリ秒		
		Kbps	×	**.125**	=	_____ バイト数/ミリ秒		
2	_____ ステップ *1* からのバイト数/ミリ秒		÷	_____ 平均パケットサイズ（バイト）	×	_____ 遅延（ミリ秒）	=	_____ キュー制限（パケット数）

TX リング制限のワークシート

次のワークシートは、TX リング制限の計算方法を示しています。この制限により、イーサネット送信ドライバが受け入れるパケットの最大数が決まります。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 最大パケット サイズ：通常、最大サイズは 1538 バイト、またはタグ付きイーサネットの場合は 1542 バイトです。ジャンボ フレームを許可する場合（プラットフォームでサポートされている場合）、パケット サイズはさらに大きくなる場合があります。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP のジッタを制御するには、20 ミリ秒を使用します。

表 *14 : TX* リング制限のワークシート

1	_____ アウトバウンド帯域幅（*Mbps* または *Kbps*）	Mbps	×	**125**	=	_____ バイト数/ミリ秒		
		Kbps	×	**0.125**	=	_____ バイト数/ミリ秒		
2	_____ ステップ *1* からのバイト数/ミリ秒		÷	_____ 最大パケット サイズ（バイト）	×	_____ 遅延（ミリ秒）	=	_____ *TX* リング制限（パケット数）

インターフェイスのプライオリティ キューの設定

物理インターフェイスでトラフィックに対するプライオリティ キューイングをイネーブルにする場合は、各インターフェイスでプライオリティ キューを作成する必要もあります。各物理インターフェイスは、プライオリティ トラフィック用と、他のすべてのトラフィック用に、2 つのキューを使用します。他のトラフィックについては、必要に応じてポリシングを設定できます。

手順

ステップ 1 インターフェイスのプライオリティ キューを作成します。

priority-queue *interface_name*

例：

```
hostname(config)# priority-queue inside
```

interface_name 引数では、プライオリティキューをどの物理インターフェイスに対して有効化するかを指定します。

ステップ 2 プライオリティ キューのサイズを変更します。

queue-limit *number_of_packets*

デフォルトのキューの制限は 1024 パケットです。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（テール ドロップと呼ばれます）。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

queue-limit コマンドの値の範囲の上限は、実行時に動的に決まります。この上限を表示するには、コマンドラインで **queue-limit?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。

指定した **queue-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。

例：

```
hostname(config-priority-queue)# queue-limit 260
```

ステップ 3 プライオリティ キューの深さを指定します。

tx-ring-limit *number_of_packets*

デフォルトの tx-ring-limit は 511 パケットです。このコマンドは、イーサネット送信ドライバが受け入れる低遅延パケットまたは通常プライオリティ パケットの最大数を設定します。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

tx-ring-limit コマンドの値の範囲の上限は、実行時に動的に決まります。この上限を表示するには、コマンド ラインで **tx-ring-limit ?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。

指定した **tx-ring-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。

例：

```
hostname(config-priority-queue)# tx-ring-limit 3
```

例

次の例は、デフォルトの queue-limit と tx-ring-limit を使用して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside
```

次の例は、queue-limit を 260 パケット、tx-ring-limit を 3 に設定して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 260
```

```
hostname(config-priority-queue)# tx-ring-limit 3
```

プライオリティ キューイングとポリシング用のサービス ルールの設定

同じポリシー マップ内の異なるクラス マップに対し、プライオリティ キューイングとポリシングを設定できます。有効な QoS 設定については、QoS 機能の相互作用のしくみ （501 ページ）を参照してください。

始める前に

- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- ポリシングでは、to-the-box トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。
- プライオリティ トラフィックの場合は、遅延が問題になるトラフィックだけを指定します。
- ポリシング トラフィックの場合は、他のすべてのトラフィックをポリシングすることも、トラフィックを特定のタイプに制限することもできます。

手順

ステップ 1 L3/L4 クラス マップを作成して、プライオリティ キューイングを実行するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map priority_traffic
hostname(config-cmap)# match access-list priority
```

詳細については、「通過トラフィック用のレイヤ 3/4 クラス マップの作成 （282 ページ）」を参照してください。

ステップ 2 L3/L4 クラス マップを作成して、プライオリティ ポリシングを実行するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map policing_traffic
hostname(config-cmap)# match access-list policing
```

ヒント　トラフィック照合にACLを使用する場合、ポリシングはACLで指定された方向にのみ適用されます。つまり、送信元から宛先に向かうトラフィックがポリシングされ、宛先から送信元に向かうトラフィックはポリシングされません。

ステップ 3　ポリシー マップを追加または変更します。**policy-map** *name*

例：

```
hostname(config)# policy-map QoS_policy
```

ステップ 4　優先されるトラフィック用に作成したクラス マップを指定し、そのクラスにプライオリティ キューイングを設定します。

```
class priority_map_name
priority
```

例：

```
hostname(config-pmap)# class priority_class
hostname(config-pmap-c)# priority
```

ステップ 5　ポリシングされるトラフィック用に作成したクラス マップを指定します。**class** *name*

例：

```
hostname(config-pmap)# class policing_class
```

ステップ 6　クラスのポリシングを設定します。

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**]] [**exceed-action** [**drop** | **transmit**]]

次のオプションがあります。

- **output**：出力方向のトラフィック フローのポリシングをイネーブルにします。
- **input**：入力方向のトラフィック フローのポリシングをイネーブルにします。

- *conform-rate*：このトラフィッククラスのレート制限を 8000 ～ 2000000000 ビット/秒の範囲で設定します。たとえば、トラフィックを 5 Mbps に制限するには、5000000 と入力します。
- *conform-burst*：（任意）適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ～ 512000000 バイトの範囲で指定します。変数を省略すると、バーストサイズはバイト単位の適合レートの 1/32 として計算されます。たとえば、5 Mbps レートのバーストサイズは 156250 です。
- **conform-action**：（任意）トラフィックがポリシングレートとバーストサイズを下回った場合に実行するアクションを設定します。トラフィックをドロップまたは送信できます。デフォルトでは、トラフィックは送信されます。
- **exceed-action**：（任意）トラフィックがポリシングレートとバーストサイズを上回った場合に実行するアクションを設定します。ポリシングレートとバーストサイズを上回ったパケットをドロップまたは送信できます。デフォルトでは、超過パケットはドロップされます。

例：

```
hostname(config-pmap-c)# police output 56000 10500
```

ステップ 7 1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy QoS_policy interface inside
```

global オプションはポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

QoS のモニター

ここでは、QoS をモニターする方法について説明します。

QoS ポリシーの統計情報

トラフィック ポリシングの QoS 統計情報を表示するには、**show service-policy police** コマンドを使用します。

```
hostname# show service-policy police
```

```
Global policy:
 Service-policy: global_fw_policy

Interface outside:
 Service-policy: qos
  Class-map: browse
   police Interface outside:
    cir 56000 bps, bc 10500 bytes
    conformed 10065 packets, 12621510 bytes; actions: transmit
    exceeded 499 packets, 625146 bytes; actions: drop
    conformed 5600 bps, exceed 5016 bps
  Class-map: cmap2
   police Interface outside:
    cir 200000 bps, bc 37500 bytes
    conformed 17179 packets, 20614800 bytes; actions: transmit
    exceeded 617 packets, 770718 bytes; actions: drop
    conformed 198785 bps, exceed 2303 bps
```

QoS プライオリティの統計情報

priority コマンドを実装するサービス ポリシーの統計情報を表示するには、**show service-policy priority** コマンドを使用します。

```
hostname# show service-policy priority
Global policy:
 Service-policy: global_fw_policy
Interface outside:
 Service-policy: qos
  Class-map: TG1-voice
   Priority:
    Interface outside: aggregate drop 0, aggregate transmit 9383
```

「Aggregate drop」は、このインターフェイスでの合計ドロップ数を示しています。「aggregate transmit」は、このインターフェイスで送信されたパケットの合計数を示しています。

QoS プライオリティ キューの統計情報

インターフェイスのプライオリティ キュー統計情報を表示するには、**show priority-queue statistics** コマンドを使用します。ベストエフォート（BE）キューと低遅延キュー（LLQ）の両方の統計情報が表示されます。次の例に、test という名前のインターフェイスに対する **show priority-queue statistics** コマンドの使用方法を示します。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
```

```
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

この統計情報レポートの内容は次のとおりです。

- 「Packets Dropped」は、このキューでドロップされたパケットの合計数を示します。
- 「Packets Transmit」は、このキューで送信されたパケットの合計数を示します。
- 「Packets Enqueued」は、このキューでキューイングされたパケットの合計数を示します。
- 「Current Q Length」は、このキューの現在の深さを示します。
- 「Max Q Length」は、このキューで発生した最大の深さを示します。

プライオリティ キューイングとポリシングの設定例

次の項では、プライオリティ キューイングとポリシングを設定する例を示します。

VPN トラフィックのクラス マップの例

次の例で、**class-map** コマンドは tcp_traffic という ACL を使用して、すべての非トンネル TCP トラフィックを分類します。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

次の例では、より限定的な一致基準を使用して、特定のセキュリティ関連のトンネル グループにトラフィックを分類します。これらの特定の一致基準では、トラフィックが特定のトンネルに分類されるために、最初の一致特性としてトンネルグループ（この例では、すでに定義されている Tunnel-Group-1）に一致する必要があります。次に、別の照合行でトラフィックを分類できます（IP DiffServ コード ポイント、緊急転送）。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

次の例では、**class-map** コマンドはトンネル トラフィックと非トンネル トラフィックの両方をトラフィック タイプに従って分類します。

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L
```

```
hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

次の例は、クラストラフィックがトンネルとして指定されておらず、トンネルを通過する場合に、トンネル内のトラフィックをポリシングする方法を示します。この例では、192.168.10.10がリモート トンネルのプライベート側のホスト マシンのアドレスで、ACL の名前は「host-over-l2l」です。クラスマップ（名前は「host-specific」）を作成すると、LAN-to-LAN 接続によるトンネルのポリシングの前に、「host-specific」クラスをポリシングできます。この例では、トンネルの前で「host-specific」トラフィックのレートが制限され、次にトンネルのレートが制限されます。

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

プライオリティとポリシングの例

次の例は、前の項で作成したコンフィギュレーションで構築されています。前の例と同様に、tcp_traffic と TG1-voice という 2 つのクラスマップがあります。

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

第3のクラスマップを追加することで、次のように、トンネルおよび非トンネルQoSポリシーを定義する基本が提供されます。トンネルおよび非トンネル トラフィックに対する単純なQoSポリシーが作成され、クラスTG1-voiceのパケットが低遅延キューに割り当てられ、tcp_trafficおよびTG1-best-effort トラフィック フローにレート制限が設定されます。

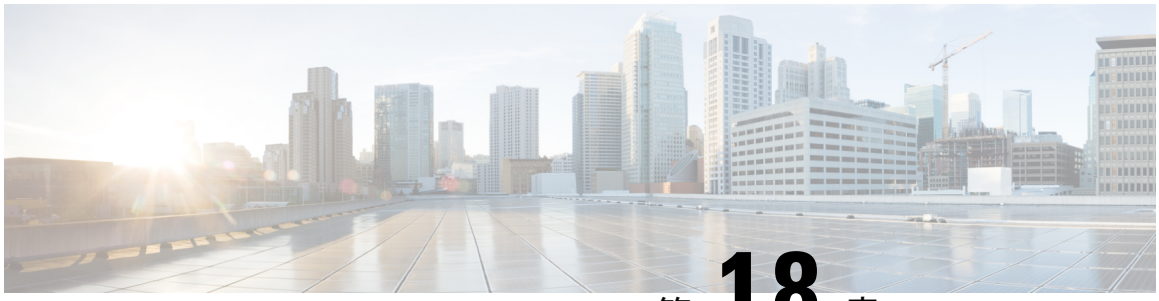
この例では、tcp_trafficクラスのトラフィックの最大レートは56,000ビット/秒で、最大バースト サイズは10,500バイト/秒です。TC1-BestEffortクラスの最大レートは200,000ビット/秒で、最大バーストは37,500バイト/秒です。TC1-voiceクラスのトラフィックは、プライオリティ クラスに属しているため、最大速度またはバースト レートでポリシングされません。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

hostname(config)# class-map TG1-voice
```

```
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos global
```

QoS の履歴

機能名	プラットフォームリリース	説明
プライオリティ キューイングとポリシング	7.0(1)	QoS プライオリティ キューイングとポリシングが導入されました。 **priority-queue**、**queue-limit**、**tx-ring-limit**、**priority**、**police**、**show priority-queue statistics**、**show service-policy police**、**show service-policy priority**、**show running-config priority-queue**、**clear configure priority-queue** の各コマンドが導入されました。
シェーピングおよび階層型プライオリティ キューイング	7.2(4)/8.0(4)	QoS シェーピングおよび階層型プライオリティ キューイングが導入されました。 **shape**、**show service-policy shape** の各コマンドが導入されました。
ASA 5585-X での 10 ギガビット イーサネットによる標準プライオリティ キューのサポート	8.2(3)/8.4(1)	ASA 5585-X の 10 ギガビット イーサネット インターフェイスでの標準プライオリティ キューのサポートが追加されました。



第 18 章

脅威の検出

次のトピックでは、脅威検出の統計情報およびスキャン脅威検出を設定する方法について説明します。

- 脅威の検出 （513 ページ）
- 脅威検出のガイドライン （516 ページ）
- 脅威検出のデフォルト （517 ページ）
- 脅威検出の設定 （518 ページ）
- 脅威検出のモニタリング （524 ページ）
- 脅威検出の例 （534 ページ）
- 脅威検出の履歴 （535 ページ）

脅威の検出

ASA の脅威検出は、攻撃に対して最前線で防御する機能です。脅威検出は、パケット ドロップの統計を分析し、トラフィック パターンに基づいた「トップ」レポートを蓄積することで、レイヤ 3 と 4 にトラフィックのベースラインを作成します。一方、IPS または次世代 IPS サービスを提供するモジュールは、ASA が許可したトラフィックの攻撃ベクトルをレイヤ 7 まで識別して軽減させますが、すでに ASA がドロップしたトラフィックは認識できません。そのため、脅威検出と IPS を一緒に使用することで、より総合的な脅威に対する防御を可能にします。

脅威検出は次の要素から構成されています。

- さまざまな脅威を収集する複数レベルの統計情報

  脅威検出統計情報は、ASA に対する脅威の管理に役立ちます。たとえば、スキャン脅威検出をイネーブルにすると、統計情報を見ることで脅威を分析できます。次の 2 種類の脅威検出統計情報を設定できます。

  - 基本脅威検出統計情報：システムに対する攻撃アクティビティについての全体的な情報を含みます。基本脅威検出統計情報はデフォルトでイネーブルになっており、パフォーマンスに対する影響はありません。「基本脅威検出統計情報 （514 ページ）」を参照してください。

- 拡張脅威検出統計情報：オブジェクト レベルでアクティビティを追跡するので、ASA は個別のホスト、ポート、プロトコル、または ACL についてのアクティビティを報告できます。拡張脅威検出統計情報は、収集される統計情報によってはパフォーマンスに大きく影響するので、デフォルトでは ACL の統計情報だけがイネーブルになっています。「拡張脅威検出統計情報 （515 ページ）」を参照してください。

- ホストがスキャンを実行する時期を決定するスキャン脅威検出機能オプションとして、スキャン脅威であることが特定されたホストを排除できます。「スキャン脅威検出 （515 ページ）」を参照してください。
- IPv4 アドレスからの次のタイプの VPN 攻撃に対して保護するために使用できる VPN サービスの脅威検出。
  - リモートアクセス VPN への過剰な認証失敗の試行（ユーザー名/パスワードをスキャンするブルートフォース攻撃など）。
  - クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。
  - 無効な VPN サービス、つまり内部専用サービスへのアクセス試行。

  アクセスに失敗したとしても、これらの攻撃によってコンピューティングリソースを消費し、場合によってはサービス拒否（DoS）を引き起こす可能性があります。VPN サービスの脅威検出の設定 （522 ページ） を参照してください。

基本脅威検出統計情報

ASA は、基本脅威検出統計情報を使用して、次の理由でドロップしたパケットおよびセキュリティ イベントの割合をモニターします。

- ACL による拒否。
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）。
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）。
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）。
- 基本ファイアウォール検査に不合格。このオプションは、このリストのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
- 疑わしい ICMP パケットの検出。
- アプリケーション インスペクションに不合格のパケット。
- インターフェイスの過負荷。

- スキャン攻撃の検出。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニターします。フル スキャン脅威検出では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します。
- 不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）。

ASA は、脅威を検出するとただちにシステム ログ メッセージ（733100）を送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバーストイベント レートの 2 種類のレートを追跡します。バースト レート間隔は、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。ASA は、受信するイベントごとに平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA は、バースト期間におけるレート タイプごとに最大 1 つのメッセージの割合で 2 つの別々のシステム メッセージを送信します。

基本脅威検出は、ドロップまたは潜在的な脅威が存在した場合にだけパフォーマンスに影響します。このようなシナリオでも、パフォーマンスへの影響はわずかです。

拡張脅威検出統計情報

拡張脅威検出統計情報は、ホスト、ポート、プロトコル、ACL などの個別のオブジェクトについて、許可されたトラフィック レートとドロップされたトラフィック レートの両方を表示します。

注意 拡張統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、ASA のパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きく影響します。トラフィックの負荷が高い場合は、このタイプの統計情報を一時的にイネーブルにすることを検討してください。ただし、ポート統計情報の影響はそれほど大きくありません。

スキャン脅威検出

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック シグニチャに基づく IPS スキャン検出とは異なり、ASA の脅威検出スキャンでは、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

スキャン脅威レートを超過すると、ASA は syslog メッセージ（733101）を送信し、必要に応じて攻撃者を排除します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。スキャン攻撃の一部と見なされるイベントが検出されるたびに、ASA は平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。

次の表に、スキャン脅威検出のデフォルトのレート制限を示します。

表 *15 :* スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。

注意 スキャンによる脅威の検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、ASA のパフォーマンスとメモリに大きく影響することがあります。

脅威検出のガイドライン

セキュリティ コンテキストのガイドライン

高度な脅威統計および VPN サービスを除き、脅威検出はシングルモードのみでサポートされます。マルチモードでは、TCP 代行受信の統計情報が唯一サポートされている統計情報です。

モニター対象トラフィックのタイプ

- 統計では、through-the-box トラフィックのみがモニターされます。to-the-box トラフィックはモニターされません。
- ACL によって拒否されたトラフィックは、スキャン脅威検出をトリガーしません。ASA から許可され、フローを作成したトラフィックだけがスキャン脅威検出の影響を受けます。
- VPN サービスの場合、IPv4 アドレスからの to-the-box トラフィックのみがモニターされます。

脅威検出のデフォルト

基本脅威検出統計情報は、デフォルトでイネーブルになっています。

次の表に、デフォルト設定を示します。これらのデフォルト設定すべてを表示するには、**show running-config all threat-detection** コマンドを 使用します。

高度な統計情報では、ACL の統計情報はデフォルトでイネーブルになっています。

VPN サービス脅威検出では、すべてのサービスがデフォルトで無効になっています。

表 *16* : 基本的な脅威の検出のデフォルト設定

パケット ドロップの理由	トリガー設定	
	平均レート	バースト レート
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしいICMPパケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 320 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 120 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 160 ドロップ/秒。
ACL による拒否	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。

パケット ドロップの理由	トリガー設定	
	平均レート	バースト レート
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 120 秒間で 6400 ドロップ/秒。

脅威検出の設定

基本脅威検出統計情報はデフォルトでイネーブルになっており、ユーザーが必要とする唯一の脅威検出サービスである場合があります。さらに脅威検出サービスを実行する場合は、次の手順を使用します。

手順

ステップ 1 基本脅威検出統計情報の設定 （518 ページ）。

基本脅威検出統計情報には、DoS 攻撃（サービス拒絶攻撃）などの攻撃に関連している可能性があるアクティビティが含まれます。

ステップ 2 拡張脅威検出統計情報の設定 （519 ページ）。

ステップ 3 スキャン脅威検出の設定 （521 ページ）。

ステップ 4 VPN サービスの脅威検出の設定 （522 ページ）。

基本脅威検出統計情報の設定

基本脅威検出統計情報は、デフォルトでイネーブルになっています。ディセーブルにすることも、一度ディセーブルにしたあと再度イネーブルにすることもできます。

手順

ステップ 1 基本脅威検出統計情報をイネーブルにします（ディセーブルになっている場合）。

threat-detection basic-threat

例：

```
hostname(config)# threat-detection basic-threat
```

基本脅威検出は、デフォルトでイネーブルになっています。これをディセーブルにするには **no threat-detection basic-threat** を使用します。

ステップ 2 （任意）各イベント タイプのデフォルト設定を変更します。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

各イベント タイプの説明については、「基本脅威検出統計情報（ページ 8-1）」を参照してください。

scanning-threat キーワードを指定してこのコマンドを使用すると、スキャン脅威検出機能でもこのコマンドが使用されます。基本脅威検出を設定しない場合でも、**scanning-threat** キーワードを指定してこのコマンドを使用し、スキャン脅威検出でのレート制限を設定できます。

イベント タイプごとに、異なるレート間隔を 3 つまで設定できます。

例：

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

拡張脅威検出統計情報の設定

広範な統計情報を収集するように ASA を設定することができます。デフォルトでは、ACL の統計情報はイネーブルになっています。他の統計情報をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 （任意）すべての統計情報をイネーブルにします。

threat-detection statistics

特定の統計情報だけをイネーブルにするには、（この手順で後に示す）各統計情報タイプに対してこのコマンドを入力し、オプションを指定しないでコマンドを入力しないようにします。**threat-detection statistics** を（何もオプションを指定しないで）入力した後、統計情報固有のオプション（たとえば **threat-detection statistics host number-of-rate 2**）を指定してコマンドを入力することで、特定の統計情報をカスタマイズできます。**threat-detection statistics** を（何もオプションを指定しないで）入力した後、特定の統計情報のコマンドを、統計情報固有のオプションを指定しないで入力した場合は、すでにイネーブルになっているので、そのコマンドによる効果は何もありません。

このコマンドの **no** 形式を入力すると、すべての **threat-detection statistics** コマンドが削除されます。これには、デフォルトでイネーブルになる **threat-detection statistics access-list** コマンドも含まれます。

例：

```
hostname(config)# threat-detection statistics
```

ステップ 2 （任意）ACL の統計情報をイネーブルにします（ディセーブルになっている場合）。

threat-detection statistics access-list

ACL の統計情報は、デフォルトでイネーブルになっています。ACL 統計情報は、show threat-detection top access-list コマンドを使用した場合にだけ表示されます。

例：

```
hostname(config)# threat-detection statistics access-list
```

ステップ 3 （任意）ホスト（host キーワード）、TCP および UDP ポート（port キーワード）、または非 TCP/UDP IP プロトコル（protocol キーワード）の統計情報を設定します。

threat-detection statistics {**host** | **port** | **protocol**} [**number-of-rate** {**1** | **2** | **3**}]

number-of-rate キーワードは、統計情報で保持するレート間隔の数を設定します。デフォルトのレート間隔の数は**1**です。メモリの使用量を低く抑えます。より多くのレート間隔を表示するには、値を **2** または **3** に設定します。たとえば、値を **3** に設定すると、直前の 1 時間、8 時間、および 24 時間のデータが表示されます。このキーワードを **1** に設定した場合（デフォルト）、最も短いレート間隔統計情報だけが保持されます。値を **2** に設定すると、短い方から 2 つの間隔が保持されます。

ホストがアクティブで、スキャン脅威ホストデータベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。

例：

```
hostname(config)# threat-detection statistics host number-of-rate 2
hostname(config)# threat-detection statistics port number-of-rate 2
hostname(config)# threat-detection statistics protocol number-of-rate 3
```

ステップ 4 （オプション）TCP 代行受信によって代行受信される攻撃の統計情報を設定します。

threat-detection statistics tcp-intercept [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

それぞれの説明は次のとおりです。

- **rate-interval** は、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間隔の間に、ASA は攻撃の数を 30 回サンプリングします。
- **burst-rate** は、syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。

- **average-rate** は、syslog メッセージ生成の平均レートしきい値を、25 ～ 2147483647 の範囲で設定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。

TCP 代行受信を有効にするには、SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信） （464 ページ） を参照してください。

（注） このコマンドは、他の threat-detection コマンドとは異なり、マルチ コンテキスト モードで用意されています。

例：

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60
burst-rate 800 average-rate 600
```

スキャン脅威検出の設定

攻撃者を識別し、必要に応じて排除するため、スキャン脅威検出を設定できます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。デフォルトでは、ホストが攻撃者として識別されると、システム ログ メッセージ 730101 が生成されます。ホストから大量のメッセージが送信されることが予想される場合は、アドレスを排除から除外するようにしてください。たとえば、Pluggable Interface Module（PIM）マルチキャストを有効にした場合、PIM ルータまたは PIM メッセージがドロップされます。

手順

ステップ 1 スキャン脅威検出をイネーブルにします。

threat-detection scanning-threat [**shun** [**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*}]]

デフォルトでは、ホストが攻撃者であると識別されると、システム ログ メッセージ 733101 が生成されます。このコマンドを複数回入力し、複数の IP アドレスまたはネットワーク オブジェクト グループを特定して遮断対象から除外できます。

例：

```
hostname(config)# threat-detection scanning-threat shun except
ip-address 10.1.1.0 255.255.255.0
```

ステップ 2 （任意）攻撃元のホストを遮断する期間を設定します。

threat-detection scanning-threat shun duration *seconds*

例：

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

ステップ 3 （任意）ASA がホストを攻撃者またはターゲットとして識別する場合のデフォルト イベント制限を変更します。

threat-detection rate scanning-threat rate-interval *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

このコマンドが基本脅威検出コンフィギュレーションの一部としてすでに設定されている場合、それらの設定はスキャン脅威検出機能でも共有され、基本脅威検出とスキャン脅威検出で個別にレートを設定することはできません。このコマンドを使用してレートを設定しない場合は、基本脅威検出機能とスキャン脅威検出機能の両方でデフォルト値が使用されます。個別にコマンドを入力することで、異なるレート間隔を 3 つまで設定できます。

例：

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200
average-rate 10 burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400
average-rate 10 burst-rate 20
```

VPN サービスの脅威検出の設定

VPN サービスの脅威検出を有効にして、IPv4 アドレスからのサービス妨害（DoS）攻撃を防ぐことができます。次のタイプの攻撃に使用できる個別のサービスがあります。

- リモートアクセス VPN ログイン認証攻撃者が、パスワードスプレー攻撃でログイン試行を繰り返し開始することで認証試行に使用されるリソースを消費し、実数のユーザーが VPN にログインできなくなる可能性があります。
- クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。パスワードスプレー攻撃と同様に、この攻撃はリソースを消費し、有効なユーザーが VPN に接続できなくなる可能性があります。
- 無効な VPN サービス、つまり内部使用専用サービスに接続しようとします。この接続を試みる IP アドレスは、ただちに排除されます。

これらのサービスを有効にすると、システムはしきい値を超えたホストを自動的に排除して、それ以上の試行されないようにします。アドレスに対して **no shun** コマンドを使用して、排除を手動で削除できます。

サービスのカウンタを手動で 0 にリセットするには、**clear threat-detection service** コマンドを使用します。

始める前に

適切なホールドダウン値としきい値を決定する場合は、環境での NAT の使用を検討してください。PAT を使用して、同じ IP アドレスから多数の要求を送信できるようにする場合は、認証失敗とクライアント開始サービスの値を大きくして、有効なユーザーが接続を完了するのに十分な時間を確保できるようにする必要があります。たとえば、多くのお客様が非常に短い時間内に接続を試みるホテルなどです。

手順

ステップ 1 リモートアクセス VPN 認証失敗の脅威検出を有効にします。

threat-detection service remote-access-authentication hold-down *minutes* **threshold** *count*

それぞれの説明は次のとおりです。

- **hold-down** *minutes* は、最後の失敗からのホールドダウン期間を定義します。攻撃者の IPv4 アドレスの排除をトリガーするには、前回の失敗とのホールドダウン期間内に連続失敗のしきい値カウントに達する必要があります。たとえば、ホールドダウン期間が 10 分でしきい値が 20 で、単一の IPv4 アドレスからの連続した認証失敗が 20 回あり、2 つの連続した失敗間のタイムスパンが 10 分を超えない場合、送信元 IPv4 アドレスは排除されます。1 ～ 1440 分の時間を指定できます。
- **threshold** *count* は、排除をトリガーするためにホールドダウン期間内に発生する必要がある試行の失敗数を定義します。1 ～ 100 のしきい値を指定できます。

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service remote-access-authentication

例：

次の例では、20 分以内に 10 回の失敗のメトリックを設定します。

```
ciscoasa(config)# threat-detection service remote-access-authentication
hold-down 10 threshold 20
```

ステップ 2 リモートアクセス VPN クライアント開始の脅威検出を有効にします。

threat-detection service remote-access-client-initiations hold-down *minutes* **threshold** *count*

それぞれの説明は次のとおりです。

- **hold-down** *minutes* は、最後の開始からのホールドダウン期間を定義します。クライアントの IPv4 アドレスの排除をトリガーするには、前回の開始とのホールドダウン期間内に、連続する開始のしきい値カウントに達する必要があります。たとえば、ホールドダウン期間が 10 分でしきい値が 20 で、単一の IPv4 アドレスからの連続した開始が 20 回あり、2

つの連続した開始間のタイムスパンが 10 分を超えない場合、送信元 IPv4 アドレスは排除されます。1 ～ 1440 分の時間を指定できます。

- **threshold** *count* は、排除をトリガーするためにホールドダウン期間内に発生する必要がある開始の数を定義します。5 ～ 100 のしきい値を指定できます。

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service remote-access-client-initiations

例：

次の例では、20 分以内に 10 回の開始のメトリックを設定します。

```
ciscoasa(config)# threat-detection service remote-access-client-initiations
hold-down 10 threshold 20
```

ステップ 3 無効な VPN サービスへの接続試行の脅威検出を有効にします。

threat-detection service invalid-vpn-access

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service invalid-vpn-access

例：

次の例では、Invalid VPN Access サービスを有効にしています。

```
ciscoasa(config)# threat-detection service invalid-vpn-access
```

脅威検出のモニタリング

次のトピックでは、脅威検出のモニタリングとトラフィック統計情報を表示する方法を説明します。

基本脅威検出統計情報のモニタリング

次のコマンドを使用して、基本脅威検出統計情報を表示します。

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

min-display-rate *min_display_rate* 引数により、毎秒あたりの最小表示レートを超過する統計情報に表示内容を限定します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

他の引数を使用すると、特定のカテゴリに表示を制限できます。各イベントタイプの説明については、基本脅威検出統計情報 （514 ページ）を参照してください。

出力には、直前の 10 分と直前の 1 時間の固定された 2 期間における平均レート（イベント数/秒）が表示されます。また、最後に終了したバースト間隔（平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほう）における現在のバースト レート（イベント数/秒）、レートが超過した回数（トリガーした回数）、およびその期間の合計イベント数も表示されます。

ASA は、各バースト期間の終わりにカウント数を保存します。合計で 30 回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

clear threat-detection rate コマンドを使用して統計情報を消去できます。

次に、**show threat-detection rate** コマンドの出力例を示します。

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

拡張脅威検出統計情報のモニタリング

拡張脅威検出統計情報をモニターするには、次の表に示すコマンドを使用します。ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASA は、各バースト期間の終わりにカウント数を保存します。合計で 30 回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、

平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

コマンド	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] **detail**]]	上位10件の統計情報を表示します。オプションを入力しない場合は、カテゴリ全体での上位 10 件の統計情報が表示されます。 **min-display-rate** *min_display_rate* 引数により、毎秒あたりの最小表示レートを超過する統計情報に表示内容を限定します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。 次の行は、オプション キーワードを示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top access-list** [**rate-1** | **rate-2** | **rate-3**]	許可 ACE と拒否 ACE の両方を含め、パケットに一致する上位 10 件の ACE を表示するには、**access-list** キーワードを使用します。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにする場合は、**show threat-detection rate acl-drop** コマンドを使用して、ACL による拒否を追跡できます。 **rate-1** キーワードを指定すると、表示できる最小固定レート間隔の統計情報が表示され、**rate-2** を指定すると次に大きなレート間隔の統計情報が表示されます。3 つの間隔が定義されている場合には、**rate-3** を指定すると最大レート間隔の統計情報が表示されます。たとえば、ディスプレイに直前の 1 時間、8 時間、および 24 時間の統計情報が表示されるとします。**rate-1** キーワードを設定すると、ASA は 1 時間の統計情報だけを表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top host** [**rate-1** | **rate-2** | **rate-3**]	ホスト統計情報だけを表示するには、**host** キーワードを使用します。 **注**：脅威検出アルゴリズムに起因して、フェールオーバー リンクとステート リンクの組み合わせとして使用されるインターフェイスは上位 10 個のホストに表示されることがあります。これは予期された動作であり、表示される IP アドレスは無視できます。

コマンド	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top port-protocol** [**rate-1** | **rate-2** | **rate-3**]	ポートおよびプロトコルの統計情報を表示するには、**port-protocol** キーワードを使用します。**port-protocol** キーワードを指定すると、ポートとプロトコルの両方の統計情報が表示され（表示するには、両方がイネーブルに設定されている必要があります）、TCP/UDP ポートと IP プロトコル タイプを組み合わせた統計情報が表示されます。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ（ポートまたはプロトコル）の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top tcp-intercept** [**all**] **detail**]]	TCP 代行受信の統計情報だけを表示するには、**tcp-intercept** キーワードを使用します。表示には、攻撃を受けて保護された上位 10 サーバーが含まれます。**all** キーワードは、トレースされているすべてのサーバーの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]	すべてのホスト、特定のホスト、または特定のサブネットの統計情報を表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[*-end_port*]]	すべてのポート、特定のポート、または特定のポート範囲の統計情報を表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol*]	すべての IP プロトコルまたは特定のプロトコルの統計情報を表示します。 *protocol_number* 引数は、0 ～ 255 の整数です。プロトコルの引数には、**ah**、**eigrp**、**esp**、**gre**、**icmp**、**icmp6**、**igmp**、**igrp**、**ip**、**ipinip**、**ipsec**、**nos**、**ospf**、**pcp**、**pim**、**pptp**、**snp**、**tcp**、**udp** のいずれかを指定できます。

ホストの脅威検出統計情報の評価

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0

  1-hour Sent byte:              2938              0       0             10580308
  8-hour Sent byte:               367              0       0             10580308
 24-hour Sent byte:               122              0       0             10580308
  1-hour Sent pkts:                28              0       0               104043
```

```
  8-hour Sent pkts:                  3               0       0                104043
 24-hour Sent pkts:                  1               0       0                104043
  20-min Sent drop:                  9               0       1                 10851
  1-hour Sent drop:                  3               0       1                 10851
  1-hour Recv byte:               2697               0       0               9712670
  8-hour Recv byte:                337               0       0               9712670
 24-hour Recv byte:                112               0       0               9712670
  1-hour Recv pkts:                 29               0       0                104846
  8-hour Recv pkts:                  3               0       0                104846
 24-hour Recv pkts:                  1               0       0                104846
  20-min Recv drop:                 42               0       3                 50567
  1-hour Recv drop:                 14               0       1                 50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                   614
  8-hour Sent byte:                  0               0       0                   614
 24-hour Sent byte:                  0               0       0                   614
  1-hour Sent pkts:                  0               0       0                     6
  8-hour Sent pkts:                  0               0       0                     6
 24-hour Sent pkts:                  0               0       0                     6
  20-min Sent drop:                  0               0       0                     4
  1-hour Sent drop:                  0               0       0                     4
  1-hour Recv byte:                  0               0       0                   706
  8-hour Recv byte:                  0               0       0                   706
 24-hour Recv byte:                  0               0       0                   706
  1-hour Recv pkts:                  0               0       0                     7
```

次の表は出力について示しています。

表 *17 : show threat-detection statistics host*

フィールド	説明
ホスト（Host）	ホストの IP アドレス。
tot-ses	ホストがデータベースに追加されて以降の、このホストでの合計セッション数。
act-ses	ホストが現在関係しているアクティブなセッションの合計数。
fw-drop	ファイアウォール ドロップの数。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケット ドロップを含む組み合わせレートです。これには、ACL での拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、および戻りデータなし UDP 攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop	アプリケーション インスペクションに不合格になったためにドロップされたパケット数。
null-ses	ヌル セッションの数。ヌル セッションは、3 秒間のタイムアウト内に完了しなかった TCP SYN セッション、およびセッション開始の 3 秒後までにサーバーからデータが送信されなかった UDP セッションです。

フィールド	説明
bad-acc	閉じられた状態のホストのポートに対する不正なアクセスの試行回数。ポートがヌルセッションと判断されると（null-sesフィールドの説明を参照）、ホストのポートの状態はHOST_PORT_CLOSEに設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。
Average(eps)	各間隔における平均レート（イベント数/秒）。 ASAは、各バースト期間の終わりにカウント数を保存します。合計で30回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が20分の場合、バースト間隔は20秒になります。最後のバースト間隔が3:00:00～3:00:20で、3:00:25に**show**コマンドを使用すると、最後の5秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の29回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。
Current(eps)	終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の1/30と10秒のうち、どちらか大きいほうの間隔。Average(eps)の説明で示された例の場合、現在レートは3:19:30～3:20:00のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に0です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の29回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

フィールド	説明
20-min、1-hour、8-hour、および24-hour	これらの固定レート間隔の統計情報。各インターバルごとに、以下を示します。 • [Sent byte]：ホストから正常に送信されたバイト数。 • [Sent pkts]：ホストから正常に送信されたパケット数。 • [Sent drop]：ホストから送信された、スキャン攻撃の一部であったためにドロップされたパケット数。 • [Recv byte]：ホストが受信した正常なバイト数。 • [Recv pkts]：ホストが受信した正常なパケット数。 • [Recv drop]：ホストが受信したパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数。

スキャン脅威検出の排除されたホスト、攻撃者、ターゲットのモニタリング

スキャン脅威検出の排除されたホスト、攻撃者、ターゲットをモニターおよび管理するには、次のコマンドを使用します。これらのコマンドは、スキャン脅威検出専用であり、他のサービスには適用されません。

- **show threat-detection shun**

  現在遮断されているホストを表示します。次に例を示します。

```
hostname# show threat-detection shun

Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

- **clear threat-detection shun** [*ip_address* [*mask*]]

  ホストを回避対象から解除します。IPアドレスを指定しない場合は、すべてのホストが遮断リストからクリアされます。

  たとえば、10.1.1.6 のホストを解除するには、次のコマンドを入力します。

```
hostname# clear threat-detection shun 10.1.1.6
```

- **show threat-detection scanning-threat** [**attacker** | **target**]

  ASAが攻撃者（遮断リストのホストを含む）と判断したホスト、および攻撃のターゲットにされたホストを表示します。オプションを入力しない場合は、攻撃者とターゲットの両方のホストが表示されます。次に例を示します。

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

VPN サービスの脅威検出のモニタリング

次のトピックで説明するように、syslog および show コマンドを使用して、VPN サービスの脅威検出をモニターできます。

VPN サービスの脅威検出の Syslog モニタリング

これらのサービスに関連する次の syslog メッセージが表示される場合があります。

- %ASA-6-733200: Threat-detection Info: *message*

  このメッセージは、脅威検出に関する一般的な情報イベントを報告します。

- %ASA-4-733201: Threat-detection: Service[*service*] Peer[*peer*]: threshold of *threshold-value* was exceeded. Adding shun to interface *interface*.*Additional_message*

  このメッセージは、指定されたサービスの不審なアクティビティが原因で、脅威検出サービスが IP アドレスを排除したことを示しています。メッセージには追加情報が含まれている場合があります。たとえば、RA VPN クライアント開始試行の場合、追加情報は「SSL（または IKEv2）：RA 過剰なクライアント開始要求（SSL (or IKEv2): RA excessive client initiation requests.）」のようになります。

  show shun コマンドを使用して、排除されたホストのリストを表示できます。IP アドレスが攻撃者ではないことがわかっている場合は、**no shun** コマンドを使用して排除を削除できます。

VPN サービスの脅威検出の show コマンドによるモニタリング

次のコマンドを使用して、VPN サービスの脅威検出の統計情報を表示します。

show threat-detection service [*service*] [**entries** | **details**]

必要に応じて、特定のサービス（**remote-access-authentication**、**remote-access-client-initiations**、または **invalid-vpn-access**）にビューを制限できます。次のパラメータを追加することで、ビューをさらに制限できます。

- **entries**：追跡対象のエントリのみを表示します。たとえば、認証試行に失敗した IP アドレスです。
- **details**：サービスの詳細とサービスエントリの両方を表示します。

選択したオプションに基づいて、ディスプレイ出力には次の情報が表示されます。

- サービスの名前
- サービスの状態：有効または無効
- サービスホールドダウン設定
- サービスしきい値設定
- サービスアクション統計情報
  - [失敗（Failed）]：報告された発生の処理中に障害が発生しました。
  - [ブロッキング（Blocking）]：報告された発生はホールドダウン期間内であり、しきい値に達したか超過しました。その結果、サービスは、不正なピアをブロックするための排除を自動的にインストールしました。
  - [記録（Recording）]：報告された発生がホールドダウン期間外であるか、しきい値に達したか超過しました。その結果、サービスは発生を記録します。
  - [サポート対象外（Unsupported）]：報告された発生は、現在自動排除をサポートしていません。
  - [無効（Disabled）]：発生が報告されました。ただし、サービスは無効になっています。

例

次の例では、すべてのサービスが有効になっており、リモートアクセス認証サービスについて潜在的な攻撃者が追跡されています。

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
```

```
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 3
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

次に、**show threat-detection service entries** コマンドの例を示します。

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721          0
  2 192.168.100.102/ 32              outside              2         486        114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

次に、**show threat-detection service details** コマンドの例を示します。

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721          0
  2 192.168.100.102/ 32              outside              2         486        114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

VPN サービス違反に適用された排除の削除

次のコマンドを使用して、VPN サービスに適用された排除をモニターし、排除を削除できます。VPN サービスの脅威検出によって適用される排除は、**show threat-detection shun** コマンドには表示されないことに注意してください。このコマンドは、スキャン脅威検出にのみ適用されます。

- **show shun** [*ip_address*]

  VPN サービスの脅威検出によって自動的に排除されたホスト、または **shun** コマンドを使用して手動で排除されたホストを含む、排除されたホストを表示します。必要に応じて、指定した IP アドレスにビューを制限できます。

- **no shun** *ip_address* [**interface** *if_name*]

  指定した IP アドレスからのみ排除を削除します。アドレスが複数のインターフェイスで排除され、一部のインターフェイスで排除をそのままにしておく場合は、オプションで排除のインターフェイス名を指定できます。

- **clear shun**

  すべての IP アドレスから排除を削除します。

脅威検出の例

次の例では、基本脅威検出統計情報を設定し、DoS 攻撃レートの設定を変更しています。すべての拡張脅威検出統計情報はイネーブルであり、ホスト統計情報のレート間隔数は 2 に減らされています。TCP 代行受信のレート間隔もカスタマイズされています。スキャン脅威検出はイネーブルで、10.1.1.0/24 を除くすべてのアドレスを自動遮断します。スキャン脅威レート間隔はカスタマイズされています。

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate
600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

脅威検出の履歴

機能名	プラットフォームリリース	説明
基本および拡張脅威検出統計情報、スキャン脅威検出	8.0(2)	基本および拡張脅威検出統計情報、スキャン脅威検出が導入されました。 次のコマンドが導入されました：**threat-detection basic-threat**、**threat-detection rate**、**show threat-detection rate**、**clear threat-detection rate**、**hreat-detection statistics**、**show threat-detection statistics**、**threat-detection scanning-threat**、**threat-detection rate scanning-threat**、**show threat-detection scanning-threat**、**show threat-detection shun**、**clear threat-detection shun**。
排除期間	8.0(4)/8.1(2)	排除期間を設定できるようになりました。 **threat-detection scanning-threat shun duration** コマンドが導入されました。
TCP 代行受信の統計情報	8.0(4)/8.1(2)	TCP 代行受信の統計情報が導入されました。 **threat-detection statistics tcp-intercept**、**show threat-detection statistics top tcp-intercept**、**clear threat-detection statistics** コマンドが変更または導入されました。
ホスト統計情報レート間隔のカスタマイズ	8.1(2)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 **threat-detection statistics host number-of-rates** コマンドが変更されました。
バースト レート間隔が平均レートの 1/30 に変更されました。	8.2(1)	以前のリリースでは、平均レートの 1/60 でした。メモリを最大限に使用するため、サンプリング間隔が平均レートの間に 30 回に減らされました。
ポートおよびプロトコル統計情報レート間隔のカスタマイズ	8.3(1)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 **threat-detection statistics port number-of-rates**、**threat-detection statistics protocol number-of-rates** コマンドが変更されました。

機能名	プラットフォームリリース	説明
メモリ使用率の向上	8.3(1)	脅威検出のメモリ使用率が向上しました。 **show threat-detection memory** コマンドが導入されました。
VPN サービスの脅威検出	9.20(3)	VPN サービスの脅威検出を設定して、IPv4 アドレスからの次のタイプの VPN 攻撃に対して保護できます。 • リモートアクセス VPN への過剰な認証失敗の試行（ユーザー名/パスワードをスキャンするブルートフォース攻撃など）。 • クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。 • 無効な VPN サービス、つまり内部専用サービスへのアクセス試行。 アクセスに失敗したとしても、これらの攻撃によってコンピューティングリソースを消費し、場合によってはサービス拒否（DoS）を引き起こす可能性があります。 **clear threat-detection service**、**show threat-detection service**、**shun**、**threat-detection service** の各コマンドが導入または変更されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。