



CLI ブック 3 : Cisco Secure Firewall ASA VPN 9.22 CLI コンフィギュレーション ガイド

最終更新 : 2025 年 8 月 29 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 NON-INFRINGEMENT 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)

© 2025 Cisco Systems, Inc. All rights reserved.



目次

はじめに :

[このマニュアルについて](#) **xv**

[本書の目的](#) **xv**

[関連資料](#) **xv**

[表記法](#) **xv**

[通信、サービス、およびその他の情報](#) **xvii**

第 1 章

[IPsec および ISAKMP](#) **1**

[トンネリング、IPsec、および ISAKMP について](#) **1**

[IPsec の概要](#) **2**

[ISAKMP および IKE の概要](#) **2**

[IKEv2 複数ピアクリプトマップについて](#) **4**

[IPsec VPN のライセンス](#) **7**

[IPsec VPN のガイドライン](#) **8**

[ISAKMP の設定](#) **8**

[IKEv1 ポリシーと IKEv2 ポリシーの設定](#) **8**

[IKE ポリシー キーワードと値](#) **10**

[外部インターフェイスでの IKE のイネーブル化](#) **12**

[IKEv1 アグレッシブモードのイネーブル化またはディセーブル化](#) **13**

[IKEv1 および IKEv2 ISAKMP ピアの識別方式の決定](#) **13**

[INVALID_SELECTORS 通知](#) **14**

[16 進数の IKEv2 事前共有キーの設定](#) **15**

[IKE 通知の送信の有効化または無効化](#) **15**

[IKEv2 フラグメンテーション オプションの設定](#) **15**

[AAA 認証と認可](#) **17**

IPsec over NAT-T のイネーブル化	17
IPsec with IKEv1 over TCP のイネーブル化	19
IKEv1 の証明書グループ照合の設定	20
IPsec の設定	22
暗号マップの定義	22
LAN-to-LAN 暗号マップの例	26
公開キー インフラストラクチャ (PKI) キーの設定	32
クリプト マップのインターフェイスへの適用	33
インターフェイス ACL の使用	33
IPsec SA のライフタイムの変更	36
VPN ルーティングの変更	37
スタティック暗号マップの作成	38
ダイナミック暗号マップの作成	43
サイトツーサイト冗長性の実現	46
IPsec VPN の管理	47
IPsec コンフィギュレーションの表示	47
リブートの前にアクティブセッションの終了を待機	48
接続解除の前にピアに警告する	48
セキュリティ アソシエーションのクリア	49
暗号マップ コンフィギュレーションのクリア	49

第 2 章

L2TP over IPsec	51
L2TP over IPsec/IKEv1 VPN について	51
IPsec の転送モードとトンネル モード	52
L2TP over IPsec のライセンス要件	53
L2TP over IPsec を設定するための前提条件	54
注意事項と制約事項	54
CLI での L2TP over Eclipse の設定	56
Windows 7 のプロポーザルに応答するための IKE ポリシーの作成	59
L2TP over IPsec の設定例	60
L2TP over IPsec の機能履歴	61

第 3 章

ハイアベイラビリティ オプション 63

ハイアベイラビリティ オプション 63

Secure Firewall eXtensible オペレーティングシステム (FXOS) シャーシ上の VPN とクラス
タリング 63

VPN ロード バランシング 64

フェールオーバー 64

VPN ロード バランシング 65

VPN ロードバランシングについて 65

VPN ロードバランシングのアルゴリズム 66

VPN ロードバランシンググループ構成 66

VPN ロード バランシング ディレクタの選択 67

VPN ロードバランシングについてよく寄せられる質問 (FAQ) 68

VPN ロードバランシングのライセンス 69

VPN ロードバランシングの前提条件 70

VPN ロード バランシングに関するガイドラインと制限事項 70

VPN ロード バランシングの設定 72

ロードバランシング用のパブリックインターフェイスとプライベートインターフェイ
スの設定 73

VPN ロードバランシンググループ属性の設定 74

VPN ロード バランシングの設定例 77

VPN ロードバランシング情報の表示 78

VPN ロードバランシングの機能履歴 78

第 4 章

全般 VPN パラメータ 79

注意事項と制約事項 79

ACL をバイパスするための IPsec の設定 80

インターフェイス内トラフィックの許可 (ヘアピニング) 81

インターフェイス内トラフィックにおける NAT の注意事項 82

アクティブな IPsec セッションまたは SSL VPN セッションの最大数の設定 83

許可される IPsec クライアント リビジョン レベル確認のためのクライアントアップデート
の使用 84

パブリック IP 接続への NAT 割り当てによる IP アドレスの実装	86
VPN NAT ポリシーの表示	87
VPN セッション制限の設定	88
ライセンス リソース割り当ての表示	89
ライセンス リソース使用率の表示	89
VPN セッションの制限	89
ID 証明書のネゴシエート時の使用	90
暗号化コアのプールの設定	90
ダイナミック スプリット トンネリングの設定	91
管理 VPN トンネルの設定	92
アクティブな VPN セッションの表示	93
IP アドレスタイプ別のアクティブな セキュアクライアント セッションの表示	93
IP アドレス タイプ別のアクティブな LAN-to-LAN VPN セッションの表示	94
ISE ポリシー適用について	94
ISE ポリシー適用に関する RADIUS サーバー グループの設定	95
ISE ポリシーの適用の設定例	99
ポリシーの適用のトラブルシューティング	99
SSL の詳細設定	100
事前認証済み SSL 接続のレート制限	107
永続的 IPsec トンネルフロー	108
CLI を使用した永続的 IPsec トンネル フローの設定	110
永続的な IPsec トンネル フローのトラブルシューティング	110
永続的 IPsec トンネル フロー機能はイネーブルになっていますか?	110
孤立したフローの検索	111
暗号アーカイブを使用したトラブルシューティング	112
SSL カウンタの使用	113
スタックした ASP テーブルエントリの削除方法	114
ASA からの WebVPN 構成のクリア	115
 第 5 章	
接続プロファイル、グループ ポリシー、およびユーザー	117
接続プロファイル、グループ ポリシー、およびユーザーの概要	117

接続プロファイル	119
接続プロファイルの一般接続パラメータ	119
IPSec トンネルグループ接続パラメータ	121
接続プロファイルの SSL VPN セッション接続パラメータ	122
接続プロファイルの設定	123
接続プロファイルの最大数	124
デフォルトの IPSec リモート アクセス接続プロファイルの設定	124
IPSec トンネルグループの一般属性	125
リモート アクセス接続プロファイルの設定	126
リモート アクセス接続プロファイルの名前とタイプの指定	126
リモート アクセス接続プロファイルの一般属性の設定	127
二重認証の設定	131
リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定	133
IPSec リモート アクセス接続プロファイルの PPP 属性の設定	136
LAN-to-LAN 接続プロファイルの設定	138
デフォルトの LAN-to-LAN 接続プロファイルのコンフィギュレーション	138
LAN-to-LAN 接続プロファイルの名前とタイプの指定	138
LAN-to-LAN 接続プロファイルの一般属性の設定	138
LAN-to-LAN IPSec IKEv1 属性の設定	139
標準ベースの IKEv2 クライアントのトンネル グループについて	142
標準ベースの IKEv2 属性のサポート	142
DAP のサポート	143
リモート アクセス クライアントのトンネル グループ選択	143
標準ベースの IKEv2 クライアントの認証サポート	143
複数証明書認証の追加	145
EAP ID を取得するためのクエリ ID オプションの設定	146
パスワード管理用の Microsoft Active Directory の設定	148
次回ログイン時にパスワードの変更をユーザーに強制するための Active Directory の使用	149
Active Directory を使用したパスワードの最大有効日数の指定	149
Active Directory を使用した最小パスワード長の強制	150

Active Directory を使用したパスワードの複雑性の強制	150
セキュアクライアントをサポートする RADIUS/SDI メッセージの接続プロファイルの設定	151
RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定	151
グループ ポリシー	153
デフォルトのグループ ポリシーの変更	154
グループ ポリシーの設定	156
外部グループ ポリシーの設定	157
内部グループ ポリシーの作成	158
一般的な内部グループ ポリシー属性の設定	159
グループ ポリシー名	159
グループ ポリシーのバナー メッセージの設定	159
リモート アクセス接続のアドレス プールの指定	159
内部グループ ポリシーへの IPv4 アドレス プールの割り当て	160
内部グループ ポリシーへの IPv6 アドレス プールの割り当て	161
グループ ポリシーのトンネリング プロトコルの指定	162
リモート アクセスの VLAN の指定またはグループ ポリシーへの統合アクセス コントロール ルールの適用	162
グループ ポリシーの VPN アクセス時間の指定	165
グループ ポリシーの同時 VPN ログインの指定	166
特定の接続プロファイルへのアクセスの制限	168
グループ ポリシーの VPN の最大接続時間の指定	168
グループ ポリシーの VPN セッションアイドル タイムアウトの指定	169
グループ ポリシーの WINS サーバーと DNS サーバーの設定	171
スプリット トンネリング ポリシーの設定	173
スプリット トンネリング用のネットワーク リストの指定	174
スプリット トンネリング用のドメイン属性の設定	176
Windows XP およびスプリット トンネリング用の DHCP 代行受信の設定	178
リモート アクセス クライアントで使用するためのブラウザ プロキシ設定の設定	178
IPSec (IKEv1) クライアントのセキュリティ属性の設定	181
IKEv1 クライアントの IPsec-UDP 属性の設定	184

VPN ハードウェア クライアントの属性の設定	185
セキュアクライアント 接続のグループポリシー属性の設定	188
バックアップ サーバー属性の設定	192
ネットワーク アドミッション コントロール パラメータの設定	193
VPN クライアント ファイアウォール ポリシーの設定	197
セキュアクライアント ファイアウォールポリシーの設定	199
Zone Labs Integrity サーバーの使用	200
ファイアウォールクライアント タイプの Zone Labs への設定	202
クライアント ファイアウォールのパラメータの設定	203
クライアント アクセス ルールの設定	205
ユーザー属性の設定	207
ユーザー名のコンフィギュレーションの表示	207
個々のユーザーの属性の設定	208
ユーザーのパスワードと特権レベルの設定	208
ユーザー属性の設定	209
VPN ユーザー属性の設定	209
VPN フィルタ ACL の設定と調整に関するベストプラクティス	217

第 6 章

VPN の IP アドレス	219
IP アドレス割り当てポリシーの設定	219
IPv4 アドレス割り当ての設定	220
IPv6 アドレス割り当ての設定	220
アドレス割り当て方式の表示	221
ローカル IP アドレス プールの設定	221
ローカル IPv4 アドレス プールの設定	222
ローカル IPv6 アドレス プールの設定	223
AAA アドレス指定の設定	223
DHCP アドレス指定の設定	224

第 7 章

リモート アクセス IPsec VPN	227
リモートアクセス IPsec VPN の概要	227

Mobike およびリモート アクセス VPN について	228
Cisco Secure Client の AnyConnect VPN モジュールのライセンス要件	229
リモートアクセス IPsec VPN の制限	229
リモート アクセス IPsec VPN の設定	230
インターフェイスの設定	230
ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化	231
アドレス プールの設定	232
ユーザーの追加	233
IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの作成	233
トンネル グループの定義	234
ダイナミック クリプト マップの作成	236
ダイナミック クリプト マップを使用するためのクリプト マップ エントリの作成	237
マルチコンテキストモードでの IPsec IKEv2 リモートアクセス VPN の設定	237
リモート アクセス IPsec VPN の設定例	238
マルチコンテキストモードでの標準ベース IPsec IKEv2 リモートアクセス VPN の設定例	239
マルチコンテキストモードでのセキュアクライアント IPsec IKEv2 リモートアクセス VPN の構成例	240
リモート アクセス VPN の機能履歴	242

第 8 章

LAN-to-LAN IPsec VPN	243
コンフィギュレーションのまとめ	243
マルチコンテキスト モードでのサイトツーサイト VPN の設定	244
インターフェイスの設定	245
ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化	246
IKEv1 接続の ISAKMP ポリシーの設定	247
IKEv2 接続の ISAKMP ポリシーの設定	248
IKEv2 の複数キー交換	249
IKEv2 複数キー交換の注意事項と制限事項	250
IKEv2 の複数キー交換の設定	250
IKEv2 複数キー交換設定の確認	252
IKEv1 トランスフォーム セットの作成	253

IKEv2 プロポーザルの作成	254
ACL の設定	255
トンネル グループの定義	256
クリプト マップの作成とインターフェイスへの適用	257
クリプト マップのインターフェイスへの適用	260

第 9 章

AnyConnect VPN Client 接続	261
セキュアクライアント VPN Client について	261
セキュアクライアント のライセンス要件	263
セキュアクライアント 接続の設定	263
クライアントを Web 展開するための ASA の設定	263
永続的なクライアント インストールのイネーブル化	265
DTLS の設定	266
リモート ユーザーに対するプロンプト	267
セキュアクライアント プロファイルダウンロードのイネーブル化	268
セキュアクライアント 遅延アップグレードのイネーブル化	270
DSCP の保存の有効化	272
追加 セキュアクライアント 機能のイネーブル化	273
Start Before Logon のイネーブル化	273
セキュアクライアント ユーザーメッセージの言語の変換	274
言語変換について	275
変換テーブルの作成	275
変換テーブルの削除	277
高度な セキュアクライアント SSL 機能の設定	278
キー再生成の有効化	278
デッドピア検出の設定	279
キープアライブの有効化	280
圧縮の使用	281
MTU サイズの調整	282
セキュアクライアント イメージの更新	283
IPv6 VPN アクセスのイネーブル化	283

SAML 2.0	284
SAML 2.0 に関する注意事項と制約事項	286
SAML 2.0 アイデンティティプロバイダー (IdP) の設定	288
SAML 2.0 サービスプロバイダー (SP) としての ASA の設定	291
SAML 認証用のデフォルト OS ブラウザの設定	292
証明書と SAML 認証の設定	293
SAML 2.0 と Onelogin の例	294
SAML 2.0 のトラブルシューティング	296
セキュアクライアント 接続のモニタリング	296
AnyConnect VPN セッションのログオフ	298
セキュアクライアント 接続機能の履歴	298

第 10 章

セキュアクライアント HostScan	301
HostScan/Secure Firewall ポスチャの前提条件	301
HostScan のライセンス	302
HostScan パッケージ	302
HostScan/Secure Firewall ポスチャのインストールまたはアップグレード	302
HostScan の有効化または無効化	303
ASA で有効になっている HostScan/Secure Firewall ポスチャバージョンの表示	304
HostScan/Secure Firewall ポスチャのアンインストール	305
グループポリシーへの セキュアクライアント 機能モジュールの割り当て	306
HostScan/Secure Firewall ポスチャ関連資料	307

第 11 章

仮想トンネル インターフェイス	309
仮想トンネル インターフェイスについて	309
仮想トンネル インターフェイスの注意事項	310
VTI トンネルの作成	313
IPsec プロポーザル (トランスフォーム セット) の追加	314
IPsec プロファイルの追加	316
VTI インターフェイスの追加	318
ダイナミック VTI インターフェイスの追加	321

仮想トンネルインターフェイスの機能履歴	324

第 12 章

VPN の外部 AAA サーバーの設定 327

外部 AAA サーバーについて	327

許可属性のポリシー適用の概要	327

外部 AAA サーバーを使用する際のガイドライン	328

複数証明書認証の設定	328

複数証明書ユーザー名の設定	329

VPN の LDAP 許可の設定	330

ASA LDAP 構成の定義	332

LDAP 許可でサポートされている Cisco 属性	332

ACL でサポートされる URL タイプ	343

Cisco-AV-Pair (ACL) 使用のガイドライン	343

Cisco-AV-Pair 属性の構文	345

Cisco-AV-Pair の ACL 例	346

Active Directory/LDAP VPN リモート アクセス許可の例	346

ユーザー ベースの属性のポリシー適用	347

セキュアクライアント トンネルのスタティック IP アドレス割り当ての適用	349

ダイヤルイン許可または拒否アクセスの適用	351

ログオン時間と Time-of-Day ルールの適用	353



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 (xv ページ)
- 関連資料 (xv ページ)
- 表記法 (xv ページ)
- 通信、サービス、およびその他の情報 (xvii ページ)

本書の目的

このマニュアルの目的は、コマンドラインインターフェイスを使用して Secure Firewall ASA 上での VPN 設定を支援することです。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 Adaptive Security Device Manager (ASDM) を使用して、ASA を設定および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。

このマニュアルは、ASA シリーズに適用されます。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全般に該当します。

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。
<i>italic</i>	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 DevNet](#) [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

IPsec および ISAKMP

- [トンネリング、IPsec、および ISAKMP について \(1 ページ\)](#)
- [IPsec VPN のライセンス \(7 ページ\)](#)
- [IPsec VPN のガイドライン \(8 ページ\)](#)
- [ISAKMP の設定 \(8 ページ\)](#)
- [IPsec の設定 \(22 ページ\)](#)
- [IPsec VPN の管理 \(47 ページ\)](#)

トンネリング、IPsec、および ISAKMP について

このトピックでは、バーチャルプライベートネットワーク（VPN）の構築に使用するインターネットプロトコルセキュリティ（IPsec）標準と Internet Security Association and Key Management Protocol（ISAKMP）標準について説明します。

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモートユーザーとプライベートな企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

ASA は、ISAKMP と IPsec のトンネリング標準を使用してトンネルの構築と管理を行っています。ISAKMP と IPsec は、次の処理を実行できます。

- トンネルパラメータのネゴシエーション
- トンネルの確立
- ユーザーとデータの認証
- セキュリティ キーの管理
- データの暗号化と復号化
- トンネル経由のデータ転送の管理
- トンネルエンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、双方向のトンネルエンドポイントとして機能します。プライベート ネットワークからプレーンパケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネ

ルの他端に送信できます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリック ネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

IPsec の概要

ASA では、LAN-to-LAN VPN 接続に IPsec が使用され、client-to-LAN VPN 接続に IPsec を使用することもできます。IPsec 用語では、ピアとは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。どちらの接続タイプについても、ASA はシスコのピアだけをサポートします。シスコは VPN の業界標準に従っているので、ASA は他ベンダーのピアとの組み合わせでも動作しますが、シスコはこのことをサポートしていません。

トンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーション (SA) をネゴシエートします。これらのネゴシエーションには、トンネルの確立 (IKE SA) と、トンネル内のトラフィックの制御 (IPsec SA) という 2 つのフェーズが含まれます。

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。IPsec LAN-to-LAN 接続では、ASA は発信側または応答側として機能することができます。IPsec client-to-LAN 接続では、ASA は応答側としてのみ機能します。発信側は SA を提案し、応答側は、設定された SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

IPsec トンネルの概要

IPsec トンネルとは、ASA がピア間に確立する SA のセットのことです。SA とは、機密データに適用するプロトコルとアルゴリズムを指定するものであり、ピアが使用するキー関連情報も指定します。IPsec SA は、ユーザ トラフィックの実際の伝送を制御します。SA は単方向ですが、通常ペア（着信と発信）で確立されます。

ピアは SA ごとに使用する設定をネゴシエートします。各 SA は次のもので構成されます。

- IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル
- クリプト マップ
- ACL
- トンネル グループ
- 事前フラグメンテーション ポリシー

ISAKMP および IKE の概要

ISAKMP は、2 台のホストで IPsec Security Association (SA; セキュリティ アソシエーション) の構築方法を一致させるためのネゴシエーション プロトコルです。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。このセキュリティ アソシエーションには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。ISAKMP のネゴシエーションは 2 つのフェーズ（フェーズ 1 とフェーズ 2）に分かれて

います。フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

IKE は、IPsec を使用するための SA の設定に ISAKMP を使用します。IKE は、ピアの認証に使用される暗号キーを作成します。

ASA は、レガシー Cisco VPN Client から接続するための IKEv1、および AnyConnect VPN クライアントの IKEv2 をサポートしています。

ISAKMP ネゴシエーションの条件を設定するには、IKE ポリシーを作成します。このポリシーには、次のものが含まれます。

- IKEv1 ピアに要求する認証タイプ。証明書を使用する RSA 署名または事前共有キー（PSK）です。
- データを保護しプライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code（HMAC）方式。
- 暗号キー決定アルゴリズムの強度を決定するデフィーヘルマン グループ。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。
- IKEv2 の場合は、別の疑似乱数関数（PRF）。IKEv2 トンネル暗号化などに必要な、キー関連情報とハッシュ操作を導出するためのアルゴリズムとして使用されます。
- ASA が暗号キーを使用する時間の制限。この時間が経過すると暗号キーを置き換えます。

IKEv1 ポリシーでは、各パラメータに対して 1 個の値を設定します。IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。この並べ替えにより、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

ASA は、IKEv2 の複数のセキュリティアソシエーション（SA）をサポートしていません。ASA は現在、検出された最初の SA でのみインバウンド IPsec トラフィックを受け入れます。IPsec トラフィックが他の SA で受信された場合は、vpn-overlap-conflict のためドロップされます。複数の IPsec SA は 2 つのピア間の重複トンネル、または非対称トンネリングからの情報を取得できません。

IKEv1 トランスフォーム セットおよび IKEv2 プロポーザルの概要

IKEv1 トランスフォーム セットや IKEv2 プロポーザルは、ASA によるデータ保護の方法を定義するセキュリティプロトコルとアルゴリズムの組み合わせです。IPsec SA のネゴシエーション時に、ピアはそれぞれトランスフォームセットまたはプロポーザルを指定しますが、これは両ピアで同一であることが必要です。ASA は、この一致しているトランスフォームセットまたはプロポーザルを使用して SA を作成し、この SA によって暗号マップに対する ACL のデータフローが保護されます。

IKEv1 トランスフォーム セットでは、各パラメータに対して 1 個の値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに対して、複数の暗号化および認証のタイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

SA の作成に使用されたトランスフォーム セットまたはプロポーザルの定義が変更された場合は、ASA はトンネルを切断します。詳細については、[セキュリティ アソシエーションのクリア](#) (49 ページ) を参照してください。



(注) トランスフォーム セットまたはプロポーザルの唯一の要素が消去または削除された場合は、ASA はそのトランスフォーム セットまたはプロポーザルを参照する暗号マップを自動的に削除します。

IKEv2 複数ピアクリプトマップについて

9.14(1) リリース以降、ASA IKEv2 は複数ピアクリプトマップをサポートするようになりました。トンネル内のピアがダウンすると、IKEv2 はリスト内の次のピアで SA の確立を試みます。最大 10 個のピアアドレスを持つクリプトマップを設定できます。IKEv2 でのこの複数ピアのサポートは、特に、複数ピアクリプトマップを使用して IKEv1 から移行する場合に役立ちます。

IKEv2 は双方向のクリプトマップのみをサポートします。したがって、複数ピアは双方向のクリプトマップにも設定され、トンネルを開始するピアからの要求を受け入れるために同じものが使用されます。

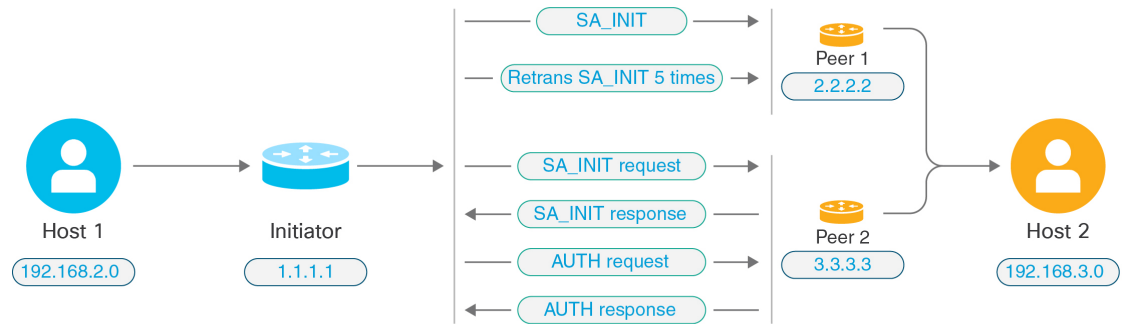
IKEv2 イニシエータの動作

IKEv2 はピア (Peer1 など) とのセッションを開始します。5 回の SA_INIT 再送信で Peer1 に到達できなかった場合、最終の再送信が実行されます。このアクティビティには約 2 分かかります。

Peer1 に障害が発生すると、SA_INIT メッセージが Peer2 に送信されます。Peer2 にも到達できない場合は、2 分後に Peer3 とのセッション確立が開始されます。

クリプトマップのピアリストにあるすべてのピアを使用すると、IKEv2 は、いずれかのピアと SA が確立されるまで、Peer1 からセッションを再度開始します。次の図に、この動作を示します。

図 1: イニシエータのプロセスフロー



- (注) IKE SA を開始するには、継続的なトラフィックが必要です。そのため、試行が失敗するたびに次のピアに移動し、最終的に、到達可能なピアが SA を確立します。トラフィックが中断された場合は、次のピアで IKE SA を開始するために手動トリガーが必要になります。

IKEv2 レスポンダの動作

IKE SA のレスポンダデバイスがクリプトマップ内の複数のピアを使用して設定されている場合、IKE SA が試行されるたびに、イニシエータ IKE SA のアドレスが、クリプトマップ内の現在アクティブなピアのアドレスで検証されます。

たとえば、クリプトマップ内の現在アクティブなピア（レスポンダとして使用）が最初のピアである場合、IKE SA は Peer1 の IP アドレスから開始されます。同様に、クリプトマップ内の現在アクティブなピア（レスポンダとして使用）が 2 番目のピアである場合、IKE SA は Peer2 の IP アドレスから開始されます。



- (注) ピアトラバーサルは、IKEv2 マルチピアトポロジのレスポンダ側ではサポートされません。

クリプトマップ変更時のピアインデックスのリセット

クリプトマップを変更すると、ピアインデックスがゼロにリセットされ、リスト内の最初のピアからトンネルが開始されます。次の表に、特定の状況での複数ピアインデックスの移行を示します。

表 1: SA 前の複数ピアインデックスの移行

SA 前の状況	ピアインデックスの移動 ○/x/リセット
到達不能なピア	対応

SA 前の状況	ピアインデックスの移動 ○/x/リセット
フェーズ 1 プロポーザルの不一致	対応
フェーズ 2 プロポーザルの不一致	対応
DPD ACK 未受信	対応
AUTH フェーズ中のトラフィックセクタの不一致	対応
Authentication failure（認証失敗）	対応
ピアに到達不能なためキー再生成に失敗	リセット

表 2: SA 後の複数ピアインデックスの移行

SA 後の状況	ピアインデックスの移動 ○/x/リセット
プロポーザルの不一致によるキー再生成の失敗	リセット
キー再生成中のトラフィックセクタの不一致	リセット
クリプトマップの変更	リセット
HA スイッチオーバー	x
clear crypto ikev2 sa	リセット
clear ipsec sa	リセット
IKEv2 SA タイムアウト	リセット

IKEv2 複数ピアの注意事項

IKEv1 および IKEv2 プロトコル

クリプトマップが両方の IKE バージョンおよび複数ピアで設定されている場合、次のピアに移動する前に、両方のバージョンの各ピアで SA の試行が行われます。

たとえば、2 つのピア P1 と P2 でクリプトマップが設定されている場合、IKEv2 の P1、IKEv1 の P1、IKEv2 の P2 のようにトンネルが開始されます。

高可用性

複数のピアを持つクリプトマップは、HA 内のレスポндаデバイスへのトンネルを開始します。最初のデバイスに到達できない場合、次のレスポндаデバイスに移動します。

イニシエータデバイスは、レスポндаデバイスへのトンネルを開始します。アクティブデバイスがダウンすると、スタンバイデバイスは、アクティブデバイスの **Peer2** の IP アドレスに移動するクリプトマップに関係なく、**Peer1** の IP アドレスからトンネルを確立しようとします。

集中クラスタ

複数のピアを持つクリプトマップは、集中クラスタの展開内にあるレスポндаデバイスへのトンネルを開始できます。最初のデバイスに到達できない場合、次のレスポндаデバイスへの移動を試みます。

イニシエータデバイスは、レスポндаデバイスへのトンネルを開始します。**Peer1** に到達できない場合、クラスタ内のすべてのノードは次の **Peer2** に移動します。

分散クラスタ

IKEv2 複数ピアクリプトマップが設定されている場合、分散クラスタリングはサポートされません。

マルチコンテキストモード

マルチコンテキストモードでは、複数ピアの動作は各コンテキストに固有となります。

デバッグ コマンド

トンネルの確立に失敗した場合は、これらのコマンドを有効にして、問題をさらに分析します。

- **debug crypto ikev2 platform 255**
- **debug crypto ikev2 protocol 255**
- **debug crypto ike-common 255**

IKEv2 複数ピアに固有のデバッグログの例を次に示します。このログには、ピアの遷移が表示されます。

```
Sep 13 10:08:58 [IKE COMMON DEBUG]Failed to initiate ikev2 SA with peer 192.168.2.2,
initiate to next peer 192.168.2.3 configured in the multiple peer list of the crypto
map.
```

IPsec VPN のライセンス



(注) この機能は、ペイロード暗号化機能のないモデルでは使用できません。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイト間 VPN では、Essentials ライセンスに付属の Other VPN ライセンスが使用されます。モデルごとの最大値については、「[Cisco ASA Series Feature Licenses](#)」を参照してください。

IPsec VPN のガイドライン

コンテキスト モードのガイドライン

シングルまたはマルチ コンテキスト モードでサポートされます。Anyconnect Apex ライセンスは、マルチコンテキスト モードのリモート アクセス VPN に必要です。ASA は AnyConnect Apex ライセンスを特異的に認識しませんが、プラットフォーム制限へのライセンス済み AnyConnect Premium、携帯電話用 セキュアクライアント、Cisco VPN フォン用 セキュアクライアント、および Advanced Endpoint Assessment など、Apex ライセンスのライセンス特性を適用します。

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。

フェールオーバーのガイドライン

IPsec VPN セッションは、アクティブ/スタンバイ フェールオーバー コンフィギュレーションでのみ複製されます。

その他のガイドライン

IKE を設定すると、システムは自動的に RADIUS UDP ポート 1645 および 1646 を予約します。この予約は syslog 713903 に記載され、ポート番号は 27910 および 28166 として示されます。この予約により、ポートが PAT 変換に使用されないように確保されます。

ISAKMP の設定

IKEv1 ポリシーと IKEv2 ポリシーの設定

IKEv1 と IKEv2 はどちらも、最大 20 個の IKE ポリシーをサポートしますが、値のセットはそれぞれ異なります。作成するポリシーのそれぞれに、固有のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

IKE ネゴシエーションが始まると、ネゴシエーションを開始したピアはそのすべてのポリシーをリモート ピアに送信し、リモート ピアは一致するポリシーを探します。リモート ピアは、一致するポリシーを見つけるまで、設定済みのポリシーに対してピアのすべてのポリシーを 1 つずつプライオリティ順に（最も高いプライオリティから）照合します。

一致と見なされるのは、2つのピアからの両方のポリシーに、同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータ値が含まれているときです。IKEv1 では、リモート ピアのポリシーで指定されているライフタイムが、開始側から送信されたポリシーのライフタイム以下であることも必要です。ライフタイムが等しくない場合、ASA は短い方のライフタイムを使用します。IKEv2 では、ライフタイムはネゴシエートされませんが、各ピアの間でローカルに管理されるので、ライフタイムを各ピアで個別に設定できます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、SA は確立されません。

各パラメータに対して特定の値を選択するときは、セキュリティとパフォーマンスの間に暗黙のトレードオフが発生します。デフォルト値で得られるセキュリティレベルは、ほとんどの組織のセキュリティ要件に十分に対応します。パラメータに対し1つの値だけをサポートしているピアと相互運用する場合は、相手のピアがサポートしている値に選択が制限されます。

ISAKMP コマンドには、それぞれプライオリティを指定する必要があります。プライオリティ番号によってポリシーが一意に識別され、IKE ネゴシエーションにおけるポリシーのプライオリティが決定されます。

手順

- ステップ 1** IKE ポリシーを作成するには、シングルまたはマルチ コンテキスト モードのグローバル コンフィギュレーションモードで **crypto ikev1 | ikev2 policy** コマンドを入力します。プロンプトは、IKE ポリシー コンフィギュレーション モードを表示します。

例：

```
hostname(config)# crypto ikev1 policy 1
```

(注)

新しい ASA コンフィギュレーションには、デフォルトの IKEv1 や IKEv2 のポリシーはありません。

- ステップ 2** 暗号化アルゴリズムを指定します。デフォルトは AES-128 です。

暗号化 [aes | aes-192 | aes-256]

例：

```
hostname(config-ikev1-policy)#  
encryption aes
```

- ステップ 3** ハッシュ アルゴリズムを指定します。デフォルト値は SHA-1 です。

hash[sha]

例：

```
hostname(config-ikev1-policy)#  
hash sha
```

- ステップ 4** 認証方式を指定します。デフォルトは事前共有キーです。

authentication[pre-shared]rsa-sig]

例 :

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

ステップ 5 Diffie-Hellman グループ識別番号を指定します。デフォルトはグループ 14 です。

group [14]

例 :

```
hostname(config-ikev1-policy)#  
group 14
```

ステップ 6 SA ライフタイムを指定します。デフォルトは 86400 秒 (24 時間) です。

lifetime seconds

例 :

この例では、4 時間 (14400 秒) のライフタイムを設定します。

```
hostname(config-ikev1-policy)# lifetime 14400
```

ステップ 7 IKEv1 ポリシー キーワード、IKEv2 ポリシー キーワード、および [IKE ポリシー キーワードと値 \(10 ページ\)](#) で入力した値を使用して追加設定を指定します。所定のポリシー パラメータに値を指定しない場合、デフォルト値が適用されます。

IKE ポリシー キーワードと値

	キーワード	意味	説明
authentication	rsa-sig	RSA 署名アルゴリズムによって生成されたキー付きのデジタル証明書	各 IPsec ピアの ID を確立するために ASA が使用する認証方式を指定します。
	pre-share (デフォルト)	事前共有キー	事前共有キーは拡大するネットワークに対応して拡張が困難ですが、小規模ネットワークではセットアップが容易です。
encryption	aes (デフォルト)	128 ビットキーを使用した AES	2 つの IPsec ピア間で伝送されるユーザー データを保護する対称暗号化アルゴリズムを指定します。 デフォルトは 128 ビットキーです。
hash	sha (デフォルト)	SHA-1 (HMAC バリエーション)	データ整合性の確保のために使用するハッシュアルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。

	キーワード	意味	説明
group			Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。
	14 (デフォルト)	グループ 14 (2048 ビット)	Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。 デフォルトグループは DH グループ 14 です。
lifetime	整数値 (86400 = デフォルト)	120 ~ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は（ある程度まで）高くなります。ただし、ライフタイムが短いほど、ASA による IPsec SA のセットアップ機能が高速になります。
	キーワード	意味	説明
integrity	sha (デフォルト)	SHA-1 (HMAC バリエーション)	データ整合性の確保のために使用するハッシュアルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュアハッシュアルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュアハッシュアルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュアハッシュアルゴリズム SHA 2 を指定します。
	null		AES-GCM が暗号化アルゴリズムとして指定されているときは、IKEv2 整合性アルゴリズムとしてヌルを選択できます。
encryption	aes (デフォルト)	AES	2 つの IPsec ピア間で伝送されるユーザー データを保護する対称暗号化アルゴリズムを指定します。 デフォルトは 128 ビット AES です。
	aes aes-192 aes-256		Advanced Encryption Standard (AES) は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。

	キーワード	意味	説明
	aes-gcm aes-gcm-192 aes-gcm-256 null	IKEv2 暗号化に使用する AES-GCM アルゴリズムのオプション	Advanced Encryption Standard (AES) は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。
policy_index			IKEv2 ポリシー サブモードにアクセスします。
prf	sha (デフォルト)	SHA-1 (HMAC バリエーション)	疑似乱数関数 (PRF) を指定します。これは、キー関連情報を生成するために使用されるアルゴリズムです。
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュアハッシュアルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュアハッシュアルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュアハッシュアルゴリズム SHA 2 を指定します。
priority			ポリシー モードを拡張します。追加の IPsec V3 機能がサポートされ、AES-GCM および ECDH の設定が Suite B サポートに含まれるようになります。
group	14 19 20 21 24	グループ 14 (2048 ビット)	Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。 Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。 デフォルトは (DH) グループ 14 です。
lifetime	整数値 (86400 = デフォルト)	120 ~ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は (ある程度まで) 高くなります。ただし、ライフタイムが短いほど、ASA による IPsec SA のセットアップ機能が高速になります。

外部インターフェイスでの IKE のイネーブル化

VPN トンネルの終端となるインターフェイスで、IKE をイネーブルにする必要があります。通常は外部 (つまり、パブリック) インターフェイスです。IKEv1 または IKEv2 を有効にするに

は、`crypto [ikev1 | ikev2] enable interface-name` コマンドを、シングルまたはマルチ コンテキスト モードのグローバル コンフィギュレーション モードで実行します。

次に例を示します。

```
hostname(config)# crypto ikev1 enable outside
```

IKEv1 アグレッシブモードのイネーブル化またはディセーブル化

フェーズ 1 の IKEv1 ネゴシエーションでは、メイン モードとアグレッシブ モードのどちらも使用できます。どちらのモードも同じサービスを提供しますが、アグレッシブモードではピア間の交換が 2 回だけで必要で、合計 3 メッセージとなります（交換が 3 回で、合計 6 メッセージではありません）。Aggressive モードの方が高速ですが、通信パーティの ID は保護されません。このため、セキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。アグレッシブ モードは、デフォルトでイネーブルになっています。



- (注) アグレッシブ モードをディセーブルにすると、Cisco VPN Client は、ASA へのトンネルを確立するための事前共有キー認証を使用できなくなります。ただし、証明書に基づく認証（つまり ASA または RSA）を使用してトンネルを確立できます。

フェーズ 1 IKEv1 ネゴシエーションでのアグレッシブモードをイネーブルにするには、シングルまたはマルチコンテキストモードで次のコマンドを入力します。

```
hostname(config)# crypto map <map-name> seq-num set ikev1 phase1-mode aggressive <group-name>
```

アグレッシブ モードをディセーブルにするには、シングルまたはマルチ コンテキスト モードで次のコマンドを入力します。

```
hostname(config)# crypto ikev1 am-disable
```

アグレッシブモードをいったんディセーブルにした後でイネーブルに戻すには、このコマンドの `no` 形式を使用します。次に例を示します。

```
hostname(config)# no crypto ikev1 am-disable
```

IKEv1 および IKEv2 ISAKMP ピアの識別方式の決定

IKEv1 または IKEv2 ISAKMP フェーズ I ネゴシエーションでは、ピアが相互に相手を識別する必要があります。この識別方式は、次のオプションから選択できます。

Address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。

Automatic (デフォルト)	接続タイプによって ISAKMP ネゴシエーションが決まります。 • 事前共有キーの IP アドレス • 証明書認証の証明書認定者名
Hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します (デフォルト)。この名前は、ホスト名とドメイン名で構成されます。
Key ID <i>key_id_string</i>	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

ASA は、ピアに送信するフェーズ I の ID を使用します。これは、事前共有キーで認証を行うメイン モードでの LAN-to-LAN IKEv1 接続を除いて、すべての VPN シナリオで行われます。

ピア識別方式を変更するには、シングルまたはマルチ コンテキスト モードで次のコマンドを入力します。

crypto isakmp identity {address | hostname | key-id id-string | auto}

たとえば、次のコマンドはピア識別方式を「ホスト名」に設定します。

```
hostname(config)# crypto isakmp identity hostname
```

INVALID_SELECTORS 通知

IPsec システムが SA 上で着信パケットを受信し、そのパケットのヘッダー フィールドが SA 用のセクタに適合しなかった場合は、そのパケットを廃棄する必要があります。このイベントの監査ログエントリには、現在の日時、SPI、IPsec プロトコル、パケットの送信元と宛先、その他の入手可能なパケットのベクトル値、および関連 SA エントリのセクタ値が含まれます。システムは、セクタチェックに合格しなかったために受信パケットが破棄されたことを示す INVALID_SELECTORS の IKE 通知を生成して、送信元 (IPsec ピア) に送信します。

ASA は、次に示す既存の syslog を使用して、CTM 内にこのイベントのログGINGを実装しています。

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>, source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

管理者は、SA 用のトラフィック セクタと一致しない着信パケットが SA 上で受信された場合に、ピアへの IKEv2 通知の送信を有効または無効にできるようになりました。有効にした場合は、IKEv2 通知メッセージが 5 秒ごとに SA あたり 1 つの通知メッセージに制限されます。IKEv2 通知は、IKEv2 情報交換でピアに送信されます。

16 進数の IKEv2 事前共有キーの設定

ローカルとリモートの両方の事前共有キー コマンドにキーワードの *hex* を追加することによって、16 進数の IKEv2 事前共有キーを設定することができます。

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>  
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

IKE 通知の送信の有効化または無効化

管理者は、IKEv2 IPsec VPN 接続上でその接続用のトラフィック セレクタと一致しない着信パケットが受信された場合に、ピアへの IKE 通知の送信を有効または無効にすることができます。この通知の送信はデフォルトで無効になっています。ASDM 証明書でユーザー名を認可する場合の IKE INVALID_SELECTORS 通知の送信は、次の CLI を使用して有効または無効にします。

[no] crypto ikev2 notify invalid-selectors

証明書認証の実行時は、証明書内の CN がユーザー名であり、認可がローカルサーバーに対して実行されます。"service-type" 属性が取得された場合は、前述のように処理されます。

IKEv2 フラグメンテーション オプションの設定

ASA では、IKEv2 フラグメンテーションをイネーブルまたはディセーブルにすることができ、IKEv2 パケットのフラグメント化で使用する MTU（最大伝送ユニット）を指定できます。また、管理者は次のコマンドを使用して、優先するフラグメンテーション方式を設定できます。

[no] crypto ikev2 fragmentation [mtu <mtu-size>] | [preferred-method [ietf | cisco]]

デフォルトでは、すべての IKEv2 フラグメンテーション方式がイネーブルになり、MTU は 576（IPv4 の場合）または 1280（IPv6 の場合）、優先される方式は IETF 標準 RFC-7383 となります。

次の点を考慮して、[mtu <mtu-size>] を指定してください。

- 使用する MTU 値には、IP（IPv4/IPv6）ヘッダー + UDP ヘッダーのサイズを含める必要があります。
- 管理者によって指定されていない場合、デフォルトの MTU は 576（IPv4 の場合）または 1280（IPv6 の場合）となります。
- 指定すると、同じ MTU が IPv4 と IPv6 の両方で使用されます。
- 有効範囲は 68 ～ 1500 です。



(注) MTU の設定時に ESP オーバーヘッドを考慮する必要があります。暗号化中に MTU に追加される ESP オーバーヘッドにより、暗号化後にパケットサイズが増加します。「packet too big」エラーが表示された場合は、MTU サイズを確認し、より低い MTU を設定してください。

次のサポートされているフラグメンテーション方式のいずれかを、IKEv2 の優先フラグメンテーション方式 `[preferred-method[ietf | cisco]]` として設定できます。

- IETF RFC-7383 標準ベースの IKEv2 フラグメンテーション。
 - この方式は、両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
 - この方式を使用すると、フラグメンテーションの後に暗号化が実行され、各 IKEv2 フラグメントメッセージが個別に保護されます。
- シスコ独自のフラグメンテーション。
 - この方式は、これがセキュアクライアントなどのピアによって提供される唯一の方法である場合、または両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
 - この方式を使用すると、暗号化の後にフラグメンテーションが実行されます。受信側のピアは、すべてのフラグメントを受信するまで、メッセージを復号することも認証することもできません。
 - この方式は、シスコ以外のピアとの相互運用性はありません。

`show running-config crypto ikev2` コマンドは現在の設定を表示し、`show crypto ikev2 sa detail` コマンドは、SA に対してフラグメンテーションが使用された場合に符号化された MTU を表示します。

始める前に

- パス MTU ディスカバリはサポートされていません。MTU は、ネットワークのニーズに合わせて手動で設定する必要があります。
- この設定はグローバルであり、設定の適用後に確立される SA に影響を及ぼします。適用以前の SA は影響を受けません。フラグメンテーションがディセーブルになっている場合でも同様です。
- 最大 100 のフラグメントを受信できます。

例

- IKEv2 フラグメンテーションをディセーブルにする場合：

```
no crypto ikev2 fragmentation
```

- デフォルト動作に戻す場合：

```
crypto ikev2 fragmentation
```

または

```
crypto ikev2 fragmentation mtu 576
preferred-method ietf
```

- MTU の値を 600 に変更する場合：
`crypto ikev2 fragmentation mtu 600`
- デフォルトの MTU 値に戻す場合：
`no crypto ikev2 fragmentation mtu 576`
- 優先するフラグメンテーション方式をシスコ方式に変更する場合：
`crypto ikev2 fragmentation preferred-method cisco`
- 優先するフラグメンテーション方式を IETF に戻す場合：
`no crypto ikev2 fragmentation preferred-method cisco`
または
`crypto ikev2 fragmentation preferred-method ietf`

AAA 認証と認可

```
aaa authentication http console LOCAL
aaa authorization http console radius
```

AAA 認証は、ユーザーが入力したユーザー名とパスワードを使用して、ローカル サーバーに対して実行されます。追加の認可は、同じユーザー名を使用して **RADIUS** サーバに対して実行されます。*service-type* 属性が取得された場合は、前述のように処理されます。

IPsec over NAT-T のイネーブル化

NAT-T を使用すると、IPsec ピアは NAT デバイスを介した接続を確立できます。このことを実現するために、IPsec トラフィックが UDP データグラムとしてカプセル化されます。これにはポート 4500 が使用されるので、これによって、NAT デバイスにポート情報が提供されます。NAT-T は NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。



- (注) セキュアクライアントの制限により、セキュアクライアントが IKEv2 を使用して接続できるようにするには NAT-T のイネーブル化が必要になります。この要件は、クライアントが NAT-T デバイスの背後になくても適用されます。

ASA は、データ交換を行うクライアントに応じて、標準の IPsec、IPsec over TCP、NAT-T、および IPsec over UDP を同時にサポートできます。

各オプションがイネーブルのときの接続の状態を次に示します。

オプション	イネーブルの機能	クライアントの位置	使用する機能
オプション 1	NAT-T がイネーブル	およびクライアントが NAT の背後にある場合は、	NAT-T が使用される
		および NAT が存在しない場合は	ネイティブ IPsec (ESP) が使用される
オプション 2	IPsec over UDP がイネーブル	およびクライアントが NAT の背後にある場合は、	IPsec over UDP が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される
オプション 3	NAT-T と IPsec over UDP の両方がイネーブル	およびクライアントが NAT の背後にある場合は、	NAT-T が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される



(注) IPsec over TCP がイネーブルになっている場合は、その他のすべての接続方式よりも優先されます。

NAT-T をイネーブルにすると、ASA は自動的に、IPsec がイネーブルになっているすべてのインターフェイス上でポート 4500 を開きます。

ASA は、LAN-to-LAN とリモート アクセス ネットワークの両方ではなく、どちらかで動作する単一の NAT/PAT デバイスの背後に設置された複数の IPsec ピアをサポートします。混合環境では、リモート アクセス トンネルのネゴシエーションに失敗します。これは、すべてのピアが同じパブリック IP アドレス、つまり NAT デバイスのアドレスから発信されたように見えるためです。また、リモート アクセス トンネルは、LAN-to-LAN トンネル グループ（つまり NAT デバイスの IP アドレス）と同じ名前を使用することが多いため、混合環境では失敗します。この名前の一致により、NAT デバイスの背後にあるピアの LAN-to-LAN とリモート アクセスの混合ネットワークでは、複数のピア間のネゴシエーションが失敗する場合があります。

NAT-T を使用するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のサイト間手順を実行します。

手順

ステップ 1 次のコマンドを入力して、ASA 上でグローバルに IPsec over NAT-T をイネーブルにします。

```
crypto isakmp nat-traversal natkeepalive
```

natkeepalive 引数の範囲は 10 ～ 3600 秒です。デフォルトは 20 秒です。

例：

次のコマンドを入力して、NAT-T をイネーブルにし、キープアライブ値を 1 時間に設定します。

```
hostname(config)# crypto isakmp nat-traversal 3600
```

ステップ 2 IPsec フラグメンテーション ポリシーに対して暗号化前オプションを選択するために、次のコマンドを入力します。

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。

IPsec with IKEv1 over TCP のイネーブル化

IPsec over TCP は、IKEv1 と IPsec の両方のプロトコルを TCP に似たパケットの中にカプセル化するものであり、NAT と PAT の両方のデバイスとファイアウォールを通過するセキュアなトンネリングを実現します。この機能はデフォルトで無効に設定されています。IPsec/IKEv1 over TCP を使用すると、標準の ESP や IKEv1 が機能できない環境や、既存のファイアウォールルールを変更した場合に限って機能できる環境で、Cisco VPN クライアントが動作できるようになります。



(注) この機能は、プロキシベースのファイアウォールでは動作しません。

IPsec over TCP は、リモートアクセスクライアントで動作します。ASA とその接続先クライアントの両方で IPsec over TCP をイネーブルにします。ASA では、すべての IKEv1 対応インターフェイス上で動作するようにグローバルにイネーブルにされます。LAN-to-LAN 接続では機能しません。

ASA は、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-Traversal、および IPSec over UDP を同時にサポートできます。IPsec over TCP は、イネーブルになっている場合、その他のすべての接続方式よりも優先されます。

最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80 (HTTP) やポート 443 (HTTPS) などの周知のポートを入力すると、そのポートに関連付けられているプロトコルがパブリック インターフェイスで機能しなくなることを示すアラートが表示されます。その結果、パブリック インターフェイスを介して ASA を管理するためにブラウザを使用することができなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

デフォルトのポートは 10000 です。

ASA だけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、ASA 用に設定したポートを少なくとも 1 つ含める必要があります。

IKEv1 の IPsec over TCP を ASA でグローバルにイネーブルにするには、次のコマンドをシングルまたはマルチ コンテキスト モードで実行します。

```
crypto ikev1 ipsec-over-tcp [port port 1...port0]
```

次の例では、IPsec over TCP をポート 45 でイネーブルにしています。

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

IKEv1 の証明書グループ照合の設定

トンネルグループは、ユーザーの接続条件とアクセス権を定義します。証明書グループ照合では、ユーザー証明書のサブジェクト DN または発行者 DN を使用して、ユーザーとトンネルグループを照合します。



- (注) 証明書グループ照合は IKEv1 と IKEv2 LAN-to-LAN 接続だけに適用されます。IKEv2 リモートアクセス接続は、トンネルグループの **webvpn** 属性および **certificate-group-map** の **webvpn** コンフィギュレーション モードなどに設定されるグループ選択のプルダウンをサポートしています。

証明書のこれらのフィールドに基づいてユーザーをトンネルグループと照合するには、まず照合基準を定義したルールを作成し、次に各ルールを目的のトンネルグループに関連付ける必要があります。

証明書マップを作成するには、**use the crypto ca certificate map** コマンドを使用します。トンネルグループを定義するには、**tunnel-group** コマンドを使用します。

また、証明書グループ照合ポリシーも設定する必要があります。これには、ルールからグループを照合する、Organizational Unit (OU) フィールドからグループを照合する、すべての証明書ユーザーにデフォルトのグループを使用する、という方式があります。これらの方式のいずれかまたはすべてを使用できます。

手順

- ステップ 1** 証明書ベースの ISAKMP セッションをトンネルグループにマッピングするためのポリシーとルールを設定し、証明書マップエントリをトンネルグループに関連付けるには、**tunnel-group-map** コマンドをシングルまたはマルチ コンテキスト モードで入力します。

```
tunnel-group-map enable {rules | ou | ike-id | peer ip}
```

```
tunnel-group-map [rule-index] enable policy
```

ポリシー	証明書からトンネルグループ名を取得するためのポリシーを指定します。 policy は次のいずれかです。 ike-id : トンネルグループがルールルックアップに基づいて特定されず、OU から取得されない場合に、証明書ベースの ISAKMP セッションをフェーズ 1 ISAKMP ID の内容に基づいてトンネルグループにマッピングすることを示します。 ou : トンネルグループをルール検索によって決定しない場合、サブジェクト識別名 (DN) の OU の値を使用することを示します。 peer-ip : トンネルグループをルール検索によって決定しない場合や OU または ike-id 方式で取得しない場合、ピアの IP アドレスを使用することを示します。 rules : 証明書ベースの ISAKMP セッションが、このコマンドによって設定された証明書マップの関連付けに基づいて、トンネルグループにマッピングされることを示します。
<i>rule index</i>	(オプション) crypto ca certificate map コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

次のことに注意してください。

- 各呼び出しが一意であり、マップインデックスを2回以上参照しない限り、このコマンドを複数回実行できます。
- ルールは 255 文字以下です。
- 1 つのグループに複数のルールを割り当てられます。複数のルールを割り当てるには、まずルールのプライオリティを追加し、グループ化します。次に、各グループに必要な数だけ基準文を定義します。1 つのグループに複数のルールを割り当てた場合、テストされる最初のルールの照合結果は一致します。
- ルールを1つだけ作成すると、すべての条件に一致したときにのみユーザーを特定のトンネルグループに割り当てることができるようになります。すべての照合基準が必要であることは、論理 AND 操作に相当します。または、ユーザーを特定のトンネルグループに割り当てる前にすべての照合基準が必要な場合は、基準ごとに1つのルールを作成します。照合基準が1つだけ必要であることは、論理 OR 操作に相当します。

ステップ 2 コンフィギュレーションでトンネルグループが指定されていない場合に使用する、デフォルトトンネルグループを指定します。

コマンドの構文は、**tunnel-group-map [rule-index] default-group tunnel-group-name** です。*rule-index* はルールの優先順位で、*tunnel-group name* は既存のトンネルグループでなければなりません。

例

次の例では、フェーズ 1 の ISAKMP ID の内容に基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ike-id
```

次の例では、ピアの IP アドレスに基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable peer-ip
```

次の例では、サブジェクト認定者名 (DN) の組織ユニット (OU) に基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ou
```

次の例では、設定されたルールに基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable rules
```

IPsec の設定

ここでは、IPsec を使用して VPN を実装するときの ASA の設定に必要な手順について説明します。

暗号マップの定義

クリプトマップは、IPsec SA でネゴシエートされる IPsec ポリシーを定義します。使用できるキーワードには次のものがあります。

- IPsec 接続が許可および保護するパケットを識別するための ACL。
- ピア ID。
- IPsec トラフィックのローカルアドレス（詳細については、[クリプトマップのインターフェイスへの適用](#)（33 ページ）を参照してください）。
- 最大 11 個の IKEv1 トランスフォームセットまたは IKEv2 プロポーザル。ピアのセキュリティ設定の照合に使用されます。

クリプトマップセットは、同じマップ名を持つ 1 つまたは複数のクリプトマップで構成されます。最初のクリプトマップを作成したときに、クリプトマップセットを作成します。次の

サイトツーサイト タスクでは、シングルまたはマルチ コンテキスト モードで暗号マップを作成または暗号マップに追加します。

crypto map map-name seq-num match address access-list-name

access-list-name では、ACL ID を、最大 241 文字の文字列または整数として指定します。



ヒント すべての大文字にすると、ACL ID がコンフィギュレーション内で見つけやすくなります。

このコマンドを続けて入力すると、クリプトマップをクリプトマップセットに追加できます。次の例では、暗号マップを追加する暗号マップセットの名前は *mymap* です。

crypto map mymap 10 match address 101

上記の構文に含まれるシーケンス番号 (*seq-num*) によって、同じ名前を持つ暗号マップがそれぞれ区別されます。暗号マップに割り当てられているシーケンス番号によって、暗号マップセット内の暗号マップ間のプライオリティが決まります。シーケンス番号が小さいほど、プライオリティが高くなります。暗号マップセットをインターフェイスに割り当てると、ASA は、そのインターフェイスを通過するすべての IP トラフィックと暗号マップセット内の暗号マップを、シーケンス番号が低い順に照合して評価します。

[no] crypto map map_name map_index set pfs [group14 | group15 | group16 | group19 | group20 | group21]

暗号化マップの完全転送秘密 (PFS) に使用する ECDH グループを指定します。暗号マップに対して **group14** および **group24** オプションを設定することはできなくなります (IKEv1 ポリシーを使用するとき)。

[no] crypto map map_name seq-num set reverse-route [dynamic]

このクリプトマップエントリに基づく接続に対して逆ルート注入 (RRI) をイネーブルにします。ダイナミックが指定されていない場合、RRI は設定時に行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。さらに、RRI ルートが、静的ルートがすでに存在する同じ宛先で設定されると、既存の静的ルートは廃棄され、RRI ルートがインストールされます。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベートネットワークまたはボーダールータに通知します。送信元/宛先 (0.0.0.0/0.0.0.0) を保護ネットワークとして指定する場合は、RRI をイネーブルにしないでください。デフォルトルートを使用するトラフィックに影響します。

ダイナミックが指定されている場合、ルートは IPsec セキュリティアソシエーション (SA) の確立成功時に作成され、IPsec SA が削除されると削除されます。

暗号マップの 1 つが実際に使用されていない場合でも、スタティック暗号マップと同じ名前のダイナミック暗号マップを設定することはできません。その逆も同様です。



(注) ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

[no] crypto map name priority set validate-icmp-errors

または

[no]crypto dynamic-map *name* *priority* set validate-icmp-errors

着信 ICMP エラーメッセージを、暗号化マップとダイナミック暗号化マップのどちらに対して検証するかを指定します。

[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df]

または

[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]

暗号化マップまたはダイナミック暗号化マップの、既存の Do Not Fragment (DF) ポリシー（セキュリティアソシエーションレベル）を設定します。

- *clear-df* : DF ビットを無視します。
- *copy-df* : DF ビットを維持します。
- *set-df* : DF ビットを設定して使用します。

[no] crypto map <name> <priority> set tfc-packets [burst <length | auto>] [payload-size <bytes | auto>] [timeout <seconds | auto>]

または

[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto>] [payload-size <bytes | auto>] [timeout <seconds | auto>]

管理者は、IPsec セキュリティアソシエーションにおける、ランダムな長さおよび間隔のダミーのトラフィックフローの機密性 (TFC) パケットをイネーブルにできます。TFC をイネーブルにするには、IKEv2 IPsec プロポーザルが設定されている必要があります。



(注) トラフィックフロー機密保持パケットを有効にすると、VPN のアイドルタイムアウトが防止されます。

暗号マップに割り当てられている ACL は、同じ ACL 名を持つすべての ACE で構成されます。コマンドの構文は次のとおりです。

access-list *access-list-name* {deny | permit} ip *source* *source-netmask* *destination* *destination-netmask*

最初の ACE を作成したときに、ACL を作成します。ACL を作成または追加するコマンドの構文は次のとおりです。

access-list *access-list-name* {deny | permit} ip *source* *source-netmask* *destination* *destination-netmask*

次の例では、ASA は 10.0.0.0 サブネットから 10.1.1.0 サブネットへのすべてのトラフィックに対して、暗号マップに割り当てられている IPsec 保護を適用します。

access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0

パケットが一致する暗号マップによって、SA ネゴシエーションで使用するセキュリティ設定が決定します。ローカルの ASA がネゴシエーションを開始する場合は、スタティック暗号マップで指定されたポリシーを使用して、指定のピアに送信するオファアを作成します。ピア

がネゴシエーションを開始する場合は、ASAはポリシーに一致するスタティック暗号マップを探しますが、見つからない場合は、暗号マップセット内のダイナミック暗号マップの中で見つかるものを探します。これは、ピアのオファーを受け入れるか拒否するかを決定するためです。

2つのピアがSAの確立に成功するには、両方のピアが互換性のあるクリプトマップを少なくとも1つ持っている必要があります。互換性が成立するには、クリプトマップが次の条件を満たす必要があります。

- クリプトマップに、互換性を持つ暗号ACL（たとえば、ミラーイメージACL）が含まれている。応答側ピアがダイナミック暗号マップを使用している場合は、ASA側でも互換性のある暗号ACLが含まれていることが、IPsecを適用するための要件の1つです。
- 各クリプトマップが他のピアを識別する（応答するピアがダイナミッククリプトマップを使用していない場合）。
- クリプトマップに、共通のトランスフォームセットまたはプロポーザルが少なくとも1つある。

1つのインターフェイスに適用できるクリプトマップセットは1つだけです。次の条件のいずれかが当てはまる場合は、ASA上の特定のインターフェイスに対して複数の暗号マップを作成します。

- 特定のピアに異なるデータフローを処理させる。
- さまざまなタイプのトラフィックにさまざまなIPsecセキュリティを適用する。

たとえば、暗号マップを1つ作成し、2つのサブネット間のトラフィックを識別するACLを割り当て、IKEv1 トランスフォームセットまたはIKEv2 プロポーザルを1つ割り当てます。別の暗号マップを作成し、別の2つのサブネット間のトラフィックを識別するACLを割り当て、VPN パラメータが異なるトランスフォームセットまたはプロポーザルを適用します。

1つのインターフェイスに複数のクリプトマップを作成する場合は、クリプトマップセット内のプライオリティを決めるシーケンス番号（seq-num）を各クリプトマップエントリに指定します。

各ACEにはpermit文またはdeny文が含まれます。次の表に、暗号マップに適用されるACLでの許可ACEと拒否ACEの特別な意味を示します。

クリプトマップ評価の結果	応答
permit文が含まれているACEの基準と一致	パケットを暗号マップセットの残りのACEと照合して評価することを停止し、パケットセキュリティ設定を、暗号マップに割り当てられているIKEv1 トランスフォームセットまたはIKEv2 プロポーザルの中の設定と照合して評価します。セキュリティ設定がトランスフォームセットまたはプロポーザルのセキュリティ設定と一致したら、ASAは関連付けられたIPsec設定を適用します。一般に発信トラフィックの場合、IPsec設定の適用とはパケットの復号化、認証、ルーティングを行うことを意味します。

クリプトマップ評価の結果	応答
deny 文が含まれている ACE の基準と一致	パケットを評価中のクリプトマップの残りの ACE と照合して評価することを中断し、次のクリプトマップ（クリプトマップに割り当てられているシーケンス番号で判断する）の ACE との照合と評価を再開します。
クリプトマップセット内のテスト済みのすべての許可 ACE と不一致	パケットを暗号化せずにルーティングします。

deny 文が含まれている ACE は、IPsec 保護が不要な発信トラフィック（たとえば、ルーティングプロトコルトラフィックなど）をフィルタリングして除外します。したがって、暗号 ACL の permit 文と照合して評価する必要のない発信トラフィックをフィルタリングするために、最初の deny 文を挿入します。

暗号化された着信パケットに対しては、セキュリティアプライアンスは送信元アドレスと ESP SPI を使用して、パラメータの復号化を決定します。セキュリティアプライアンスは、パケットを復号化した後で、復号化されたパケットの内部ヘッダーを、そのパケットの SA に関連付けられている ACL の許可 ACE と比較します。内部ヘッダーがプロキシと一致しない場合、セキュリティアプライアンスはそのパケットをドロップします。内部ヘッダーがプロキシと一致する場合、セキュリティアプライアンスはそのパケットをルーティングします。

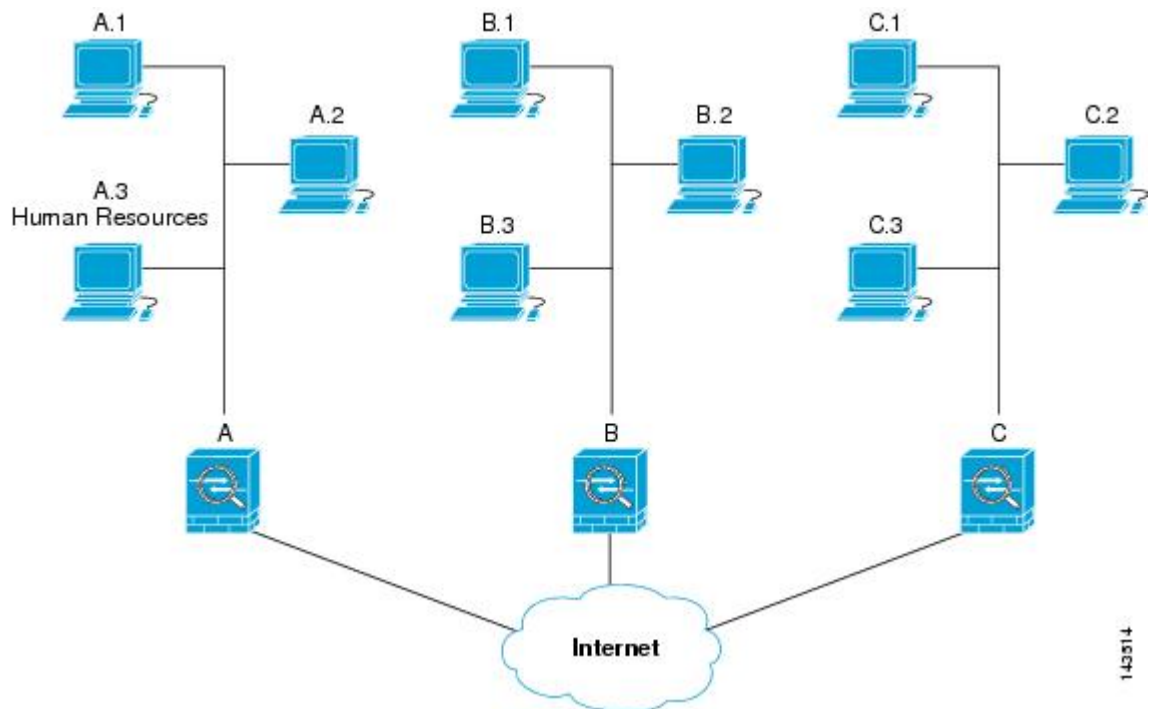
暗号化されていない着信パケットの内部ヘッダーを比較する場合は、セキュリティアプライアンスはすべての拒否ルールを無視します。これは、拒否ルールによってフェーズ 2 の SA の確立が妨げられるためです。



(注) 暗号化されていない着信トラフィックをクリアテキストとしてルーティングするには、ACE の許可の前に ACE の拒否を挿入します。ASA は、スプリットトンネルアクセスリストで 28 を超える ACE をプッシュすることはできません。

LAN-to-LAN 暗号マップの例

この LAN-to-LAN ネットワークの例において、セキュリティアプライアンス A、B、および C を設定する目的は、ホストのいずれか 1 台から発信され、別のホストを宛先とするすべてのトラフィックのトンネリングを許可することです。ただし、ホスト A.3 から発信されるトラフィックには人事部の機密データが含まれるため、他のトラフィックよりも強固な暗号化と頻繁なキー再生が必要です。そのため、ホスト A.3 から発信されるトラフィックには特別なトランスフォームセットを割り当てます。



この図に示され、また以下の説明で使用されている単純なアドレス表記は、抽象化したものです。実際の IP アドレスを使用した例は、この説明の後に示します。

セキュリティアプライアンス A を発信トラフィック用に設定するには、2 つの暗号マップを作成します。1 つはホスト A.3 からのトラフィック用で、もう 1 つはネットワーク A の他のホストからのトラフィック用です。次に例を示します。

```
Crypto Map Seq_No_1
  deny packets from A.3 to B
  deny packets from A.3 to C
  permit packets from A to B
  permit packets from A to C
Crypto Map Seq_No_2
  permit packets from A.3 to B
  permit packets from A.3 to C
```

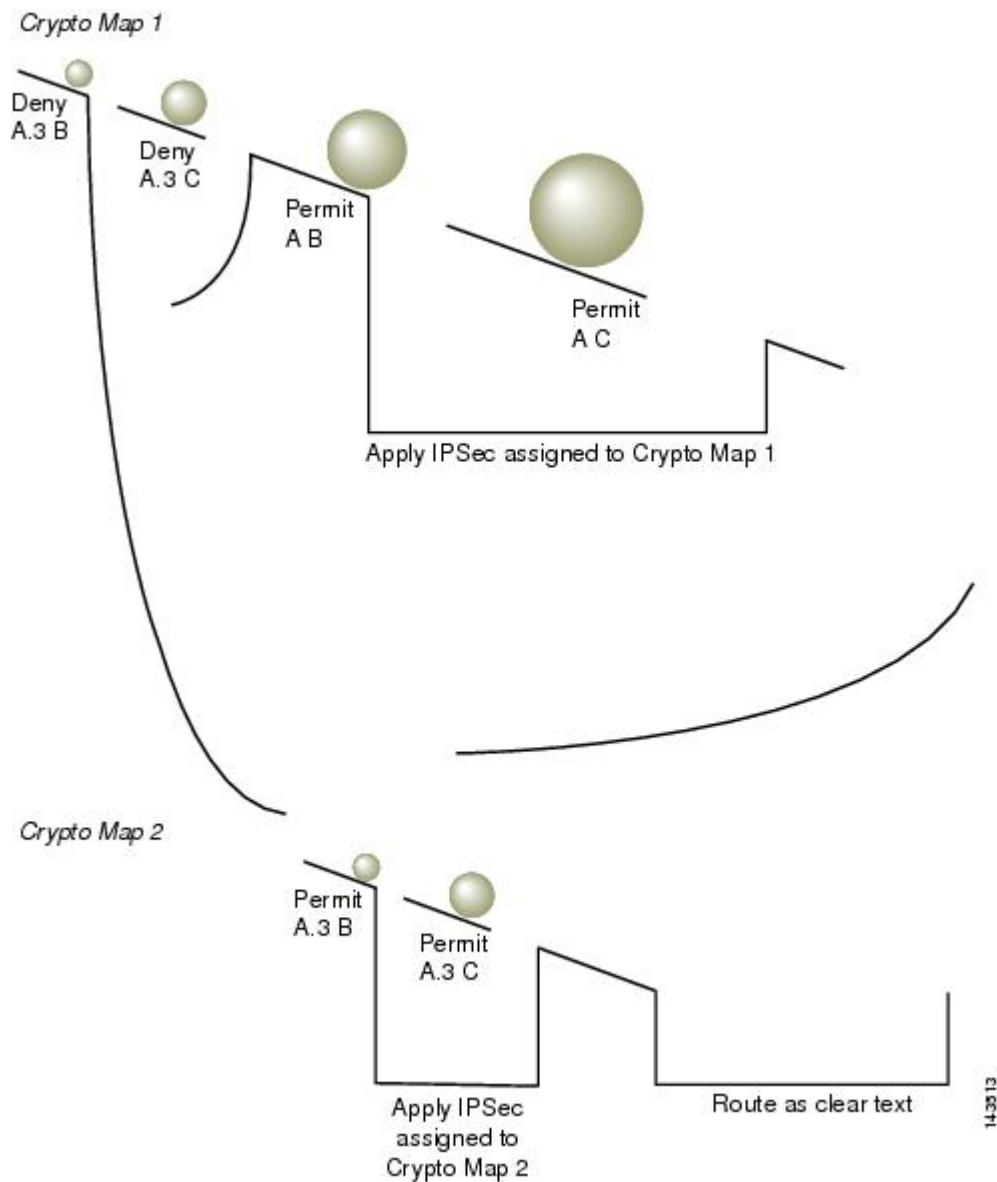
ACL を作成したら、一致するパケットごとに必要な IPsec を適用するためのトランスフォームセットを各暗号マップに割り当てます。

カスケード ACL とは、拒否 ACE を挿入することで、ACL の評価をバイパスし、クリプトマップセット内の次の ACL の評価を再開するものです。クリプトマップごとに異なる IPsec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックに対応するクリプトマップでの以後の評価から除外し、異なるセキュリティを提供する別のクリプトマップ、または異なるセキュリティを必要とする別のクリプトマップの permit 文と特別なトラフィックを照合することができます。暗号 ACL に割り当てられているシーケンス番号によって、暗号マップセット内の評価の順序が決まります。

次の図に、この例の概念的な ACE から作成されたカスケード ACL を示します。各記号の意味は、次のとおりです。

	クリプト マップ セット内のクリプト マップ。
	(すき間がある直線) パケットが ACE に一致した時点でクリプト マップの照合を終了します。
	1 つの ACE の説明と一致したパケット。それぞれの大きさのボールは、図中の別々の ACE に一致する異なるパケットを表しています。大きさの違いは、各パケットの発信元と宛先が異なることを示しています。
	クリプト マップ セット内での次のクリプト マップへのリダイレクション。
	パケットが ACE に一致するか、またはクリプト マップ セット内のすべての許可 ACE に一致しない場合の応答。

図 2: 暗号マップセット内のカスケード ACL



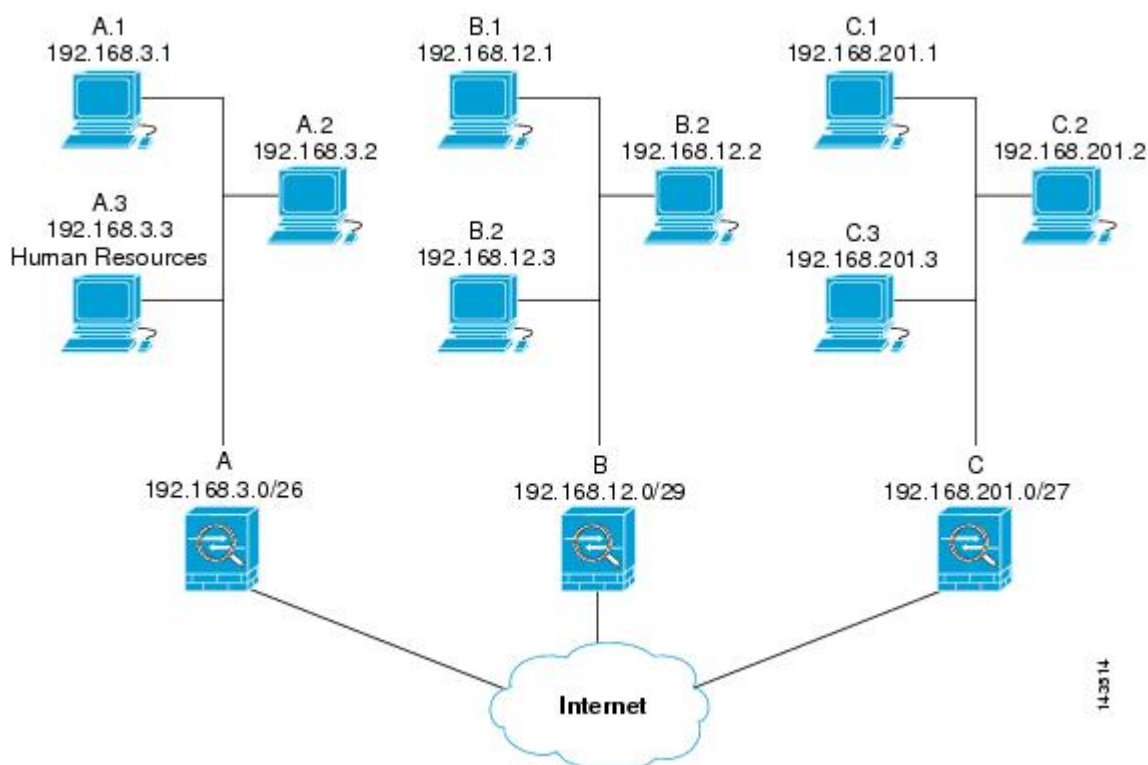
セキュリティアプライアンス A は、ホスト A.3 から発信されたパケットが許可 ACE と一致するまで評価し、クリプトマップに関連付けられている IPsec セキュリティの割り当てを試行します。このパケットが拒否 ACE と一致すると、ASA はこの暗号マップの残りの ACE を無視し、次の暗号マップ（暗号マップに割り当てられているシーケンス番号で判断する）との照合と評価を再開します。この例では、セキュリティアプライアンス A がホスト A.3 から発信されたパケットを受信すると、このパケットを最初のクリプトマップの拒否 ACE と照合し、次のクリプトマップでの照合と評価を再開します。パケットが 2 番目のクリプトマップの許可 ACE と一致すると、関連付けられた IPsec セキュリティ（強固な暗号化と頻繁なキー再生）がパケットに適用されます。

ネットワーク例の ASA 設定を完了するために、ASA B と C にミラー暗号マップを割り当てますが、ASA は、暗号化された着信トラフィックの評価時に deny ACE を無視するため、deny A.3 B ACE と deny A.3 C ACE のミラーに相当するものを除外できます。したがって、暗号マップ 2 のミラーに相当するものは必要ありません。このため、ASA B と C のカスケード ACL の設定は不要です。

次の表に、ASA A、B、および C のすべてに設定された暗号マップに割り当てられる ACL を示します。

セキュリティアプライアンス A		セキュリティアプライアンス B		セキュリティアプライアンス C	
クリプトマップ シーケンス 番号	ACE パターン	クリプトマップ シーケンス 番号	ACE パターン	クリプトマップ シーケンス 番号	ACE パターン
1	A.3 B を拒否	1	B A を許可	1	C A を許可
	A.3 C を拒否				
	A B を許可				
	A C を許可		B C を許可		C B を許可
2	A.3 B を許可				
	A.3 C を許可				

次の図は、上で示した概念上のアドレスを実際の IP アドレスにマッピングしたものです。



次の表に示す実際の ACE では、そのネットワーク上で評価されるすべての IPsec パケットに適切な IPsec 設定が適用されます。

セキュリティ アプライアンス	クリプト マップ シーケンス 番号	ACE パターン	実際の ACE
A	1	A.3 B を拒否	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を拒否	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.248
		A B を許可	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		A C を許可	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.248
	2	A.3 B を許可	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を許可	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.248
B	必要なし	B A を許可	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.248
		B C を許可	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.248

セキュリティ アプライアンス	クリプト マップ シーケンス 番号	ACE パターン	実際の ACE
C	必要なし	C A を許可	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.19
		C B を許可	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.2

この例のネットワークで示した論法を応用すると、カスケード ACL を使用して、1 台の ASA で保護されているさまざまなホストまたはサブネットにそれぞれ異なるセキュリティ設定を割り当てることができます。



- (注) デフォルトでは、ASA は、IPsec 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を宛先とする IPsec トラフィックはサポートしません。このタイプのトラフィックには、Uターン、ハブアンドスポーク、ヘアピニングなどの名称があります。ただし、Uターントラフィックをサポートするように IPsec を設定できます。それには、そのネットワークとの間のトラフィックを許可する ACE を挿入します。たとえば、セキュリティ アプライアンス B で Uターントラフィックをサポートするには、概念上の「B B を許可」ACE を ACL1 に追加します。実際の ACE は次のようになります。 **permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248**

公開キー インフラストラクチャ (PKI) キーの設定

キー ペアを生成またはゼロ化するときに Suite-B ECDSA アルゴリズムを選択できるようにするには、公開キー インフラストラクチャ (PKI) を設定する必要があります。

始める前に

RSA または ECDSA のトラストポイントを認証に使用するように暗号化マップを設定する場合は、最初にキー セットを生成する必要があります。これで、そのトラストポイントを作成して、トンネル グループ コンフィギュレーションの中で参照できるようになります。

手順

ステップ 1 キー ペアを生成するときに Suite-B ECDSA アルゴリズムを選択します。

```
crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 | 4096] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]
```

ステップ 2 キー ペアをゼロ化するときに Suite B ECDSA アルゴリズムを選択します。

```
crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]
```

クリプト マップのインターフェイスへの適用

暗号マップセットは、IPsec トラフィックが通過する各インターフェイスに割り当てする必要があります。ASA は、すべてのインターフェイスで IPsec をサポートします。暗号マップセットをインターフェイスに割り当てると、ASA は、すべてのトラフィックを暗号マップセットと照合して評価し、接続中またはネゴシエーション中は指定されたポリシーを使用します。

クリプト マップをインターフェイスに割り当てると、SA データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期設定されます。クリプト マップを修正してインターフェイスに再割り当てすると、ランタイム データ構造はクリプト マップ設定と再同期化されます。また、新しいシーケンス番号を使用して新しいピアを追加し、クリプト マップを再割り当てしても、既存の接続が切断されることはありません。

インターフェイス ACL の使用

ASA では、デフォルトで IPsec パケットがインターフェイス ACL をバイパスするようになっています。インターフェイス ACL を IPsec トラフィックに適用する場合は、**no** 形式の **sysopt connection permit-vpn** コマンドを使用します。

発信インターフェイスにバインドされている暗号マップ ACL は、VPN トンネルを通過する IPsec パケットの許可と拒否を行います。IPsec は、IPsec トンネルから来たパケットの認証と解読を行い、トンネルに関連付けられている ACL とパケットを照合して評価します。

ACL は、どの IP トラフィックを保護するかを定義します。たとえば、2 つのサブネット間または 2 台のホスト間のすべての IP トラフィックを保護するための ACL を作成できます（これらの ACL は、**access-group** コマンドで使用される ACL とよく似ています。ただし、**access-group** コマンドでは、ACL がインターフェイスで転送するトラフィックと阻止するトラフィックを決めます）。

暗号マップを割り当てるまで、ACL は IPsec の使用に限定されません。各暗号マップは ACL を参照し、パケットが ACL のいずれか 1 つで **permit** と一致した場合に適用する IPsec プロパティを決めます。

IPsec 暗号マップに割り当てられている ACL には、次の 4 つの主要機能があります。

- IPsec で保護する発信トラフィックを選択する（**permit** に一致したものが保護の対象）。
- 確立された SA がない状態で移動するデータに対して ISAKMP ネゴシエーションをトリガーする。
- 着信トラフィックを処理して、IPsec で保護すべきであったトラフィックをフィルタリングして廃棄する。
- ピアからの IKE ネゴシエーションを処理するときに、IPsec SA の要求を受け入れるかどうかを決定する（ネゴシエーションは **ipsec-isakmp crypto map** エントリにだけ適用されま

す)。ピアは、**ipsec-isakmp crypto map** コマンド エントリが関連付けられているデータフローを許可する必要があります。これは、ネゴシエーション中に確実に受け入れられるようにするためです。



(注) ACL の要素を 1 つだけ削除すると、ASA は関連付けられている暗号マップも削除します。

現在 1 つまたは複数の暗号マップが参照している ACL を修正する場合は、**crypto map interface** コマンドを使用してランタイム SA データベースを再初期化します。詳細については、**crypto map** コマンドを参照してください。

ローカル ピアで定義するスタティック暗号マップに対して指定するすべての暗号 ACL について、リモートピアで「ミラーイメージ」暗号 ACL を定義することを推奨します。また、クリプトマップは共通トランスフォームをサポートし、他のシステムをピアとして参照する必要があります。これにより、両方のピアで IPsec が正しく処理されます。



(注) すべてのスタティック暗号マップで ACL と IPsec ピアを定義する必要があります。どちらかが定義されていないと、暗号マップは不完全なものになり、ASA は、前の完全な暗号マップにまだ一致していないトラフィックをドロップします。**show conf** コマンドを使用して、すべての暗号マップが完全なものになるようにします。不完全なクリプトマップを修正するには、クリプトマップを削除し、欠けているエントリを追加してからクリプトマップを再適用します。

暗号 ACL は、重複するエントリをサポートしません。

暗号 ACL で送信元アドレスまたは宛先アドレスの指定に **any** キーワードを使用すると問題が発生するため、このキーワードの使用は避けてください。**permit any any** コマンド文を使用すると次の現象が発生するため、使用は極力避けてください。

- すべての発信トラフィックが保護されます。これには、対応するクリプトマップで指定されているピアに送信される保護済みのトラフィックも含まれます。
- すべての着信トラフィックに対する保護が必要になります。

このシナリオでは、ASA は IPsec 保護されていないすべての着信パケットを通知なしでドロップします。

保護するパケットを定義したことを確認してください。**permit** 文に **any** キーワードを使用する場合は、その文の前に一連の **deny** 文をおき、保護対象外のトラフィックをすべてフィルタリングして排除します。これを行わないと、その **permit** 文に保護対象外のトラフィックが含まれることになります。



(注) **no sysopt connection permit-vpn** が設定されているときに、外部インターフェイスのアクセスグループが **deny ip any any** アクセスリストを呼び出すように設定されていたとしても、クライアントからの復号化された通過トラフィックは許可されます。

保護されたネットワークへの、サイトツーサイトまたはリモートアクセス VPN 経由でのアクセスをコントロールするために、**no sysopt permit** コマンドを外部インターフェイス上のアクセスコントロールリスト (ACL) と組み合わせて使用しようとしても、うまくいきません。

このような状況では、内部の管理アクセスがイネーブルになっていると、ACL は適用されず、ユーザーはまだセキュリティアプライアンスへの SSH を使用して接続できます。内部ネットワーク上のホストへのトラフィックは ACL によって正しくブロックされますが、内部インターフェイスへの復号化された通過トラフィックはブロックできません。

ssh および **http** コマンドは、ACL よりもプライオリティが高くなります。つまり、VPN セッションからデバイスへの SSH、Telnet、または ICMP トラフィックを拒否するには、IP ローカルプールを拒否する **ssh**、**telnet**、および **icmp** コマンドを追加する必要があります。

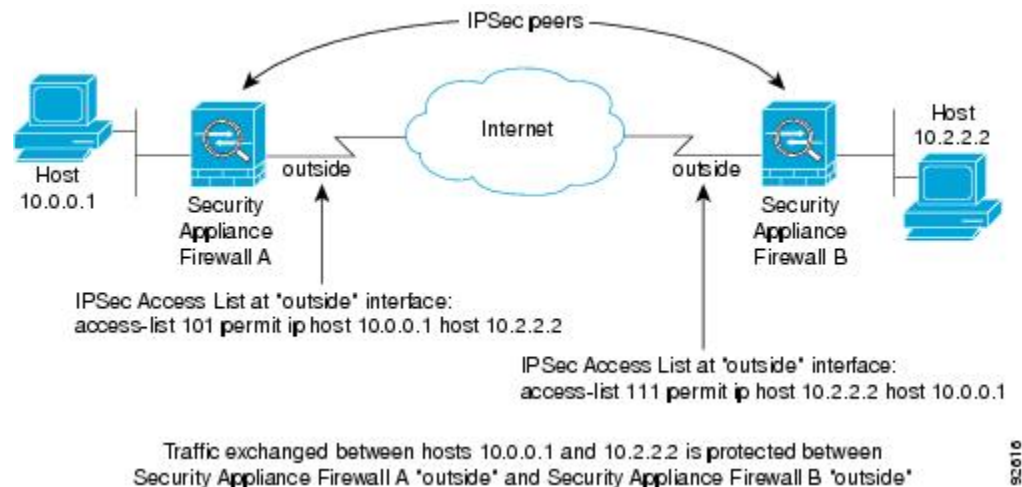
トラフィックが着信か発信かに関係なく、ASA は、インターフェイスに割り当てられている ACL とトラフィックを照合して評価します。インターフェイスに IPsec を割り当てるには、次の手順を実行します。

手順

- ステップ 1** IPsec に使用する ACL を作成します。
- ステップ 2** 作成したアクセスリストを、同じクリプトマップ名を使用して1つまたは複数のクリプトマップにマッピングします。
- ステップ 3** データ フローに IPsec を適用するために、暗号マップに IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルをマッピングします。
- ステップ 4** 共有するクリプトマップ名を割り当てて、クリプトマップを一括してクリプトマップセットとしてインターフェイスに適用します。

例

この例では、データが ASA A 上の外部インターフェイスを出てホスト 10.2.2.2 に向かうときに、ホスト 10.0.0.1 とホスト 10.2.2.2 の間のトラフィックに IPsec 保護が適用されます。



ASA A は、ホスト 10.0.0.1 からホスト 10.2.2.2 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.0.0.1
- 宛先 = ホスト 10.2.2.2

また、ASA A は、ホスト 10.2.2.2 からホスト 10.0.0.1 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.2.2.2
- 宛先 = ホスト 10.0.0.1

評価中のパケットと最初に一致した permit 文によって、IPsec SA のスコープが決まります。

IPsec SA のライフタイムの変更

ASA が新しい IPsec SA とネゴシエートするときに使用する、グローバル ライフタイム値を変更できます。特定のクリプト マップのグローバル ライフタイム値を上書きできます。

IPsec SA では、取得された共有秘密キーが使用されます。このキーは SA に不可欠な要素です。キーは同時にタイムアウトするので、キーのリフレッシュが必要です。各 SA には、「指定時刻」と「トラフィック量」の 2 種類のライフタイムがあります。それぞれのライフタイムを過ぎると SA は失効し、新しい SA のためのネゴシエーションが開始します。デフォルトのライフタイムは、28,800 秒（8 時間）および 4,608,000 キロバイト（10 メガバイト/秒で 1 時間）です。

グローバル ライフタイムを変更すると、ASA はトンネルをドロップします。変更後に確立された SA のネゴシエーションでは、新しい値が使用されます。

暗号マップに設定されたライフタイム値がなく、ASA から新しい SA を要求された場合、暗号マップは、ピアに送信される新しい SA 要求に、既存の SA で使用されているグローバル ライ

フタイム値を挿入します。ピアがネゴシエーション要求を受け取ると、このピアが提案するライフタイム値とローカルに設定されているライフタイム値のうち小さい方の値を、新しい SA のライフタイム値として使用します。

既存 SA のライフタイムのしきい値を超える前に、ピアは新しい SA をネゴシエートします。このようにして、既存 SA の有効期限が切れる前に、新しい SA の準備が整います。既存 SA の残りのライフタイムが約 5 ～ 15% になると、ピアは新しい SA をネゴシエートします。



- (注) キー再生成の衝突を回避するために、サイト間 IKEv2 トンネルの両側で異なるセキュリティアソシエーション タイマーを設定することを推奨します。

VPN ルーティングの変更

デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係ルックアップが行われ、IPSec トンネル経由で送信されるパケットに対してはルックアップが行われません。

一部のネットワーク トポロジでは、ルーティング アップデートによって内部パケットのパスが変更され、ローカル IPsec トンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。

これを防止するには、IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。

始める前に

この機能がデフォルトでディセーブルになっているのは、こうしたルックアップによるパフォーマンスの低下を回避するためです。この機能は、必要な場合にのみイネーブルにしてください。

手順

IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。

[no] [crypto] ipsec inner-routing-lookup

(注)

このコマンドが設定されている場合、非 VTI ベースのトンネルにのみ適用されます。

例

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
```

```
crypto ipsec ikev2 ipsec-proposal GCM
protocol esp encryption aes-gcm
protocol esp integrity null
crypto ipsec inner-routing-lookup
```

スタティック暗号マップの作成

スタティッククリプトマップを使用する基本的な IPsec コンフィギュレーションを作成するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力して、保護するトラフィックを定義する ACL を作成します。

access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask

access-list-name では、ACL ID を、最大 241 文字の文字列または整数として指定します。

destination-netmask と *source-netmask* では、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。この例では、**permit** キーワードによって、指定の条件に一致するトラフィックすべてが暗号で保護されます。

例：

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

ステップ 2 トラフィックを保護する方法を定義する IKEv1 トランスフォーム セットを設定するには、次のコマンドを入力します。

crypto ipsec ikev1 transform-set transform-set-name encryption [authentication]

encryption では、IPsec データ フローを保護するための暗号化方式を指定します。

- **esp-aes** : AES と 128 ビット キーを使用します。
- **esp-aes-192** : AES と 192 ビット キーを使用します。
- **esp-aes-256** : AES と 256 ビット キーを使用します。
- **esp-null** : 暗号化なし。

authentication では、IPsec データ フローを保護するための暗号化方式を指定します

- **esp-sha-hmac** : ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。
- **esp-none** : HMAC 認証なし。

例：

この例では、myset1、myset2、aes_set がトランスフォーム セットの名前です。

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-aes esp-sha-hmac
```



```
hostname(config)#
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

ステップ 3 トラフィックを保護する方法も定義する IKEv2 プロポーザルを設定するには、次のコマンドを入力します。

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

proposal tag は IKEv2 IPsec プロポーザルの名前です。1 ～ 64 文字の文字列です。

プロポーザルを作成し、IPsec プロポーザル コンフィギュレーションモードを開始します。このコンフィギュレーションモードでは、プロポーザルに対して複数の暗号化タイプと整合性タイプを指定できます。

例：

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
```

この例では、**secure** がプロポーザルの名前です。プロトコルおよび暗号化タイプを入力します。

```
hostname(config-ipsec-proposal)# protocol esp encryption aes
```

例：

このコマンドでは、どの AES-GCM または AES-GMAC アルゴリズムを使用するかを選択します。

[no] protocol esp encryption [*aes* | *aes-192* | *aes-256* | *aes-gcm* | *aes-gcm-192* | *aes-gcm-256* | *null*]

SHA-2 またはヌルが選択されている場合は、どのアルゴリズムを IPsec 整合性アルゴリズムとして使用するかを選択する必要があります。AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

[no] protocol esp integrity [*sha-1* | *sha-256* | *sha-384* | *sha-512* | *null*]

(注)

AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。SHA-256 は IKEv2 トンネルを確立するために整合性や PRF に使用できますが、ESP 整合性保護にも使用できます。

ステップ 4 (任意) 管理者はパス最大伝送単位 (PMTU) エージングをイネーブルにして、PMTU 値を元の値にリセットする間隔を設定することができます。

[no] crypto ipsec security-association pmtu-aging *reset-interval*

ステップ 5 暗号マップを作成するには、シングルまたはマルチ コンテキスト モードを使用して、次のサイトツーサイト手順を実行します。

a) ACL を暗号マップに割り当てます。

crypto map *map-name seq-num match address access-list-name*

暗号マップセットとは、暗号マップエントリの集合です。エントリはそれぞれ異なるシーケンス番号 (*seq-num*) を持ちますが、*map name* が同じです。*access-list-name* では、ACL ID を、最大 241 文字の文字列または整数として指定します。次の例では、**mymap** がクリ

プトマップセットの名前です。マップセットのシーケンス番号は10です。シーケンス番号は、1つのクリプトマップセット内の複数のエントリにリンクを付けるために使用します。シーケンス番号が小さいほど、プライオリティが高くなります。

例：

この例では、ACL 101 が暗号マップ `mymap` に割り当てられます。

```
crypto map mymap 10 match address 101
```

- b) IPsec で保護されたトラフィックの転送先となるピアを指定します。

```
crypto map map_name sequence numberset peer ip_address1 [ip_address2] [...]
```

例：

```
crypto map mymap 10 set peer 192.168.1.100
```

ASA は、ピアに IP アドレス 192.168.1.100 が割り当てられている SA をセットアップします。

(注)

9.14(1) 以降、ASA は IKEv2 クリプトマップの複数ピアをサポートしています。最大 10 ピアをリストに追加できます。

- c) このクリプトマップに対して、IKEv1 トランスフォームセットと IKEv2 プロポーザルのどちらを許可するかを指定します。複数のトランスフォームセットまたはプロポーザルを、プライオリティ順（最高のプライオリティのものが最初）に列挙します。1つの暗号マップに最大 11 個のトランスフォームセットまたはプロポーザルを指定できます。次の 2 つのいずれかのコマンドを使用します。

```
crypto map map-name seq-num set ikev1 transform-set transform-set-name1 [transform-set-name2, ...transform-set-name11]
```

または

```
crypto map map-name seq-num set ikev2 ipsec-proposal proposal-name1 [proposal-name2, ...proposal-name11]
```

`proposal-name1` と `proposal-name11` では、IKEv2 の IPsec プロポーザルを 1 つ以上指定します。各暗号マップエントリは、最大 11 個のプロポーザルをサポートします。

例：

IKEv1 の場合のこの例では、トラフィックが ACL 101 に一致したときに、SA は、どのトランスフォームセットがピアのトランスフォームセットに一致するかによって、`myset1`（第 1 プライオリティ）と `myset2`（第 2 プライオリティ）のいずれかを使用できます。

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

- d) （任意）IKEv2 では、トンネルに ESP 暗号化と認証を適用するための **mode** を指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

crypto map map-name seq-num set ikev2 mode [transport | tunnel | transport-require]

- **[Tunnel mode]** (デフォルト) : カプセル化モードがトンネルモードになります。トンネルモードでは、ESP 暗号化と認証が元の IP パケット全体 (IP ヘッダーとデータ) に適用されるため、本来の送信元アドレスと宛先アドレスが非表示になります。元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。

このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。

トンネルモードの大きな利点は、エンドシステムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネルモードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません (これらがトンネルのエンドポイントと同じ場合でも同様)。

- **[Transport mode]** : ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きの転送モードになります。transport モードでは IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。

このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。転送モードでは、中間ネットワークでの特別な処理 (たとえば QoS) を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。

- **[Transport Required]** : カプセル化モードは転送モードにしかありません。トンネルモードにフォールバックすることはできません。

デフォルトは **tunnel** カプセル化モードです。transport カプセル化モードは、ピアがこのモードをサポートしていない場合に tunnel モードにフォールバックできる転送モードであり、transport-require カプセル化モードでは、転送モードのみが適用されます。

(注)

転送モードは、リモート アクセス VPN には推奨されません。

カプセル化モードのネゴシエーションの例は次のとおりです。

- イニシエータが転送モードを提案し、レスポндаがトンネルモードで応答した場合、イニシエータはトンネルモードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport モードで応答した場合、応答側は tunnel モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport-require モードの場合、応答側はプロポーザルを送信しません。
- 同様に、イニシエータが transport-require モードで、レスポндаがトンネルモードの場合は、レスポндаから NO PROPOSAL CHOSEN が送信されます。

- e) (任意) グローバル ライフタイムを上書きする場合は、クリプトマップの SA ライフタイムを指定します。

```
crypto map map-name seq-num set security-association lifetime { seconds number | kilobytes  
{number | unlimited}}
```

map-name では、暗号マップセットの名前を指定します。*seq-num* では、暗号マップエントリに割り当てる番号を指定します。時間または送信されたデータに基づいて両方のライフタイムを設定できます。ただし、データ送信ライフタイムはサイト間 VPN にのみ適用され、リモートアクセス VPN には適用されません。

例：

この例では、クリプト マップ *mymap* の指定時刻ライフタイムを 10 ～ 2700 秒 (45 分) に短縮します。トラフィック量ライフタイムは変更されません。

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

- f) (任意) IPsec がこのクリプト マップに対して新しい SA を要求するときに PFS を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

```
crypto map map_name seq-num set pfs [group14 | group15 | group16 | group19 | group20 |  
group21]
```

例：

この例では、暗号マップ *mymap 10* に対して新しい SA をネゴシエートするときに PFS が必要です。ASA は、2048 ビット Diffie-Hellman プライムモジュラスグループを新しい SA で使用します。

```
crypto map mymap 10 set pfs group14
```

- g) (任意) このクリプト マップ エントリに基づく接続に対して逆ルート注入 (RRI) をイネーブルにします。

```
crypto map map_name seq-num set reverse-route [dynamic]
```

ダイナミックが指定されていない場合、RRI は設定時に行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。送信元/宛先 (0.0.0.0/0.0.0.0) を保護 ネットワークとして指定する場合は、RRI をイネーブルにしないでください。デフォルト ルートを使用するトラフィックに影響します。

ダイナミックが指定されている場合、ルートは IPsec セキュリティ アソシエーション (SA) の確立成功時に作成され、IPsec SA が削除されると削除されます。

(注)

ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

例：

```
crypto map mymap 10 set reverse-route dynamic
```

ステップ 6 IPsec トラフィックを評価するために、クリプトマップセットをインターフェイスに適用します。

```
crypto map map-name interface interface-name
```

map-name では、暗号マップセットの名前を指定します。*interface-name* では、ISAKMP IKEv1 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

例：

この例では、ASA は外部インターフェイスを通過するトラフィックを暗号マップ *mymap* と照合して評価し、保護が必要かどうかを判断します。

```
crypto map mymap interface outside
```

ダイナミック暗号マップの作成

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、不足しているパラメータが、ピアの要件に合うように後でダイナミックに取得される（IPsec ネゴシエーションの結果として）ポリシー テンプレートの役割を果たします。ASA は、スタティック暗号マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック暗号マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

LAN-to-LAN のピア、およびリモートアクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。ASA は、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

通常、リモートアクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベート IP アドレスを持っています。一般に、LAN-to-LAN トンネルには事前に決定されたプライベート ネットワークのセットがあります。これがスタティック マップの設定に使用されるので、結果として IPsec SA の確立にも使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントには、スタティック IP アドレスがなく、IPsec ネゴシエーションを発生させるためのダイナミック クリプト マップが必要です。たとえば、ヘッドエンドは IKE ネゴシエーション中に IP アドレスを Cisco VPN Client に割り当て、クライアントはこのアドレスを使用して IPsec SA をネゴシエートします。



(注) ダイナミック クリプト マップには **transform-set** パラメータが必要です。

ダイナミック暗号マップを使用すると、IPsec のコンフィギュレーションが簡単になります。ピアが常に事前に決定されるとは限らないネットワークでを使用することを推奨します。ダイナミック クリプト マップは、Cisco VPN Client (モバイルユーザーなど)、およびダイナミックに割り当てられた IP アドレスを取得するルータに対して使用してください。



ヒント ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリを ACL に挿入します。ネットワークとサブネットブロードキャスト トラフィックに対して、また IPsec で保護しないその他のトラフィックに対しては、必ず **deny** エントリを挿入してください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。ASA は、ダイナミック暗号マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック暗号マップでは、発信トラフィックが ACL の **permit** エントリと一致しても、対応する SA がまだ存在しない場合、ASA はそのトラフィックをドロップします。

クリプトマップセットには、ダイナミック クリプト マップを含めることができます。ダイナミック暗号マップのセットには、暗号マップセットで一番低いプライオリティ (つまり、一番大きいシーケンス番号) を設定し、ASA が他の暗号マップを先に評価するようにする必要があります。セキュリティアプライアンスは、他の (スタティック) マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じ **dynamic-map-name** を持つすべてのダイナミック クリプト マップを含めます。**dynamic-seq-num** によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック暗号マップを設定する場合は、IPsec ピアのデータ フローを暗号 ACL で識別するために、ACL の許可を挿入します。このように設定しないと、ASA は、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。



注意 ダイナミック暗号マップセットを使用して設定された、ASA インターフェイスにトンネリングされるトラフィックに対して、モジュールのデフォルトルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモートアクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレスプールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

シングル コンテキスト モードとマルチ コンテキスト モードのどちらかを使用して、ダイナミック暗号マップのエントリを作成します。1つのクリプトマップセット内で、スタティックマップ エントリとダイナミック マップ エントリを組み合わせることができます。

手順

ステップ 1 (任意) ACL をダイナミック暗号マップに割り当てます。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num match address access-list-name
```

これによって、保護するトラフィックと保護しないトラフィックが決まります。

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

例：

この例では、ACL 101 がダイナミック暗号マップ dyn1 に割り当てられます。マップのシーケンス番号は 10 です。

```
crypto dynamic-map dyn1 10 match address 101
```

ステップ 2 このダイナミック暗号マップに対して、どの IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを許可するかを指定します。複数のトランスフォームセットまたはプロポーザルをプライオリティ順に（最高のプライオリティのものが最初）指定します。IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルに応じたコマンドを使用してください。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev1 transform-set transform-set-name1, [transform-set-name2, ...transform-set-name9]
```

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev2 ipsec-proposal proposal-name1 [proposal-name2, ... proposal-name11]
```

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。*transform-set-name* は、作成または変更するトランスフォーム セットの名前です。*proposal-name* では、IKEv2 の IPsec プロポーザルの名前を 1 つ以上指定します。

例：

IKEv1 の場合のこの例では、トラフィックが ACL 101 に一致したときに、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、myset1（第 1 プライオリティ）と myset2（第 2 プライオリティ）のいずれかを使用できます。

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

ステップ 3 (任意) グローバル ライフタイム 値を無効にする場合は、暗号ダイナミック マップ エントリの SA ライフタイムを指定します。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set security-association lifetime { seconds number | kilobytes {number | unlimited}}
```

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。時間または送信されたデータに基づいて両方のライフタイムを設定できます。ただし、データ送信ライフタイムはサイト間 VPN にのみ適用され、リモートアクセス VPN には適用されません。

例：

この例では、ダイナミック クリプトマップ *dyn1* の指定時刻ライフタイムを 10 ～ 2700 秒（45 分）に短縮します。トラフィック量ライフタイムは変更されません。

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

ステップ 4 （任意） IPsec がこのダイナミック暗号マップに対して新しい SA を要求するときに PFS を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

```
crypto dynamic-map dynamic-map-name dynamic-seq-numset
pfs[group14|group15|group16|group19|group20|group21]
```

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

例：

```
crypto dynamic-map dyn1 10 set pfs group14
```

ステップ 5 ダイナミック クリプトマップセットをスタティック クリプトマップセットに追加します。

ダイナミック マップを参照するクリプトマップは、必ずクリプトマップセットの中でプライオリティ エントリを最低（シーケンス番号が最大）に設定してください。

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name
```

map-name では、暗号マップセットの名前を指定します。*dynamic-map-name* では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。

例：

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

サイトツーサイト冗長性の実現

暗号マップを使用して複数の IKEv1 ピアを定義すると、冗長性を持たせることができます。このコンフィギュレーションはサイトツーサイト VPN に便利です。この機能は、IKEv2 ではサポートされません。

あるピアが失敗すると、ASA は、暗号マップに関連付けられている次のピアへのトンネルを確立します。ネゴシエーションが成功したピアにデータが送信され、そのピアがアクティブピアになります。アクティブピアとは、後続のネゴシエーションのときに、ASA が常に最初に試みるピアのことです。これは、ネゴシエーションが失敗するまで続きます。ネゴシエーションが失敗した時点で、ASA は次のピアに移ります。暗号マップに関連付けられているすべてのピアが失敗すると、ASA のサイクルは最初のピアに戻ります。

IPsec VPN の管理

IPsec コンフィギュレーションの表示

これらは、IPsec コンフィギュレーションに関する情報を表示するためにシングルまたはマルチ コンテキスト モードで入力できるコマンドです。

表 3: IPsec コンフィギュレーション情報を表示するためのコマンド

show running-configuration crypto	IPsec、クリプトマップ、ダイナミック クリプトマップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。
show running-config crypto ipsec	IPsec コンフィギュレーション全体を表示します。
show running-config crypto isakmp	ISAKMP コンフィギュレーション全体を表示します。
show running-config crypto map	クリプトマップ コンフィギュレーション全体を表示します。
show running-config crypto dynamic-map	ダイナミック クリプトマップのコンフィギュレーションを表示します。
show all crypto map	すべてのコンフィギュレーション パラメータ（デフォルト値を持つパラメータも含む）を表示します。
show crypto ikev2 sa detail	暗号化統計情報での Suite-B アルゴリズム サポートを表示します。
show crypto ipsec sa	シングルまたはマルチ コンテキスト モードでの Suite-B アルゴリズム サポートおよび ESPv3 IPsec 出力を表示します。

show ipsec stats	シングルまたはマルチ コンテキスト モードでの IPsec サブシステムに関する情報を表示します。ESPv3 統計情報は、受信した TFC パケットおよび有効および無効な ICMP エラーに表示されます。

リブートの前にアクティブセッションの終了を待機

すべてのアクティブセッションが自発的に終了した場合に限り ASA をリブートするように、スケジュールを設定できます。この機能はデフォルトで無効に設定されています。

reload コマンドを使用して、ASA をリブートします。**reload-wait** コマンドを設定すると、**reload quick** コマンドを使用して **reload-wait** 設定を無効にできます。**reload** コマンドと **reload-wait** コマンドは特権 EXEC モードで使用できます。どちらにも **isakmp** プレフィックスは付けません。

手順

すべてのアクティブセッションが自発的に終了するのを待って ASA をリブートする機能をイネーブルにするには、次のサイトツーサイトタスクをシングルまたはマルチコンテキストモードで実行します。

crypto isakmp reload-wait

例：

```
hostname(config)# crypto isakmp reload-wait
```

接続解除の前にピアに警告する

リモート アクセスや LAN-to-LAN のセッションがドロップする理由には、さまざまなものがあります。たとえば、ASA のシャットダウンまたはリブート、セッションアイドルタイムアウト、最大接続時間の超過、管理者による停止です。

ASA では、（LAN-to-LAN コンフィギュレーションまたは VPN クライアントの）限定されたピアに対して、セッションが接続解除される直前に通知できます。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント ログまたはポップアップ ペインに表示します。この機能はデフォルトで無効に設定されています。

限定されたクライアントとピアには次のものが含まれます。

- アラートがイネーブルになっているセキュリティ アプライアンス
- Cisco VPN Client のうち、バージョン 4.0 以降のソフトウェアを実行しているもの（コンフィギュレーションは不要）

IPsec ピアへの切断通知をイネーブルにするには、**crypto isakmp disconnect-notify** コマンドをシングルまたはマルチ コンテキスト モードで入力します。

セキュリティ アソシエーションのクリア

一部のコンフィギュレーション変更は、後続の SA をネゴシエートしている間だけ有効になります。新しい設定をただちに有効にするには、既存の SA をクリアして、変更後のコンフィギュレーションで SA を再確立します。ASA がアクティブに IPsec トラフィックを処理している場合は、SA データベースのうち、コンフィギュレーション変更の影響を受ける部分だけをクリアします。SA データベースを完全にクリアするのは、大規模な変更の場合や、ASA が処理している IPsec トラフィック量が少ない場合に限定するようにしてください。

次の表に示すコマンドを入力すると、シングルまたはマルチ コンテキスト モードで IPsec SA をクリアして再初期化することができます。

表 4: IPsec SA のクリアおよび再初期化用のコマンド

clear configure crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を削除します。
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップを削除します。特定のダイナミック クリプト マップを削除できるキーワードもあります。
clear configure crypto map	すべてのクリプト マップを削除します。特定のクリプト マップを削除できるキーワードもあります。
clear configure crypto isakmp	ISAKMP コンフィギュレーション全体を削除します。
clear configure crypto isakmp policy	すべての ISAKMP ポリシーまたは特定のポリシーを削除します。
clear crypto isakmp sa	ISAKMP SA データベース全体を削除します。

暗号マップ コンフィギュレーションのクリア

clear configure crypto コマンドには、IPsec、暗号マップ、ダイナミック暗号マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、ISAKMP など、暗号コンフィギュレーションの要素を削除できる引数が含まれます。

引数を指定しないで **clear configure crypto** コマンドを入力すると、暗号コンフィギュレーション全体（すべての認証も含む）が削除されることに注意してください。

詳細については、『Cisco Secure Firewall ASA Series Command Reference』の **clear configure crypto** コマンドを参照してください。



第 2 章

L2TP over IPsec

この章では、ASA での L2TP over IPsec/IKEv1 の設定方法について説明します。

- [L2TP over IPsec/IKEv1 VPN について \(51 ページ\)](#)
- [L2TP over IPsec のライセンス要件 \(53 ページ\)](#)
- [L2TP over IPsec を設定するための前提条件 \(54 ページ\)](#)
- [注意事項と制約事項 \(54 ページ\)](#)
- [CLI での L2TP over Eclipse の設定 \(56 ページ\)](#)
- [L2TP over IPsec の機能履歴 \(61 ページ\)](#)

L2TP over IPsec/IKEv1 VPN について

Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリング プロトコル) は、リモート クライアントがパブリック IP ネットワークを使用して、企業のプライベート ネットワーク サーバーと安全に通信できるようにする VPN トンネリング プロトコルです。L2TP は、データのトンネリングに PPP over UDP (ポート 1701) を使用します。

L2TP プロトコルは、クライアント/サーバー モデルを基本にしています。機能は L2TP ネットワーク サーバー (LNS) と L2TP アクセス コンセントレータ (LAC) に分かれています。LNS は、通常、ルータなどのネットワーク ゲートウェイで実行されます。一方、LAC は、ダイヤルアップの Network Access Server (NAS; ネットワーク アクセス サーバー) や、Microsoft Windows、Apple iPhone、または Android などの L2TP クライアントが搭載されたエンドポイント デバイスで実行されます。

リモート アクセスのシナリオで、IPsec/IKEv1 を使用する L2TP を設定する最大の利点は、リモート ユーザーがゲートウェイや専用回線を使わずにパブリック IP ネットワークを介して VPN にアクセスできることです。これにより、実質的にどの場所からでも POTS を使用してリモート アクセスが可能になります。この他に、Cisco VPN Client ソフトウェアなどの追加のクライアント ソフトウェアが必要ないという利点もあります。



(注) L2TP over IPsec は、IKEv1 だけをサポートしています。IKEv2 はサポートされていません。

IPsec/IKEv1 を使用する L2TP の設定では、事前共有キーまたは RSA シグニチャ方式を使用する証明書、および（スタティックではなく）ダイナミック クリプト マップの使用がサポートされます。ただし、ここで説明する概要手順では、IKEv1、および事前共有キーまたは RSA 署名の設定が完了していることを前提にしています。事前共有キー、RSA、およびダイナミック クリプト マップの設定手順については、一般的操作用コンフィギュレーション ガイドの第 41 章「Digital Certificates」を参照してください。



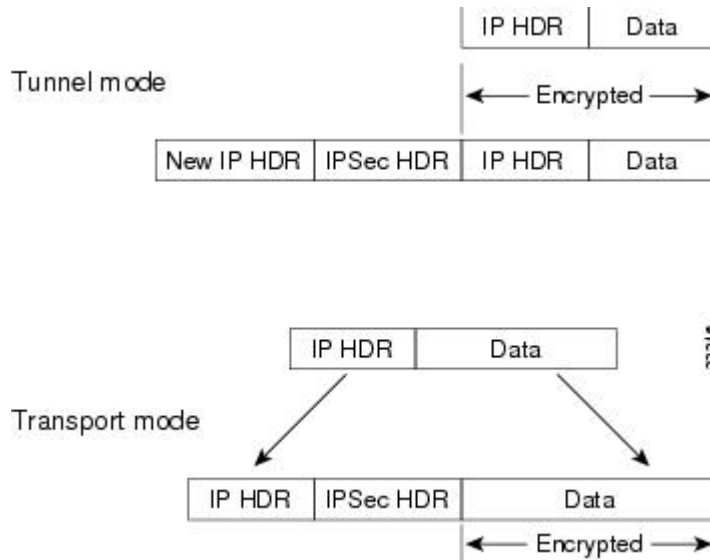
(注) ASA で IPsec を使用する L2TP を設定すると、Windows、MAC OS X、Android および Cisco IOS などのオペレーティング システムに統合されたネイティブ VPN クライアントと LNS が相互運用できるようになります。IPsec を使用する L2TP だけをサポートしています。ネイティブ L2TP は、ASA では対応していません。Windows クライアントがサポートしている IPsec セキュリティ アソシエーションの最短ライフタイムは、300 秒です。ASA でライフタイムを 300 秒未満に設定している場合、Windows クライアントはこの設定を無視して、300 秒のライフタイムに置き換えます。

IPsec の転送モードとトンネル モード

ASA は、デフォルトで IPsec トンネル モードを使用します。このモードでは、元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネルモードの大きな利点は、エンドシステムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネルモードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

ただし、Windows の L2TP/IPsec クライアントは、IPsec 転送モードを使用します。このモードでは IP ペイロードだけが暗号化され、元の IP ヘッダーは暗号化されません。このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。次の図に、IPsec のトンネルモードと転送モードの違いを示します。

図 3: IPsec のトンネル モードと転送モード



Windows の L2TP および IPsec クライアントから ASA に接続するには、**crypto ipsec transform-set trans_name mode transport** コマンドを使用してトランスフォームセット用に IPsec 転送モードを設定する必要があります。このコマンドは、設定手順で使用されます。。



- (注) ASA は、スプリットトンネル アクセスリストで 28 を超える ACE をプッシュすることはできません。

このような転送が可能になると、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。転送モードでは、IP ヘッダーがクリア テキストで送信されると、攻撃者に何らかのトラフィック分析を許すことになります。

L2TP over IPsec のライセンス要件



- (注) この機能は、ペイロード暗号化機能のないモデルでは使用できません。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。IKEv1 を使用した IPsec リモートアクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイト間 VPN では、Essentials ライセンスに付属の Other VPN ライセンスが使用されます。モデルごとの最大値については、「[Cisco ASA Series Feature Licenses](#)」を参照してください。

L2TP over IPsec を設定するための前提条件

L2TP over IPsec の設定については、次の前提条件があります。

- **グループ ポリシー**：デフォルト グループ ポリシー (DfltGrpPolicy) またはユーザー定義グループ ポリシーを L2TP/IPsec 接続に対して設定できます。どちらの場合も、L2TP/IPsec トンネリングプロトコルを使用するには、グループ ポリシーを設定する必要があります。L2TP/IPsec トンネリングプロトコルがユーザー定義グループ ポリシーに対して設定されていない場合は、DfltGrpPolicy を L2TP/IPsec トンネリングプロトコルに対して設定し、ユーザー定義グループ ポリシーにこの属性を継承させます。
- **接続プロファイル**：「事前共有キー」認証を実行する場合は、デフォルトの接続プロファイル (トンネル グループ)、DefaultRAGroup を設定する必要があります。証明書ベースの認証を実行する場合は、証明書 ID に基づいて選択できるユーザー定義接続プロファイルを使用できます。
- **IP 接続性をピア間で確立する必要があります**。接続性をテストするには、エンドポイントから ASA への IP アドレスの ping と、ASA からエンドポイントへの IP アドレスの ping を実行します。
- 接続パス上のどの場所でも、UDP ポート 1701 がブロックされていないことを確認してください。
- Windows 7 のエンドポイント デバイスが、SHA のシグニチャ タイプを指定する証明書を使用して認証を実行する場合、シグニチャ タイプは、ASA のシグニチャ タイプと SHA1 または SHA2 のいずれかが一致している必要があります。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

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 モードでサポートされています。

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 モードでのみサポートされています。トランスペアレント モードはサポートされていません。

フェールオーバーのガイドライン

L2TP over IPsec セッションはステートフル フェールオーバーではサポートされていません。

IPv6 のガイドライン

L2TP over IPsec に対してネイティブの IPv6 トンネル セットアップのサポートはありません。

すべてのプラットフォームでのソフトウェアの制限

現時点では、IPsec トンネルを介した 4096 L2TP のみをサポートしています。

認証のガイドライン

ローカル データベースの場合、ASA は、PPP 認証方式として PAP および Microsoft CHAP のバージョン 1 と 2 だけをサポートします。EAP と CHAP は、プロキシ認証サーバーによって実行されます。そのため、リモートユーザーが **authentication eap-proxy** または **authentication chap** コマンドで設定したトンネルグループに所属している場合、ASA でローカル データベースを使用するように設定すると、このユーザーは接続できなくなります。

サポートされている PPP 認証タイプ

ASA 上の L2TP over IPsec 接続は、次の図に示す PPP 認証タイプだけをサポートします。

表 5: AAA サーバー サポートと PPP 認証タイプ

AAA サーバー タイプ	サポートされている PPP 認証タイプ
LOCAL	PAP、MSCHAPv1、MSCHAPv2
RADIUS	PAP、CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+	PAP、CHAP、MSCHAPv1
LDAP	PAP
NT	PAP
SDI	SDI

表 6: PPP 認証タイプの特性

キーワード	認証タイプ	特性
chap	CHAP	サーバーのチャレンジに対する応答で、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザー名を返します。このプロトコルは、PAP より安全ですが、データは暗号化されません。
eap-proxy	EAP	EAP をイネーブルにします。これによってセキュリティ アプライアンスは、PPP 認証プロセスを外部の RADIUS 認証サーバーにプロキシします。

キーワード	認証タイプ	特性
ms-chap-v1 ms-chap-v2	Microsoft CHAP、バージョン 1 Microsoft CHAP、バージョン 2	CHAP と似ていますが、サーバーは、CHAP のようなクリアテキストのパスワードではなく、暗号化されたパスワードだけを保存および比較するのでよりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。
pap	PAP	認証中にクリアテキストのユーザー名とパスワードを渡すので、セキュアではありません。

CLI での L2TP over Eclipse の設定

ネイティブ VPN クライアントが L2TP over Eclipse プロトコルを使用して ASA に VPN 接続できるように IKEv1 (ISAKMP) ポリシーを設定する必要があります。

- IKEv1 フェーズ 1 : SHA1 ハッシュ方式を使用する AES 暗号化。
- Eclipse フェーズ 2 : SHA ハッシュ方式を使用する AES 暗号化
- PPP 認証 : PAP、MS-CHAPv1、または MSCHAPv2 (推奨)
- 事前共有キー (iPhone の場合に限る)

手順

- ステップ 1** 特定の ESP 暗号化タイプおよび認証タイプで、トランスフォーム セットを作成します。
- ```
crypto ipsec ike_version transform-set transform_name ESP_Encryption_Type ESP_Authentication_Type
```
- 例 :
- ```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-aes esp-sha-hmac
```
- ステップ 2** Eclipse にトンネルモードではなく転送モードを使用するように指示します。
- ```
crypto ipsec ike_version transform-set trans_name mode transport
```
- 例 :
- ```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```
- ステップ 3** L2TP/Eclipse を vpn トンネリングプロトコルとして指定します。
- ```
vpn-tunnel-protocol tunneling_protocol
```
- 例 :
- ```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

- ステップ 4** (任意) 適応型セキュリティアプライアンスに DNS サーバー IP アドレスをグループポリシーのクライアントに送信するように指示します。

dns value [none | *IP_Primary* | *IP_Secondary*]

例 :

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2
```

- ステップ 5** (任意) 適応型セキュリティアプライアンスに WINS サーバー IP アドレスをグループポリシーのクライアントに送信するように指示します。

wins-server value [none | *IP_primary* [*IP_secondary*]]

例 :

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4
```

- ステップ 6** (任意) IP アドレス プールを作成します。

ip local pool *pool_name* *starting_address-ending_address* **mask** *subnet_mask*

例 :

```
hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0
```

- ステップ 7** (任意) IP アドレス プールを接続プロファイル (トンネル グループ) と関連付けます。

address-pool *pool_name*

例 :

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

- ステップ 8** グループ ポリシーの名前を接続プロファイル (トンネル グループ) にリンクします。

default-group-policy *name*

例 :

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
```

- ステップ 9** L2TP over IPSec 接続を試行するユーザーを確認する認証サーバーを指定します。サーバーが使用できない場合に認証をローカル認証にフォールバックする場合は、コマンドの末尾に LOCAL を追加します。

authentication-server-group *server_group* [*local*]

例 :

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL
```

- ステップ 10** L2TP over Eclipse 接続を試行するユーザーの認証方式を、接続プロファイル (トンネルグループ) に対して指定します。ローカル認証の実行に ASA を使用していない場合や、ローカル認証にフォールバックする場合は、コマンドの末尾に LOCAL を追加します。

authentication *auth_type*

例：

```
hostname(config)# tunnel-group DefaultRAGroup ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

ステップ 11 接続プロファイル（トンネル グループ）の事前共有キーを設定します。

tunnel-group tunnel group name ipsec-attributes

例：

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

ステップ 12 （任意） 接続プロファイル（トンネル グループ）に対して、L2TP セッション用に AAA アカウニングの開始レコードと終了レコードを生成します。

accounting-server-group aaa_server_group

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# accounting-server-group sales_aaa_server
```

ステップ 13 hello メッセージの間隔を（秒単位で）設定します。範囲は 10 ～ 300 秒です。デフォルトインターバルは 60 秒です。

l2tp tunnel hello seconds

例：

```
hostname(config)# l2tp tunnel hello 100
```

ステップ 14 （任意） ESP パケットが 1 つ以上の NAT デバイスを通過できるように、NAT-Traversal をイネーブルにします。

NAT デバイスの背後に適応型セキュリティアプライアンスへの L2TP over Eclipse 接続を試行する L2TP クライアントが複数あると予想される場合、NAT-Traversal をイネーブルにする必要があります。

crypto isakmp nat-traversal seconds

NAT トラバーサルをグローバルにイネーブルにするには、ISAKMP がグローバルコンフィギュレーション モードでイネーブルになっていることを確認し（**crypto isakmp enable** コマンドでイネーブルにできます）、次に **crypto isakmp nat-traversal** コマンドを使用します。

例：

```
hostname(config)# crypto ikev1 enable
hostname(config)# crypto isakmp nat-traversal 1500
```

ステップ 15 （任意） トンネル グループのスイッチングを設定します。トンネル グループのスイッチングにより、ユーザーがプロキシ認証サーバーを使用して認証する場合に、VPN 接続の確立が容易になります。トンネル グループは、接続プロファイルと同義語です。

strip-group

strip-realm

例：

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
```

ステップ 16 (任意) ユーザー名 **jdoue**、パスワード **j!doe1** でユーザーを作成します。mschap オプションは、パスワードを入力した後に、そのパスワードが Unicode に変換され、MD4 を使用してハッシュされることを示します。

この手順が必要になるのは、ローカル ユーザー データベースを使用する場合だけです。

username name password password mschap

例 :

```
asa2(config)# username jdoue password j!doe1 mschap
```

ステップ 17 フェーズ 1 の IKE ポリシーを作成し、番号を割り当てます。

crypto ikev1 policy priority

group Diffie-Hellman Group

IKE ポリシーの設定可能なパラメータは数種類あります。ポリシーの Diffie-Hellman グループも指定できます。ASA が IKE ネゴシエーションを完了するために、isakmp ポリシーが使用されます。

例 :

```
hostname(config)# crypto ikev1 policy 14
hostname(config-ikev1-policy)# group14
```

Windows 7 のプロポーザルに回答するための IKE ポリシーの作成

Windows 7 の L2TP/IPsec クライアントは、ASA との VPN 接続を確立するために、数種類の IKE ポリシーのプロポーザルを送信します。Windows 7 の VPN ネイティブ クライアントからの接続を容易にするために、次の IKE ポリシーのいずれかを定義します。

ASA の L2TP over IPsec を設定する手順に従います。Windows 7 のネイティブ VPN クライアントの IKE ポリシーを設定するには、このタスクに新しいステップを追加します。

手順

ステップ 1 既存の IKE ポリシーの属性と番号をすべて表示します。

例 :

```
hostname(config)# show run crypto ikev1
```

ステップ 2 IKE ポリシーを設定します。number 引数には、設定する IKE ポリシーの番号を指定します。この番号は、**show run crypto ikev1** コマンドの出力で表示されたものです。

crypto ikev1 policy number

ステップ 3 各 IPsec ピアの ID を確立し、事前共有キーを使用するために、ASA が使用する認証方式を設定します。

例：

```
hostname(config-ikev1-policy)# authentication pre-share
```

ステップ 4 2 つの IPsec ピア間で伝送されるユーザー データを保護する対称暗号化方式を選択します。Windows 7 の場合は、**aes aes-256**（128 ビット AES の場合）を選択します。

encryption {aes|aes-256}

ステップ 5 データの整合性を保証するハッシュ アルゴリズムを選択します。Windows 7 の場合は、SHA-1 アルゴリズムに **sha** を指定します。

例：

```
hostname(config-ikev1-policy)# hash sha
```

ステップ 6 Diffie-Hellman グループ識別番号を選択します。aes、aes-256 暗号化タイプには 14 を指定できます。

例：

```
hostname(config-ikev1-policy)# group 14
```

ステップ 7 SA ライフタイム（秒）を指定します。Windows 7 の場合は、86400 秒（24 時間）を指定します。

例：

```
hostname(config-ikev1-policy)# lifetime 86400
```

L2TP over IPsec の設定例

次に、任意のオペレーティングシステム上のネイティブ VPN クライアントと ASA との互換性を保持するコンフィギュレーション ファイルのコマンドの例を示します。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
  wins-server value 209.165.201.3 209.165.201.4
  dns-server value 209.165.201.1 209.165.201.2
  vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
  default-group-policy sales_policy
  address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
  pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
  no authentication pap
  authentication chap
  authentication ms-chap-v1
```

```

authentication ms-chap-v2

crypto ipsec ikev1 transform-set trans esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set trans mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share

encryption aes
hash sha

group 14
lifetime 86400

```

L2TP over IPsec の機能履歴

機能名	リリース	機能情報
L2TP over IPsec	7.2(1)	L2TP over IPsec は、単一のプラットフォームで IPsec VPN、L2TP VPN、および L2TP over IPsec の統合サービスとともに L2TP VPN ソリューションを提供します。 リモート アクセスのシナリオで、L2TP over IPsec を設定すると、リモート ユーザーがゲートウェイや専用回線を使わずに IP ネットワークを介して VPN にアクセスできることです。実質的にどの場所からでも POTS を使用してリモート アクセスが可能です。この他に、VPN にアクセスするクライアントは、Microsoft Dial-Up Networking (DUN; ダイアルアップ ネットワーク) を使用するだけでよいという利点もあります。Cisco VPN Client など、追加のクライアント ソフトウェアは必要ありません。 authentication eap-proxy、authentication ms-chap-v1、authentication ms-chap-v2、authentication pap、l2tp tunnel hello、および vpn l2tp-ipsec コマンドが導入または変更されました。
IKE/IPsec 暗号化および整合性/PRF 暗号の廃止 DH グループ 14 での IKEv1 のサポート	9.13(1)	次の暗号化/整合性/PRF 暗号は廃止され、以降のリリースで廃止されます。 • 3DES 暗号化 • DES 暗号化 • MD5 の整合性 IKEv1 での DH グループ 14 (デフォルト) サポートが追加で廃止され、グループ 2 およびグループ 5 コマンドオプションは廃止され、リリース 9.14(1) で削除されます。



第 3 章

ハイアベイラビリティ オプション

- [ハイアベイラビリティ オプション](#) (63 ページ)
- [VPN ロード バランシング](#) (65 ページ)

ハイアベイラビリティ オプション

分散型 VPN クラスタリング、ロード バランシング、およびフェールオーバーは、それぞれ機能と要件が異なるハイアベイラビリティ機能です。状況によっては、複数の機能を導入環境で使用することがあります。以降では、これらの機能について説明します。分散型 VPN とフェールオーバーの詳細については、『[ASA General Operations CLI Configuration Guide](#)』の適切なリリースを参照してください。ロード バランシングの詳細は以下に記載されています。

Secure Firewall eXtensible オペレーティングシステム (FXOS) シャーシ上の VPN とクラスタリング

ASA FXOS クラスタは、S2S VPN に対する相互排他的な 2 つのモード（集中型または分散型）のいずれかをサポートしています。

- 集中型 VPN モード。デフォルト モードです。集中モードでは、VPN 接続はクラスタの制御ユニットとのみ確立されます。

VPN 機能を使用できるのは制御ユニットだけであり、クラスタの高可用性機能は活用されません。制御ユニットで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN 接続されたユーザーにとってはサービスの中断となります。新しい制御ユニットが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的に制御ユニットに転送されます。VPN 関連のキーと証明書は、すべてのユニットに複製されます。

- 分散型 VPN モード。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散され、拡張性が提供されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。



- (注) 集中型 VPN クラスタリング モードは、S2S IKEv1 と S2S IKEv2 をサポートしています。
- 分散型 VPN クラスタリング モードは、S2S IKEv2 のみをサポートしています。
- 分散型 VPN クラスタリング モードは、Firepower 9300 でのみサポートされています。
- リモート アクセス VPN は、集中型または分散型の VPN クラスタリング モードではサポートされていません。

VPN ロード バランシング

VPN ロードバランシングは、VPN ロードバランシンググループ内のデバイス間でリモートアクセス VPN トラフィックを均一に分散するメカニズムです。この機能は、スループットまたはその他の要因を考慮しない単純なトラフィックの分散に基づいています。VPN ロードバランシンググループは、2つ以上のデバイスで構成されます。1つのデバイスがディレクタとなり、その他のデバイスはメンバーデバイスとなります。グループのデバイスは、完全に同じタイプである必要はなく、同じソフトウェアバージョンや構成を使用する必要もありません。

VPN ロードバランシンググループ内のすべてのアクティブなデバイスがセッションの負荷を送ります。VPN ロードバランシングにより、トラフィックはグループ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システムリソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

フェールオーバー

フェールオーバー コンフィギュレーションでは、2台の同一の ASA が専用のフェールオーバーリンクで接続され、必要に応じて、ステートフル フェールオーバー リンク（任意）でも接続されます。アクティブインターフェイスおよび装置のヘルスがモニターされて、所定のフェールオーバー条件に一致しているかどうか判断されます。これらの条件に一致した場合は、フェールオーバーが行われます。フェールオーバーは、VPN とファイアウォールの両方のコンフィギュレーションをサポートします。

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの2つのフェールオーバー設定をサポートしています。

アクティブ/アクティブ フェールオーバーでは、両方の装置がネットワーク トラフィックを渡すことができます。これは、同じ結果になる可能性があります、真のロードバランシングではありません。フェールオーバーが行われると、残りのアクティブ装置が、設定されたパラメータに基づいて結合されたトラフィックの通過を引き継ぎます。したがって、アクティブ/アクティブフェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにする必要があります。

アクティブ/スタンバイ フェールオーバーでは、1つの装置だけがトラフィックを通過させることができ、もう1つの装置はスタンバイ状態で待機して、トラフィックを通過させません。アクティブ/スタンバイ フェールオーバーでは、2 番目の ASA を使用して、障害の発生した装置の機能を引き継ぎます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてス

スタンバイ装置がアクティブ状態に変わります。アクティブになる装置が、障害の発生した装置の IP アドレス（または、トランスペアレントファイアウォールの場合は管理 IP アドレス）および MAC アドレスを引き継いで、トラフィックの転送を開始します。現在スタンバイになっている装置が、アクティブ装置のスタンバイの IP アドレスを引き継ぎます。アクティブ装置で障害が発生すると、スタンバイ装置は、クライアント VPN トンネルを中断することなく引き継ぎます。

VPN ロード バランシング

VPN ロードバランシングについて

リモートクライアント構成で、複数の ASA を同じネットワークに接続してリモートセッションを処理している場合、VPN ロードバランシンググループを作成して、これらのデバイスでセッション負荷を分担するように設定できます。VPN ロードバランシングでは、最も負荷の低いデバイスにセッショントラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これにより、システムリソースを効率的に利用でき、パフォーマンスと可用性が向上します。

VPN ロードバランシンググループ内のすべてのデバイスがセッションの負荷を伝送します。グループ内の1つのデバイスであるディレクタは、着信接続要求をメンバーデバイスと呼ばれる他のデバイスに転送します。ディレクタは、グループ内のすべてのデバイスを監視し、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。ディレクタの役割は、1つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在のディレクタで障害が発生すると、グループ内のメンバーデバイスの1つがその役割を引き継いで、すぐに新しいディレクタになります。

VPN ロードバランシンググループは、外部のクライアントには1つの仮想 IP アドレスとして表示されます。この IP アドレスは、特定の物理デバイスに結び付けられていません。これは現在のディレクタに属しています。接続の確立を試みている VPN クライアントは、最初に仮想 IP アドレスに接続します。ディレクタは、グループ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2回めのトランザクション（ユーザーに対しては透過的）になると、クライアントはホストに直接接続します。VPN ロードバランシンググループのディレクタは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

グループ内の ASA で障害が発生すると、終了されたセッションはただちに仮想 IP アドレスに再接続できます。次に、ディレクタは、グループ内の別のアクティブデバイスにこれらの接続を転送します。ディレクタで障害が発生した場合、グループ内のメンバーデバイスが、ただちに新しいディレクタを自動的に引き継ぎます。グループ内の複数のデバイスで障害が発生しても、グループ内のいずれかのデバイスが稼働していて使用可能である限り、ユーザーはグループに引き続き接続できます。

VPN ロード バランシング クラスタ デバイスごとに、パブリック/外部（lbpublic）およびプライベート/内部（lbprivate）インターフェイスを設定する必要があります。

- [パブリックインターフェイス (Public interface)] : クラスタ IP アドレスへの初期通信に使用されるデバイスの外部インターフェイス。このインターフェイスは、Hello ハンドシェイクに使用されます。
- [プライベートインターフェイス (Private interface)] : ロードバランシング クラスタ メンバー間のメッセージングに使用されるデバイスの内部インターフェイス。これらのメッセージには、ロードバランシングに関連するキープアライブ、トポロジメッセージ、およびアウトオブサービス メッセージが含まれます。

VPN ロードバランシングのアルゴリズム

VPN ロードバランシング グループ ディレクタは、IP アドレスの昇順でソートされたグループ メンバーのリストを保持します。各メンバーの負荷は、整数のパーセンテージ（アクティブなセッションの数）として計算されます。セキュアクライアント 非アクティブセッションは、VPN ロードバランシングで SSL VPN ロードに含まれません。ディレクタは、IPsec トンネルと SSL VPN トンネルを負荷が最も低いデバイスに、その他のデバイスより負荷が 1% 高くなるまでリダイレクトします。すべてのメンバーがディレクタよりも 1% 高くなると、ディレクタはトラフィックを自身にリダイレクトします。

たとえば、1 つのディレクタと 2 つのメンバーがある場合、次のサイクルが当てはまります。



(注) すべてのノードは 0% から始まり、すべての割合は四捨五入されます。

1. ディレクタは、すべてのメンバーにディレクタよりも 1% 高い負荷がある場合、接続を使用します。
2. ディレクタが接続を使用しない場合、最も負荷率の低いメンバーがセッションを処理します。
3. すべてのメンバーに同じ割合の負荷がかかっている場合、セッション数が最も少ないメンバーがセッションを取得します。
4. すべてのメンバーに同じ割合の負荷と同じ数のセッションがある場合、IP アドレスが最も小さいメンバーがセッションを取得します。

VPN ロードバランシンググループ構成

VPN ロードバランシンググループは、同じリリースまたは混在リリースの ASA から構成できます。ただし、次の制約があります。

- 同じリリースの 2 台の ASA から構成される VPN ロードバランシンググループは、IPsec、セキュアクライアント、およびクライアントレス SSL VPN クライアントセッションの組み合わせに対して VPN ロードバランシングを実行できます。
- 混在リリースの ASA を含む VPN ロードバランシンググループは、IPsec セッションをサポートできます。ただし、このようなコンフィギュレーションでは、ASA はそれぞれの IPsec のキャパシティに完全に達しない可能性があります。

グループのディレクタは、グループのメンバーにセッション要求を割り当てます。ASAは、すべてのセッション、SSL VPN または IPsec を同等と見なし、それらを同等に割り当てます。許可する IPsec セッションと SSL VPN セッションの数は、コンフィギュレーションおよびライセンスで許可されている最大数まで設定できます。

VPN ロード バランシング グループでは最大 10 のノードがテスト済みです。これより大きなグループも機能しますが、そのようなトポロジは正式にはサポートされていません。

VPN ロード バランシング ディレクタの選択

ディレクタの選択プロセス

仮想クラスタ内の各非マスターは、ローカル トポロジ データベースを維持します。このデータベースは、クラスタのトポロジが変更されるたびにマスターによって更新されます。各非マスターは、マスターから Hello 応答を受信できないか、最大再試行回数に達してもマスターからキープアライブ応答を受信できない場合に、マスター選択状態になります。

メンバーは、ディレクタ選択の際に次の機能を実行します。

- ローカル トポロジ データベースで検出された各ロードバランシングユニットの優先順位を比較します。
- 同じ優先順位のユニットが 2 つ検出された場合は、下位の IP アドレスが選択されます。
- そのメンバー自体が選択された場合、選択されたメンバーは仮想 IP アドレスを要求します。
- 他のいずれかのメンバーが選択された場合、最初のメンバーは選択されたマスターに Hello 要求を送信します。
- 2 つのメンバーユニットが仮想 IP アドレスを要求しようとする、ARP サブシステムが IP アドレスの重複状態を検出し、上位の MAC アドレスを持つメンバーにディレクタロールを辞退するように求める通知を送信します。

Hello ハンドシェイク

各メンバーは、起動時に外部インターフェイスの仮想クラスタ IP アドレスに Hello 要求を送信します。Hello 要求を受信すると、マスターは固有の Hello 要求をメンバーに送信します。ディレクタ以外のメンバーは、ディレクタからの Hello 要求を受信すると、Hello 応答を返します。これで Hello ハンドシェイクは終了になります。

Hello ハンドシェイクが完了すると、暗号化が設定されている場合、内部インターフェイスで接続が開始されます。最大再試行回数に達してもメンバーが Hello 応答を受信できない場合、メンバーはマスター選択状態になります。

キープアライブ メッセージ

メンバーとディレクタの間で Hello ハンドシェイクが完了すると、各メンバーユニットは、キープアライブ要求を負荷情報とともにマスターに定期的送信します。ディレクタからの未処理のキープアライブ応答がない場合、通常の処理中にメンバーユニットによってキープアライブ

要求が1秒間隔で送信されます。これは、前の要求からのキープアライブ応答が受信されている限り、次のキープアライブ要求が1秒後に送信されることを意味します。メンバーが前のキープアライブ要求に対するディレクタからのキープアライブ応答を受信しなかった場合、1秒後にキープアライブ要求は送信されません。代わりに、メンバーのキープアライブタイムアウト ロジックが開始されます。

キープアライブタイムアウトは次のように機能します。

1. メンバーがディレクタからの未処理のキープアライブ応答を待っている場合、そのメンバーは通常の1秒間隔のキープアライブ要求を送信しません。
2. メンバーは3秒間待機し、4秒後にキープアライブ要求を送信します。
3. メンバーは、ディレクタからのキープアライブ応答がない限り、上のステップ2を5回繰り返します。
4. その後、メンバーはディレクタの不在を宣言し、新しいディレクタ選択サイクルを開始します。

VPN ロードバランシングについてよく寄せられる質問 (FAQ)

- [マルチ コンテキスト モード](#)
- [IP アドレス プールの枯渇](#)
- [固有の IP アドレス プール](#)
- [同じデバイスでの VPN ロードバランシングとフェールオーバーの使用](#)
- [複数のインターフェイスでの VPN ロードバランシング](#)
- [VPN ロードバランシンググループの最大同時セッション数](#)

マルチ コンテキスト モード

- Q.** マルチコンテキストモードで VPN ロードバランシングはサポートされますか。
- A.** VPN ロードバランシングもステートフル フェールオーバーもマルチコンテキストモードではサポートされていません。

IP アドレス プールの枯渇

- Q.** ASA は、IP アドレス プールの枯渇をその VPN ロードバランシング方式の一部と見なしますか。
- A.** いいえ。リモートアクセス VPN セッションが、IP アドレス プールが枯渇したデバイスに転送された場合、セッションは確立されません。ロードバランシングアルゴリズムは、負

荷に基づき、各メンバーが提供する整数の割合（アクティブセッション数および最大セッション数）として計算されます。

固有の IP アドレス プール

- Q.** VPN ロードバランシングを導入するには、異なる ASA 上のセキュアクライアントまたは IPsec クライアントの IP アドレスプールを固有にする必要がありますか。
- A.** はい。IP アドレス プールはデバイスごとに固有にする必要があります。

同じデバイスでの VPN ロードバランシングとフェールオーバーの使用

- Q.** 単一のデバイスで、VPN ロードバランシングとフェールオーバーの両方を使用できますか。
- A.** はい。この構成では、クライアントはグループの IP アドレスに接続し、グループ内で最も負荷の少ない ASA にリダイレクトされます。そのデバイスで障害が発生すると、スタンバイ装置がすぐに引き継ぎ、VPN トンネルにも影響を及ぼしません。

複数のインターフェイスでの VPN ロードバランシング

- Q.** 複数のインターフェイスで SSL VPN をイネーブルにする場合、両方のインターフェイスに VPN ロードバランシングを実装することはできますか。
- A.** パブリックインターフェイスとして VPN ロードバランシンググループに参加するインターフェイスは1つしか定義できません。これは、CPU 負荷のバランスをとることを目的としています。複数のインターフェイスは同じ CPU に集中するため、複数のインターフェイスで VPN ロードバランシングを使用してもパフォーマンスは向上しません。

VPN ロードバランシンググループの最大同時セッション数

- Q.** それぞれ 100 ユーザーの SSL VPN ライセンスを持つ 2 つの Firepower 1150 が展開されているとします。この場合、VPN ロードバランシンググループで許可されるユーザーの最大合計数は、200 同時セッションでしょうか。または 100 同時セッションだけでしょうか。さらに 100 ユーザー ライセンスを持つ 3 台目のデバイスを追加した場合、300 の同時セッションをサポートできますか。
- A.** VPN ロードバランシングを使用すると、すべてのデバイスがアクティブになるため、グループでサポートできる最大セッション数は、グループ内の各デバイスのセッション数の合計になります。この例の場合は、300 になります。

VPN ロードバランシングのライセンス

VPN ロードバランシングのライセンス要件は次のとおりです。

- アクティブな 3DES/AES ライセンス。

ASA は、VPN ロードバランシングを有効にする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES ライセンスを検出できない場

合、ASA は、VPN ロードバランシングのイネーブル化を回避し、さらにライセンスがこの使用を許可していない限り、VPN ロードバランシングシステムによる 3DES の内部構成も回避します。

- ファイアウォールでアクティブ化された、この機能の有効な Security Plus ライセンス。
- 準拠するには、スマートアカウントに十分な Security Plus ライセンスが必要です。

VPN ロードバランシングの前提条件

VPN ロードバランシングに関するガイドラインと制限事項 (70 ページ) も参照してください。

- VPN ロードバランシングはデフォルトでは無効になっています。VPN ロードバランシングは明示的にイネーブルにする必要があります。
- 最初にパブリック (外部) およびプライベート (内部) インターフェイスを設定しておく必要があります。この項では、これ以降の参照に外部および内部の名前を使用します。
これらのインターフェイスに異なる名前を設定するには、**interface** コマンドと **nameif** コマンドを使用します。
- 仮想 IP アドレスが参照するインターフェイスを事前に設定する必要があります。共通仮想 IP アドレス、UDP ポート (必要に応じて)、およびグループの IPsec 共有秘密を確立します。
- グループに参加するすべてのデバイスは、IP アドレス、暗号設定、暗号キー、およびポートというクラスタ固有の同一値を共有する必要があります。
- VPN ロードバランシンググループの暗号化を使用するには、まず、内部インターフェイスを指定して **crypto ikev1 enable** コマンドを実行することで、内部インターフェイスで IKEv1 をイネーブルにする必要があります。そうしない場合、VPN ロードバランシンググループの暗号化を設定しようとすると、エラーメッセージが表示されます。
- アクティブ/アクティブ ステートフル フェールオーバー、または VPN ロードバランシングを使用している場合、ローカル CA 機能はサポートされません。ローカル CA を別の CA の下位に置くことはできません。ローカル CA はルート CA にしかねられません。

VPN ロードバランシングに関するガイドラインと制限事項

適格なクライアント

VPN ロードバランシングは、次のクライアントで開始されるリモートセッションでのみ有効です。

- Secure Client (リリース 3.0 以降)
- ASA 5505 (Easy VPN クライアントとして動作している場合)

- Firepower 1010 (Easy VPN クライアントとして動作している場合)
- IKE リダイレクトをサポートする IOS EZVPN クライアント デバイス (IOS 831/871)

クライアントの考慮事項

VPN ロードバランシングは、IPsec クライアントセッションと SSL VPN クライアントセッションで機能します。LAN-to-LAN を含めて、他のすべての VPN 接続タイプ (L2TP、PPTP、L2TP/IPsec) は、VPN ロードバランシングがイネーブルになっている ASA に接続できますが、VPN ロードバランシングには参加できません。

複数の ASA ノードがロードバランシングのためにグループ化され、セキュアクライアント 接続にグループ URL の使用が必要な場合、個々の ASA ノードで以下を行う必要があります。

- 各リモートアクセス接続プロファイルに、各 VPN ロードバランシング仮想アドレス (IPv4 および IPv6) のグループ URL を設定します。
- このノードの VPN ロードバランシング パブリック アドレスに対してグループ URL を設定します。

ロードバランシンググループ

ASA は、VPN ロードバランシンググループごとに 10 台のデバイスをサポートします。

コンテキスト モード

マルチ コンテキスト モードでは、VPN ロード バランシングはサポートされません。

FIPS

クラスタ暗号化は FIPS ではサポートされていません。

証明書の確認

セキュアクライアントで VPN ロードバランシングの証明書確認を実行し、IP アドレスによって接続がリダイレクトされている場合、クライアントによるすべての名前チェックは、この IP アドレスを通して実行されます。リダイレクト IP アドレスが証明書の一般名、つまり **subject alt name** に一覧表示されていることを確認する必要があります。IP アドレスがこれらのフィールドに存在しない場合、証明書は非信頼と見なされます。

RFC 2818 で定義されたガイドラインに従って、**subject alt name** が証明書に組み込まれている場合、名前チェックにのみ **subject alt name** を使用し、一般名は無視します。証明書を提示しているサーバーの IP アドレスが証明書の **subject alt name** で定義されていることを確認します。

スタンドアロン ASA の場合、IP アドレスはその ASA の IP です。VPN ロードバランシンググループ環境では、証明書の構成により異なります。グループが1つの証明書を使用している場合、証明書は、仮想 IP アドレスおよびグループ FQDN の SAN 拡張機能を保持するほか、各 ASA の IP および FQDN を備えたサブジェクト代替名の拡張機能を含む必要があります。グ

ループが複数の証明書を使用している場合、各 ASA の証明書は、仮想 IP の SAN 拡張機能、グループ FQDN、個々の ASA の IP アドレスおよび FQDN を保持する必要があります。

地理的 VPN ロードバランシング

VPN ロードバランシング環境において DNS 解決が一定の間隔で変化する場合、存続可能時間（TTL）の値をどのように設定するかを慎重に検討する必要があります。DNS ロードバランス構成がセキュアクライアントとの組み合わせで適切に機能するには、ASA が選択された時点からトンネルが完全に確立されるまでの間、ASA の名前からアドレスへのマッピングが同じままである必要があります。所定の時間が経過してもクレデンシャルが入力されない場合は、ルックアップが再び開始して別の IP アドレスが解決済みアドレスとなることがあります。DNS のマッピング先が別の ASA に変更された後でクレデンシャルが入力された場合は、VPN トンネルの確立に失敗します。

VPN の地理的ロードバランシングでは、Cisco Global Site Selector（GSS）が使用されることがあります。GSS では DNS がロードバランシングに使用され、DNS 解決の存続可能時間（TTL）のデフォルト値は 20 秒となっています。GSS での TTL の値を大きくすると、接続失敗の確率を大幅に引き下げることができます。値を大きくすると、ユーザーがクレデンシャルを入力してトンネルを確立するときの認証フェーズに十分な時間を取ることができます。

クレデンシャル入力のための時間を増やすには、「起動時接続」をディセーブルにすることも検討してください。

IKE/IPSec セキュリティ アソシエーション

クラスタ暗号化セッションは、VPN ロードバランサトポロジのスタンバイに同期されません。

VPN ロード バランシングの設定

リモートクライアントコンフィギュレーションで、複数の ASA を同じネットワークに接続してリモートセッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能は VPN ロードバランシングと呼ばれ、最も負荷の低いデバイスにセッショントラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。VPN ロードバランシングにより、システムリソースが効率的に使用され、パフォーマンスとシステムの可用性が向上します。

VPN ロードバランシングを使用するには、グループ内の各デバイスで以下を実行します。

- 共通の VPN ロードバランシンググループ属性を設定することによって、VPN ロードバランシンググループを設定します。これには、仮想 IP アドレス、UDP ポート（必要に応じて）、およびグループの IPsec 共有秘密が含まれます。グループに参加するすべてのデバイスには、グループ内でのデバイスの優先順位を除き、同一のグループ構成を設定する必要があります。
- デバイスで VPN ロードバランシングを有効にし、パブリックアドレスとプライベートアドレスなどのデバイス固有のプロパティを定義することにより、参加するデバイスを設定します。これらの値はデバイスによって異なります。

ロードバランシング用のパブリックインターフェイスとプライベートインターフェイスの設定

VPN ロードバランシンググループのデバイス用のパブリック（外部）インターフェイスとプライベート（内部）インターフェイスを設定するには、次の手順を実行します。

手順

- ステップ 1** VPN ロードバランシング コンフィギュレーション モードで、**lbpublic** キーワードを指定して **interface** コマンドを入力し、ASA にパブリック インターフェイスを設定します。このコマンドは、このデバイスの VPN ロードバランシングのためのパブリックインターフェイスの名前または IP アドレスを指定します。

例：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

- ステップ 2** VPN ロードバランシング コンフィギュレーション モードで、**lbprivate** キーワードを指定して **interface** コマンドを入力し、ASA にプライベート インターフェイスを設定します。このコマンドは、このデバイスの VPN ロードバランシングのためのプライベート インターフェイスの名前または IP アドレスを指定します。

例：

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

- ステップ 3** グループ内でこのデバイスに割り当てる優先順位を設定します。値の範囲は 1 ～ 10 です。優先順位は、デバイスの起動時または既存のディレクタで障害が発生したときに、このデバイスがグループディレクタになる可能性を表します。優先順位を高く設定すると（たとえば 10）、このデバイスがグループディレクタになる可能性が高くなります。

例：

たとえば、このデバイスにグループ内での優先順位 6 を割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

- ステップ 4** このデバイスにネットワークアドレス変換を適用する場合は、デバイスに割り当てられた NAT アドレスを指定して **nat** コマンドを入力します。IPv4 および IPv6 アドレスを定義するか、デバイスのホスト名を指定できます。

例：

たとえば、このデバイスに NAT アドレス 192.168.30.3 および 2001:DB8::1 を割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

VPN ロードバランシンググループ属性の設定

グループ内の各デバイスの VPN ロードバランシンググループ属性を設定するには、次の手順を実行します。

手順

ステップ 1 グローバル コンフィギュレーション モードで **vpn load-balancing** コマンドを入力して、VPN ロードバランシングを設定します。

例：

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

これで **vpn-load-balancing** コンフィギュレーション モードに入るため、ここで残りのロードバランシング属性を設定できます。

ステップ 2 このデバイスが属しているグループの IP アドレスまたは完全修飾ドメイン名を設定します。このコマンドは、VPN ロードバランシンググループ全体を表す単一の IP アドレスまたは FQDN を指定します。グループ内のすべての ASA が共有するパブリックサブネットのアドレス範囲内で、IP アドレスを選択します。IPv4 を指定する必要があります（必須）。オプションで、IPv6 アドレスを指定できます。

例：

仮想 IPv4 および IPv6 アドレスを設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster ip address 192.168.10.1 1000::2
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster ip address 192.168.10.1 1000::2
cluster encryption
```

VPN ロードバランシングクラスタの IPv6 アドレスを設定するには、IPv4 アドレスの設定が必須です。仮想 IPv6 アドレスのみを設定すると、エラーメッセージが表示されます。

```
hostname(config-load-balancing)#show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
```

```
cluster key *****
cluster encryption
participate
hostname(config-load-balancing)# cluster ip address 1000::2
ERROR: Virtual IPv4 address is not set
```

ステップ 3 グループポートを設定します。このコマンドは、このデバイスが参加する VPN ロードバランシンググループの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロードバランシングに使用する UDP の宛先ポート番号を入力します。

例：

たとえば、グループポートを 4444 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

ステップ 4 （任意）VPN ロードバランシンググループに対する IPsec 暗号化をイネーブルにします。

デフォルトでは暗号化は使用されません。このコマンドは、IPsec 暗号化をイネーブルまたはディセーブルにします。このチェック属性を設定する場合は、まず共有秘密を指定して検証する必要があります。VPN ロードバランシンググループ内の ASA は、IPsec を使用して LAN-to-LAN トンネル経由で通信します。デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにするには、この属性をイネーブルにします。

（注）

VPN ロードバランシンググループの暗号化を使用するには、まず、内部インターフェイスを指定して **crypto ikev1 enable** コマンドを実行することで、内部インターフェイスで IKEv1 をイネーブルにする必要があります。そうしない場合、VPN ロードバランシンググループの暗号化を設定しようとすると、エラーメッセージが表示されます。

グループの暗号化を設定したときに IKEv1 をイネーブルにしても、グループへのデバイスの参加を設定する前にディセーブルにした場合は、**participate** コマンドを入力するとエラーメッセージが表示され、そのグループに対して暗号化はイネーブルになりません。

例：

```
hostname(config)# crypto ikev1 enable inside
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

ステップ 5 グループの暗号化をイネーブルにする場合は、**cluster key** コマンドを入力して IPsec 共有秘密も指定する必要があります。このコマンドは、IPsec 暗号化をイネーブルにしてある場合、IPsec ピア間に共有秘密を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。すでに暗号化されたキーを入力する必要がある場合（たとえば、別の構成からコピーしたキー）は、**cluster key 8 key** コマンドを入力します。

例：

たとえば、共有秘密情報を 123456789 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

ステップ 6 **participate** コマンドを入力して、グループへのこのデバイスの参加をイネーブルにします。

例：

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

次のタスク

複数の ASA ノードがロードバランシングのためにグループ化され、セキュアクライアント 接続にグループ URL の使用が必要な場合、個々の ASA ノードで以下を行う必要があります。

- 各リモートアクセス接続プロファイルに、各ロードバランシング仮想アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロードバランシング パブリック アドレスに対してグループ URL を設定します。

tunnel-group、**general-attributes**、**group-url** コマンドを使用して、次のグループの URL を設定します。

完全修飾ドメイン名を使用したりダイレクションのイネーブル化

デフォルトでは、ASA は VPN ロードバランシングのリダイレクトで IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、メンバーデバイスにリダイレクトされるとその証明書は無効になります。

この ASA は VPN ロードバランシング ディレクタとして、VPN クライアント接続を別のメンバーデバイス（グループ内の別の ASA）にリダイレクトするときに、DNS 逆ルックアップを使用して、そのメンバーデバイスの（外部 IP アドレスではなく）完全修飾ドメイン名（FQDN）を送信できます。

VPN ロードバランシングモードで完全修飾ドメイン名を使用したりダイレクトをイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードで **redirect-fqdn enable** コマンドを使用します。この動作は、デフォルトではディセーブルになっています。

始める前に

グループ内の VPN ロードバランシングデバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

手順

ステップ 1 VPN ロード バランシング での FQDN の使用をイネーブルにします。

redirect-fqdn {enable | disable}

例 :

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)#
```

ステップ 2 DNS サーバーに、各 ASA 外部インターフェイスのエントリを追加します（エントリが存在しない場合）。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3 **dns domain-lookup inside** コマンドを使用して、ASA で DNS ルックアップをイネーブルにします。inside の部分には、DNS サーバーへのルートを持つ任意のインターフェイスを指定します。

ステップ 4 ASA で DNS サーバー IP アドレスを定義します。例 : **dns name-server 10.2.3.4** (DNS サーバーの IP アドレス)。

VPN ロード バランシング の設定例

基本の VPN ロード バランシング CLI 設定

次に、完全修飾ドメイン名のリダイレクトをイネーブルにし、グループのパブリックインターフェイスを **test** と指定し、グループのプライベート インターフェイスを **foo** と指定するインターフェイスコマンドを含む、VPN ロード バランシング コマンドシーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

VPN ロードバランシング情報の表示

VPN ロードバランシンググループのディレクタは、アクティブな セキュアクライアント セッション、クライアントレスセッション、そして設定された制限またはライセンス数制限に基づく最大許可セッションがあるグループ内の各 ASA からメッセージを定期的に受信します。グループ内のある ASA の容量が 100% いっぱいである と示される場合、グループディレクタはこれに対してさらに接続をリダイレクトすることはできません。ASA がいっぱいである と示されても、ユーザーによっては非アクティブまたは再開待ち状態となり、ライセンスを消費する可能性があります。回避策として、セッション合計数ではなく、セッション合計数から非アクティブ状態のセッション数を引いた数が各 ASA によって提供されます。ASA コマンドリファレンスの **-sessiondb summary** コマンドを参照してください。つまり、非アクティブなセッションはグループディレクタに報告されません。ASA が（非アクティブなセッションによって）いっぱいになっている場合でも、グループディレクタは必要に応じて接続を ASA に引き続きリダイレクトします。ASA が新しい接続を受信すると、最も長く非アクティブになっていたセッションがログオフされ、新しい接続がそのライセンスを引き継ぎます。

次の例は、100 個の SSL セッション（アクティブのみ）と 2% の SSL 負荷を示しています。これらの数字には、非アクティブなセッションは含まれていません。つまり、非アクティブなセッションは VPN ロードバランシングの負荷に数えられません。

```
hostname# show vpn load-balancing
Status :    enabled
Role :     Master
Failover :   Active
Encryption : enabled
Cluster IP : 192.168.1.100
Peers :     1

Load %
Sessions
Public IP   Role  Pri Model   IPsec SSL IPsec SSL
192.168.1.9 Master 7   ASA-5540 4     2   216   100
192.168.1.19 Backup 9   ASA-5520 0     0    0     0
```

VPN ロードバランシングの機能履歴

機能名	リリース	機能情報
SAML を使用した VPN ロードバランシング	9.17(1)	ASA は、SAML 認証を使用した VPN ロードバランシングをサポートするようになりました。
VPN ロードバランシング	7.2(1)	この機能が導入されました。



第 4 章

全般 VPN パラメータ

バーチャルプライベートネットワークの ASA の実装には、カテゴリの枠を越えた便利な機能があります。この章では、これらの機能のいくつかについて説明します。

- [注意事項と制約事項 \(79 ページ\)](#)
- [ACL をバイパスするための IPsec の設定 \(80 ページ\)](#)
- [インターフェイス内トラフィックの許可 \(ヘアピンング\) \(81 ページ\)](#)
- [アクティブな IPsec セッションまたは SSL VPN セッションの最大数の設定 \(83 ページ\)](#)
- [許可される IPsec クライアント リビジョンレベル確認のためのクライアントアップデートの使用 \(84 ページ\)](#)
- [パブリック IP 接続への NAT 割り当てによる IP アドレスの実装 \(86 ページ\)](#)
- [VPN セッション制限の設定 \(88 ページ\)](#)
- [ID 証明書のネゴシエート時の使用 \(90 ページ\)](#)
- [暗号化コアのプールの設定 \(90 ページ\)](#)
- [ダイナミック スプリット トンネリングの設定 \(91 ページ\)](#)
- [管理 VPN トンネルの設定 \(92 ページ\)](#)
- [アクティブな VPN セッションの表示 \(93 ページ\)](#)
- [ISE ポリシー適用について \(94 ページ\)](#)
- [SSL の詳細設定 \(100 ページ\)](#)
- [事前認証済み SSL 接続のレート制限 \(107 ページ\)](#)
- [永続的 IPsec トンネルフロー \(108 ページ\)](#)
- [暗号アーカイブを使用したトラブルシューティング \(112 ページ\)](#)
- [SSL カウンタの使用 \(113 ページ\)](#)
- [スタックした ASP テーブルエントリの削除方法 \(114 ページ\)](#)
- [ASA からの WebVPN 構成のクリア \(115 ページ\)](#)

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

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 モードとマルチ コンテキスト モードでサポートされています。『[ASA General Operations CLI Configuration Guide](#)』の適切なリリースでは、マルチ コンテキスト モードでサポートされていないもののリストについては『*Guidelines for Multiple Context Mode*』を参照してください。また「*New Features*」には、リリースを通して追加されたものの明細が示されています。

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 モードでのみサポートされています。トランスペアレント モードはサポートされていません。

Network Address Translation (NAT)

NAT 構成に関する注意事項などについては、『*Cisco Secure Firewall ASA Series Firewall CLI Configuration Guide*』の「*NAT for VPN*」セクションを参照してください。

ACL をバイパスするための IPsec の設定

IPsec トンネルから送信されるすべてのパケットに対して、ACL で発信元インターフェイスと宛先インターフェイスをチェックせずに許可するには、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを入力します。

IPsec トラフィックのインターフェイス ACL をバイパスする必要があるのは、ASA の背後で別の VPN コンセントレータを使用し、なおかつ ASA のパフォーマンスを最大限にする場合などです。通常、IPsec パケットを許可する ACL を **access-list** コマンドを使用して作成し、これを発信元インターフェイスに適用します。ACL を使用すると、ASA を通過できるトラフィックを正確に指定できます。

次の例では、ACL をチェックせずに ASA を通過する IPsec トラフィックをイネーブルにします。

```
hostname(config)# sysopt connection permit-vpn
```



(注) **no sysopt connection permit-vpn** が設定されているときに、外部インターフェイスのアクセスグループが **deny ip any any** ACL を呼び出すように設定されていたとしても、クライアントからの復号化された通過トラフィックは許可されます。

保護されたネットワークへの、サイトツーサイトまたはリモート アクセス VPN 経由でのアクセスをコントロールするために、**no sysopt permit-vpn** コマンドを外部インターフェイス上のアクセス コントロール リスト (ACL) と組み合わせて使用しようとしても、うまくいきません。

sysopt connection permit-vpn は、その対象のトラフィックの暗号マップが有効になっているインターフェイスに対する ACL (インとアウトの両方) と、他のすべてのインターフェイスの出力 (アウト) ACL (入力 (イン) ACL ではない) をバイパスします。

このような状況では、内部の管理アクセスがイネーブルになっていると、ACL は適用されず、ユーザーは SSH を使用して ASA に引き続き接続できます。内部ネットワーク上へのホストへのトラフィックは ACL によって正しくブロックされますが、内部インターフェイスへの復号化された通過トラフィックはブロックされません。

ssh および **http** コマンドは、ACL よりもプライオリティが高くなります。VPN セッションからボックスへの SSH、Telnet、または ICMP トラフィックを拒否するには、**ssh**、**telnet**、および **icmp** コマンドを使用します。

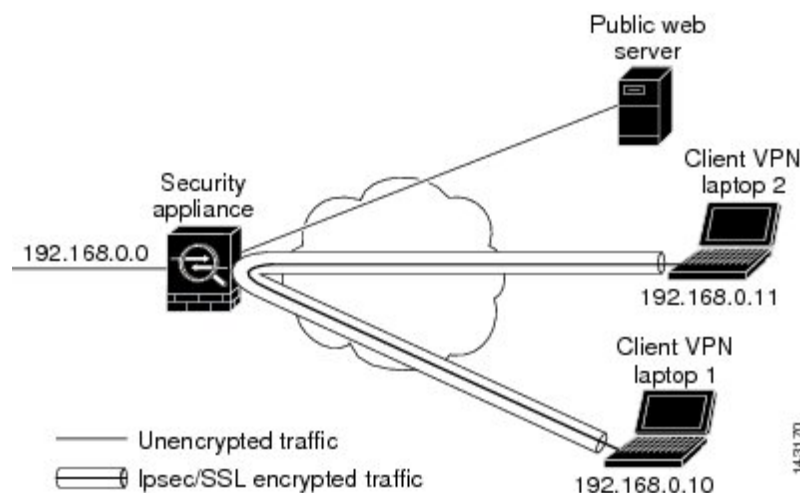
インターフェイス内トラフィックの許可（ヘアピニング）

ASA には、IPsec で保護されたトラフィックに対して、同じインターフェイスの出入りを許可することにより、VPN クライアントが別の VPN ユーザーに IPsec で保護されたトラフィックを送信できる機能があります。「ヘアピニング」とも呼ばれるこの機能は、VPN ハブ (ASA) を介して接続している VPN スポーク (クライアント) と見なすことができます。

ヘアピニングにより、着信 VPN トラフィックを同じインターフェイスを介して暗号化されていないトラフィックとしてリダイレクトすることもできます。この機能は、たとえば、スプリット トンネリングがない状態で、VPN へのアクセスと Web のブラウズの両方を行う必要がある VPN クライアントに役立つ可能性があります。

下の図は、VPN クライアント 1 が VPN クライアント 2 に対してセキュアな IPsec トラフィックを送信し、パブリック Web サーバーに対しては暗号化されていないトラフィックを送信していることを示しています。

図 4: ヘアピニングにインターフェイス内機能を使用する VPN クライアント



この機能を設定するには、グローバル コンフィギュレーション モードで `intra-interface` 引数を指定して `same-security-traffic` コマンドを実行します。

コマンドの構文は、`same-security-traffic permit {inter-interface | intra-interface}` です。

次の例では、インターフェイス内トラフィックをイネーブルにする方法を示しています。

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```



(注) **same-security-traffic** コマンドに **inter-interface** 引数を指定すると、セキュリティレベルが同一のインターフェイス間の通信が許可されます。この機能は、IPsec 接続に固有のものではありません。詳細については、このマニュアルの「インターフェイスパラメータの設定」の章を参照してください。

ヘアピニングを使用するには、「インターフェイス内トラフィックにおける NAT の注意事項」に記載されているように、適切な NAT ルールを ASA インターフェイスに適用する必要があります。

インターフェイス内トラフィックにおける NAT の注意事項

ASA がインターフェイスを介して暗号化されていないトラフィックを送信するには、そのインターフェイスに対する NAT をイネーブルにし、プライベート IP アドレスをパブリックにルーティング可能なアドレスに変換する必要があります（ただし、ローカル IP アドレスプールですでにパブリック IP アドレスを使用している場合は除きます）。次の例では、クライアント IP プールから発信されたトラフィックに、インターフェイス PAT ルールを適用しています。

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
```

```
hostname(config-network-object)# nat (outside,outside) interface
```

ただし、ASA がこの同じインターフェイスから暗号化された VPN トラフィックを送信する場合、NAT は任意です。VPN 間へアピニングは、NAT を使用してもしなくても機能します。すべての発信トラフィックに NAT を適用するには、上記のコマンドを実装するだけです。VPN 間トラフィックを NAT から免除するには、次のように、VPN 間トラフィックの NAT 免除を実装するコマンドを（上記のコマンドに）追加します。

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static  
vpn_nat vpn_nat
```

NAT ルールの詳細については、このマニュアルの「NAT の適用」の章を参照してください。

アクティブな IPsec セッションまたは SSL VPN セッションの最大数の設定

VPN セッションの数を ASA が許可する数よりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb** コマンドを入力します。

```
vpn-sessiondb {max-anyconnect-premium-or-essentials-limit <number> | max-other-vpn-limit  
<number>}
```

max-anyconnect-premium-or-essentials-limit キーワードは、セキュアクライアントセッションの最大数を 1 以上ライセンス許容最大数以下で指定します。



(注) 正しいライセンス、用語、階層、およびユーザー数は、これらのコマンドで決定されなくなりました。『セキュアクライアント Ordering Guide』（<http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf>）を参照してください。

max-other-vpn-limit キーワードは、（セキュアクライアントセッション以外の）VPN セッションの最大数を 1 以上ライセンス許容最大数以下で指定します。これには、Cisco VPN Client (IPsec IKEv1) および LAN-to-LAN VPN セッションが含まれます。

このセッション数の制限は、VPN ロードバランシング用に算出されたロード率に影響します。

次に、最大 Anyconnect VPN セッション数の制限を 450 に設定する例を示します。

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450  
hostname(config)#
```

許可される IPsec クライアント リビジョン レベル確認のためのクライアント アップデートの使用



(注) この項の情報は、IPsec 接続にのみ適用されます。

クライアント アップデート機能を使用すると、中央にいる管理者は、VPN クライアント ソフトウェアをアップデートする時期を VPN クライアント ユーザーに自動的に通知できます。

リモートユーザーは、旧式の VPN ソフトウェアバージョンまたはハードウェアクライアントバージョンを使用している可能性があります。**client-update** コマンドを使用すると、いつでもクライアントリビジョンのアップデートをイネーブルにして、アップデートを適用するクライアントのタイプおよびリビジョン番号を指定し、アップデートを取得する URL または IP アドレスを提供できます。また、Windows クライアントの場合は、オプションで、VPN クライアントバージョンをアップデートする必要があることをユーザーに通知できます。Windows クライアントに対しては、更新を実行するメカニズムをユーザーに提供できます。このコマンドは、IPsec リモートアクセス トンネル グループ タイプにのみ適用されます。

クライアント アップデートを実行するには、一般コンフィギュレーション モードまたはトンネル グループ ipsec 属性コンフィギュレーション モードで **client-update** コマンドを入力します。リビジョン番号のリストにあるソフトウェアバージョンをすでに実行しているクライアントの場合は、ソフトウェアを更新する必要はありません。リストにあるソフトウェアバージョンを実行していないクライアントの場合は、ソフトウェアを更新する必要があります。次の手順は、クライアント アップデートの実行方法を示しています。

手順

- ステップ 1** グローバル コンフィギュレーション モードで、次のコマンドを入力してクライアント アップデートをイネーブルにします。

```
hostname(config)# client-update enable  
hostname(config)#
```

- ステップ 2** グローバル コンフィギュレーション モードで、特定のタイプのすべてのクライアントに適用するクライアントアップデートのパラメータを指定します。つまり、クライアントのタイプ、アップデートイメージを取得する URL または IP アドレス、および許可されるリビジョン番号または対象クライアントの番号を指定します。最大4つのリビジョン番号をカンマで区切って指定できます。

ユーザーのクライアントリビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントをアップデートする必要はありません。このコマンドは、ASA 全体にわたって指定されているタイプのすべてのクライアントのクライアントアップデート値を指定します。

次の構文を使用します。

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers  
hostname(config)#
```

使用可能なクライアントのタイプは、**win9X**（Windows 95、Windows 98、および Windows ME プラットフォームを含む）、**winnt**（Windows NT 4.0、Windows 2000、および Windows XP プラットフォームを含む）、**windows**（Windows ベースのすべてのプラットフォームを含む）です。

リビジョン番号のリストにあるソフトウェアバージョンをすでに実行しているクライアントの場合は、ソフトウェアを更新する必要はありません。リストにあるソフトウェアバージョンを実行していないクライアントの場合は、ソフトウェアを更新する必要があります。これらのクライアントアップデートエントリから3つまで指定することができます。キーワード **windows** を指定すると、許可されるすべての Windows プラットフォームがカバーされます。**windows** を指定する場合は、個々の Windows クライアント タイプは指定しないでください。

（注）

すべての Windows クライアントでは、URL のプレフィックスとしてプロトコル **http://** または **https://** を使用する必要があります。

次の例では、リモートアクセス トンネル グループのクライアントアップデートパラメータを設定しています。リビジョン番号 4.6.1 とアップデートを取得するための URL

（**https://support/updates**）を指定します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1  
hostname(config)#
```

あるいは、特定のタイプのすべてのクライアントではなく、個々のトンネルグループだけのためのクライアント アップデートを設定できます（ステップ 3 を参照）。

（注）

URL の末尾にアプリケーション名を含めることで（例：

https://support/updates/vpnclient.exe）、アプリケーションを自動的に起動するようにブラウザを設定できます。

ステップ 3 特定の ipsec-ra トンネル グループの client-update パラメータのセットを定義します。

トンネルグループ ipsec 属性モードで、トンネルグループ名とそのタイプ、アップデートされたイメージを取得する URL または IP アドレス、およびリビジョン番号を指定します。ユーザーのクライアントのリビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合、クライアントをアップデートする必要はありません。たとえば、Windows クライアントの場合、次のコマンドを入力します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra  
hostname(config)# tunnel-group remotegrp ipsec-attributes  
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/  
rev-nums 4.6.1  
hostname(config-tunnel-ipsec)#
```

ステップ 4 (任意) クライアントのアップデートが必要な旧式の Windows クライアントを使用しているアクティブなユーザーに通知を送信します。これらのユーザーにはポップアップウィンドウが表示され、ブラウザを起動して、URL で指定したサイトからアップデートされたソフトウェアをダウンロードする機会が提供されます。このメッセージで設定可能な部分は URL だけです (ステップ 2 または 3 を参照)。アクティブでないユーザーは、次回ログオン時に通知メッセージを受信します。この通知は、すべてのトンネル グループのすべてのアクティブ クライアントに送信するか、または特定のトンネル グループのクライアントに送信できます。たとえば、すべてのトンネル グループのすべてのアクティブ クライアントに通知する場合は、特権 EXEC モードで次のコマンドを入力します。

```
hostname# client-update all
hostname#
```

ユーザーのクライアントのリビジョン番号が指定されているリビジョン番号のいずれかと一致している場合、そのクライアントをアップデートする必要はなく、通知メッセージはユーザーに送信されません。

次のタスク



(注) クライアント更新のタイプを **windows** (Windows ベースのすべてのプラットフォーム) に指定し、その後、同じエンティティに **win9x** または **winnt** のクライアント更新タイプを入力する必要がある場合は、まずこのコマンドの **no** 形式で **windows** クライアント タイプを削除してから、新しい **client-update** コマンドを使用して新しいクライアント タイプを指定します。

パブリック IP 接続への NAT 割り当てによる IP アドレスの実装

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 アドレスに戻す場合があります。

ASA では、内部/保護対象ネットワークの VPN クライアントの割り当てられた IP アドレスをパブリック (送信元) IP アドレスに変換する方法が導入されました。この機能は、内部ネットワークおよびネットワーク セキュリティ ポリシーのターゲット サーバー/サービスが、社内ネットワークの割り当てられた IP ではなく、VPN クライアントのパブリック/送信元 IP との通信を必要とするシナリオをサポートします。

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。

- レガシー (IKEv1) クライアントと セキュアクライアント だけをサポートします。
- 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。
- 割り当てられた IPv4 およびパブリック アドレスだけをサポートします。
- NAT/PAT デバイスの背後にある複数のピアはサポートされません。
- 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)。
- ローミングはサポートされません。

手順

ステップ1 グローバル コンフィギュレーション モードで、**tunnel general** を入力します。

ステップ2 アドレス変換をイネーブルにするには、次の構文を使用します。

```
hostname(config-tunnel-general)# nat-assigned-to-public-ip interface
```

このコマンドは、送信元のパブリック IP アドレスに、割り当てられた IP アドレスの NAT ポリシーをダイナミックにインストールします。*interface* は、NAT の適用先を決定します。

ステップ3 アドレス変換をディセーブルにするには、次の構文を使用します。

```
hostname(config-tunnel-general)# no nat-assigned-to-public-ip
```

VPN NAT ポリシーの表示

アドレス変換は、基礎となるオブジェクト NAT メカニズムを使用します。そのため、VPN NAT ポリシーは、手動設定されたオブジェクト NAT ポリシーと同様に表示されます。次の例では、割り当てられた IP として 95.1.226.4 を使用して、ピアのパブリック IP として 75.1.224.21 を使用します。

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
   translate_hits = 315, untranslate_hits = 315

prompt# show nat detail
```

```

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
   translate_hits = 315, untranslate_hits = 315
   Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32

```

outside はセキュアクライアントが接続するインターフェイスであり、*inside* は新しいトンネルグループに固有のインターフェイスです。



(注) VPN NAT ポリシーがダイナミックであり、設定に追加されないため、VPN NAT オブジェクトおよび NAT ポリシーは、`show run object` レポートおよび `show run nat` レポートから非表示になります。

VPN セッション制限の設定

IPsec セッションと SSL VPN セッションは、プラットフォームと ASA ライセンスがサポートする限り、いくつでも実行できます。ASA の最大セッション数を含むライセンス情報を表示するには、グローバル コンフィギュレーション モードで **show version** コマンドを入力し、ライセンスのセクションを探します。次の例は、このコマンドの出力からのコマンドとライセンスの情報を示しています。もう一方の出力は明確にするために編集されています。

```

hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited      perpetual
Maximum VLANs                   : 500          perpetual
Inside Hosts                     : Unlimited     perpetual
Failover                         : Active/Active perpetual
Encryption-DES                   : Enabled       perpetual
Encryption-3DES-AES              : Enabled       perpetual
Security Contexts                : 100          perpetual
Carrier                          : Enabled        perpetual
AnyConnect Premium Peers         : 5000         perpetual
AnyConnect Essentials            : 5000         perpetual
Other VPN Peers                  : 5000         perpetual
Total VPN Peers                  : 5000         perpetual
AnyConnect for Mobile            : Enabled       perpetual
AnyConnect for Cisco VPN Phone   : Enabled       perpetual
Advanced Endpoint Assessment     : Enabled       perpetual
Shared License                   : Disabled     perpetual
Total TLS Proxy Sessions         : 3000         perpetual
Botnet Traffic Filter            : Disabled     perpetual
IPS Module                       : Disabled     perpetual
Cluster                         : Enabled       perpetual
Cluster Members                  : 2            perpetual

This platform has an ASA5555 VPN Premium license.

```

ライセンス リソース割り当ての表示

リソース割り当てを表示するには、次のコマンドを使用します。

```
asa2(config)# sh resource allocation
Resource      Total    % of Avail
Conns[rate]   100(U)    0.00%
Inspects[rate] unlimited
Syslogs[rate] unlimited
Conns         unlimited
Hosts         unlimited
IPsec         unlimited
Mac-addresses unlimited
ASDM          10        5.00%
SSH           10        10.00%
Telnet        10        10.0%
Xlates        unlimited
AnyConnect    1000      10%
AnyConnectBurst 200       2%
OtherVPN      2000      20%
OtherVPNBurst 1000      10%
```

ライセンス リソース使用率の表示

リソース使用率を表示するには、次のコマンドを使用します。



(注) **sh resource usage system controller all 0** コマンドを使用して、プラットフォーム制限として制限があるシステム レベルの使用率を表示することもできます。

```
ASA(config-ca-trustpoint)# sh resource usage
Resource      Current Peak Limit Denied Context
Conns         1      16  280000 0      System
Hosts         2      10   N/A    0      System
AnyConnect    2      25   1000  0      cust1
AnyConnectBurst 0      0    200   0      cust1
OtherVPN      1      1    2000  0      cust2
OtherVPNBurst 0      0    1000  0      cust2
```

VPN セッションの制限

AnyConnect VPN セッション (IPsec/IKEv2 または SSL) を ASA で許可されているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-anyconnect-premium-or-essentials-limit** コマンドを使用します。セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。

ASA のライセンスで 500 の SSL VPN セッションが許可されていて、AnyConnect VPN セッション数を 250 に制限する場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

ID 証明書のネゴシエート時の使用

セキュアクライアントで IKEv2 トンネルをネゴシエートするときに、ASA は ID 証明書を使用する必要があります。IKEv2 リモート アクセス トラストポイントの設定には、次のコマンドを使用します。

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

このコマンドを使用すると、セキュアクライアントは、エンドユーザーのグループ選択をサポートできるようになります。2つのトラストポイントを同時に設定できます。RSA を 2 つ、ECDSA を 2 つ、またはそれぞれ 1 つずつ設定できます。ASA は、設定したトラストポイントリストをスキャンし、クライアントがサポートする最初の 1 つを選択します。ECDSA を使用する場合は、RSA トラストポイントの前に、このトラストポイントを設定する必要があります。

行番号オプションは、トラストポイントを挿入する行番号の場所を指定します。通常、このオプションは、別の行を削除および再追加しないで一番上にトラストポイントを挿入するために使用されます。行が指定されていない場合、ASA はリストの末尾にトラストポイントを追加します。

すでに存在するトラストポイントを追加しようとする、エラーが表示されます。削除するトラストポイント名を指定しないで `no crypto ikev2 remote-access trustpoint` コマンドを使用すると、すべてのトラストポイント コンフィギュレーションが削除されます。

暗号化コアのプールの設定

対称型マルチプロセッシング (SMP) プラットフォームでの暗号化コアの割り当てを変更して、セキュアクライアント TLS/DTLS トラフィックのスループットを向上させることができます。この変更によって、SSL VPN データパスが高速化され、セキュアクライアント、スマートトンネル、およびポート転送において、ユーザーが認識できるパフォーマンス向上が実現します。次の手順では、シングル コンテキスト モードまたはマルチ コンテキスト モードで暗号化コアのプールを設定します。

手順

暗号化アクセラレータ プロセッサの割り当てを指定します。

crypto engine accelerator-bias

- [balanced] : 暗号化ハードウェア リソースを均等に分散します (Admin/SSL および IPsec コア)。

- [ipsec] : IPsec を優先するように暗号化ハードウェア リソースを割り当てます (SRTP 暗号化音声トラフィックを含む)。
- [ssl] : Admin/SSL を優先するように暗号化ハードウェア リソースを割り当てます。SSL ベースのセキュアクライアント リモートアクセス VPN セッションをサポートする場合は、このバイアスを使用します。

例 :

```
hostname(config)# crypto engine accelerator-bias ssl
```

ダイナミック スプリット トンネリングの設定

ダイナミック スプリット トンネリングでは、トンネルの確立後に、DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。ダイナミック スプリット トンネリングを設定するには、カスタム属性を作成し、グループ ポリシーに追加します。

始める前に

この機能を使用するには、AnyConnect リリース 4.5 (またはそれ以降) が必要です。詳細については、「[About Dynamic Split Tunneling](#)」を参照してください。

手順

- ステップ 1** 次のコマンドで、WebVPN コンテキストにおけるカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```
- ステップ 2** VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Webサービスについて、属性名を定義します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。属性値は VPN トンネルから除外するドメイン名のリストを含み、次の例のように、カンマ区切り値 (CSV) 形式にする必要があります。

```
anyconnect-custom-data dynamic-split-exclude-domains webex.com, webexconnect.com, tags.tiqcdn.com
```
- ステップ 3** 次のコマンドで、以前に定義されているカスタム属性を特定のポリシーグループに追加します。これは、group-policy 属性のコンテキストで実行されます。anyconnect-custom dynamic-split-exclude-domains value webex_service_domains

次のタスク

スプリットを含むトンネリングが設定されている場合、ダイナミック スプリット 除外は、スプリットを含むネットワークに DNS 応答 IP アドレスが 1 つ以上含まれる場合のみ、実行されま

す。DNS 応答 IP アドレスとスプリットを含むネットワークのいずれかの間にまったく重なりがない場合、すべての DNS 応答 IP アドレスに一致するトラフィックはすでにトンネリングから除外されているため、ダイナミック スプリット除外の実行は不要です。

管理 VPN トンネルの設定

管理 VPN トンネルにより、エンドユーザーによって VPN 接続が確立されるときだけでなく、クライアント システムの電源が入るたびに社内ネットワークの接続が確保されます。オフィス ネットワークに VPN を介してユーザが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで Patch Management を行うことができます。この機能には、社内ネットワークの接続を必要とするエンドポイント OS ログインスクリプトに対するメリットもあります。

管理 VPN トンネルはエンドユーザーに対し透過的であるため、ユーザアプリケーションによって開始されたネットワーク トラフィックはデフォルトで影響を受けませんが、代わりに管理 VPN トンネルの外部に転送されます。

ログインが低速であるとユーザーから報告された場合、管理トンネルが適切に設定されていない可能性があります。追加の要件、非互換性、制限、および管理 VPN トンネルのトラブルシューティングについては、『[Cisco Secure Client Administration Guide](#)』を参照してください。

始める前に

AnyConnect リリース 4.7（またはそれ以降）が必要

手順

- ステップ 1** アップロードしたプロファイル（`profileMgmt`）を管理トンネル接続で使用されているトンネルグループにマッピングされているグループ ポリシー（`MgmtTunGrpPolicy`）に追加します。

プロファイルが AnyConnect 管理 VPN プロファイルであることを示すには、`anyconnect profiles` コマンドに `type vpn-mgmt` を含めます。通常の AnyConnect VPN プロファイルは `type user` です。

```
group-policy MgmtTunGrpPolicy attributes
  webvpn
    anyconnect profiles value profileMgmt type vpn-mgmt
```

- ステップ 2** ユーザ トンネル接続を使用して管理 VPN プロファイルを展開するには、アップロードされたプロファイル（`profileMgmt`）をユーザ トンネル接続で使用されているトンネルグループにマッピングされたグループ ポリシー（`DfltGrpPolicy`）に追加します。

```
group-policy DfltGrpPolicy attributes
  webvpn
    anyconnect profiles value profileMgmt type vpn-mgmt
```

アクティブな VPN セッションの表示

次のトピックでは、VPN セッション情報を表示する方法について説明します。

IP アドレスタイプ別のアクティブな セキュアクライアント セッションの表示

コマンドライン インターフェイスを使用して、アクティブな セキュアクライアント セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb anyconnect filter p-ipversion** または **show vpn-sessiondb anyconnect filter a-ipversion** コマンドを入力します。

- エンドポイントのパブリック IPv4 または IPv6 アドレスでフィルタリングされたアクティブなセキュアクライアントセッションを表示します。パブリックアドレスは、企業によってエンドポイントに割り当てられたアドレスです。

```
show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}
```

- エンドポイントの割り当てられた IPv4 または IPv6 アドレスでフィルタリングされたアクティブなセキュアクライアントセッションを表示します。割り当て済みアドレスは、ASA によってセキュアクライアントに割り当てられたアドレスです。

```
show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}
```

show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] コマンドの出力例

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4
```

```
Session Type: AnyConnect
```

```
Username       : user1                      Index       : 40
Assigned IP    : 192.168.17.10              Public IP    : 198.51.100.1
Protocol       : AnyConnect-Parent SSL-Tunnel
License        : AnyConnect Premium
Encryption     : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing        : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx       : 10570                      Bytes Rx     : 8085
Group Policy   : GroupPolicy_SSLACCLIENT
Tunnel Group   : SSLACCLIENT
Login Time     : 15:17:12 UTC Mon Oct 22 2012
Duration      : 0h:00m:09s
Inactivity     : 0h:00m:00s
NAC Result     : Unknown
VLAN Mapping   : N/A                      VLAN         : none
```

show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6] コマンドの出力

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6
```

```

Session Type: AnyConnect

Username      : user1                      Index      : 45
Assigned IP   : 192.168.17.10
Public IP     : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
Assigned IPv6 : 2001:DB8:9:1::24
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx      : 10662                      Bytes Rx   : 17248
Group Policy  : GroupPolicy_SSL_IPv6       Tunnel Group : SSL_IPv6
Login Time    : 17:42:42 UTC Mon Oct 22 2012
Duration      : 0h:00m:33s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                       VLAN       : none

```

IP アドレス タイプ別のアクティブな LAN-to-LAN VPN セッションの表示

コマンドラインインターフェイスを使用して、アクティブなクライアントレス SSL VPN セッションを表示するには、特権 EXEC モードで **show vpn-sessiondb l2l filter ipversion** コマンドを入力します。

このコマンドは、接続のパブリック IPv4 アドレスまたはパブリック IPv6 アドレスでフィルタリングされたアクティブな LAN-to-LAN VPN セッションを表示します。

パブリック アドレスは、企業によってエンドポイントに割り当てられたアドレスです。

```
show vpn-sessiondb l2l filter ipversion {v4 | v6}
```

ISE ポリシー適用について

Cisco Identity Services Engine (ISE) は、セキュリティ ポリシー管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティ コンプライアンスを自動化し、シンプルにします。Cisco ISE は主に、Cisco TrustSec と連携してセキュアアクセスとゲストアクセスを提供し、個人所有デバイス持ち込み (BYOD) イニシアティブをサポートし、使用ポリシーを適用するために使用されます。

ISE Change of Authorization (CoA) 機能は、認証、認可、およびアカウントティング (AAA) セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザーまたはユーザー グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インラインポスチャ実施ポイント (IPEP) は、ASA によって確立された各 VPN セッションにアクセス コントロール リスト (ACL) を適用する必要はありません。

ISE ポリシーの実施は、次の VPN クライアントでサポートされています。

- IPSec

- セキュアクライアント
- L2TP/IPSec



(注) ダイナミック ACL (dACL) やセキュリティグループタグ (SGT) などの一部のポリシー要素はサポートされていますが、VLAN 割り当てや IP アドレス割り当てなどのポリシー要素はサポートされていません。

システム フローは次のとおりです。

1. エンドユーザーが VPN 接続を要求します。
2. ASA は、ISE に対してユーザーを認証し、ネットワークへの限定アクセスを提供するユーザー ACL を受け取ります。
3. アカウンティング開始メッセージが ISE に送信され、セッションが登録されます。
4. ポスチャアセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。
5. ISE が CoA の「ポリシー プッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワーク アクセス権限を高める新しいユーザー ACL が識別されます。



(注) 後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

このフローモデルは、RADIUS CoA を使用するほとんどのシナリオとは異なります。有線/ワイヤレス 802.1x 認証の場合、RADIUS CoA には属性は含まれません。DACL などのすべての属性がアタッチされた 2 番目の認証のみをトリガーします。ASA VPN ポスチャの場合、2 番目の認証はありません。すべての属性が RADIUS CoA で返されます。VPN セッションがアクティブになり、ほとんどの VPN ユーザー設定を変更できません。CoA のアクティブ化によって変更できる設定は、RedirectURL、RedirectACL、およびセキュリティグループタグ (SGT) のみです。

ISE ポリシー適用に関する RADIUS サーバー グループの設定

ISE ポリシーの評価と適用をイネーブルにするには、ISE サーバーの RADIUS AAA サーバーグループを設定し、サーバーをグループに追加します。VPN にトンネルグループを設定する場合は、グループで AAA サービスにこのサーバーグループを指定します。

手順

ステップ 1 RADIUS AAA サーバーグループを作成します。

aaa-server group_name protocol radius

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

ステップ 2 AAA サーバー グループの RADIUS 動的認可 (CoA) サービスをイネーブルにします。

dynamic-authorization [port number]

ポートの指定は任意です。デフォルトは 1700 です。指定できる範囲は 1024 ~ 65535 です。

VPN トンネルでサーバー グループを使用すると、対応する RADIUS サーバー グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリスンします。

```
hostname(config-aaa-server-group)# dynamic-authorization
```

ステップ 3 認証に ISE を使用しない場合は、RADIUS サーバー グループに対し認可専用モードを有効にします。

authorize-only

これは、サーバー グループを認可に使用するとき、RADIUS アクセス要求メッセージが、AAA サーバー用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。**radius-common-pw** コマンドを使用して RADIUS サーバーの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバー グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウントिंगにこのサーバー グループを使用する可能性があるからです。

```
hostname(config-aaa-server-group)# authorize-only
```

ステップ 4 RADIUS 中間アカウントングアップデート メッセージの定期的な生成をイネーブルにします。

interim-accounting-update [periodic [hours]]

ISE は、ASA などの NAS デバイスから受信するアカウントング レコードに基づいて、アクティブセッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知 (アカウントング メッセージまたはポスチャ トランザクション) を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブセッションについて ISE に定期的に中間アカウントング更新メッセージを送信するように、グループを設定します。

- **periodic[hours]** は、対象のサーバー グループにアカウントング レコードを送信するように設定されたすべての VPN セッションのアカウントング レコードの定期的な生成と伝送をイネーブルにします。オプションで、これらの更新の送信間隔 (時間単位) を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ~ 120 時間です。
- (パラメータなし) 。 **periodic** キーワードなしでこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときのみ中間アカ

ウンティング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティングアップデートが生成されます。

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

ステップ 5 (任意) ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。

merge-dacl {before-avpair | after-avpair}

このオプションは、VPN 接続にのみ適用されます。VPN ユーザーの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

before-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの前に配置されるように指定します。

after-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの後に配置されるように指定します。

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

ステップ 6 (任意) 次のサーバーを試す前にグループ内の RADIUS サーバーに送信する要求の最大数を指定します。

max-failed-attempts number

範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバーが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。サーバーグループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバーにアクセスしようとします。

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

ステップ 7 (任意) グループ内で障害の発生したサーバーを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {depletion [deadtime minutes] | timed}

それぞれの説明は次のとおりです。

- **depletion [deadtime minutes]** は、グループ内のすべてのサーバーが非アクティブになった後でのみ、障害が発生したサーバーを再アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバーがディセーブルになってから、その後すべてのサーバーを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定できます。デフォルトは 10 分です。
- **timed 30** 秒のダウン時間の後、障害が発生したサーバーを再アクティブ化します。

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

ステップ 8 (任意) グループ内のすべてのサーバーにアカウントिंग メッセージを送信します。

accounting-mode simultaneous

アクティブ サーバーだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

ステップ 9 グループに ISE RADIUS サーバーを追加します。

aaa-server group_name [(interface_name)] host {server_ip | name} [key]

それぞれの説明は次のとおりです。

- **group_name** は、RADIUS サーバー グループの名前です。
- **(interface_name)** は、サーバーが到達するために使用するインターフェイスの名前です。デフォルトは (inside) です。カッコは必須です。
- **host{server_ip | name}** は、ISE RADIUS サーバーの IP アドレスまたはホスト名です。
- **key** は、接続を暗号化するためのオプションキーです。aaa-server-host モードに入った後で **key** コマンドを使用することで、このキーをより簡単に入力できます。キーを設定しないと、接続は暗号化されません（プレーンテキスト）。このキーは 127 文字までの英数字から構成され、大文字と小文字の区別があり、RADIUS サーバー上のキーと同じ値になります。

グループには複数のサーバーを追加できます。

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

ISE ポリシーの適用の設定例

パスワードによる ISE ダイナミック認証のための VPN トンネルの設定

次の例は、ISE サーバー グループに、動的認可 (CoA) のアップデートと時間ごとの定期的なアカウントिंगを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

ISE 認証のみの VPN トンネルの設定

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。サーバー グループは認証用に使用されないため、authorize-only コマンドをサーバー グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

ポリシーの適用のトラブルシューティング

次のコマンドは、デバッグに使用できます。

CoA のアクティビティを追跡するには：

```
debug radius dynamic-authorization
```

リダイレクト URL 機能を追跡するには：

```
debug aaa url-redirect
```

URL リダイレクト機能に対応する NP 分類ルールを表示するには：

```
show asp table classify domain url-redirect
```

SSL の詳細設定

ASA は、Secure Sockets Layer (SSL) プロトコルと Transport Layer Security (TLS) を使用して、ASDM、クライアントレス SSL VPN、VPN、およびブラウザベースの各セッションのセキュアなメッセージ伝送を実現します。ASA が SSL ベースの VPN 接続と管理接続でサポートしているプロトコルは、SSLv3、TLSv1、TLSv1.1、TLSv1.2、および TLSv1.3 です。また、DTLS は Cisco Secure Client の AnyConnect VPN モジュールの接続に使用されます。

説明したように、次の暗号方式がサポートされています。

暗号化方式	TLSv1.1 / DTLS V1	TLSv1.2 / DTLSV 1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	いいえ	いいえ	はい
TLS_CHACHA20_POLY1305_SHA256	いいえ	いいえ	はい
TLS_AES_256_GCM_SHA384	いいえ	いいえ	はい
AES128-GCM-SHA256	いいえ	はい	いいえ
AES128-SHA	はい	はい	いいえ
AES128-SHA256	いいえ	はい	いいえ
AES256-GCM-SHA384	いいえ	はい	いいえ
AES256-SHA	はい	はい	いいえ
AES256-SHA256	いいえ	はい	いいえ
DERS-CBC-SHA	いいえ	いいえ	いいえ
DES-CBC-SHA	はい	はい	いいえ

暗号化方式	TLSv1.1 / DTLS V1	TLSv1.2 / DTLSV 1.2	TLSv1.3
DHE-RSA-AES128-GCM-SHA256	いいえ	はい	いいえ
DHE-RSA-AES128-SHA	はい	はい	いいえ
DHE-RSA-AES128-SHA256	いいえ	はい	いいえ
DHE-RSA-AES256-GCM-SHA384	no	1	×
DHE-RSA-AES256-SHA	はい	はい	いいえ
ECDHE-ECDSA-AES128-GCM-SHA256	いいえ	はい	いいえ
ECDHE-ECDSA-AES128-SHA256	いいえ	はい	いいえ
ECDHE-ECDSA-AES256-GCM-SHA384	いいえ	はい	いいえ
ECDHE-ECDSA-AES256-SHA384	いいえ	はい	いいえ
ECDHE-RSA-AES128-GCM-SHA256	はい	はい	いいえ
ECDHE-RSA-AES128-SHA256	いいえ	はい	いいえ
ECDHE-RSA-AES256-GCM-SHA384	いいえ	はい	いいえ
ECDHE-RSA-AES256-SHA384	いいえ	はい	いいえ
NULL-SHA	いいえ	いいえ	いいえ
RC4-MD5	いいえ	いいえ	いいえ
RC4-SHA	いいえ	いいえ	いいえ



(注) リリース 9.4 (1) では、SSLv3 キーワードはすべて ASA 設定から削除されており、SSLv3 のサポートが ASA から削除されました。SSLv3 がイネーブルになっている場合は、SSLv3 オプションを指定したコマンドからブート時エラーが表示されます。ASA はデフォルトの TLSv1 に戻ります。

Citrix モバイルレシーバは TLS 1.1/1.2 プロトコルをサポートしていない可能性があります。互換性については、
https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf
 を参照してください。

ASA が SSL/TLS および DTLS 接続をネゴシエートする最小プロトコルバージョンを指定するには、次の手順を実行します。

手順

ステップ 1 ASA が接続をネゴシエートする最小プロトコルバージョンを設定します。

ssl server-version [tlsv1 | tlsv1.1 | tlsv1.2 | tlsv1.3] [dtls1 | dtls1.2]

それぞれの説明は次のとおりです。

- **tlsv1** : SSLv2 クライアントの hello を受け入れ、TLSv1 (以降) をネゴシエートするには、このキーワードを入力します。
- **tlsv1.1** : SSLv2 クライアントの hello を受け入れ、TLSv1.1 (以降) をネゴシエートするには、このキーワードを入力します。
- **tlsv1.2** : SSLv2 クライアントの hello を受け入れ、TLSv1.2 (以降) をネゴシエートするには、このキーワードを入力します。
- **tlsv1.3** : SSLv2 クライアントの hello を受け入れ、TLSv1.3 (以降) をネゴシエートするには、このキーワードを入力します。
- **dtls1** : DTLSv1 クライアントの hello を受け入れ、DTLSv1 (以降) をネゴシエートするには、このキーワードを入力します。
- **dtls1.2** : DTLSv1.2 クライアントの hello を受け入れ、DTLSv1.2 (以降) をネゴシエートするには、このキーワードを入力します。

(注)

DTLS の設定および使用は、セキュアクライアント リモートアクセス接続のみに適用されます。

DTLS と同等以上の TLS バージョンを使用して、TLS セッションを DTLS セッションと同等以上にセキュアにする必要があります。これにより、dtls1.2 を選択したときに、tlsv1.2 が許容される唯一の TLS バージョンになります。また、すべての TLS バージョンは DTLS 1.0 と同等以上であるため、任意の TLS バージョンを dtls1 と一緒に使用することができます。

例 :

例 :

```
hostname(config)# ssl server-version tlsv1.1
```

```
hostname(config)# ssl server-version tlsv1.2 dtlsv1.2
```

ステップ 2 ASA がサーバーとして動作する場合に使用する SSL/TLS プロトコルの最大バージョンを指定します。

```
ssl server-max-version [tlsv1 | tlsv1.1 | tlsv1.2 | tlsv1.3]
```

server-max-version が TLSV1.2 として設定されている場合、server-version として TLSV1.3 を設定することはできません。

ステップ 3 ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。

```
ssl client-version [tlsv1 | tlsv1.1 | tlsv1.2 | tlsv1.3]
```

ここで、

- **tlsv1** : このキーワードを指定すると、ASA は TLSv1 クライアントの hello を送信し、TLSv1 (以上) をネゴシエートします。
- **tlsv1.1** : このキーワードを指定すると、ASA は TLSv1.1 クライアントの hello を送信し、TLSv1.1 (以上) をネゴシエートします。
- **tlsv1.2** : このキーワードを指定すると、ASA は TLSv1.2 クライアントの hello を送信し、TLSv1.2 (以上) をネゴシエートします。
- **tlsv1.3** : このキーワードを指定すると、ASA は TLSv1.3 クライアントの hello を送信し、TLSv1.3 (以上) をネゴシエートします。

SSL クライアントロールに対して DTLS を使用することはできません。

例 :

例 :

```
hostname(config)# ssl client-version tlsv1
```

ステップ 4 ASA がクライアントとして動作する場合に使用する SSL/TLS プロトコルの最大バージョンを指定します。

```
ssl client-max-version [tlsv1 | tlsv1.1 | tlsv1.2 | tlsv1.3]
```

client-max-version が TLSV1.2 として設定されている場合、client-version として TLSV1.3 を設定することはできません。

ステップ 5 SSL、DTLS、および TLS プロトコルの暗号化アルゴリズムを指定します。

```
ssl cipher version [ level | custom string]
```

それぞれの説明は次のとおりです。

- **version** 引数は、SSL、DTLS、または TLS プロトコルバージョンを指定します。サポートされているバージョンは次のとおりです。
 - **default** : 発信接続用の暗号セット。
 - **dtls** : DTLSv1 着信接続用の暗号。
 - **dtls1.2** : DTLSv1.2 着信接続用の暗号。
 - **tls** : TLSv1 着信接続用の暗号。
 - **tls1.1** : TLSv1.1 着信接続用の暗号。
 - **tls1.2** : TLSv1.2 着信接続用の暗号。
 - **tls1.3** : TLSv1.3 着信接続用の暗号。
- **level** 引数は、暗号強度を指定し、設定されている暗号の最低レベルを示します。次に、強度の有効な値を強度の低い順に示します。
 - **all** : すべての暗号方式が含まれます。
 - **low** : NULL-SHA を除くすべての暗号が含まれます。
 - **medium** (これはすべてのプロトコルバージョンのデフォルト値です) : NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除くすべての暗号が含まれます。
 - **fips** : NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く FIPS 準拠のすべての暗号が含まれます。
 - **high** (TLSv1.2 および TLSv1.3 にのみ適用) : TLSv1.2 用の SHA-2 暗号を使用する AES-256 のみが含まれます。すべての TLSv1.3 暗号の強度は **high** です。
- **customstring** オプションを指定すると、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。詳細については、<https://www.openssl.org/docs/apps/ciphers.html> を参照してください。

推奨設定は **[medium]** です。**[high]** を使用すると、接続が制限されることがあります。**custom** を使用すると、少数の暗号のみが設定されている場合は、機能が制限されることがあります。デフォルトのカスタム値を制限すると、クラスタリングを含めて発信接続が制限されることがあります。

ASA によってサポートされる暗号の優先順位は次のとおりです。詳細については、コマンドリファレンスを参照してください。

このコマンドは、バージョン 9.3(2) から廃止された `ssl encryption` コマンドに代わるものです。

ステップ 6 1 つのインターフェイスで複数のトラストポイントを可能にします。

ssl trust-point name [**[interface vpnlb-ip]**] | [**domain domain-name**]

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

name 引数は、トラストポイントの名前を指定します。**interface** 引数は、トラストポイントが設定されているインターフェイスの名前を指定します。**vpnlb-ip** キーワードは、インターフェイスにのみ適用され、このトラストポイントがこのインターフェイス上の VPN ロード バランシング クラスターの IP アドレスに関連付けます。**domain****domain-name** キーワードと引数のペアは、インターフェイスへのアクセスに使用される特定のドメイン名に関連付けられたトラストポイントを指定します。

インターフェイスあたり最大 16 個のトラストポイントを設定できます。

インターフェイスまたはドメインを指定しない場合は、トラストポイントが設定されていないすべてのインターフェイス用のフォールバック トラストポイントが作成されます。

ssl trustpoint ? コマンドを入力すると、使用可能な設定済みのトラストポイントが表示されます。**ssl trust-point name ?** コマンド（たとえば、**ssl trust-point mysslcert ?**）を入力した場合、trustpoint-SSL 証明書アソシエーションに使用可能な設定済みのインターフェイスが表示されます。

このコマンドを使用するときは、次のガイドラインに従ってください。

- **trustpoint** の値は、**crypto ca trustpoint name** コマンドで設定された CA トラストポイントの **name** である必要があります。
- **interface** の値は、あらかじめ設定されたインターフェイスの **nameif** 名である必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照する **ssl trust-point** エントリも削除されます。
- **ssl trust-point** エントリは、インターフェイスごとに 1 つと、インターフェイスを指定しないもの 1 つを保持できます。
- 同じトラストポイントを複数のエントリで再利用できます。
- **domain** キーワードで設定したトラストポイントは、複数のインターフェイスに適用されることがあります（接続方法によって異なります）。
- **domain-name** の値ごとに 1 つの **ssl trust-point** のみを保持できます。
- このコマンドを入力すると、次のエラーが表示される場合があります。

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values mismatch@x509_cmp.c:339
```

これは、ユーザーが新しい証明書を設定して、以前に設定された証明書と置き換えたことを示しています。特に対処の必要はありません。

- 証明書は次の順序で選択されます。
 - 接続が **domain** キーワードの値に一致した場合、その証明書が最初に選択されます。（**ssl trust-point namedomain domain-name** コマンド）

- ロードバランシングアドレスへの接続が確立された場合、vpnlb-ip 証明書が選択されます。（**ssl trust-point name interface vpnlb-ip** コマンド）
- インターフェイスに対して設定された証明書。（**ssl trust-point name interface** コマンド）
- インターフェイスに関連付けられていないデフォルトの証明書。（**ssl trust-point name**）
- ASA の自己署名付き自己生成証明書。

ステップ 7 TLS の DHE-RSA 暗号方式で使用する DH グループを指定します。

```
ssl dh-group [group14 | group15]
hostname(config)# ssl dh-group group14
```

group14、15 キーワードは、DH グループ 14（2048 ビットモジュラス、224 ビット素数位数サブグループ）を設定します。

グループ 14 は Java 7 と互換性がありません。すべてのグループが Java 8 と互換性があります。グループ 14 は FIPS 準拠です。デフォルト値は **ssl dh-group group14** です。

ステップ 8 TLS の ECDHE-ECDSA 暗号方式で使用するグループを指定します。

```
ssl ecdh-group [group19 | group20 | group21]
hostname(config)# ssl ecdh-group group20
```

group19 キーワードは、グループ 19（256 ビット EC）を設定します。group20 キーワードは、グループ 20（384 ビット EC）を設定します。group21 キーワードは、グループ 21（521 ビット EC）を設定します。

デフォルト値は **ssl ecdh-group group19** です。

（注）

優先度が最も高いのは ECDSA 暗号および DHE 暗号です。

次のタスク

次のコマンドを使用して、TLS/DTLS 設定を表示できます。

- デフォルトの TLS/DTLS バージョンではない場合は、**show run ssl**。
- デフォルトの TLS/DTLS バージョンである場合は、**show run ssl all**。

事前認証済み SSL 接続のレート制限

事前認証された SSL 接続は、ユーザーまたはデバイスが認証プロセスを完了する前に確立されるセキュアな接続です。ASA は、複数の事前認証された SSL 接続を受信できますが、そのために、デバイスのメモリ使用率が高くなってしまい、新しい SSL 接続が妨げられ、デバイスが応答なくなり、パフォーマンスに影響が及ぶ可能性があります。

ASA は、これらの事前認証された SSL 接続のレートを制限できます。この制限は、デバイスの VPN 接続制限の 3 倍として計算されます。この機能はデフォルトで有効になっており、ASA Virtual でのみサポートされています。たとえば、ASAv10 の場合、VPN 接続制限は 250 です。SSL 接続の事前認証の制限は、 $3 \times 250 = 750$ になります。

デバイスの場合、事前認証された接続の制限を超えると、新しい SSL 接続が許可されなくなります。ただし、この制限は管理接続には適用されません。デバイスは、事前認証された SSL 接続数がゼロになった後にのみ、新しい SSL 接続を許可します。

サポートされるデバイス

- ASAv5
- ASAv10
- ASAv30
- ASAv50
- ASAv100

Syslog

デバイスが事前認証済み SSL 接続数のレート制限しきい値に達した場合、デバイスは syslog 725025 を生成します。この syslog は、事前認証済み SSL 接続数が多い場合（制限の 90%）、または少ない場合（制限の 70%）に生成されます。syslog は、10 秒ごとに 1 つの syslog にレート制限されます。

カウンタ

レート制限された事前認証済み SSL 接続について、次の 3 つの新しいカウンタがあります。

- **SOCK_PRE_AUTH_COUNT_EXCEEDED** : 1 ずつ増加し、事前認証済み SSL 同時接続数が VPN 制限を超えたことを示します。新しい接続試行は、SOCK_PRE_AUTH_COUNT カウンタが 0 になるまでブロックされます。
- **SOCK_COUNT_RATE_LIMIT** : レート制限を超えた後に ASA がリセットした接続を示します。
- **SOCK_PRE_AUTH_COUNT** : 任意の時点での同時事前認証接続の数。

これらのカウンタの詳細を表示するには、**show counters** コマンドを使用します。

debug コマンド

デバッグ出力は CPU プロセスで高い優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。デバッグコマンドは、Cisco TAC とのトラブルシューティングセッション中にのみ使用することを推奨します。

この機能の以下のデバッグコマンドを使用できます。

- **debug menu ctm 1205** : 機能を無効に、または再度有効にします。
- **debug menu ctm 1206** : この機能の現在のステータスを確認します。

```
vASA# debug menu ctm 1205
Disabling SSL pre-auth connection rate monitoring

vASA# debug menu ctm 1206
SSL PRE-AUTH connection rate monitoring is Disabled
```

永続的 IPSec トンネル フロー

リリース 8.0.4 よりも前の ASA ソフトウェア バージョンを実行するネットワークでは、IPSec トンネルを通過する既存の IPsec LAN-to-LAN またはリモート アクセス TCP トラフィック フローは、トンネルがドロップするとドロップされます。これらのフローは、トンネルが元に戻ると、必要に応じて再作成されます。このポリシーは、リソース管理およびセキュリティの観点から有効です。ただし、このような動作がユーザー（特に PIX から ASA のみの環境に移行しているユーザー）およびレガシー TCP アプリケーション（容易に再起動しない、またはトンネルを頻繁にドロップするゲートウェイが含まれたネットワーク内にある）に問題を引き起こす場合があります（詳細については、CSCsj40681 および CSCsi47630 を参照してください）。

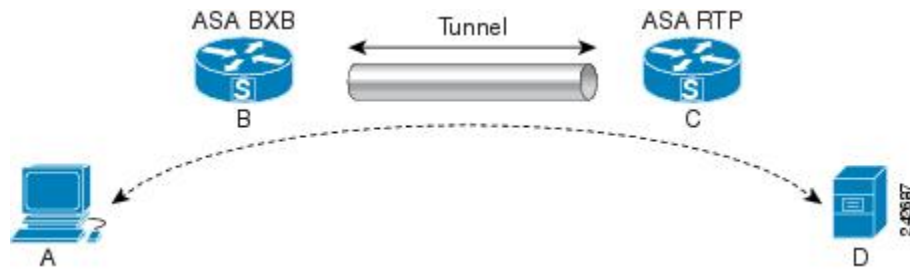
永続的な IPsec トンネル フロー機能で、この問題に対処します。この機能をイネーブルにすると、ASA はステートフル (TCP) トンネルフローを維持して再開します。他のすべてのフローは、トンネルがドロップしたときにドロップされ、新しいトンネルが設定されたときに再確立する必要があります。



-
- (注) この機能は、ネットワーク拡張モードで実行されている IPsec LAN-to-LAN トンネルおよび IPsec リモート アクセス トンネルをサポートします。IPSec または AnyConnect/SSL VPN リモート アクセス トンネルはサポートしていません。
-

次に、永続的 IPSec トンネル フロー機能がどのように動作するか例を示します。

図 5: ネットワーク シナリオ



この例では、BXB および RTP ネットワークが 1 対のセキュリティ アプライアンスによりセキュア LAN-to-LAN トンネルを介して接続しています。BXB ネットワークの PC は RTP ネットワークのサーバーからセキュア トンネルを介して FTP 転送を実行しています。このシナリオでは、PC がサーバーにログインし、転送を開始した後でトンネルが何らかの理由でドロップしたと想定しています。この時点でもデータは流れようとしているため、トンネルは再確立されていますが、FTP 転送が完了しません。ユーザーは、サーバーにログインして転送を終了させ、もう一度やり直す必要があります。ただし、永続的 IPsec トンネルフローがイネーブルになっていれば、タイムアウト間隔以内にトンネルが再作成される限り、セキュリティアプライアンスはこのフローの履歴（状態情報）を維持するため、データは新しいトンネルを通じて正常に流れ続けます。

シナリオ

次の項では、ドロップ後に復旧されたトンネルのデータフローの状態を、永続的 IPsec トンネルフロー機能がディセーブルになっている場合と、この機能がイネーブルになっている場合の順に説明します。どちらの場合も、ネットワークのイラストについては前の図を参照してください。この図の場合：

- ・フロー B-C は、トンネルを定義し、暗号化された ESP データを送送します。
- ・フロー A-D は、FTP 転送の TCP 接続で、フロー B-C で定義されたトンネルを通過します。このフローには、ファイアウォールで TCP/FTP フローを検査するときに使用される状態情報も含まれています。状態情報は重要であり、転送が進行するとファイアウォールによって継続的にアップデートされます。



(注) 各方向の逆フローは簡略化のため省略されています。

ディセーブル化された永続的な IPsec トンネル フロー

LAN-to-LAN トンネルがドロップすると、A-D フローと B-C フローの両方と、それらに属するすべての状態情報が削除されます。その後、トンネルが再確立され、フロー B-C が再作成され、トンネリングされたデータの伝送を再開できるようになります。ただし、TCP/FTP フロー A-D に問題が発生します。この時点までの FTP 転送のフローを説明する状態情報が削除されているため、ステートフルファイアウォールは、インフライト FTP データをブロックし、A-D フローの作成を拒否します。今まで存在していたこのフロー履歴が失われると、ファイアウォール

ルは FTP 転送を迷子の TCP パケットとして処理し、ドロップします。これはデフォルトの動作です。

イネーブル化された永続的な IPsec トンネル フロー

永続的 IPsec トンネル フロー機能がイネーブルの場合、タイムアウト時間内にトンネルが再作成される限り、ASA は A-D フローの状態情報にアクセスできるため、データは正常に流れ続けます。

この機能がイネーブルの場合、ASA はフローを個別に処理します。つまり、B-C フローによって定義されたトンネルがドロップされても、A-D フローは削除されません。ASA はステートフル (TCP) トンネルフローを維持し、再開します。他のフローはすべてドロップされ、新しいトンネルで再確立される必要があります。これは、トンネルフローのセキュリティポリシーを弱めることはありません。ASA はトンネルがダウンしているときに A-D フローに到着するパケットをドロップするからです。

トンネル TCP フローはドロップされないため、クリーンアップは TCP タイムアウトに依存します。ただし、特定のトンネルフローのタイムアウトがディセーブルになっている場合、手動または他の方法 (ピアからの TCP RST など) によってクリアされるまで、そのフローはシステム内で保持されます。

CLI を使用した永続的 IPsec トンネル フローの設定

設定例

永続的な IPsec トンネル フローのトラブルシューティング

show asp table コマンドと **show conn** コマンドは両方とも、永続的 IPsec トンネル フローの問題のトラブルシューティングに役立ちます。

永続的 IPsec トンネル フロー機能はイネーブルになっていますか？

特定のトンネルでこの機能がイネーブルになっているかを確認するには、**show asp table** コマンドを使用してトンネルに関連付けられた VPN コンテキストを調べます。show asp table vpn-context コマンドは、次の例に示すように (読みやすくするために太字を追加)、トンネルがドロップした後にステートフル フローを維持する各コンテキストに「+PRESERVE」フラグを表示します。

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

```
-----
hostname(config)# show asp table vpn-context detail
```

```
VPN CTX  = 0x0005FF54
```



```

Peer IP    = ASA_Private
Pointer    = 0x6DE62DA0
State      = UP
Flags      = DECR+ESP+PRESERVE
SA         = 0x001659BF
SPI        = 0xB326496C
Group      = 0
Pkts       = 0
Bad Pkts   = 0
Bad SPI    = 0
Spoof      = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN CTX    = 0x0005B234

Peer IP    = ASA_Private
Pointer    = 0x6DE635E0
State      = UP
Flags      = ENCR+ESP+PRESERVE
SA         = 0x0017988D
SPI        = 0x9AA50F43
Group      = 0
Pkts       = 0
Bad Pkts   = 0
Bad SPI    = 0
Spoof      = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.

```

孤立したフローの検索

LAN-to-LANまたはネットワーク拡張モードトンネルがドロップし、タイムアウト前に復旧しなかった場合、孤立したトンネルフローが数多く発生することがあります。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。これらのフローを確認するには、**show conn** コマンドを次の例に示すように使用します（強調するため、およびユーザー入力を示すために太字を追加）。

```

asa2(config)# show conn detail
9 in use, 14 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module

```

次の例に、**show conn** コマンドの出力例を示します。**V** フラグで示されているとおり、孤立したフローが存在します。

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOB
```

孤立したフローがあるこのような接続へのレポートを制限するには、次の例で示すように、**show conn state** コマンドに **vpn_orphan** オプションを追加します。

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags UOVB
```

暗号アーカイブを使用したトラブルシューティング

暗号アーカイブについて

暗号の問題はトリアージが困難です。暗号アーカイブは、これらの問題のトラブルシュートに役立ちます。暗号アーカイブには、暗号要求に関する暗号セッション情報、ピア情報、暗号要求を送信したコンポーネント、およびタイムアウトした暗号セッション情報が含まれます。ASA は、セッションのキーおよび初期化ベクトル (IV) を保存しません。SSL および IPsec の場合は、次の情報も表示できます。

- SSL の場合：セッション SSL バージョン、送信元、宛先 IP アドレス、およびポート。
- IPsec の場合：IPsec セキュリティ アソシエーション情報。

リングには、2000 の暗号コマンドエントリを保持できます。ASA は、リングの 1 つに暗号コマンドをプッシュし、暗号要求の完了後に結果を引き出します。暗号アーカイブファイルに、タイムアウトした暗号要求のリングおよびエントリ指数が含まれるようになりました。リングとそのエントリ指数は、問題のある暗号コマンドのトラブルシューティングに役立ちます。

暗号アーカイブには、テキストファイルとバイナリファイルの 2 つの形式があります。**debug menu ctm 103** コマンドを使用して、バイナリファイルを復号できます。

次に例を示します。

```
ASA# debug menu ctm 103 crypto_eng0_arch_4.bin
[Nitrox V Archive Header v1.0 Info]
ASA Image Version: PIX (9.20) #0: Tue Mar 29 16:20:30 GMT 2022
...
SE SSL microcode: CNN5x-MC-SE-SSL-0011
AE microcode: CNN5x-MC-AE-MAIN-0002
Crypto Engine 0
Crash type: SE Ring Timeout
...
Core Soft Resets: 11
...
Timeout Ring (SE): 12
Timeout Entry: 642
```

```

SE TIMEOUT:
Core SE 6 Touts: 2
Core SE 8 Touts: 2
Core SE 12 Touts: 4
Core SE 32 Touts: 2
Core SE 37 Touts: 1
.....
[Timeout Session Info]
Active: TRUE
Sync: FALSE
Callback: TRUE
Saved Callback: FALSE
Commands in progress: 1
Engine : hardware
Device : n5 (Nitrox V)
Session : ssl
Priority: normal
NP VPN context handle : 0x00000000
Flag : 0
vcid : 0
Block size : 2050
async cb ring index: 0
tls offload rsa: FALSE
Session context:
SSL Version : dtls1.2
SSL Context Type : handshake
Encryption Mode : gcm
Auth Algorithm : null
Hash Algorithm : none
Key Size : 32
SSL V : dtls1.2
Source IP : 82.1.2.2
Source Port : 51915
Dest IP : 82.29.155.32
Dest Port : 443

```

上記の例では、強調表示された情報に、タイムアウトリング、クラッシュ時間（タイムアウトエントリ）、および SSL セッション情報が表示されます。

暗号アーカイブでサポートされるデバイス

Nitrox V 暗号アクセラレータを備えた次のデバイスは、暗号アーカイブをサポートします。

- Cisco Firepower 3105、3110、3120、3130、3140
- Cisco Firepower 4112、4115、4125、4145
- Cisco Firepower 9300 SM-40、SM-48、および SM-56

SSL カウンタの使用

SSL カウンタを使用して、SSL トンネル情報とログを表示できます。接続の確立に関するステートマシンの遷移、追加の状態、および詳細に関する情報は、デバッグに役立ちます。

debug ssl state コマンドは、次の情報を提供します。

- 関連付けられた IP、ポート、およびプロトコルを持つリモートデバイスとインターフェイス。
- SSL 接続確立エラーのデバッグ。
- 復号化されたデータのパディング長を確認するためのデバッグ。

SSL カウンタを表示するには、**show counters** コマンドを使用します。バージョン 9.20.1 からデバッグに使用できる SSL カウンタが増えました。たとえば次のようなものがあります。

- CNT_SSL_NP_CP_EVENT_NULL
- CNT_SSL_NP_CP_EVENT_ENQUEUE_ERR
- CNT_SSL_NP_CP_EVENT_RELEASE
- CNT_SSL_NP_SNP_FLOW_HNDSHK_FAIL
- CNT_SSL_NP_HDL_LOCK_RELEASE
- CNT_SSL_NP_VERIFY_PADDING
- CNT_SSL_NP_MAX_PAD_LEN_EXCEEDED
- CNT_SSL_NP_NO_CIPHERS_COMPATIBLE
- CNT_SSL_NP_CIPHER_LIC_NOT_GOOD

スタックした ASP テーブルエントリの削除方法

バージョン 9.19.1 以前では、ASP 暗号化ルールがスタックしている場合、デバイスを再起動する必要があります。バージョン 9.20.1 以降では、**debug menu asp 100 <encrypt_rule_id>** コマンドを使用して、デバイスを再起動せずに ASP テーブルからスタックした暗号化ルールを削除できます。*encrypted_rule_id* を検索するには、**show asp table classify domain encrypt** コマンドを使用します。

ガイドライン

- デバッグ出力は CPU プロセスで高い優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このデバッグコマンドは、Cisco TAC とのトラブルシューティングセッション中にのみ使用することを推奨します。
- ルールがスタックしているかどうかを確認する検証はありません。このコマンドを使用して以前に削除したルールをシステムが削除しようとする、と、デバイスがクラッシュします。
- コマンド ID パラメータは、ASP テーブルの実際の ID と正確に一致する必要があります。

例

次の例では、トラフィックが適切なルール **0x7f039846bbbb** ではなくスタックしたルール **0x7f039846aaaa** にヒットすると、トラフィックがドロップされます。ヒット数からスタックしたルールを特定できます。スタックしたルールのヒット数は9999ですが、適切なルールのヒット数は0です。

1. ASP ルールを表示するには、**show asp table classify domain encrypt** コマンドを使用します。

```
ASAv(config)# show asp table classify domain encrypt
...
out id=0x7f039846aaaa, priority=70, domain=encrypt, deny=false
hits=9999, user_data=0xaaaa, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
out id=0x7f039846bbbb, priority=70, domain=encrypt, deny=false //this is a good rule
hits=0, user_data=0xbbbb, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
...
```

2. ASP テーブルからスタックした暗号化ルールを削除するには、**debug menu asp 100 <encrypt_rule_id>** コマンドを使用します。

```
ASAv(config)# debug menu asp 100 id=0x7f039846aaaa
Encrypt rule 0x7f0398469510 was successfully deleted.
```

3. ASA がスタックした ASP ルールを削除したかどうかを確認するには、**show asp table classify domain encrypt** コマンドを使用します。

```
ASAv(config)# show asp table classify domain encrypt
...
out id=0x7f039846bbbb, priority=70, domain=encrypt, deny=false //now this rule has
hits
hits=10, user_data=0xbbbb, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
```

ASA からの WebVPN 構成のクリア

no webvpn コマンドと **clear configure webvpn** コマンドを使用しても、デフォルトの WebVPN 構成は削除されません。**http_in** カウンタと **http_out** カウンタは、圧縮統計情報を照合するために保持されます。

ASA から WebVPN 構成をクリアするには、次のいずれかを実行します。

- **no compression all** コマンドを使用して、起動後に圧縮統計情報を無効にします。
- **clear compression all** コマンドを使用して、圧縮統計情報カウンタをクリアします。



第 5 章

接続プロファイル、グループ ポリシー、およびユーザー

この章では、VPN 接続プロファイル（以前は「トンネル グループ」と呼ばれていました）、グループ ポリシー、およびユーザーの設定方法について説明します。この章は、次の項で構成されています。

- [接続プロファイル、グループ ポリシー、およびユーザーの概要（117 ページ）](#)
- [接続プロファイル（119 ページ）](#)
- [接続プロファイルの設定（123 ページ）](#)
- [グループ ポリシー（153 ページ）](#)
- [Zone Labs Integrity サーバーの使用（200 ページ）](#)
- [ユーザー属性の設定（207 ページ）](#)
- [VPN フィルタ ACL の設定と調整に関するベストプラクティス（217 ページ）](#)

接続プロファイル、グループポリシー、およびユーザーの概要

グループとユーザーは、バーチャル プライベート ネットワーク（VPN）のセキュリティ管理と ASA の設定における中核的な概念です。グループとユーザーで指定される属性によって、VPN へのユーザー アクセスと VPN の使用方法が決定されます。グループは、ユーザーの集合を1つのエンティティとして扱うものです。ユーザーの属性は、グループポリシーから取得されます。接続プロファイルでは、特定の接続用のグループポリシーを指定します。ユーザーに対して特定のグループ ポリシーを割り当てない場合は、接続のデフォルト グループ ポリシーが適用されます。

要約すると、最初に接続プロファイルを設定して、接続用の値を設定します。次に、グループポリシーを設定します。グループポリシーでは、ユーザーの集合に関する値が設定されます。その後、ユーザーを設定します。ユーザーはグループの値を継承でき、さらに個別のユーザー単位に特定の値を設定することができます。この章では、これらのエンティティを設定する方法と理由について説明します。



(注) 接続プロファイルは、**tunnel-group** コマンドを使用して設定します。この章では、「接続プロファイル」と「トンネル グループ」は頻繁にほとんど同じ意味で使用されています。

接続プロファイルとグループ ポリシーを使用すると、システム管理が簡略化されます。コンフィギュレーション タスクを効率化するために、ASA にはデフォルトの LAN-to-LAN 接続プロファイル (DefaultL2Lgroup)、IKEv2 VPN 用のデフォルトのリモートアクセス接続プロファイル (DefaultRAGroup)、クライアントレス SSL およびセキュアクライアント SSL 接続用のデフォルトの接続プロファイル (DefaultWEBVPNgroup)、およびデフォルトのグループ ポリシー (DfltGrpPolicy) が用意されています。デフォルトの接続プロファイルとグループ ポリシーでは、多くのユーザーに共通すると考えられる設定が提供されます。ユーザーを追加するときに、グループ ポリシーからパラメータを「継承」するように指定できます。これにより、数多くのユーザーに対して迅速に VPN アクセスを設定できます。

すべての VPN ユーザーに同一の権限を許可する場合は、特定の接続プロファイルやグループ ポリシーを設定する必要はありませんが、VPN がそのように使用されることはほとんどありません。たとえば、経理グループ、カスタマー サポート グループ、および MIS (経営情報システム) グループが、プライベートネットワークのそれぞれ異なる部分にアクセスできるようにする場合が考えられます。また、MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合があります。接続プロファイルとグループ ポリシーにより、このような柔軟な設定を安全に実行することができます。



(注) ASA には、オブジェクトグループという概念もあります。これは、ネットワークリストのスーパーセットです。オブジェクトグループを使用すると、ポートやネットワークに対する VPN アクセスを定義することができます。オブジェクトグループは、グループ ポリシーや接続プロファイルよりも、ACL と関連があります。オブジェクトグループの使用の詳細については、一般的操作用コンフィギュレーション ガイドの第 20 章「Objects」を参照してください。

セキュリティアプライアンスでは、さまざまなソースから属性値を適用できます。次の階層に従って、属性値を適用します。

1. Dynamic Access Policy (DAP) レコード
2. ユーザー名
3. グループ ポリシー
4. 接続プロファイル用のグループ ポリシー
5. デフォルトのグループ ポリシー

そのため、属性の DAP 値は、ユーザー、グループ ポリシー、または接続プロファイル用に設定された値よりもプライオリティが高くなっています。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA はその値を適用して実行します。たとえば、DAP webvpn コンフィギュレーション モードで HTTP プロキシをディセーブルにすると、ASA はそれ以上値を検索しません。代わりに、`http-proxy` コマンドの `no` 値を使用すると、属性は DAP レコードには存在しないため、セキュリティ アプライアンスは適用する値を見つけるために、ユーザー名および必要に応じてグローバル ポリシーの AAA 属性に移動して検索します。ASA クライアントレス SSL VPN コンフィギュレーションは、それぞれ 1 つの `http-proxy` コマンドと 1 つの `https-proxy` コマンドのみサポートしています。ASDM を使用して DAP を設定することをお勧めします。

接続プロファイル

接続プロファイルは、トンネル接続ポリシーを決定するレコードのセットで構成されます。これらのレコードは、トンネルユーザーが認証先サーバー、および接続情報の送信先となるアカウントティングサーバー（存在する場合）を特定します。また、これらのレコードには、接続用のデフォルト グループ ポリシーも指定され、さらにプロトコル固有の接続パラメータも含まれています。接続プロファイルには、トンネル自体の作成に関連する少数の属性が含まれます。接続プロファイルには、ユーザー関連の属性を定義するグループポリシーへのポインタも含まれます。

ASA には、LAN-to-LAN 接続用の `DefaultL2Lgroup`、IPSEC リモートアクセス接続用の `DefaultRAGroup`、および SSL VPN（ブラウザベースおよびセキュアクライアント ベース）接続用の `DefaultWEBVPNGroup` というデフォルト接続プロファイルがあります。これらのデフォルト接続プロファイルは変更できますが、削除はできません。また、環境に固有の接続プロファイルを 1 つ以上作成することもできます。接続プロファイルは、ASA のローカルな設定であり、外部サーバーでは設定できません。



- (注) 一部のプロファイル（フェーズ 1 の IKEv1 など）は、エンドポイントがリモート アクセスまたは LAN-to-LAN かどうかを判別できないことがあります。トンネル グループを判別できない場合、デフォルトで

```
tunnel-group-map default-group <tunnel-group-name>
```

に設定されます（デフォルト値は `DefaultRAGroup` です）。

接続プロファイルの一般接続パラメータ

一般パラメータは、すべての VPN 接続に共通です。一般パラメータには、次のものがあります。

- 接続プロファイル名：接続プロファイル名は、接続プロファイルを追加または編集するときに指定します。次の注意事項があります。
 - 認証に事前共有キーを使用するクライアントの場合、接続プロファイル名はクライアントが ASA に渡すグループ名と同じです。

- 認証に証明書を使用するクライアントはこの名前を証明書の一部として渡し、ASAが証明書からこの名前を抽出します。
- 接続タイプ：接続タイプには、IKEv1 リモート アクセス、IPsec LAN-to-LAN、および AnyConnect (SSL/IKEv2) が含まれます。接続プロファイルでは、1 つの接続タイプだけ指定できます。
- 認証、認可、アカウンティング サーバー：これらのパラメータでは、ASA が次の目的で使用するサーバーのグループまたはリストを指定します。
 - ユーザーの認証
 - ユーザーがアクセスを認可されたサービスに関する情報の取得
 - アカウンティング レコードの保存

サーバー グループは、1 つ以上のサーバーで構成されます。

- 接続用のデフォルトグループポリシー：グループポリシーは、ユーザー関連の属性のセットです。デフォルトグループポリシーは、ASA がトンネルユーザーを認証または認可する際にデフォルトで使用する属性を含んだグループポリシーです。
- クライアントアドレスの割り当て方式：この方式には、ASA がクライアントに割り当てる 1 つ以上の DHCP サーバーまたはアドレス プールの値が含まれます。
- パスワード管理：このパラメータを使用すると、現在のパスワードが指定日数（デフォルトは 14 日）で期限切れになることをユーザーに警告して、パスワードを変更する機会をユーザーに提供できます。
- グループ除去およびレルム除去：これらのパラメータにより、ASA が受信するユーザー名を処理する方法が決まります。これらは、`user@realm` の形式で受信するユーザー名にだけ適用されます。

領域は @ デリミタ付きでユーザー名に付加される管理ドメインです (`user@abc`)。レルムを除去する場合、ASA はユーザー名およびグループ（ある場合）を認証に使用します。グループを除去すると、ASA は認証にユーザー名およびレルム（ある場合）を使用します。

レルム修飾子を除去するには `strip-realm` コマンドを入力し、認証中にユーザー名からグループ修飾子を削除するには `strip-group` コマンドを入力します。両方の修飾子を削除すると、認証は `username` だけに基づいて行われます。それ以外の場合、認証は `username@realm` 文字列全体または `username<delimiter> group` 文字列に基づいて行われます。サーバーでデリミタを解析できない場合は、`strip-realm` を指定する必要があります。

さらに、L2TP/IPsec クライアントの場合に `strip-group` コマンドを指定すると、ASA は VPN クライアントが提示したユーザー名からグループ名を取得してユーザー接続の接続プロファイル（トンネルグループ）を選択します。

- 認可の要求：このパラメータを使用すると、ユーザー接続の前に認可を要求したり、またはその要求を取り下げたりできます。

- 認可 DN 属性：このパラメータは、認可を実行するときに使用する認定者名属性を指定します。

IPSec トンネルグループ接続パラメータ

IPSec パラメータには、次のものがあります。

- クライアント認証方式：事前共有キー、証明書、または両方。
 - 事前共有キーに基づいた IKE 接続の場合、接続ポリシーに関連付けられた英数字のキー自体です（最大 128 文字）。
 - ピア ID 確認の要求：このパラメータでは、ピアの証明書を使用してピア ID の確認を要求するかどうかを指定します。
 - 認証方式に証明書または両方を指定する場合、エンドユーザーは認証のために有効な証明書を指定する必要があります。

- 拡張ハイブリッド認証方式：XAUTH およびハイブリッド XAUTH。

isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザー認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。

- ISAKMP (IKE) キープアライブの設定：この機能により、ASA はリモートピアの継続的な存在をモニターし、自分自身の存在をピアに報告できます。ピアが応答なくなると、ASA は接続を削除します。IKE キープアライブをイネーブルにすると、IKE ピアが接続を失ったときに接続がハングしません。

IKE キープアライブにはさまざまな形式があります。この機能が動作するには、ASA とリモートピアが共通の形式をサポートしている必要があります。この機能は、次のピアに対して動作します。

- Cisco AnyConnect VPN Client
- Cisco IOS ソフトウェア
- Cisco Secure PIX Firewall

シスコ以外の VPN クライアントは IKE キープアライブをサポートしません。

IKE キープアライブをサポートするピアとサポートしないピアが混在するグループを設定する場合は、グループ全体に対して IKE キープアライブをイネーブルにします。この機能をサポートしないピアに影響はありません。

IKE キープアライブをディセーブルにすると、応答しないピアとの接続はタイムアウトになるまでアクティブのままになるため、アイドルタイムアウトを短くすることを推奨します。アイドルタイムアウトを変更するには、[グループポリシーの設定 \(156 ページ\)](#) を参照してください。



(注) ISDN 回線経由で接続するクライアントがグループに含まれる場合は、接続コストを削減するために IKE キープアライブをディセーブルにしてください。通常、ISDN 接続はアイドルになると切断されますが、IKE キープアライブのメカニズムによって接続がアイドル状態にならないため、切断されなくなります。

IKE キープアライブをディセーブルにすると、クライアントは IKE キーと IPSec キーのどちらかの期限が満了した場合にだけ切断されます。IKE キープアライブがイネーブルになっている場合とは異なり、障害が発生したトラフィックは Peer Timeout Profile 値を持つトンネルから切断されません。

IKE メインモードを使用する LAN-to-LAN コンフィギュレーションの場合は、2つのピアの IKE キープアライブのコンフィギュレーションが同じであることを確認してください。両方のピアで IKE キープアライブがイネーブルになっているか、または両方のピアで IKE キープアライブがディセーブルになっている必要があります。

- デジタル証明書を使用して認証を設定する場合、証明書チェーン全体を送信する（ID 証明書と発行するすべての証明書をピアに送信する）か、証明書だけを発行する（ルート証明書とすべての下位 CA 証明書を含む）かを指定できます。
- Windows クライアント ソフトウェアの古いバージョンを使用しているユーザーに、クライアントをアップデートする必要があることを通知し、アップデートされたクライアントバージョンをユーザーが取得するためのメカニズムを提供できます。すべての接続プロファイルまたは特定の接続プロファイルに対して、`client-update` を設定および変更できます。
- デジタル証明書を使用して認証を設定する場合は、IKE ピアに送信する証明書を識別するトラストポイントの名前を指定できます。

接続プロファイルの SSL VPN セッション接続パラメータ

次の表は、SSL VPN（セキュアクライアントおよびクライアントレス）接続に固有の接続プロファイル属性のリストです。これらの属性に加えて、すべての VPN 接続に共通の一般接続プロファイルの属性を設定します。



(注) 以前のリリースでは、「接続プロファイル」が「トンネルグループ」と呼ばれていました。接続プロファイルは、`tunnel-group` コマンドを使用して設定します。この章では、この2つの用語が同義的によく使用されています。

表 7: SSL VPN 用接続プロファイルの属性

	機能
authentication	認証方式、AAA または証明書を設定します。
customization	適用するすでに定義済みのカスタマイゼーションの名前を指定します。カスタマイゼーションによって、ログイン時にユーザーに表示されるウィンドウの外観が決まります。カスタマイゼーションパラメータは、クライアントレス SSL VPN の設定の一部として設定します。
nbns-server	CIFS 名前解決に使用する NetBIOS ネーム サービス サーバー (nbns-server) の名前を指定します。
group-alias	サーバーから接続プロファイルを参照できる1つ以上の代替名を指定します。ログイン時に、ユーザーはドロップダウン メニューからグループ名を選択します。
group-url	1 つ以上のグループ URL を指定します。この属性を設定する場合、指定した URL にアクセスするユーザーは、ログイン時にグループを選択する必要はありません。 セキュアクライアント 接続にグループ URL を使用するロードバランシング展開では、クラスタ内の各 ASA ノードで、ノードのロードバランシングのパブリックアドレスのグループ URL と同様に、仮想クラスタアドレスのグループ URL を設定する必要があります。
dns-group	DNS サーバー名、ドメイン名、ネーム サーバー、リトライ回数、および接続ファイルで使用する DNS サーバーのタイムアウト値を指定する DNS サーバー グループを指定します。
hic-fail-group-policy	Cisco Secure Desktop Manager を使用して、グループベース ポリシー属性を「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合は、VPN 機能ポリシーを指定します。
override-svc-download	AnyConnect VPN クライアントをリモート ユーザーにダウンロードするために、設定されているグループ ポリシー属性またはユーザー名属性のダウンロードが上書きされます。
radius-reject-message	認証が拒否されたときに、ログイン画面に RADIUS 拒否メッセージを表示します。

接続プロファイルの設定

ここでは、シングル コンテキスト モードまたはマルチ コンテキスト モードの両方での接続プロファイルの内容および設定について説明します。



- (注) マルチコンテキストモードは IKEv1 および IKEv2 サイトツーサイトにのみ適用され、IKEv1 IPSec のセキュアクライアント、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、または cTCP には適用されません。

デフォルトの接続プロファイルを変更し、3つのトンネルグループタイプのいずれかで新しい接続プロファイルを設定できます。接続プロファイル内で明示的に設定しない属性に対しては、その値がデフォルトの接続プロファイルから取得されます。デフォルトの接続プロファイルタイプはリモートアクセスです。その後のパラメータは、選択したトンネルタイプによって異なります。デフォルト接続プロファイルも含めて、すべての接続プロファイルの現在のコンフィギュレーションとデフォルトのコンフィギュレーションを確認するには、**show running-config all tunnel-group** コマンドを入力します。

接続プロファイルの最大数

1つのASAがサポートできる接続プロファイル（トンネルグループ）の最大数は、プラットフォームの同時VPNセッションの最大数+5の関数です。制限を超えるトンネルグループを追加しようとすると、「ERROR: The limit of 30 configured tunnel groups has been reached」メッセージが表示されます。

デフォルトの IPsec リモート アクセス接続プロファイルの設定

デフォルトのリモート アクセス接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
no address-pool
no ipv6-address-pool
authentication-server-group LOCAL
accounting-server-group RADIUS
default-group-policy DfltGrpPolicy
no dhcp-server
no strip-realm
no password-management
no override-account-disable
no strip-group
no authorization-required
authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
hic-fail-group-policy DfltGrpPolicy
customization DfltCustomization
authentication aaa
no override-svc-download
no radius-reject-message
dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
no pre-shared-key
peer-id-validate req
no chain
no trust-point
```

```

isakmp keepalive threshold 1500 retry 2
no radius-sdi-xauth
isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
no authentication pap
authentication chap
authentication ms-chap-v1
no authentication ms-chap-v2
no authentication eap-proxy

tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
no address-pool
no ipv6-address-pool
authentication-server-group LOCAL
accounting-server-group RADIUS
default-group-policy DfltGrpPolicy
no dhcp-server
no strip-realm
no password-management
no strip-group
no authorization-required
authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
hic-fail-group-policy DfltGrpPolicy
customization DfltCustomization
authentication aaa
no override-svc-download
no radius-reject-message
dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
no pre-shared-key
peer-id-validate req
no chain
no trust-point
isakmp keepalive threshold 1500 retry 2
no radius-sdi-xauth
isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
no authentication pap
authentication chap
authentication ms-chap-v1
no authentication ms-chap-v2
no authentication eap-proxy

```

IPsec トンネルグループの一般属性

一般属性は、複数のトンネルグループタイプに共通です。IPsec リモートアクセス トンネルとクライアントレス SSL VPN トンネルでは、同じ一般属性の大部分を共有しています。IPsec LAN-to-LAN トンネルは、サブセットを使用します。すべてのコマンドの詳細については、『*Cisco Secure Firewall ASA Series Command Reference*』を参照してください。ここでは、リモートアクセス接続プロファイルおよび LAN-to-LAN 接続プロファイルを設定する方法について順に説明します。

リモート アクセス接続プロファイルの設定

次のリモートクライアントと中央サイトのASAの間に接続を設定する場合は、リモートアクセス接続プロファイルを使用します。

- Secure Client (SSL または IPsec/IKEv2 と接続)
- クライアントレス SSL VPN (SSL とのブラウザベースの接続)
- Cisco ASA 5500 Easy VPN ハードウェア クライアント (IPsec/IKEv1 と接続)

また、DfltGrpPolicy という名前のデフォルト グループ ポリシーも提供します。

リモート アクセス接続プロファイルを設定するには、最初にトンネル グループ一般属性を設定し、次にリモート アクセス属性を設定します。次の項を参照してください。

- [リモートアクセス接続プロファイルの名前とタイプの指定 \(126 ページ\)](#) を使用して無効にすることができます。
- [リモートアクセス接続プロファイルの一般属性の設定 \(127 ページ\)](#) を使用して無効にすることができます。
- [二重認証の設定 \(131 ページ\)](#)
- [リモートアクセス接続プロファイルの IPSec IKEv1 属性の設定 \(133 ページ\)](#) を使用して無効にすることができます。
- [IPSec リモートアクセス接続プロファイルの PPP 属性の設定 \(136 ページ\)](#)

リモート アクセス接続プロファイルの名前とタイプの指定

手順

名前とタイプを指定して **tunnel-group** コマンドを入力することで、接続プロファイルを作成します。

リモート アクセス トンネルの場合、タイプは **remote-access** です。

tunnel-group tunnel_group_name type remote-access

例 :

たとえば、TunnelGroup1 という名前のリモート アクセス接続プロファイルを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

リモート アクセス接続プロファイルの一般属性の設定

接続プロファイルの一般属性を設定または変更するには、次の手順でパラメータを指定します。

手順

- ステップ 1** 一般属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで **tunnel-group general-attributes** タスクを入力します。これで、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開始されます。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

- ステップ 2** 認証サーバー グループがある場合、使用するグループの名前を指定します。指定したサーバーグループに障害が発生したときにローカルデータベースを認証に使用する場合は、キーワード **LOCAL** を追加します。

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

認証サーバー グループの名前は、最大 16 文字です。

オプションで、グループ名の後ろにインターフェイス名を指定することにより、インターフェイス固有の認証を設定することもできます。トンネルの終了場所を指定するインターフェイス名は、丸カッコで囲む必要があります。次のコマンドでは、認証にサーバー **servergroup1** を使用する **test** という名前のインターフェイスのインターフェイス固有の認証が設定されます。

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

- ステップ 3** 使用する認可サーバー グループの名前を指定します（存在する場合）。この値を設定する場合、ユーザーは接続する認可データベースに存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

認可サーバー グループの名前は、最大 16 文字です。たとえば、次のコマンドは、認可サーバーグループ **FinGroup** を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-groupFinGroup
hostname(config-tunnel-general)#
```

- ステップ 4** アカウンティングサーバー グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

アカウントिंग サーバー グループの名前は、最大 16 文字です。たとえば、次のコマンドは、アカウントングサーバー グループ **comptroller** を使用することを指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

ステップ5 デフォルト グループ ポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

グループ ポリシーの名前は、最大 64 文字です。次の例では、デフォルトグループ ポリシーの名前として **DfltGrpPolicy** を設定しています。

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

ステップ6 DHCP サーバー（最大 10 サーバー）の名前または IP アドレス、および DHCP アドレス プール（最大 6 プール）の名前を指定します。デフォルトでは、DHCP サーバーとアドレス プールは使用されません。**dhcp-server** コマンドにより、VPN クライアントの IP アドレスを取得しようとするときに、指定の DHCP サーバーに追加オプションを送信するように ASA を設定できるようになります。詳細については、『Cisco Secure Firewall ASA Series Command Reference』ガイドの **dhcp-server** コマンドを参照してください。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

（注）

インターフェイス名を指定する場合は、丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して設定します。

ステップ7 ネットワーク アドミッション コントロールを使用している場合は、ネットワーク アドミッション コントロール ポスチャ 検証で使用する認証サーバーのグループを特定するために、NAC 認証サーバー グループの名前を指定します。NAC をサポートするように、少なくとも 1 つのアクセス コントロール サーバーを設定します。ACS グループの名前を指定するには、**aaa-server** コマンドを使用します。次に、その同じ名前をサーバー グループに使用して、**nac-authentication-server-group** コマンドを使用します。

次に、NAC ポスチャ 検証に使用される認証サーバー グループとして **acs-group1** を識別する例を示します。

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1  
hostname(config-group-policy)
```

次に、デフォルトのリモート アクセス グループから認証サーバー グループを継承する例を示します。

```
hostname(config-group-policy)# no nac-authentication-server-group  
hostname(config-group-policy)
```

(注)

NAC を使用するには、リモート ホスト上に Cisco Trust Agent が存在する必要があります。

ステップ 8 ユーザー名を AAA サーバーに渡す前に、ユーザー名からグループまたは領域を除去するかどうかを指定します。デフォルトでは、グループ名もレルムも除去されません。

```
hostname(config-tunnel-general)# strip-group  
hostname(config-tunnel-general)# strip-realm  
hostname(config-tunnel-general)#
```

レルムとは管理ドメインのことです。レルムを除去する場合、ASA はユーザー名およびグループ（ある場合）認証を使用します。グループを除去すると、ASA は認証にユーザー名およびレルム（ある場合）を使用します。レルム修飾子を削除するには **strip-realm** コマンドを入力し、認証中にユーザー名からグループ修飾子を削除するには **strip-group** コマンドを使用します。両方の修飾子を削除すると、認証は *username* だけに基づいて行われます。それ以外の場合、認証は *username@realm* 文字列全体または *username<delimiter> group* 文字列に基づいて行われます。サーバーでデリミタを解析できない場合は、**strip-realm** を指定する必要があります。

ステップ 9 サーバーが RADIUS、RADIUS with NT、または LDAP サーバーの場合、オプションで、パスワード管理をイネーブルにできます。

(注)

認証に LDAP ディレクトリ サーバーを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

Sun : Sun ディレクトリ サーバーにアクセスするために ASA に設定されている DN が、サーバーのデフォルトパスワードポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザーを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。

Microsoft : Microsoft Active Directory でパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

この機能はデフォルトでディセーブルになっており、現在のパスワードの有効期限が近づくとユーザーに警告を表示します。デフォルトでは、期限切れの 14 日前に警告が開始されます。

```
hostname(config-tunnel-general)# password-management  
hostname(config-tunnel-general)#
```

サーバーが LDAP サーバーの場合、有効期限が近いことに関する警告が開始されるまでの日数 (0 ~ 180) を指定できます。

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

(注)

トンネルグループ一般属性コンフィギュレーション モードで入力した **password-management** コマンドによって、トンネルグループ **ipsec** 属性モードで事前に入力された非推奨の **radius-with-expiry** コマンドが置き換えられます。

password-management コマンドを設定すると、リモートユーザーがログインするときに、ASA は、ユーザーの現在のパスワードの有効期限が近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザーがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザーはそのパスワードを使用してログインし続けることができます。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

これによってパスワードが期限切れになるまでの日数が変更されるわけではなく、ASA がパスワードが期限切れになる何日前にユーザーへの警告を開始するかが変更されるという点に注意してください。

password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。

このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。ASA は、ユーザーに対して失効が迫っていることを通知しませんが、失効後にユーザーはパスワードを変更できます。

詳細については、[パスワード管理用の Microsoft Active Directory の設定 \(148 ページ\)](#) を参照してください。

ASA Version 7.1 以降では、LDAP または MS-CHAPv2 をサポートする RADIUS 接続で認証を行うときに、AnyConnect VPN Client 接続、Cisco IPSec VPN Client 接続、SSL VPN 完全トンネリングクライアント接続、およびクライアントレス接続に対するパスワード管理が一般的にサポートされています。AD (Windows パスワード) または NT 4.0 ドメインに対するこれらの接続タイプのいずれでも、パスワード管理はサポートされていません。

MS-CHAP をサポートしている一部の RADIUS サーバーは、現在 MS-CHAPv2 をサポートしていません。**password-management** コマンドを使用するには、MS-CHAPv2 が必要なため、ベンダーに確認してください。

(注)

RADIUS サーバー (Cisco ACS など) は、認証要求を別の認証サーバーにプロキシする場合があります。ただし、ASA からは RADIUS サーバーとのみ通信しているように見えます。

LDAP でパスワードを変更するには、市販の LDAP サーバーごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバーに対してのみ、独自のパスワード管理ロジックを実装しています。ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

ステップ 10

ステップ 11 証明書から認可クエリー用の名前を得るために使用する 1 つまたは複数の属性を指定します。この属性により、サブジェクト DN フィールドのどの部分を認可用のユーザー名として使用するかが指定されます。

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute  
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN 属性を認可用のユーザー名として使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-dn-attributes CN  
hostname(config-tunnel-general)#
```

authorization-dn-attributes は、**C** (国)、**CN** (通常名)、**DNQ** (DN 修飾子)、**EA** (電子メールアドレス)、**GENQ** (世代修飾子)、**GN** (名)、**I** (イニシャル)、**L** (地名)、**N** (名前)、**O** (組織)、**OU** (組織ユニット)、**SER** (シリアル番号)、**SN** (姓)、**SP** (州または都道府県)、**T** (役職)、**UID** (ユーザー ID)、および **UPN** (ユーザープリンシパルネーム) があります。

ステップ 12 ユーザーに接続を許可する前に、そのユーザーが正常に認可されている必要があるかどうかを指定します。デフォルトでは認可は要求されません。

```
hostname(config-tunnel-general)# authorization-required  
hostname(config-tunnel-general)#
```

二重認証の設定

二重認証は、ユーザーがログイン画面に追加の認証クレデンシャル (2 つ目のユーザー名とパスワードなど) を入力するよう要求するオプションの機能です。二重認証を設定するには、次のコマンドを指定します。

手順

ステップ 1 セカンダリ認証サーバー グループを指定します。このコマンドはセカンダリ AAA サーバーとして使用する AAA サーバー グループを指定します。

(注)

このコマンドは、AnyConnect VPN 接続にだけ適用されます。

セカンダリのサーバー グループでは SDI サーバー グループを指定できません。デフォルトでは、セカンダリ認証は必要ありません。

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
```

```
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

none キーワードを指定すると、セカンダリ認証は要求されません。*groupname* 値は AAA サーバー グループ名を示します。ローカルは内部サーバー データベースを使用することを示し、*groupname* 値と併用すると、LOCAL はフォールバックを示します。

たとえば、プライマリ認証サーバー グループを *sdi_group* に、セカンダリ認証サーバー グループを *ldap_server* に設定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

(注)

use-primary-name キーワードを使用する場合、ログイン ダイアログは 1 つのユーザー名だけ要求します。また、ユーザー名をデジタル証明書から抽出する場合、プライマリ ユーザー名だけが認証に使用されます。

ステップ 2 セカンダリ ユーザー名を証明書から取得する場合は、**secondary-username-from-certificate** を入力します。

```
hostname(config-tunnel-general)# secondary-username-from-certificate C | CN | ... |
use-script
```

セカンダリ ユーザー名として使用するために証明書から抽出する DN フィールドの値は、プライマリの **username-from-certificate** コマンドと同じです。または、**use-script** キーワードを指定して、ASDM によって生成されたスクリプト ファイルを使用するよう ASA に指示できます。

たとえば、プライマリ ユーザー名フィールドとして通常名を、セカンダリ ユーザー名フィールドとして組織ユニットを指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# username-from-certificate cn
hostname(config-tunnel-general)# secondary-username-from-certificate ou
```

ステップ 3 認証で使用するためにクライアント証明書からセカンダリ ユーザー名を抽出できるようにするには、トンネルグループ *webvpn* 属性モードで **secondary-pre-fill-username** コマンドを使用します。このコマンドをクライアントレス接続または SSL VPN クライアント (AnyConnect) 接続に適用するかどうか、抽出されたユーザー名をエンドユーザーに非表示にするかどうかを指定するキーワードを使用します。この機能はデフォルトで無効に設定されています。クライアントレス オプションと SSL クライアント オプションは同時に使用できますが、それぞれ別個のコマンドで設定する必要があります。

```
hostname(config-tunnel-general)# secondary-pre-fill-username-from-certificate
{clientless | client} [hide]
```

たとえば、接続のプライマリとセカンダリの両方の認証に **pre-fill-username** を使用するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# pre-fill-username client
hostname(config-tunnel-general)# secondary-pre-fill-username client
```

ステップ 4 接続に適用する認可属性を取得するために使用する認証サーバーを指定します。デフォルトの選択は、プライマリ認証サーバーです。このコマンドは二重認証でのみ意味を持ちます。

```
hostname(config-tunnel-general)# authentication-attr-from-server {primary | secondary}
```

たとえば、セカンダリ認証サーバーを指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authentication-attr-from-server secondary
```

ステップ 5 セッションと関連付ける認証ユーザー名（プライマリまたはセカンダリ）を指定します。デフォルト値はプライマリです。二重認証をイネーブルにすると、2つの別のユーザー名でセッションを認証できます。管理者はセッションのユーザー名として認証されたユーザー名のいずれかを指定する必要があります。セッションのユーザー名は、アカウントिंग、セッションデータベース、syslog、デバッグ出力に提供されるユーザー名です。

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

たとえば、セッションと関連付ける認証ユーザー名をセカンダリ認証サーバーから取得するよう指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

リモート アクセス接続プロファイルの IPSec IKEv1 属性の設定

リモートアクセス接続プロファイルの IPSec IKEv1 属性を設定するには、次の手順を実行します。次の説明は、リモートアクセス接続プロファイルをすでに作成していることを前提としています。リモートアクセス接続プロファイルには、LAN-to-LAN 接続プロファイルよりも多くの属性があります。

手順

ステップ 1 リモートアクセス トンネル グループの IPSec 属性を指定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のコマンドを入力してトンネルグループ ipsec 属性モードを開始します。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
```

```
hostname(config-tunnel-ipsec)#
```

このコマンドにより、トンネルグループ **ipsec** 属性コンフィギュレーションモードが開始されます。このモードでは、シングルコンテキストモードまたはマルチコンテキストモードでリモート アクセス トンネルグループの IPsec 属性を設定します。

たとえば、次のコマンドは、TG1 という名前の接続プロファイルに関するトンネルグループ **ipsec** 属性モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ **ipsec** 属性モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

ステップ 2 事前共有キーに基づく IKEv1 接続をサポートするために、事前共有キーを指定します。たとえば、次のコマンドは、IPsec IKEv1 リモート アクセス接続プロファイルの IKEv1 接続をサポートするために、事前共有キー **xyzx** を指定しています。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

ステップ 3 ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できるオプション値は、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。

たとえば、次のコマンドは **peer-id** 検証が必要なことを指定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

ステップ 4 証明書チェーンを送信できるかどうかを指定します。次のコマンドは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべての IPsec トンネルグループ タイプに適用されます。

ステップ 5 IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

次のコマンドは、IKE ピアに送信する証明書の名前として **mytrustpoint** を指定しています。


```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

ステップ 6 ISAKMP キープアライブのしきい値と許可されるリトライ回数を指定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

threshold パラメータでは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数（10 ～ 3600）で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です（2 ～ 10 秒）。IKE キープアライブは、デフォルトでイネーブルです。ISAKMP キープアライブをディセーブルにするには、**isakmp keepalive disable** と入力します。

たとえば、次のコマンドは、IKE キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、リモートアクセスの場合は 300、LAN-to-LAN の場合は 10 です。また、**retry** パラメータのデフォルト値は 2 です。

中央サイト（セキュア ゲートウェイ）で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7 ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザー認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する場合がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合せてハイブリッド認証と呼ばれます。

- ASA は、標準の公開キー技術を使用して、リモート VPN ユーザーに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
- 次に、XAUTH 交換がリモート VPN ユーザーを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注）

認証タイプをハイブリッドに設定するには、事前に認証サーバーを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

isakmp ikev1-user-authentication コマンドとオプションの **interface** パラメータを使用して、特定のインターフェイスを指定できます。**interface** パラメータを省略すると、このコマンドはすべてのインターフェイスに適用され、インターフェイスごとにコマンドが指定され

ていない場合のバックアップとして機能します。接続プロファイルに 2 つの **isakmp ikev1-user-authentication** コマンドを指定していて、1 つは **interface** パラメータを使用し、もう 1 つは使用しない場合、インターフェイスを指定するコマンドはその特定のインターフェイスを優先します。

たとえば、次のコマンドは、**example-group** と呼ばれる接続プロファイルの内部インターフェイスでハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

IPSec リモート アクセス接続プロファイルの PPP 属性の設定

リモートアクセス接続プロファイルのポイントツーポイントプロトコル属性を設定するには、次の手順を実行します。PPP 属性は、IPSec リモート アクセスの接続プロファイルにだけ適用されます。次の説明は、IPSec リモート アクセス接続プロファイルをすでに作成していることを前提としています。

手順

ステップ 1 トンネルグループ **ppp** 属性コンフィギュレーションモードに入ります。このモードで、次のコマンドを入力して、リモートアクセス トンネルグループ PPP 属性を設定します。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

たとえば、次のコマンドは、TG1 という名前の接続プロファイルに関係するトンネルグループ **ppp** 属性モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ **ppp** 属性モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

ステップ 2 PPP 接続に対する固有のプロトコルを使用する認証をイネーブルにするかどうかを指定します。プロトコルの値は次のいずれかになります。

- **pap** : PPP 接続で Password Authentication Protocol (パスワード認証プロトコル) の使用をイネーブルにします。

- **chap** : PPP 接続で Challenge Handshake Authentication (チャレンジハンドシェイク認証プロトコル) の使用をイネーブルにします。
- **ms-chap-v1** または **ms-chap-v2** : PPP 接続で Microsoft Challenge Handshake Authentication Protocol (Microsoft チャレンジハンドシェイク認証プロトコル) のバージョン 1 またはバージョン 2 の使用をイネーブルにします。
- **eap** : PPP 接続で Extensible Authentication Protocol (拡張認証プロトコル) の使用をイネーブルにします。

CHAP と MSCHAPv1 は、デフォルトでイネーブルになっています。

このコマンドの構文は次のとおりです。

```
hostname(config-tunnel-ppp) # authentication protocol
hostname(config-tunnel-ppp) #
```

特定のプロトコルの認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-tunnel-ppp) # no authentication protocol
hostname(config-tunnel-ppp) #
```

たとえば、次のコマンドは PPP 接続で PAP プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp) # authentication pap
hostname(config-tunnel-ppp) #
```

次のコマンドは、PPP 接続で MS-CHAP バージョン 2 プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp) # authentication ms-chap-v2
hostname(config-tunnel-ppp) #
```

次のコマンドは、PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。

```
hostname(config-tunnel-ppp) # authentication pap
hostname(config-tunnel-ppp) #
```

次のコマンドは、PPP 接続で MS-CHAP バージョン 1 プロトコルの使用をディセーブルにします。

```
hostname(config-tunnel-ppp) # no authentication ms-chap-v1
hostname(config-tunnel-ppp) #
```

LAN-to-LAN 接続プロファイルの設定

IPSec LAN-to-LAN VPN 接続プロファイルは、LAN-to-LAN IPSec クライアント接続にだけ適用されます。設定するパラメータの多くはIPSec リモートアクセスの接続プロファイルのものと同じですが、LAN-to-LAN トンネルの方がパラメータの数は少なくなります。ここでは、LAN-to-LAN 接続プロファイルを設定する方法について説明します。

- [LAN-to-LAN 接続プロファイルの名前とタイプの指定 \(138 ページ\)](#)
- [LAN-to-LAN 接続プロファイルの一般属性の設定 \(138 ページ\)](#)
- [LAN-to-LAN IPSec IKEv1 属性の設定 \(139 ページ\)](#)

デフォルトの LAN-to-LAN 接続プロファイルのコンフィギュレーション

デフォルトの LAN-to-LAN 接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

LAN-to-LAN 接続プロファイルのパラメータはリモートアクセス接続プロファイルのパラメータより少なく、そのほとんどはどちらのグループでも同じです。実際に接続を設定する場合の利便性を考え、ここではこのグループのパラメータを個別に説明します。明示的に設定しないパラメータはすべて、デフォルトの接続プロファイルからその値を継承します。

LAN-to-LAN 接続プロファイルの名前とタイプの指定

接続プロファイルの名前とタイプを指定するには、次のように **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

LAN-to-LAN トンネルの場合、タイプは **ipsec-l2l** になります。たとえば、**docs** という名前の LAN-to-LAN 接続プロファイルを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

LAN-to-LAN 接続プロファイルの一般属性の設定

接続プロファイルの一般属性を設定するには、次の手順を実行します。

手順

- ステップ 1** シングル コンテキスト モードまたはマルチ コンテキスト モードで **general-attributes** キーワードを指定して、トンネルグループ一般属性モードを開始します。

tunnel-group tunnel-group-name general-attributes

例 :

docs という名前の接続プロファイルの場合は、次のコマンドを入力します。

```
hostname(config)# tunnel-group docs general-attributes
hostname(config-tunnel-general)#
```

プロンプトが変化して、**config-general** モードに入ったことがわかります。トンネルグループの一般属性は、このモードで設定します。

- ステップ 2** デフォルト グループ ポリシーの名前を指定します。

default-group-policy policyname

例 :

次のコマンドは、デフォルト グループ ポリシーの名前に **MyPolicy** を指定しています。

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

LAN-to-LAN IPSec IKEv1 属性の設定

IPsec IKEv1 属性を設定するには、次の手順を実行します。

手順

- ステップ 1** トンネルグループ IPSec IKEv1 属性を設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで **IPsec-attributes** キーワードを指定して **tunnel-group** コマンドを入力し、トンネルグループ **ipsec** 属性コンフィギュレーション モードを開始します。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドでは、**config-ipsec** モードを開始し、TG1 という名前の接続プロファイルのパラメータを設定できます。

```
hostname(config)# tunnel-group TG1 ipsec-attributes
```

```
hostname(config-tunnel-ipsec)#
```

プロンプトが変化して、トンネルグループ **ipsec** 属性コンフィギュレーションモードに入ったことがわかります。

ステップ 2 事前共有キーに基づく IKEv1 接続をサポートするために、事前共有キーを指定します。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、LAN-to-LAN 接続プロファイルの IKEv1 接続をサポートするために、事前共有キー **XYZX** を指定しています。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

ステップ 3 ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できるオプションは、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。たとえば、次のコマンドは、**peer-id-validate** オプションを **nocheck** に設定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

ステップ 4 証明書チェーンを送信できるかどうかを指定します。次のアクションは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネルグループタイプに適用できます。

ステップ 5 IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、トラストポイント名を **mytrustpoint** に設定しています。

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネルグループタイプに適用できます。

ステップ 6 ISAKMP (IKE) キープアライブのしきい値と許可されるリトライ回数を指定します。**threshold** パラメータでは、ピアがキープアライブモニタリングを開始するまでの最長アイドル時間を秒数 (10 ~ 3600) で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です (2 ~ 10 秒)。IKE キープアライブは、デフォルトでイネーブルです。IKE キープアライブをディセーブルにするには、**isakmp** コマンドの **no** 形式を入力します。

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、ISAKMP キープアライブのしきい値を 15 秒に設定し、リトライインターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、LAN-to-LAN の場合は 10 です。**retry** パラメータのデフォルト値は 2 です。

中央サイト (セキュア ゲートウェイ) で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7 ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、ASA 認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザー認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する場合がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合せてハイブリッド認証と呼ばれます。

- a) ASA は、標準の公開キー技術を使用して、リモート VPN ユーザーに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
- b) 次に、XAUTH 交換がリモート VPN ユーザーを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

(注)

認証タイプをハイブリッドに設定するには、事前に認証サーバーを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

たとえば、次のコマンドは、**example-group** と呼ばれる接続プロファイルのハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
```

```
hostname(config-tunnel-ipsec)#
```

標準ベースの IKEv2 クライアントのトンネルグループについて

トンネルグループは、トンネル接続ポリシーを格納したレコードのセットです。AAA サーバーを識別するトンネルグループを設定し、接続パラメータを指定し、デフォルトのグループポリシーを定義します。ASA は、トンネルグループを内部的に保存します。

IPSec リモートアクセスのデフォルト トンネルグループは **DefaultRAGroup** です。デフォルト トンネルグループは、変更することはできますが、削除することはできません。

IKEv2 では、別のローカルおよびリモート認証 CLI を使用して非対称認証方式を設定できます（つまり、送信元に対しては事前共有キー認証を設定し、応答側に対しては証明書認証または EAP 認証を設定できます）。したがって、IKEv2 を使用すると、両方の側がそれぞれ異なるクレデンシャルで認証する非対称認証を使用できます（事前共有キー、証明書、または EAP）。

DefaultRAGroup は EAP 認証用に設定する必要があります。これは、証明書認証が証明書 DN 照合に使用されていない場合は、これらのクライアント接続を特定のトンネルグループにマッピングすることができないためです。

標準ベースの IKEv2 属性のサポート

ASA では、次の IKEv2 属性がサポートされます。

- **INTERNAL_IP4_ADDRESS/INTERNAL_IP6_ADDRESS** : IPv4 または IPv6 アドレス



(注) デュアルスタック（IPv4 と IPv6 の両方のアドレス割り当て）は、IKEv2 ではサポートされません。IPv4 アドレスと IPv6 アドレスの両方が要求され、両方のアドレスが割り当て可能な場合は、IPv4 アドレスのみが割り当てられます。

- **INTERNAL_IP4_NETMASK** : IPv4 アドレス ネットワーク マスク
- **INTERNAL_IP4_DNS/INTERNAL_IP6_DNS** : プライマリ/セカンダリ DNS アドレス
- **INTERNAL_IP4_NBNS** : プライマリ/セカンダリ WINS アドレス
- **INTERNAL_IP4_SUBNET/INTERNAL_IP6_SUBNET** : スプリット トンネリングのリスト
- **APPLICATION_VERSION** : 無視されます。セキュリティ上の理由から、ASA のバージョン情報を伝達しないように応答は送信されません。ただし、クライアント設定ペイロード要求にこの属性を含めることができ、文字列が ASA の **vpn-sessiondb** コマンド出力と **syslog** に表示されます。

DAF のサポート

接続タイプごとの DAF ポリシー設定を許可するには、新しいクライアント タイプの IPsec-IKEv2-Generic-RA を使用してこの接続タイプに特定のポリシーを適用することができます。

リモート アクセス クライアントのトンネル グループ選択

次の表に、リモート アクセス クライアントと使用可能なトンネル グループ オプションのリストを示します。

リモート アクセス クライアント	トンネル グループ リスト	グループ URL	証明書 DN 照合	デフォルト グループ (DefaultRAGroup)	その
AnyConnect VPN クライアント	対応	対応	対応	対応	該当
Windows L2TP/IPsec (メイン モード IKEv1)	非対応	非対応	• 対応 (ローカル マシンの証明書を使用する場合) • なし (PSK を使用する場合)	対応	該当
標準ベースの IKEv2	非対応	非対応	• 対応 (ローカル マシンの証明書を使用する場合) • なし (EAP 認証を使用する場合)	対応 (注) DefaultRAGroup トンネル グループを使用する必要があります。	該当

標準ベースの IKEv2 クライアントの認証サポート

次の表に、標準ベースの IKEv2 クライアントとサポートされている認証方式のリストを示します。



- (注) 認証方式の制限は、ASA 上ではなく、クライアント上のサポートの有無に基づきます。すべての EAP 方式の認証は、クライアントと EAP サーバー間で ASA によってプロキシされます。EAP 方式のサポートは、クライアントと EAP サーバーの EAP 方式のサポートに基づきます。

クライアントタイプ/認証方式	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	証明書のみ	PSK
Linux 上の StrongSwan	該当なし	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	対応	対応
Android 上の StrongSwan	該当なし	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	非対応	対応	該当なし
Windows 7/8/8.1	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	該当なし	対応	NA
Windows Phone	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	該当なし	該当なし	該当なし

クライアントタイプ/認証方式	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	証明書のみ	PSK
Samsung Knox	該当なし	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	対応	該当なし
iOS 8	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	該当なし	対応	対応
Android ネイティブクライアント	該当なし	• ISE : 対応 • ACS : 対応 • FreeRadius : 対応 • FreeRadius 経由の AD : 対応	該当なし	対応	対応

複数証明書認証の追加

マルチ証明書認証のプロトコル交換を定義し、これを両方のセッションタイプで利用できるように、集約認証プロトコルが拡張されました。クライアントが SSL 接続を行なって集約認証を開始すると、別の SSL 接続が行なわれ、ASA は、クライアントが証明書認証を必要としクライアント証明書を要求していることを確認します。

ASA は、リモートアクセスタイプのトンネルグループのセキュアクライアント 接続に必要な認証を設定します。トンネルグループマッピングは、証明書ルールマッピング、group-url などの既存の方法で実行されますが、必要な認証方法はクライアントとネゴシエートされます。

例

```
tunnel-group <name> webvpn-attributes
```

```
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml] | saml  
[certificate | multiple-certificate]}
```

認証オプションは、AAA のみ、証明書のみ、複数証明書のみ、AAA と証明書、AAA と複数証明書、SAML、SAML と証明書、または複数証明書と SAML です。

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa      Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml     Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa      Use username and password for authentication
saml     Use SAML for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>ASA(config-tunnel-webvpn)# authentication aaa?

ASA(config-tunnel-webvpn)# authentication saml?
tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

EAP ID を取得するためのクエリ ID オプションの設定

Microsoft Windows 7 IKEv2 クライアントは、Cisco ASA サーバーがトンネル グループ検索に使用できないようにするために、IP アドレスをインターネット キー交換 (IKE) ID として送信します。ASA は、ASA がクライアントから有効な EAP ID を取得できるように、EAP 認証用の **query-identity** オプションを使用して設定する必要があります。

証明書ベースの認証の場合は、次のように、ASA サーバーと Microsoft Windows 7 クライアントの証明書に拡張キー使用法 (EKU) フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバー証明書では、EKU フィールド = サーバー認証証明書です。

証明書は、Microsoft Certificate Server またはその他の CA サーバーから取得できます。

EAP 認証の場合は、Microsoft Windows 7 IKEv2 クライアントが他の EAP 要求の前に EAP ID 要求を待ちます。クライアントに EAP ID 要求を送信するには、IKEv2 ASA サーバー上のトンネ

ルグループプロファイル内で **query-identity** キーワードが設定されていることを確認してください。



- (注) Windows でスプリット トンネリングが実行できるように IKEv2 では DHCP 代行受信がサポートされます。この機能は、IPv4 スプリット トンネリング属性でのみ動作します。

手順

- ステップ 1** 接続タイプを IPsec リモート アクセスに設定するには、**tunnel-group** コマンドを入力します。構文は、**tunnel-group nametype type** です。ここで、name はトンネル グループに割り当てる名前であり、type はトンネルのタイプです。

次の例では、IKEv2 事前共有キーが 44kkaol59636jnfx に設定されます。

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

- (注)
認証を完了するには、**ikev2 remote-authentication pre-shared-key** コマンドまたは **ikev2 remote-authentication certificate** コマンドを設定する必要があります。

- ステップ 2** 標準ベースのサードパーティ IKEv2 リモート アクセス クライアントを使用したユーザー認証をサポートする方式として拡張認証プロトコル (EAP) を指定するには、**ikev2 remote-authentication eap [query-identity]** コマンドを使用します。

- (注)
リモート認証で EAP をイネーブルにするには、証明書を使用してローカル認証を設定し、**ikev2 local-authentication {certificate trustpoint}** コマンドを使用して有効なトラストポイントを設定する必要があります。そうしなかった場合は、EAP 認証要求が拒否されます。

クライアントが、リモート認証用に設定されたオプションのすべてではなく、一部を使用できるようにする複数のオプションがあります。

IKEv2 接続の場合、トンネル グループのマッピングで、リモート認証に使用できる認証方式 (PSK、証明書、および EAP) とローカル認証に使用できる認証方式 (PSK および証明書)、およびローカル認証で使用するトラストポイントを特定する必要があります。現在、マッピングの実行には、ピアまたはピア証明書のフィールドの値から取得 (証明書マップを使用) された IKE ID が使用されます。両方のオプションが失敗した場合は、着信接続がデフォルトのリモートアクセス トンネルグループ DefaultRAGroup にマッピングされます。証明書マップは、リモート ピアが証明書で認証された場合にのみ適用されるオプションです。このマップにより、異なるトンネルグループへのマッピングが可能です。証明書認証の場合のみ、ルールまたはデフォルトの設定を使用してトンネル グループの参照が行われます。EAP 認証および PSK 認証の場合は、クライアント (トンネル グループ名が一致するクライアント) の IKE ID またはデフォルトの設定を使用してトンネル グループの参照が行われます。

EAP 認証で、クライアントが IKEID とユーザー名を個別に設定できない場合は、DefaultRAGroup トンネル グループを使用する必要があります。

次の例では、EAP 認証要求が拒否されています。

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

ステップ 3 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

トンネルが稼働中であることを確認するには、**show vpn-sessiondb summary** または **show crypto ipsec sa** コマンドを使用します。

パスワード管理用の Microsoft Active Directory の設定

認証に LDAP ディレクトリ サーバーを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

- **Sun** : Sun ディレクトリ サーバーにアクセスするために ASA に設定されている DN が、サーバーのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザーを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- **Microsoft** : Microsoft Active Directory でパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。

Microsoft Active Directory でパスワード管理を使用するには、一定の Active Directory パラメータを設定し、ASA でパスワード管理を設定する必要があります。この項では、さまざまなパスワード管理アクションに関連する Active Directory の設定について説明します。これらの説明は、ASA でのパスワード管理がイネーブルになっていて、対応するパスワード管理属性が設定されていることを前提としています。この項の特定の手順では、Windows 2000 における Active Directory の用語に言及しています。この項では、認証に LDAP ディレクトリ サーバーを使用していることを前提としています。

次回ログイン時にパスワードの変更をユーザーに強制するための **Active Directory** の使用

次回ログイン時にユーザー パスワードの変更をユーザーに強制するには、ASA の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で **password-management** コマンドを指定して、Active Directory で次の手順を実行します。

手順

- ステップ 1 [Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] の順に選択します。
- ステップ 2 右クリックして、[Username] > [Properties] > [Account] を選択します。
- ステップ 3 [User must change password at next logon] チェックボックスをオンにします。

このユーザーが次回ログインするときに、ASA で次のプロンプトが表示されます「New password required. Password change required. You must enter a new password with a minimum length n to continue.」最小必須パスワード長 n は、[Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] で Active Directory 設定の一部として設定できます。[Minimum password length] を選択します。

Active Directory を使用したパスワードの最大有効日数の指定

セキュリティを強化するために、一定の日数経過後パスワードが期限切れになるように指定できます。ユーザー パスワードの最大有効日数を指定するには、ASA の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で **password-management** コマンドを指定し、Active Directory で次の手順を実行します。



- (注) 以前、パスワードの有効日数の設定機能を実行するためにトンネルグループリモートアクセスコンフィギュレーションの一部として設定されていた **radius-with-expiry** コマンドは非推奨になっています。このコマンドは、トンネルグループ一般属性モードで入力される **password-management** コマンドに置き換えられます。

手順

- ステップ 1 [Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] > [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。
- ステップ 2 [Maximum password age] をダブルクリックします。
- ステップ 3 [Define this policy setting] チェックボックスをオンにして、許可する [Maximum password age] を日単位で指定します。

Active Directory を使用した最小パスワード長の強制

パスワードの最小長を強制するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを指定し、Active Directory で次の手順を実行します。

手順

- ステップ 1 [Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] を選択します。
- ステップ 2 [Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。
- ステップ 3 [Minimum Password Length] をダブルクリックします。
- ステップ 4 [Define this policy setting] チェックボックスをオンにして、パスワードに含める必要がある最小文字数を指定します。

Active Directory を使用したパスワードの複雑性の強制

複雑なパスワード、たとえば、大文字と小文字、数字、および特殊文字を含むパスワードを要求するには、ASA のトンネルグループ一般属性コンフィギュレーション モードで **password-management** コマンドを入力し、Active Directory で次の手順を実行します。

手順

- ステップ 1 [Start] > [Programs] > [Administrative Tools] > [Domain Security Policy] を選択します。[Windows Settings] > [Security Settings] > [Account Policies] > [Password Policy] を選択します。
- ステップ 2 [Password must meet complexity requirements] をダブルクリックして、[Security Policy Setting] ダイアログボックスを開きます。
- ステップ 3 [Define this policy setting] チェックボックスをオンにして、[Enable] を選択します。

パスワードの複雑性の強制は、ユーザーがパスワードを変更するときだけに有効になります。たとえば、次回ログイン時にパスワード変更を強制する、または n 日後にパスワードが期限切れになるように設定した場合です。ログイン時に、新しいパスワードの入力を求めるプロンプトが表示され、システムは複雑なパスワードだけを受け入れます。

セキュアクライアントをサポートする RADIUS/SDI メッセージの接続プロファイルの設定

この項では、RSA SecureID ソフトウェア トークンを使用する AnyConnect VPN クライアントが、SDI サーバーにプロキシする RADIUS サーバー経由でクライアントに配信されるユーザープロンプトに正しく応答できるようにする手順について説明します。



(注) 二重認証機能を設定した場合、SDI 認証はプライマリ認証サーバーでだけサポートされます。

リモート ユーザーが AnyConnect VPN クライアントで ASA に接続し、RSA SecurID トークンを使用して認証を試みると、ASA は RADIUS サーバーと通信を行い、次に、認証について SDI サーバーと通信を行います。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジメッセージを提示します。これらのチャレンジメッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージテキストは、ASA が SDI サーバーと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。そのため、セキュアクライアントにネイティブ SDI サーバーとして認識させるために、ASA は RADIUS サーバーからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージテキストの全体または一部が、SDI サーバのメッセージテキストと一致する必要があります。一致しない場合、リモートクライアントユーザに表示されるプロンプトが、認証中に必要とされるアクションに対して適切でない場合があります。そのため、セキュアクライアントが応答できずに、認証が失敗する可能性があります。

[RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定 \(151 ページ\)](#) クライアントと SDI サーバー間の認証を確実に成功させるように ASA を設定する方法について説明します。

RADIUS/SDI メッセージをサポートするためのセキュリティ アプライアンスの設定

SDI 固有の RADIUS 応答メッセージを解釈し、セキュアクライアント ユーザーに適切なアクションを求めるプロンプトを表示するように ASA を設定するには、次の手順を実行します。

手順

ステップ 1 トンネルグループ webvpn コンフィギュレーション モードで **proxy-auth sdi** コマンドを使用して、SDI サーバーとの直接通信をシミュレートする方法で、RADIUS 応答メッセージを転送するための接続プロファイル（トンネル グループ）を設定します。SDI サーバーに認証されるユーザーは、この接続プロファイルを介して接続する必要があります。

例：

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

ステップ 2 トンネルグループ webvpn コンフィギュレーション モードで **proxy-auth_map sdi** コマンドを使用して、RADIUS サーバーによって送信されるメッセージテキストと全体または一部が一致する RADIUS 応答メッセージテキストを ASA で設定します。

ASA が使用するデフォルトのメッセージテキストは、Cisco Secure Access Control Server (ACS) で使用されるデフォルトのメッセージテキストです。Cisco Secure ACS を使用していて、デフォルトのメッセージテキストを使用している場合、ASA でメッセージテキストを設定する必要はありません。それ以外の場合は、**proxy-auth_map sdi** コマンドを使用して、メッセージテキストが一致するようにします。

次の表に、メッセージコード、デフォルトの RADIUS 応答メッセージテキスト、および各メッセージの機能を示します。セキュリティ アプライアンスは、テーブルに表示される順番に文字列を検索するため、メッセージテキストに使用する文字列は別の文字列のサブセットではないようにする必要があります。

たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージテキストのサブセットであるとして、new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを照合します。

SDI 操作コード、デフォルトのメッセージテキスト、およびメッセージの機能

メッセージコード	デフォルトの RADIUS 応答メッセージテキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザが提供した PIN の確認のために ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。

メッセージコード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code-and-reauth	new PIN with the next card code	PIN 操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	ユーザがシステム生成の PIN に対する準備ができていることを示すために ASA が内部的に使用します。

次の例では、aaa-server-host モードに入り、RADIUS 応答メッセージ new-pin-sup のテキストを変更します。

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your
new PIN"
```

グループポリシー

この項では、グループポリシーとその設定方法について説明します。

グループポリシーは、IPSec 接続用のユーザー関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の RADIUS サーバーに保存されます。接続プロファイルでは、トンネル確立後、ユーザー接続の条件を設定するグループポリシーが使用されます。グループポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

ユーザーにグループポリシーを割り当てたり、特定のユーザーのグループポリシーを変更したりするには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

ASA には、デフォルトのグループポリシーが含まれています。変更はできても削除はできないデフォルトのグループポリシーに加え、自分の環境に固有の 1 つ以上のグループポリシーを作成することもできます。

内部グループポリシーと外部グループポリシーを設定できます。内部グループは ASA の内部データベースで設定されます。外部グループは RADIUS などの外部認証サーバーに設定されます。グループポリシーには、次の属性があります。

- Identity
- サーバーの定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル

- IPsec の設定
- ハードウェア クライアントの設定
- Filters
- クライアント コンフィギュレーションの設定
- 接続の設定

デフォルトのグループ ポリシーの変更

ASA では、デフォルトのグループ ポリシーが提供されます。このデフォルト グループ ポリシーは変更できますが、削除はできません。デフォルトのグループ ポリシーは、**DfltGrpPolicy** という名前で ASA に常に存在していますが、このデフォルトのグループ ポリシーは、ASA でそれを使用するように設定しない限り有効にはなりません。その他のグループ ポリシーを設定する場合、明示的に指定しない属性の値はデフォルトのグループ ポリシーから継承されます。



- (注) **DfltGrpPolicy** に設定されている（その後に割り当てられた）すべてのセキュアクライアント プロファイルタイプ（Network Access Manager、Cisco Umbrella など）を含むセキュアクライアント プロファイルは、他のグループポリシーが **DfltGrpPolicy** から継承するように明示的に設定されていない限り、他のグループポリシーによって継承されません。つまり、特定のセキュアクライアントプロファイルがグループポリシーで設定されている場合、**DfltGrpPolicy** に関連付けられているセキュアクライアントプロファイルは継承されません。

デフォルトのグループ ポリシーを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

デフォルトのグループ ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```



- (注) デフォルトのグループ ポリシーは、常に内部（internal）です。コマンドの構文は、**hostname(config)# group-policy DfltGrpPolicy {internal|external}** ですが、タイプを外部（external）に変更することはできません。

デフォルトのグループ ポリシーの任意の属性を変更する場合は、**group-policy attributes** コマンドを使用して属性モードに入り、その後、変更対象の属性を変更するためのコマンドを指定します。

```
hostname(config)# group-policy DfltGrpPolicy attributes
```



(注) 属性モードは内部グループポリシーにだけ適用されます。

ASA で提供されるデフォルトのグループポリシー DfltGrpPolicy は、次のとおりです。

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  banner none
  wins-server none
  dns-server value 10.10.10.1
  dhcp-network-scope none
  vpn-access-hours none
  vpn-simultaneous-logins 3
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1
  vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client

password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain value cisco.com
split-dns none
split-tunnel-all-dns disable
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
client-bypass-protocol disable
gateway-fqdn none
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
msie-proxy lockdown enable
vlan none
nac-settings none
address-pools none
ipv6-address-pools none
smartcard-removal-disconnect enable
scep-forwarding-url none
client-firewall none
```

```

client-access-rule none
webvpn
  url-list none
  filter none
  homepage none
  html-content-filter none

http-proxy disable

anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface private none
anyconnect firewall-rule client-interface public none
anyconnect keep-installer installed
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression lzs
anyconnect modules none
anyconnect profiles none
anyconnect ask none
customization none
keep-alive-ignore 4
http-comp gzip
download-max-size 2147483647
upload-max-size 2147483647
post-max-size 2147483647
user-storage none
storage-objects value cookies,credentials
storage-key none
hidden-shares none

activex-relay enable
unix-auth-uid 65534
unix-auth-gid 65534
file-entry enable
file-browsing enable
url-entry enable
deny-message value Login was successful, but because certain criteria have not been
met or due to some specific group policy, you do not have permission to use any of the
VPN features. Contact your IT administrator for more information

anyconnect ssl df-bit-ignore disable
anyconnect routing-filtering-ignore disable

always-on-vpn profile-setting

```

デフォルト グループ ポリシーは変更可能です。また、環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

グループ ポリシーの設定

グループポリシーは、すべての種類のトンネルに適用できます。どちらの場合も、パラメータが明示的に指定されていなければ、そのグループはデフォルト グループ ポリシーの値を使用します。

設定タスクは、シングル コンテキスト モードまたはマルチ コンテキスト モードの両方で実行できます。



- (注) マルチ コンテキスト モードは IKEv1 および IKEv2 サイトツーサイトにのみ適用され、IKEv1 IPSec の AnyConnect、クライアントレス SSL VPN、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、または cTCP には適用されません。

外部グループポリシーの設定

外部グループポリシーの属性値には、指定する外部サーバーの値が取得されます。外部グループポリシーの場合は、ASA が属性のクエリーを実行できる AAA サーバー グループを特定し、その外部 AAA サーバー グループから属性を取得するときに使用するパスワードを指定する必要があります。外部認証サーバーを使用して、外部グループポリシー属性が、認証する予定のユーザーと同じ RADIUS サーバーにある場合、それらの間で名前が重複しないようにする必要があります。



- (注) ASA での外部グループ名は、RADIUS サーバーのユーザー名を参照しています。つまり、ASA に外部グループ X を設定した場合、RADIUS サーバーはクエリーをユーザー X に対する認証要求と見なします。したがって、外部グループは、ASA にとって特別な意味を持つ RADIUS サーバー上のユーザーアカウントにすぎません。外部グループ属性が認証する予定のユーザーと同じ RADIUS サーバーに存在する場合、それらの間で名前を重複させることはできません。

ASA は、外部 LDAP または RADIUS サーバーでのユーザー認証をサポートしています。外部サーバーを使用するように ASA を設定する前に、適切な ASA 認可属性を指定してサーバーを設定し、それらの属性のサブセットから個々のユーザーに対する特定の許可を割り当てる必要があります。外部サーバーを設定するには、[VPN の外部 AAA サーバーの設定 \(327 ページ\)](#)の説明に従ってください。

手順

外部グループポリシーを設定するには、次の手順を実行して、server-group 名とパスワードとともにグループポリシーの名前とタイプを指定します。

```
hostname(config)# group-policy group_policy_name type server-group server_group_name  
password server_password  
hostname(config)#
```

- (注)
外部グループポリシーの場合、サポートされる AAA サーバー タイプは RADIUS だけです。

たとえば、次のコマンドは、ExtGroup という名前の外部グループ ポリシーが作成します。このグループ ポリシーの属性は、ExtRAD という名前の外部 RADIUS サーバーから取得され、属性を取得するときに使用されるパスワードが newpassword に指定されます。

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

(注)

[VPN の外部 AAA サーバーの設定 \(327 ページ\)](#) に説明されているように、いくつかのベンダー固有属性 (VSA) を設定できます。RADIUS サーバーが Class 属性 (#25) を返すように設定されている場合、ASA は、グループ名の認証にその属性を使用します。RADIUS サーバーでは、属性は次の形式で指定する必要があります。OU=groupname。ここで、groupname は、ASA で設定されたグループ名と同一です。例、OU=Finance。

内部グループ ポリシーの作成

内部グループ ポリシーを設定するには、コンフィギュレーション モードを開始します。group-policy コマンドを使用して、グループ ポリシーの名前と **internal** タイプを指定します。

```
hostname(config)# group-policy group_policy_name internal
hostname(config)#
```

たとえば、次のコマンドは GroupPolicy1 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```



(注) いったん作成したグループ ポリシーの名前は変更できません。

キーワード **from** を追加して既存のポリシーの名前を指定することにより、既存のグループ ポリシーの値をコピーして、内部グループ ポリシーの属性を設定できます。

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
```

たとえば、次のコマンドは GroupPolicy1 の属性をコピーして、GroupPolicy2 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```


一般的な内部グループポリシー属性の設定

グループポリシー名

グループポリシーの名前は内部グループポリシーの作成時に選択されています。いったん作成されたグループポリシーの名前は変更できません。詳細については、[内部グループポリシーの作成 \(158 ページ\)](#) を参照してください。

グループポリシーのバナー メッセージの設定

表示するバナーまたは初期メッセージ（ある場合）を指定します。デフォルトでは、バナーは表示されません。指定したメッセージは、リモートクライアントが接続したときに、そのクライアントに表示されます。バナーを指定するには、グループポリシー コンフィギュレーション モードで **banner** コマンドを入力します。バナー テキストの長さは 500 文字までです。復帰改行を挿入する場合は、「\n」シーケンスを入力します。

VPN リモートクライアントでのログイン後に表示される全体的なバナーの長さは、ASA バージョン 9.5.1 で 510 ～ 4000 文字に増加しました。



(注) バナー内の復帰改行は、2 文字として数えられます。

バナーを削除するには、このコマンドの **no** 形式を入力します。このコマンドの **no** 形式を使用すると、グループポリシーのすべてのバナーが削除されることに注意してください。

グループポリシーは、別のグループポリシーからこの値を継承できます。値を継承しないようにするには、次のように、バナー文字列の値を指定する代わりに **none** キーワードを入力します。

```
hostname(config-group-policy)# banner {value banner_string | none}
```

次の例は、FirstGroup という名前のグループポリシーにバナーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

リモート アクセス接続のアドレス プールの指定

リモートアクセスクライアントがASAに接続する場合、ASAは、接続に指定されたグループポリシーに基づいてIPv4 またはIPv6 アドレスをクライアントに割り当てることができます。

ローカルアドレスの割り当てに使用する最大 6 個のローカルアドレス プールのリストを指定できます。プールの指定順序は重要です。ASAでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

内部グループ ポリシーへの IPv4 アドレス プールの割り当て

始める前に

IPv4 アドレス プールを作成します。

手順

ステップ 1 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 value attributes

例 :

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

ステップ 2 ipv4-pool1、ipv4-pool2、および ipv4-pool3 という名前のアドレス プールを FirstGroup グループ ポリシーに割り当てます。グループ ポリシーには、最大 6 個のアドレス プールを指定できます。

address-pools value pool-name1 pool-name2 pool-name6

例 :

```
asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
asa4(config-group-policy)#
```

ステップ 3 (任意) グループ ポリシー設定からアドレス プールを削除し、アドレス プール設定を戻して DefltGroupPolicy などの他のソースからのアドレス プール情報を継承するには、**no address-pools value pool-name** コマンドを使用します。

no address-pools value pool-name1 pool-name2 pool-name6

例 :

```
hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
hostname(config-group-policy)#
```

ステップ 4 (任意) **address-pools none** コマンドは、ポリシーの別のソース (DefltGrpPolicy など) からこの属性を継承することをディセーブルにします。

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

ステップ 5 (任意) **no address pools none** コマンドは、**address-pools none** コマンドをグループ ポリシーから削除して、デフォルト値 (継承の許可) に戻します。

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

内部グループポリシーへのIPv6アドレスプールの割り当て

始める前に

IPv6 アドレス プールを作成します。[VPN の IP アドレス \(219 ページ\)](#) を参照してください。

手順

ステップ 1 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 value attributes

例 :

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

ステップ 2 ipv6-pool という名前のアドレス プールを FirstGroup グループ ポリシーに割り当てます。グループ ポリシーには、最大 6 個の IPv6 アドレス プールを割り当てることができます。

例 :

この例では、ipv6-pool1、ipv6-pool2、および ipv6-pool3 が FirstGroup グループ ポリシーに割り当てられています。

```
hostname(config-group-policy)# ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

ステップ 3 (任意) グループ ポリシー設定からアドレス プールを削除し、アドレス プール設定を戻して DfltGroupPolicy などの他のソースからのアドレス プール情報を継承するには、**no ipv6-address-pools value pool-name** コマンドを使用します。

no ipv6-address-pools value pool-name1 pool-name2 pool-name6

例 :

```
hostname(config-group-policy)# no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

ステップ 4 (任意) この属性が DfltGrpPolicy など他のポリシーのソースから継承されないようにするには、**ipv6-address-pools none** コマンドを使用します。

```
hostname(config-group-policy)# ipv6-address-pools none
hostname(config-group-policy)#
```

ステップ 5 (任意) **no ipv6-address pools none** コマンドを使用して、**ipv6-address-pools none** コマンドをグループポリシーから削除して、デフォルト値（継承の許可）に戻します。

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

グループポリシーのトンネリングプロトコルの指定

グループポリシー コンフィギュレーション モードで **vpn-tunnel-protocol{ikev1|ikev2|l2tp-ipsec|ssl-client}** コマンドを入力して、このグループポリシーのVPNトンネルタイプを指定します。

デフォルト値は、デフォルトグループポリシーの属性を継承することです。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

このコマンドのパラメータの値には次のものがあります。

- **ikev1** : 2つのピア（Cisco VPN Client または別のセキュアゲートウェイ）間のIPsec IKEv1 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティアソシエーションを作成します。
- **ikev2** : 2つのピア（セキュアクライアント または別のセキュアゲートウェイ）間のIPsec IKEv2 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティアソシエーションを作成します。
- **l2tp-ipsec** : L2TP 接続のIPsec トンネルをネゴシエートします。
- **ssl-client** : セキュアクライアントでTLSまたはDTLSを使用して、SSL トンネルをネゴシエートします。

このコマンドを入力して、1つ以上のトンネリングモードを設定します。VPNトンネルを介して接続するユーザーには、少なくとも1つのトンネリングモードを設定する必要があります。

次の例は、FirstGroup という名前のグループポリシーにIPsec IKEv1 トンネリングモードを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

リモートアクセスのVLANの指定またはグループポリシーへの統合アクセスコントロールルールの適用

フィルタは複数のルールから構成されています。これらのルールは、ASAを介して着信したトンネリングデータパケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。グループポリシーのIPv4またはIPv6統合アクセスコ

ントロールリストを指定するか、またはデフォルトグループポリシーで指定された ACL を継承するようにできます。

次のオプションのいずれかを選択して、リモートアクセス用の出力 VLAN（「VLAN マッピング」とも呼ばれる）、またはトラフィックをフィルタリングする ACL を指定します。



- (注) IPv6 を使用して VLAN マッピングを実行する場合、復号化されたトラフィックが内部ネットワークにルーティングされるようにするために、外部（宛先）アドレスは VLAN ごとに固有にする必要があります。異なる VLAN およびルートメトリックに対して同じ宛先ネットワークを使用することはできません。

- グループポリシーコンフィギュレーションモードで次のコマンドを入力して、このグループポリシーまたはこのグループポリシーを継承するグループポリシーに割り当てられているリモートアクセス VPN セッション用の出力 VLAN を指定します。

[no] vlan {vlan_id | none}

no vlan は、グループポリシーから **vlan_id** を削除します。グループポリシーは、デフォルトのグループポリシーから **vlan** 値を継承します。

none は、グループポリシーから **vlan_id** を削除し、このグループポリシーに対する VLAN マッピングをディセーブルにします。グループポリシーは、デフォルトのグループポリシーから **vlan** 値を継承しません。

vlan_id は、このグループポリシーを使用するリモートアクセス VPN セッションに割り当てる VLAN の番号（10 進表記）です。VLAN は、一般的操作コンフィギュレーションガイドの「Configuring VLAN Subinterfaces and 802.1Q Trunking」の手順に従って、この ASA で設定する必要があります。



- (注) クライアントレス VPN 接続の場合、出力 VLAN 機能は HTTP プロトコルでのみ機能します。

- グループポリシーモードで **vpn-filter** コマンドを使用して、VPN セッションに適用するアクセスコントロールルール（ACL）の名前を指定します。**vpn-filter** コマンドを使用して、IPv4 または IPv6 ACL を指定できます。



- (注) この属性はユーザー名モードで設定することもできます。その場合、ユーザー名の下で設定された値がグループポリシーの値よりも優先されます。

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

ACL を設定して、このグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを入力して、これらの ACL を適用します。

vpn-filter none コマンドを入力して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、ACL 名を指定する代わりに、**none** キーワードを入力します。**none** キーワードは、ACL がないことを示します。このキーワードにより、ヌル値が設定され、ACL が拒否されます。

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

vpn-filter コマンドは、トンネルから出た後の復号化後のトラフィックと、トンネルに入る前の暗号化前のトラフィックに適用されます。**vpn-filter** に使用される ACL を **interface access-group** にも使用することはできません。**vpn-filter** コマンドを、リモート アクセス VPN クライアント接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のクライアント割り当て IP アドレスおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter コマンドを、LAN-to-LAN VPN 接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のリモート ネットワークおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter 機能で使用するために ACL を設定する場合は、注意する必要があります。ACL は、復号化後のトラフィックに対して構築されていることに留意してください。ただし、ACL は反対方向のトラフィックに対しても適用されます。トンネル宛ての、暗号化前のこのトラフィックについては、ACL は **src_ip** の位置と **dest_ip** の位置を入れ替えたものに対して構築されています。

VPN フィルタは初期接続にのみ適用されることにも留意してください。アプリケーション インспекションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。

次の例では、**vpn-filter** をリモート アクセス VPN クライアントと共に使用します。この例では、クライアント割り当て IP アドレスを 10.10.10.1/24、ローカル ネットワークを 192.168.1.0/24 としています。

次の ACE によって、リモート アクセス VPN クライアントがローカル ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

次のACEによって、ローカルネットワークがリモートアクセスクライアントにTelnetを使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255  
eq 23 192.168.1.0 255.255.255.0
```



- (注) ACEの **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23** によって、ローカルネットワークは、送信元ポート23を使用している場合に任意のTCPポートでのリモートアクセスクライアントへの接続開始が許可されます。ACEの **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0** によって、リモートアクセスクライアントは、送信元ポート23を使用している場合に任意のTCPポートでのローカルネットワークへの接続開始が許可されます。

次の例では、vpn-filterをLAN-to-LAN VPN接続と共に使用します。この例では、リモートネットワークを10.0.0.0/24、ローカルネットワークを192.168.1.0/24としています。次のACEによって、リモートネットワークがローカルネットワークにTelnetを使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0  
192.168.1.0 255.255.255.0 eq 23
```

次のACEによって、ローカルネットワークがリモートネットワークにTelnetを使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0 eq  
23 192.168.1.0 255.255.255.0
```



- (注) ACEの **access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23** によって、ローカルネットワークは、送信元ポート23を使用している場合に任意のTCPポートでのリモートネットワークへの接続開始が許可されます。ACEの **access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0** によって、リモートネットワークは、送信元ポート23を使用している場合に任意のTCPポートでのローカルネットワークへの接続開始が許可されます。

グループポリシーのVPNアクセス時間の指定

始める前に

時間の範囲を作成します。一般的操作用コンフィギュレーションガイドの「Configuring Time Ranges」を参照してください。

手順

ステップ 1 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 value attributes

例 :

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

ステップ 2 グループポリシー コンフィギュレーション モードで **vpn-access-hours** コマンドを使用して、グループポリシーと設定済みの **time-range** ポリシーを関連付けることによって、VPN アクセス時間を設定できます。このコマンドは、**business-hours** という名前の VPN アクセス時間範囲を **FirstGroup** という名前のグループポリシーに割り当てます。

グループポリシーは、デフォルトまたは指定されたグループポリシーの **time-range** の値を継承することができます。この継承が発生しないようにするには、このコマンドで **time-range** の名前ではなく **none** キーワードを入力します。このキーワードにより、VPN アクセス時間がヌル値に設定され、**time-range** ポリシーは許可されなくなります。

vpn-access-hours value {time-range-name | none}

例 :

```
hostname(config-group-policy)# vpn-access-hours value business-hours
hostname(config-group-policy)#
```

グループポリシーの同時 VPN ログインの指定

特定のユーザーがグループポリシーに対して維持できる同時セッション数の制限を設定できます。デフォルトの同時セッション数は 3 です。

失効したセキュアクライアント、IPsec クライアント、またはクライアントレスセッション（異常終了したセッション）は、同じユーザー名で「新しい」セッションが確立されても、セッションデータベースに残る場合があります。

許可される同時セッション数が 1 で、異常終了後に同じユーザーが再度ログインした場合、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザーが別の PC などから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

許可される同時セッション数が 1 より大きい場合、その最大数に達した状態でユーザーが再度ログインを試みると、最もアイドル時間が長いセッションがログオフされます。現在のすべて

のセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

最大セッション制限に達すると、システムが最も古いセッションを削除するまでに時間がかかります。そのため、ユーザーはすぐにログオンできず、削除が正常に完了する前に新しい接続を再試行する必要がある場合があります。ユーザーが想定どおりにログオフした場合、これは問題になりません。必要に応じて、削除の完了を待たずにすぐに新しいユーザー接続を許可するようにシステムを設定することで、遅延を解消できます。

手順

	コマンドまたはアクション	目的
ステップ 1	グループ ポリシー コンフィギュレーション モードで vpn-simultaneous-logins integer コマンドを使用して、任意のユーザーに許可される同時ログイン数を指定します。	vpn-simultaneous-logins 整数 デフォルト値は3です。値の範囲は0～2147483647の整数です。グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。ログインをディセーブルにしてユーザーのアクセスを禁止するには、0を入力します。次に、FirstGroup という名前のグループ ポリシーに対して最大4つの同時ログインを許可する例を示します。 <pre>hostname(config)# group-policy FirstGroup attributes hostname(config-group-policy)# vpn-simultaneous-logins 4</pre> (注) - 同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。 - 異なるグループポリシーを使用して異なるトンネルグループに接続すると、vpn-simultaneous-logins は、既存のセッションで異なるグループポリシーが使用されている場合でも、ユーザーセッションを削除します。
ステップ 2	(オプション) 同時ログインの制限に達した場合に、最も古いセッションが削除	vpn-simultaneous-login-delete-no-delay このオプションはデフォルトでは無効になっています。

	コマンドまたはアクション	目的
	されるのを待たずに新しいセッションを確立するようにシステムを設定します。	hostname(config)# group-policy FirstGroup attributes hostname(config-group-policy)# vpn-simultaneous-login-delete-no-delay

特定の接続プロファイルへのアクセスの制限

グループポリシー コンフィギュレーション モードで **group-lock** コマンドを使用して、接続プロファイルを介してのみアクセスするようにリモートユーザーを制限するかどうかを指定します。

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

tunnel-grp-name 変数は、ASA がユーザーの接続に関して要求する既存の接続プロファイルの名前を指定します。group-lock は、VPN クライアントで設定されたグループが、そのユーザーが割り当てられている接続プロファイルと同じかどうかをチェックすることによって、ユーザーを制限します。一致していない場合、ASA はユーザーが接続できないようにします。グループロックを設定しない場合、ASA は、割り当てられたグループとは関係なく、ユーザーを認証します。グループのロックは、デフォルトではディセーブルになっています。

group-lock 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、別のグループポリシーの値を継承できます。

group-lock をディセーブルにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。none キーワードにより、group-lock はヌル値に設定され、group-lock の制限が拒否されます。また、デフォルトまたは指定されたグループポリシーから group-lock の値が継承されなくなります。

グループポリシーの VPN の最大接続時間の指定

手順

ステップ 1 (任意) グループポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **vpn-session-timeout** {minutes コマンドを使用して、VPN 接続の最大時間を設定します。

最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。この期間が終了すると、ASA は接続を終了します。

次に、FirstGroup という名前のグループポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

次の例は、anyuser という名前のユーザーに 180 分の VPN セッションタイムアウトを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

[no] **vpn-session-timeout** {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- このポリシーから属性を削除し、継承を許可するには、このコマンドの **no vpn-session-timeout** 形式を入力します。
- 無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**vpn-session-timeout none** を入力します。

ステップ 2 **vpn-session-timeout alert-interval**{minutes | } コマンドを使用して、セッションタイムアウトのアラートメッセージがユーザーに表示される時間を設定します。

このアラートメッセージは、VPN セッションが自動的に切断されるまでに何分あるかをユーザーに伝えます。次に、VPN セッションが切断される 20 分前にユーザーに通知されるよう指定する例を示します。1 ～ 30 分の範囲を指定できます。

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

[no] **vpn-session-timeout alert-interval** {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- VPN セッションタイムアウトアラート間隔属性がデフォルトグループポリシーから継承されることを示すには、このコマンドの **no** 形式を使用します。

```
hostname(config-webvpn)# no vpn-session-timeout alert-interval
```

- **vpn-session-timeout alert-interval none** は、ユーザーが通知を受信しないことを示します。

グループポリシーのVPNセッションアイドルタイムアウトの指定

手順

ステップ 1 (任意) VPN アイドルタイムアウト期間を設定するには、グループポリシー コンフィギュレーションモードまたはユーザー名コンフィギュレーションモードで **vpn-idle-timeout minutes** コマンドを使用します。

この期間中に接続上で通信アクティビティがない場合、ASAは接続を終了します。最小時間は1分、最大時間は35791394分であり、デフォルトは30分です。

次の例は、FirstGroup という名前のグループポリシーに15分のVPNアイドルタイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

[no] **vpn-idle-timeout** {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- VPN アイドルタイムアウトを無効にし、タイムアウト値を継承しないようにするには、**vpn-idle-timeout none** を入力します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout none
hostname(config-group-policy)#
```

これにより、セキュアクライアント（SSL と IPsec/IKEv2 の両方）およびクライアントレスVPNがグローバル **webvpn default-idle-timeout seconds** 値を使用するようになります。このコマンドは、**webvpn** コンフィギュレーション モードで入力します。たとえば、**hostname(config-webvpn)# default-idle-timeout 300** のように入力します。デフォルトは1800秒（30分）で、範囲は60～86400秒です。

すべての **webvpn** 接続において、**default-idle-timeout** 値が適用されるのは、グループポリシー/ユーザー名属性に **vpn-idle-timeout none** が設定されている場合のみです。すべてのセキュアクライアント接続で、ASAによりゼロ以外のアイドルタイムアウト値が要求されます。

サイト間（IKEv1、IKEv2）およびIKEv1リモートアクセスVPNの場合は、タイムアウトをディセーブルにし、無制限のアイドル期間を許可することを推奨します。

- このグループポリシーまたはユーザーポリシーのアイドルタイムアウトを無効にするには、**no vpn-idle-timeout** を入力します。値は継承されます。
- **vpn-idle-timeout** をまったく設定しない場合、値は継承されます。デフォルトは30分です。

ステップ2 （任意） オプションで、**vpn-idle-timeout alert-interval {minutes}** コマンドを使用して、アイドルタイムアウトのアラートメッセージがユーザーに表示される時間を設定できます。

このアラートメッセージは、VPNセッションが非アクティブ状態のため切断されるまでに何分あるかをユーザーに伝えます。デフォルトのアラート間隔は1分です。

次の例は、anyuser という名前のユーザーに3分のVPNアイドルタイムアウトのアラート間隔を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

[no] vpn-idle-timeout alert-interval {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- **none** パラメータは、ユーザーが通知を受信しないことを示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- このグループまたはユーザー ポリシーのアラート間隔を削除するには、**no vpn-idle-timeout alert-interval** を入力します。値は継承されます。
- このパラメータをまったく設定しない場合、デフォルトのアラート間隔は 1 分です。

グループ ポリシーの WINS サーバーと DNS サーバーの設定

プライマリおよびセカンダリの WINS サーバーと DNS サーバーを指定できます。それぞれのデフォルト値は **none** です。これらのサーバーを指定するには、次の手順を実行します。

手順

ステップ 1 プライマリとセカンダリの WINS サーバーを指定します。

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ WINS サーバーの IP アドレスです。2 番目（任意）の IP アドレスはセカンダリ WINS サーバーの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、WINS サーバーにヌル値が設定されます。この設定により、WINS サーバーは許可されず、デフォルトまたは指定のグループ ポリシーから値が継承されなくなります。

wins-server コマンドを入力するたびに、既存の設定がオーバーライドされます。たとえば、WINS サーバー x.x.x.x を設定してから WINS サーバー y.y.y.y を設定すると、2 番目のコマンドによって最初の設定が上書きされ、y.y.y.y が唯一の WINS サーバーになります。サーバーを複数設定する場合も同様です。設定済みのサーバーを上書きするのではなく、WINS サーバーを追加するには、このコマンドを入力するときに、すべての WINS サーバーの IP アドレスを含めます。

次の例は、FirstGroup という名前のグループポリシーに、IP アドレスが 10.10.10.15 と 10.10.10.30 である WINS サーバーを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

ステップ 2 プライマリとセカンダリの DNS サーバーを指定します。

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ DNS サーバーの IP アドレスです。2 番目（任意）の IP アドレスはセカンダリ DNS サーバーの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、DNS サーバーにヌル値が設定されます。この設定により、DNS サーバーは許可されず、デフォルトまたは指定のグループポリシーから値が継承されなくなります。DNS サーバー アドレスは最大 4 つ、IPv4 アドレスと IPv6 アドレスで 2 つずつ指定できます。

dns-server コマンドを入力するたびに、既存の設定がオーバーライドされます。たとえば、DNS サーバー **x.x.x.x** を設定し、次に DNS サーバー **y.y.y.y** を設定した場合、2 番目のコマンドは最初のコマンドを上書きし、**y.y.y.y** が唯一の DNS サーバーになります。サーバーを複数設定する場合も同様です。以前に設定された DNS サーバーを上書きする代わりにサーバーを追加するには、このコマンドを入力するときにすべての DNS サーバーの IP アドレスを含めます。

次に、**FirstGroup** という名前のグループポリシーで、IP アドレスが 10.10.10.15、10.10.10.30、2001:DB8::1、および 2001:DB8::2 の DNS サーバーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30
2001:DB8::1 2001:DB8::2
hostname(config-group-policy)#
```

ステップ 3 DefaultDNS DNS サーバーグループにデフォルトのドメイン名が指定されていない場合は、デフォルトドメインを指定する必要があります。たとえば、**example.com.** というドメイン名およびトップレベルドメインを使用します。

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

ステップ 4 （オプション）DHCP ネットワーク スコープを次のように設定します。

```
dhcp-network-scope {ip_address | none}
```

接続プロファイルのアドレスプールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用する DHCP サーバーで定義されているアドレスプールのサブセットを選択できます。

ネットワーク スコープを定義しない場合、DHCP サーバーはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

スコープを指定するには、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを入力します。DHCP サーバーは、この IP アドレスが属するサブネットを判別し、そのプールからの IP アドレスを割り当てます。

ルーティングの目的で可能な場合は常に、インターフェイスの IP アドレスを使用することを推奨します。たとえば、プールが 10.100.10.2 ～ 10.100.10.254 で、インターフェイスアドレスが 10.100.10.1/24 の場合、DHCP スコープとして 10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP は IPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

none を指定すると、たとえば、デフォルトまたは継承されたグループポリシーから DHCP アドレスが割り当てられなくなります。

例：

次の例では、FirstGroup の属性コンフィギュレーション モードを開始し、DHCP スコープを 10.100.10.1 に設定します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

スプリット トンネリング ポリシーの設定

IPv4 トラフィックのスプリット トンネリング ポリシーを指定して、トラフィックのトンネリング ルールを設定します。

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

IPv6 トラフィックのスプリット トンネリング ポリシーを指定して、トラフィックのトンネリング ルールを設定します。

ipv6-split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no ipv6-split-tunnel-policy

ポリシー オプションは次のとおりです。

- **tunnelspecified**：トンネルを通じてネットワーク リストに指定されているネットワークに対するすべてのトラフィックをトンネリングします。その他すべてのアドレスに対するデータは、クリアテキストで送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。

ASA 9.1.4 以降のバージョンでは、インクルード リストを指定するときに、インクルード範囲内のサブネットにエクスクルード リストも指定できます。除外されたサブネットのアドレスは、トンネリングされず、インクルード リストの残りの部分がトンネリングされます。エクスクルージョン リストのネットワークはトンネルを介して送信されません。エクスクルージョン リストは拒否エントリを使用して指定され、インクルージョン リストは許可エントリを使用して指定されます。

- **excludespecified** ネットワークリストに指定されているネットワークとの双方向のトラフィックをトンネリングしません。その他すべてのアドレスに対するトラフィックはトンネリングされます。を使用します。クライアント上でアクティブになっている VPN クライアントプロファイルでは、ローカル LAN アクセスを有効にしておく必要があります。このオプションは、セキュアクライアント クライアントでのみ機能します。



(注) インクルード リストのサブネットではないエクスクリージョン リスト内のネットワークは、クライアントで無視されます。

- **tunnelall** —すべてのトラフィックがトンネルを通過するよう指定します。このポリシーは、スプリット トンネリングをディセーブルにします。リモート ユーザーは企業ネットワークにアクセスできますが、ローカルネットワークへはアクセスできません。これがデフォルトのオプションです。



(注) スプリット トンネリングはセキュリティ機能ではなく、トラフィック管理機能です。最大限のセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

例

次に、IPv4 と IPv6 の FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

スプリット トンネリング用のネットワーク リストの指定

スプリットトンネリングでは、トンネルを通過するネットワークトラフィックがネットワークリストによって決定されます。セキュアクライアントは、ACL であるネットワークリストに基づいてスプリットトンネリングに関する決定を行います。

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

- **value access-list name** : トンネリングを実行するネットワークまたは実行しないネットワークを列挙した ACL を指定します。ACL には、IPv4 と IPv6 の両方のアドレスを指定する ACE が含まれている統合 ACL を指定できます。

- **none** : スプリット トンネリング用のネットワーク リストが存在しないことを示し、ASA はすべてのトラフィックをトンネリングします。**none** キーワードを指定すると、スプリット トンネリングのネットワーク リストにヌル値が設定され、スプリット トンネリングが拒否されます。また、これにより、デフォルトまたは指定されたグループポリシーから、デフォルトのスプリット トンネリング ネットワーク リストが継承されなくなります。

ネットワーク リストを削除するには、このコマンドの **no** 形式を入力します。すべてのスプリット トンネリング ネットワーク リストを削除するには、引数を指定せずに **no split-tunnel-network-list** コマンドを入力します。このコマンドにより、**none** キーワードを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのネットワーク リストが削除されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザーはデフォルトのグループポリシーまたは指定したグループポリシー内に存在するネットワーク リストを継承します。ユーザーがこのようなネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを入力します。

例

次に、FirstList という名前のネットワーク リストを作成し、FirstGroup という名前のグループポリシーに追加する例を示します。FirstList はエクスクリュージョンリストであり、エクスクリュージョン リストのサブネットであるインクルージョン リストです。

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

次に、v6 という名前のネットワーク リストを作成し、GroupPolicy_ipv6-ikev2 という名前のグループポリシーに v6 スプリット トンネル ポリシーを追加する例を示します。v6 はエクスクリュージョン リストであり、エクスクリュージョン リストのサブネットであるインクルージョン リストです。

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value v6
```

スプリットトンネル設定の確認

show runn group-policy attributes コマンドを実行して、設定を確認します。次の例は、管理者が IPv4 と IPv6 の両方のネットワーク ポリシーを設定し、両方のポリシーに対してネットワーク リスト（統合 ACL）**FirstList** を使用したことを示しています。

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
  split-tunnel-policy tunnelspecified
  ipv6-split-tunnel-policy tunnelspecified
  split-tunnel-network-list value FirstList
```

スプリットトンネリング用のドメイン属性の設定

デフォルトドメイン名、またはスプリットトンネルを介して解決する、スプリットDNSと呼ばれるドメインのリストを指定できます。

AnyConnect 3.1 は、Windows および Mac OS X のプラットフォームのツール スプリット DNS 機能をサポートします。セキュリティアプライアンスのグループポリシーにより Split-Include トンネリングがイネーブルになっており、トンネリング対象の DNS 名が指定されている場合、AnyConnect は、この名前に一致するすべての DNS クエリーをプライベート DNS サーバーにトンネリングします。ツール スプリット DNS を使用すると、ASA によってクライアントにプッシュダウンされたドメインに一致する DNS 要求へのトンネルアクセスのみが許可されます。これらの要求は、クリアテキストでは送信されません。一方、DNS 要求が ASA によってプッシュダウンされたドメインに一致しない場合は、AnyConnect は、クライアントのオペレーティングシステムにある DNS リゾルバから、DNS 解決に使用されるホスト名を暗号化せずに送信させます。



- (注) スプリット DNS は、標準クエリーおよび更新クエリー (A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など) をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。

Mac OS X の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのツール スプリット DNS を使用できます。

- グループポリシーで、スプリット DNS が 1 つの IP プロトコル (IPv4 など) に設定されており、クライアントバイパスプロトコルがもう片方の IP プロトコル (IPv6 など) に設定されている (後者の IP プロトコルにはアドレスプールは設定されていない)。
- スプリット DNS が両方の IP プロトコルに設定されている。

デフォルトのドメイン名の定義

ASA はセキュアクライアントにデフォルトドメイン名を渡します。クライアントは、ドメインフィールドを省略した DNS クエリーにドメイン名を追加します。このドメイン名は、トンネルパケットにだけ適用されます。デフォルトのドメイン名がない場合、ユーザーはデフォルトグループポリシーのデフォルトドメイン名を継承します。

グループポリシーのユーザーのデフォルトドメイン名を指定するには、グループポリシーコンフィギュレーションモードで **default-domain** コマンドを入力します。ドメイン名を削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# default-domain {value domain-name | none}
```

```
hostname(config-group-policy)# no default-domain [domain-name]
```

value domain-name パラメータは、グループのデフォルト ドメイン名を識別します。デフォルト ドメイン名が存在しないことを指定するには、**none** キーワードを入力します。このコマンドにより、デフォルト ドメイン名にヌル値が設定され、デフォルト ドメイン名が拒否されます。また、デフォルトまたは指定されたグループ ポリシーからデフォルト ドメイン名が継承されなくなります。

すべてのデフォルト ドメイン名を削除するには、引数を指定せずに **no default-domain** コマンドを入力します。このコマンドにより、**none** キーワードを指定し、**default-domain** コマンドを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのデフォルト ドメイン名が削除されます。**no** 形式を使用すると、ドメイン名の継承が許可されます。

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

スプリット トンネリング用のドメイン リストの定義

デフォルトのドメイン名のほかに、スプリット トンネルを介して解決されるドメインのリストを入力します。グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを入力します。リストを削除するには、このコマンドの **no** 形式を入力します。

スプリット トンネリング ドメインのリストがない場合、ユーザーはデフォルトのグループ ポリシー内に存在するリストを継承します。ユーザーがこのようなスプリット トンネリング ドメイン リストを継承しないようにするには、**none** キーワードを指定して **split-dns** コマンドを入力します。

すべてのスプリット トンネリング ドメイン リストを削除するには、引数を指定せずに **no split-dns** コマンドを入力します。これにより、**none** キーワードを指定して **split-dns** コマンドを発行して作成したヌル リストを含めて、設定済みのすべてのスプリット トンネリング ドメイン リストが削除されます。

パラメータ **value domain-name** では、ASA がスプリット トンネルを介して解決するドメイン名を指定します。**none** キーワードは、スプリット DNS リストが存在しないことを示します。また、このキーワードにより、スプリット DNS リストにヌル値が設定されます。そのため、スプリット DNS リストは拒否され、デフォルトまたは指定されたグループ ポリシーのスプリット DNS リストが継承されなくなります。このコマンドの構文は次のとおりです。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2... domain-nameN]
| none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

ドメインのリスト内で各エントリを区切るには、スペースを1つ入力します。エントリ数に制限はありませんが、ストリング全体の長さは492文字以下にします。英数字、ハイフン (-)、およびピリオド (.) のみを使用できます。デフォルト ドメイン名がトンネルを介して解決される場合は、そのドメイン名をこのリストに明示的に含める必要があります。

次の例は、FirstGroup という名前のグループ ポリシーで、Domain1、Domain2、Domain3、Domain4の各ドメインがスプリット トンネリングを介して解決されるように設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```



(注) スプリット DNS を設定する場合、指定したプライベート DNS サーバーが、クライアント プラットフォームに設定されている DNS サーバーと重複していないことを確認します。重複していると、名前解決が正しく動作せず、クエリーがドロップされる可能性があります。

Windows XP およびスプリット トンネリング用の DHCP 代行受信の設定

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、ASA で送信ルートの数を 27～40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信によって、Microsoft Windows XP クライアントは ASA でスプリット トンネリングを使用できるようになります。ASA は、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows XP 以前の Windows クライアントの場合、DHCP 代行受信によってドメイン名とサブネット マスクが提供されます。これは、DHCP サーバーを使用するのが効果的でない環境で役立ちます。

intercept-dhcp コマンドは、DHCP 代行受信をイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

netmask 変数で、トンネル IP アドレスのサブネット マスクを提供します。このコマンドの **no** 形式は、コンフィギュレーションから DHCP 代行受信を削除します。

[no] intercept-dhcp

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

リモート アクセス クライアントで使用するためのブラウザ プロキシ 設定の設定

クライアントのプロキシ サーバー パラメータを設定するには、次の手順を実行します。

手順

- ステップ1** グループポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力し、クライアント デバイスのブラウザのプロキシ サーバーとポートを設定します。

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

デフォルト値は **none** で、クライアント デバイスのブラウザでプロキシ サーバーの設定を指定していません。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

プロキシサーバーのIPアドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、ブラウザプロキシサーバーとして IP アドレス 192.168.10.1 を設定し、ポート 880 を使用し、FirstGroup というグループポリシーを対象にする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

- ステップ2** グループポリシー コンフィギュレーションモードで **msie-proxy method** コマンドを入力して、クライアント デバイスのブラウザプロキシアクション（「メソッド」）を設定します。

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify |  
no-proxy | use-server]
hostname(config-group-policy)#
```

デフォルト値は **no-modify** です。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy method [auto-detect | no-modify  
| no-proxy | use-server]
hostname(config-group-policy)#
```

使用できる方法は、次のとおりです。

- **auto-detect** : クライアント デバイスのブラウザでプロキシ サーバーの自動検出の使用をイネーブルにします。

- **no-modify** : このクライアント デバイスで使用しているブラウザの HTTP ブラウザ プロキシ サーバーの設定をそのままにします。
- **no-proxy**—このクライアント デバイスでは、ブラウザの HTTP プロキシ設定をディセーブルにします。
- **use-server—msie-proxy server** コマンドに設定された値を使用するように、ブラウザの HTTP プロキシ サーバー設定を設定します。

プロキシサーバーの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、FirstGroup というグループ ポリシーのブラウザ プロキシ設定として自動検出を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

次に、クライアント デバイスのサーバーとしてサーバー QASERVER、ポート 1001 を使用するように、FirstGroup というグループ ポリシーのブラウザ プロキシ設定を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAServer:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

ステップ 3 グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** コマンドを入力して、クライアント デバイスのブラウザがローカルでプロキシをバイパスするために使用するプロキシの例外リストを設定します。これらのアドレスは、プロキシサーバーによってアクセスされません。このリストは、[Proxy Settings] ダイアログボックスにある [Exceptions] ボックスに相当します。

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value server:port** : このクライアント デバイスに適用する MSIE サーバーの IP アドレスまたは名前、およびポートを指定します。ポート番号は任意です。
- **none** : IP アドレスまたはホスト名またはポートがないことを示し、例外リストを継承しません。

デフォルトでは、**msie-proxy except-list** はディセーブルになっています。

プロキシサーバーの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

次に、ブラウザのプロキシ例外リストを設定する例を示します。IP アドレス 192.168.20.1 のサーバーで構成され、ポート 880 を使用し、**FirstGroup** というグループポリシーを対象とします。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

ステップ 4 グループポリシー コンフィギュレーション モードで **msie-proxy local-bypass** コマンドを入力し、クライアントデバイスで使用するブラウザが、プロキシをローカルでバイパスする設定をイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

デフォルトでは、**msie-proxy local-bypass** はディセーブルになっています。

次に、**FirstGroup** というグループポリシーのブラウザのプロキシ ローカル バイパスをイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

IPSec (IKEv1) クライアントのセキュリティ属性の設定

グループのセキュリティ設定を指定するには、次の手順を実行します。

手順

ステップ 1 グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **password-storage** コマンドを使用し、ユーザーがログイン パスワードをクライアント システ

ムに保存できるようにするかどうかを指定します。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを使用します。

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

セキュリティ上の理由から、パスワード保存はデフォルトでディセーブルになっています。セキュアサイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。

password-storage 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

no 形式を指定すると、**password-storage** の値を別のグループ ポリシーから継承することができます。

このコマンドは、対話的なハードウェア クライアント認証やハードウェア クライアントの個別ユーザー認証には適用されません。

次に、**FirstGroup** という名前のグループ ポリシーに対してパスワード保存をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

ステップ 2 デフォルトではディセーブルになっている IP 圧縮をイネーブルにするかどうかを指定します。

(注)

IPSec IKEv2 接続では、IP 圧縮はサポートされていません。

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-comp** コマンドを入力します。IP 圧縮をディセーブルにするには、**disable** キーワードを指定して **ip-comp** コマンドを入力します。

ip-comp 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーの値を継承できます。

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```


データ圧縮をイネーブルにすると、モデムで接続するリモートダイヤルインユーザーのデータ伝送レートが向上する場合があります。

ヒント

データ圧縮を使用すると、ユーザーセッションごとのメモリ要求と CPU 使用率が増加し、結果として ASA のスループット全体が低下します。そのため、データ圧縮はモデムで接続しているリモートユーザーに対してだけイネーブルにすることを推奨します。モデムユーザーに固有のグループポリシーを設計し、それらのユーザーに対してだけ圧縮をイネーブルにします。

ステップ 3 グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **re-xauth** コマンドを使用し、IKE キーが再生成される際にユーザーが再認証を受ける必要があるかどうかを指定します。

(注)

IKEv2 接続では、IKE キー再生成はサポートされていません。

IKE キー再生成時の再認証をイネーブルにすると、ASA では、最初のフェーズ 1 IKE ネゴシエーションにおいてユーザーに対してユーザー名とパスワードの入力が求められ、その後 IKE キー再生成が行われるたびにユーザー認証が求められます。再認証によって、セキュリティが強化されます。

設定されているキー再生成間隔が極端に短い場合、ユーザーは認証を繰り返し求められることに不便を感じることがあります。認可要求が何度も繰り返されないようにするには、再認証をディセーブルにします。設定されているキー再生成インターバルを確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを入力して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータのキロバイト単位のライフタイムを表示します。IKE キーが再生成される際のユーザーの再認証をディセーブルにするには、**disable** キーワードを入力します。IKE キーが再生成される際の再認証は、デフォルトではディセーブルになっています。

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

IKE キーが再生成される際の再認証用の値を別のグループポリシーから継承することをイネーブルにするには、このコマンドの **no** 形式を入力して、実行コンフィギュレーションから **re-xauth** 属性を削除します。

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

(注)

接続先にユーザーが存在しない場合、再認証は失敗します。

ステップ 4 完全転送秘密をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、完全転送秘密により、新しい各暗号キーは以前のどのキーとも関連性がないことが保証されます。グループポリシーは、別のグループポリシーから完全転送秘密の値を継承できます。完全転送秘密は、デフォルトではディセーブルになっています。完全転送秘密をイネーブルにするに

は、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **pfs** コマンドを使用します。

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

完全秘密転送をディセーブルにするには、**disable** キーワードを指定して **pfs** コマンドを入力します。

完全秘密転送属性を実行コンフィギュレーションから削除して、値を継承しないようにするには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

IKEv1 クライアントの IPsec-UDP 属性の設定

IPsec over UDP（IPsec through NAT と呼ばれることもあります）を使用すると、ハードウェア クライアントは、NAT を実行している ASA に UDP 経由で接続できます。この機能はデフォルトではディセーブルになっています。IPsec over UDP は、リモートアクセス接続だけに適用される専用の機能で、モードコンフィギュレーションが必要です。ASA は、SA のネゴシエーション時にクライアントとの間でコンフィギュレーションパラメータをやり取りします。IPsec over UDP を使用すると、システム パフォーマンスが若干低下します。

IPsec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、次のように **enable** キーワードを指定して **ipsec-udp** コマンドを設定します。

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

IPsec over UDP を使用するには、この項の説明に従って、**ipsec-udp-port** コマンドも設定する必要があります。

IPsec over UDP をディセーブルにするには、**disable** キーワードを入力します。IPsec over UDP 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーから IPsec over UDP の値を継承できるようになります。

次に、FirstGroup というグループ ポリシーの IPsec over UDP を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

IPsec over UDP をイネーブルにした場合は、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドも設定する必要があります。このコマンドにより、IPsec over UDP 用の UDP ポート番号が設定されます。IPsec ネゴシエーションでは、ASA は設定されたポー

トでリッスンし、他のフィルタルールでUDPトラフィックがドロップされていても、そのポート宛てのUDPトラフィックを転送します。ポート番号の範囲は4001～49151です。デフォルトのポート値は10000です。

UDPポートをディセーブルにするには、このコマンドの **no** 形式を入力します。これにより、別のグループポリシーからIPsec over UDPポートの値を継承できるようになります。

```
hostname(config-group-policy)# ipsec-udp-port port
```

次に、FirstGroup というグループポリシーのIPsec UDPポートをポート4025に設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

VPN ハードウェア クライアントの属性の設定

手順

ステップ1 (任意) 次のコマンドを使用して、ネットワーク拡張モードを設定します。

[no] nem [enable |disable]

ネットワーク拡張モードを使用すると、ハードウェアクライアントは、単一のルーティング可能なネットワークをVPNトンネルを介してリモートプライベートネットワークに提供できません。PATは適用されません。したがって、EasyVPNサーバーの背後にあるデバイスは、EasyVPNリモートの背後にあるプライベートネットワーク上のデバイスに、トンネルを介して（トンネルを介してのみ）直接アクセスできます。逆の場合も同様です。トンネルはハードウェアクライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。

例：

次に、FirstGroup というグループポリシーのNEMを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

NEMをディセーブルにするには、**disable** キーワードを入力します。このNEM属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、別のグループポリシーの値を継承できます。

ステップ2 (任意) 次のコマンドを使用して、セキュアユニット認証を設定します。

[no] secure-unit-authentication [enable |disable]

セキュアユニット認証では、VPNハードウェアクライアントがトンネルを開始するたびにユーザー名とパスワードを使用した認証を要求することで、セキュリティが強化されます。この機

能をイネーブルにすると、ハードウェア クライアントは保存されているユーザー名とパスワードを使用しません（設定されている場合）。セキュア ユニット認証はデフォルトでディセーブルになっています。

セキュア ユニット認証では、ハードウェア クライアントが使用する接続プロファイルに対して認証サーバー グループが設定されている必要があります。プライマリ ASA でセキュア ユニット認証が必要な場合は、どのバックアップ サーバーにもセキュア ユニット認証を設定する必要があります。

（注）

この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザーがユーザー名とパスワードを入力する必要があります。

例：

次の例は、FirstGroup という名前のグループ ポリシーに対して、セキュア ユニット認証をイネーブルにする方法を示しています。

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

セキュア ユニット認証をディセーブルにするには、**disable** キーワードを入力します。セキュア ユニット認証属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを指定すると、他のグループ ポリシーからセキュア ユニット認証の値を継承できます。

ステップ 3 （任意） 次のコマンドを使用して、ユーザー認証を設定します。

[no] user-authentication [enable | disable]

ユーザー認証をイネーブルにすると、ハードウェア クライアントの背後にいる個々のユーザーは、トンネルを介してネットワークにアクセスするために認証を受けることが必要となります。個々のユーザーは、設定した認証サーバーの順序に従って認証されます。ユーザー認証はデフォルトでディセーブルになっています。

プライマリ ASA でユーザー認証が必要な場合は、どのバックアップ サーバーにもユーザー認証を設定する必要があります。

例：

次の例は、FirstGroup という名前のグループ ポリシーに対して、ユーザー認証をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

ユーザー認証をディセーブルにするには、**disable** キーワードを入力します。ユーザー認証属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、別のグループポリシーからユーザー認証の値を継承できます。

ステップ 4 次のコマンドを使用して、認証した個々のユーザーのアイドル タイムアウトを設定します。

[no] user-authentication-idle-timeout minutes | none]

minutes パラメータで、アイドルタイムアウト時間（分単位）を指定します。最短時間は1分、デフォルトは30分、最長時間は35791394分です。

アイドルタイムアウト期間中にハードウェアクライアントの背後のユーザーによる通信アクティビティがない場合、ASAはそのクライアントのアクセスを終了させます。このタイマーは、VPNトンネル自体ではなく、VPNトンネルを通過するクライアントのアクセスだけを終了します。

例：

次の例は、FirstGroup という名前のグループポリシーに45分のアイドルタイムアウト値を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)#user-authentication-idle-timeout 45
```

アイドルタイムアウト値を削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、他のグループポリシーからアイドルタイムアウト値を継承できます。アイドルタイムアウト値を継承しないようにするには、**none** キーワードを指定して **user-authentication-idle-timeout** コマンドを入力します。このコマンドにより、アイドルタイムアウトにヌル値が設定されます。ヌル値を設定すると、アイドルタイムアウトが拒否され、デフォルトまたは指定されたグループポリシーからユーザー認証のアイドルタイムアウト値が継承されなくなります。

(注)

show uauth コマンドへの応答で示されるアイドルタイムアウトは、常に Cisco Easy VPN リモートデバイスのトンネルを認証したユーザーのアイドルタイムアウト値になります。

ステップ 5 次のコマンドを使用して、IP Phone Bypass を設定します。

ip-phone-bypass enable

IP Phone Bypass を使用すると、ハードウェアクライアントの背後にある IP フォンが、ユーザー認証プロセスなしで接続できます。IP Phone Bypass は、デフォルトでディセーブルになっています。これは、IUA がイネーブルになっている場合にのみ適用されます。

(注)

また、これらのクライアントの認証を免除するには、クライアントに MAC アドレス免除を設定する必要があります。

IP Phone Bypass をディセーブルにするには、**disable** キーワードを入力します。IP Phone Bypass 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションにより、別のグループポリシーから IP Phone Bypass の値を継承できます。

ステップ 6 次のコマンドを使用して、LEAP Bypass を設定します。

leap-bypass enable

LEAP Bypass は、**user-authentication** がイネーブルになっている場合にのみ適用されます。このコマンドにより、Cisco ワイヤレス アクセス ポイントデバイスからの LEAP パケットは、

LEAP 認証を確立してから、ユーザー認証ごとに認証を実行できるようになります。LEAP Bypass は、デフォルトでディセーブルになっています。

ハードウェアクライアントの後ろにいる LEAP ユーザーには、面倒な問題があります。トンネルで中央サイト デバイスの後ろにある RADIUS サーバーにクレデンシャルを送信することができないため、LEAP 認証をネゴシエートできません。トンネル経由でクレデンシャルを送信できない理由は、無線ネットワークで認証されていないためです。この問題を解決するために、LEAP バイパスは、個別のユーザー認証の前に LEAP パケット（LEAP パケットだけ）をトンネルで転送し、RADIUS サーバーへの無線接続を認証できるようにします。これによって、ユーザーは、個別のユーザー認証に進むことができます。

LEAP Bypass は、次の条件下で適切に機能します。

- **secure-unit-authentication** がディセーブルになっていること。インタラクティブ ユニット認証がイネーブルの場合、トンネルを使用して LEAP デバイスが接続できるようになる前に、非 LEAP（有線）デバイスがハードウェアクライアントを認証する必要があります。
- **user-authentication** がイネーブルになっていること。イネーブルになっていないと、LEAP Bypass が適用されません。
- 無線環境のアクセス ポイントが、Cisco Discovery Protocol (CDP) を実行している Cisco Aironet Access Point であること。PC の NIC カードは、他のブランドの製品でもかまいません。

例：

次の例は、FirstGroup という名前のグループポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

LEAP Bypass をディセーブルにするには、**disable** キーワードを入力します。LEAP Bypass 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、LEAP Bypass の値を別のグループポリシーから継承できます。

セキュアクライアント 接続のグループポリシー属性の設定

「[AnyConnect VPN Client 接続（261 ページ）](#)」に示すように、セキュアクライアント接続をイネーブルにした後は、グループポリシーのセキュアクライアント機能をイネーブルまたは必須にできます。グループポリシー webvpn コンフィギュレーションモードで次の手順を実行します。

手順

ステップ 1 グループポリシー webvpn コンフィギュレーションモードを開始します。次に例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

ステップ 2 エンドポイントコンピュータ上でセキュアクライアントの永続的なインストールをディセーブルにするには、**none** キーワードを指定して **anyconnect keep-installer** コマンドを使用します。次に例を示します。

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

デフォルトでは、クライアントの永続的なインストールはイネーブルになっています。クライアントは、セキュアクライアントセッションの終了時にエンドポイントにインストールされたままになります。

ステップ 3 グループポリシーのセキュアクライアント SSL 接続経由で HTTP データの圧縮をイネーブルにするには、**anyconnect ssl compression** コマンドを入力します。デフォルトでは、圧縮は **none**（ディセーブル）に設定されています。圧縮をイネーブルにするには、**deflate** キーワードを使用します。次に例を示します。

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

ステップ 4 [デッドピア検出の設定（279 ページ）](#)

ステップ 5 デバイスが接続のアイドル状態を維持する時間を制限する場合でも、プロキシ、ファイアウォール、または NAT デバイス経由のセキュアクライアント 接続を開いたままにすることができます。これを行うには、**anyconnect ssl keepalive command:** を使用してキープアライブメッセージの頻度を調整します。

anyconnect ssl keepalive {none | seconds}

また、キープアライブを調整すると、リモートユーザーが Microsoft Outlook または Microsoft Internet Explorer などのソケットベース アプリケーションをアクティブに実行していない場合でも、セキュアクライアント クライアントは切断および再接続されません。

次の例では、セキュアクライアントがキープアライブメッセージを 300 秒（5 分）の頻度で送信できるようにセキュリティアプライアンスを設定します。

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

ステップ 6 セキュアクライアントが SSL セッションでキーを再生成できるようにするには、`anyconnect ssl rekey` コマンドを使用します。

```
anyconnect ssl rekey {method {ssl | new-tunnel} | time minutes | none}}
```

デフォルトでは、キー再生成はディセーブルになっています。

`method` を `new-tunnel` に指定すると、SVC キーの再生成中に セキュアクライアントが新しいトンネルを確立するように指定されます。`method` を `none` に指定すると、キー再生成はディセーブルになります。`method` を `ssl` に指定すると、SSL の再ネゴシエーションはキー再生成中に行われます。`method` を指定する代わりに、セッションの開始からキー再生成が行われるまでの時間を 1 ～ 10080 (1 週間) の分数で指定できます。

次の例では、キー再生成中に セキュアクライアントが SSL と再ネゴシエートするように設定し、キー再生成がセッション開始の 30 分後に発生するように設定しています。

```
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
hostname(config-group-webvpn)#
```

ステップ 7 クライアントプロトコルバイパス機能を使用すると、セキュアクライアントが IPv6 トラフィックだけを予期しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定することができます。

セキュアクライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ASA がセキュアクライアント接続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合に、ASA が IP アドレスを割り当てなかったネットワークトラフィックについて、クライアントプロトコルバイパスによってそのトラフィックをドロップさせるか、または ASA をバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するかを設定できるようになりました。

たとえば、ASA がセキュアクライアント接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされていると想定します。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアントバイパスプロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアントバイパスプロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリアテキストとして送信されます。

SSL 接続ではなく IPsec トンネルを確立している場合は、クライアントで IPv6 が有効になっているかどうか ASA に通知されないため、ASA は常にクライアントバイパスプロトコル設定をプッシュダウンします。

`client-bypass-protocol` コマンドを使用して、クライアントバイパスプロトコル機能をイネーブルまたはディセーブルにします。コマンド構文は次のとおりです。

```
client-bypass-protocol {enable | disable}
```

次に、クライアントバイパスプロトコルをイネーブルにする例を示します。

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

次に、クライアントバイパスプロトコルをディセーブルにする例を示します。


```
hostname(config-group-policy) # client-bypass-protocol disable  
hostname(config-group-policy) #
```

次に、イネーブルまたはディセーブルになっているクライアント バイパス プロトコル設定を削除する例を示します。

```
hostname(config-group-policy) # no client-bypass-protocol enable  
hostname(config-group-policy) #
```

ステップ 8 ASA 間にロードバランシングを設定した場合は、VPN セッションの再確立に使用される ASA IP アドレスを解決するために、ASA の FQDN を指定します。この設定は、さまざまな IP プロトコルのネットワーク間のクライアント ローミングをサポートするうえで重要です (IPv4 から IPv6 など)。

セキュアクライアント プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス (トンネルが確立されているデバイス) と一致しない場合があります。

デバイスの FQDN がクライアントに配信されない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル (IPv4 から IPv6) のネットワーク間のローミングをサポートするには、セキュアクライアントは、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合は常に、ASA によってプッシュされた (また、グループポリシーで管理者が設定した) デバイス FQDN を使用します。FQDN が設定されていない場合、ASA は、[Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得 (およびクライアントに送信) します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

gateway-fqdn コマンドを使用して、ASA の FQDN を設定します。コマンド構文は次のとおりです。

gateway-fqdn { value FQDN_Name | none } または **no gateway-fqdn**

次に、ASA の FQDN を ASAName.example.cisco.com として定義する例を示します。

```
hostname(config-group-policy) # gateway-fqdn value ASAName.example.cisco.com  
hostname(config-group-policy) #
```

次に、グループ ポリシーから ASA の FQDN を削除する例を示します。グループ ポリシーは、デフォルト グループ ポリシーからこの値を継承します。

```
hostname(config-group-policy) # no gateway-fqdn  
hostname(config-group-policy) #
```

次に、FQDN を空の値として定義する例を示します。hostname コマンドおよび domain-name コマンドを使用して設定されたグローバル FQDN が使用されます (使用可能な場合)。

```
hostname(config-group-policy)# gateway-fqdn none
hostname(config-group-policy)#
```

バックアップ サーバー属性の設定

バックアップ サーバーを設定します（使用する予定がある場合）。IPsec バックアップ サーバーを使用すると、VPN クライアントはプライマリ ASA が使用不可の場合も中央サイトに接続することができます。バックアップ サーバーを設定すると、ASA は、IPsec トンネルを確立するときにクライアントにサーバー リストを渡します。クライアント上またはプライマリ ASA 上にバックアップ サーバーを設定しない限り、バックアップ サーバーは存在しません。

バックアップ サーバーは、クライアント上またはプライマリ ASA 上に設定します。ASA 上にバックアップ サーバーを設定すると、バックアップ サーバー ポリシーがグループ内のクライアントにプッシュされ、クライアント上のバックアップ サーバー リスト（設定されている場合）が置き換わります。



- (注) ホスト名を使用する場合は、バックアップ DNS サーバーおよびバックアップ WINS サーバーを、プライマリ DNS サーバーおよびプライマリ WINS サーバーとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェアクライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバーとの接続が失われ、バックアップ サーバーに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。また、ホスト名を使用している場合に DNS サーバーが使用不可になると、大幅な遅延が発生するおそれがあります。

バックアップ サーバーを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを入力します。

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

バックアップ サーバーを削除するには、バックアップ サーバーを指定してこのコマンドの **no** 形式を入力します。backup-servers 属性を実行コンフィギュレーションから削除し、backup-servers の値を他のグループポリシーから継承できるようにするには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config キーワードは、クライアントでバックアップ サーバーを使用しないことを指定します。ASA は、ヌルのサーバー リストをプッシュします。

keep-client-config キーワードは、ASA がバックアップ サーバー情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバー リストを使用します（設定されている場合）。これはデフォルトです。

server1 server 2... server10 パラメータ リストは、プライマリの ASA が使用不可の場合に VPN クライアントが使用するサーバーをプライオリティ順にスペースで区切ったリストです。このリストには、サーバーを IP アドレスまたはホスト名で指定します。このリストの長さは 500 文字までで、格納できるエントリは最大 10 個までです。

次の例は、FirstGroup という名前のグループポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバーを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes  
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

ネットワーク アドミッションコントロールパラメータの設定

この項で説明するグループポリシー NAC コマンドには、すべてデフォルトの値があります。どうしても必要な場合を除き、これらのパラメータのデフォルト値は変更しないでください。

ASA は、拡張認証プロトコル (EAP) over UDP (EAPoUDP) のメッセージを使用して、リモートホストのポスチャを確認します。ポスチャ検証では、リモートホストにネットワークアクセスポリシーを割り当てる前に、そのホストがセキュリティの必要条件を満たしているかどうか調べられます。セキュリティアプライアンスでネットワークアドミッションコントロールを設定する前に、NAC 用に Access Control Server を設定しておく必要があります。

Access Control Server は、システムのモニタリング、レポートの作成、デバッグ、およびロギングに役立つ情報を示すポスチャトークン (ACS で設定可能な文字列) をセキュリティアプライアンスにダウンロードします。一般的なポスチャトークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。ポスチャ検証またはクライアントなしの認証が終わると、ACS はセッション用のアクセスポリシーをセキュリティアプライアンスにダウンロードします。

デフォルトのグループポリシーまたは代替グループポリシーのネットワークアドミッションコントロールを設定するには、次の手順を実行します。

手順

ステップ 1 (任意) ステータスクエリータイマーの期間を設定します。セキュリティアプライアンスは、ポスチャ検証が問題なく終わり、ステータスクエリーの応答を受け取るたびに、ステータスクエリーのタイマーを始動させます。このタイマーの期限が切れると、ホストのポスチャの変更を調べるクエリー (ステータスクエリー) が発行されます。タイマーの期限を 30 ～ 1800 の秒数で入力します。デフォルトの設定は 300 秒です。

ネットワークアドミッションコントロールのセッションで、ポスチャ検証が問題なく終わり、ポスチャの変更を調べる次のクエリーが発行されるまでの間隔を指定するには、グループポリシーコンフィギュレーションモードで **nac-sq-period** コマンドを使用します。

```
hostname(config-group-policy)# nac-sq-period seconds
hostname(config-group-policy)#
```

デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-sq-period [seconds]
hostname(config-group-policy)#
```

次に、ステータス クエリー タイマーの値を 1800 秒に変更する例を示します。

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)#
```

次の例では、デフォルト グループ ポリシーからステータス クエリー タイマーの値を継承しています。

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)#
```

ステップ 2 (任意) NAC の再検証の期間を設定します。セキュリティ アプライアンスは、ポスチャ検証が問題なく終わるたびに、再検証タイマーを始動させます。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。セキュリティ アプライアンスは、それまでと同じ方法でポスチャを再検証します。ポスチャ検証または再検証中にアクセスコントロール サーバーが使用できない場合、デフォルトのグループ ポリシーが有効になります。ポスチャを検証する間隔を秒数で入力します。範囲は 300 ～ 86400 秒です。デフォルトの設定は 36000 秒です。

ネットワーク アドミッション コントロールのセッションでポスチャを検証する間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-reval-period** コマンドを使用します。

```
hostname(config-group-policy)# nac-reval-period seconds
hostname(config-group-policy)#
```

再検証タイマーの値をデフォルト グループ ポリシーから継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac-reval-period [seconds]
hostname(config-group-policy)#
```

次に、再検証タイマーを 86400 秒に変更する例を示します。

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)#
```

次の例では、デフォルトのグループ ポリシーから再検証タイマーの値を継承しています。

```
hostname(config-group-policy) # no nac-reval-period
hostname(config-group-policy) #
```

ステップ3 (任意) NAC 用デフォルト ACL を設定します。セキュリティ アプライアンスは、ポストチャを検証できない場合に、選択された ACL に関連付けられているセキュリティ ポリシーを適用します。**none** または拡張 ACL を指定します。デフォルト設定は**none**です。**none** に設定すると、セキュリティ アプライアンスは、ポストチャを検証できなかったときにデフォルトのグループ ポリシーを適用します。

ポストチャを検証できなかったネットワーク アドミSSION コントロール セッションのデフォルト ACL として使用される ACL を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-default-acl** コマンドを使用します。

```
hostname(config-group-policy) # nac-default-acl {acl-name | none}
hostname(config-group-policy) #
```

デフォルトのグループ ポリシーから ACL を継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy) # no nac-default-acl [acl-name | none]
hostname(config-group-policy) #
```

このコマンドの要素は次のとおりです。

- **acl-name** : **aaa-server host** コマンドを使用して ASA に設定されている、ポストチャを検証するサーバーグループの名前を指定します。この名前は、そのコマンドに指定された **server-tag** 変数に一致する必要があります。
- **none** : デフォルト グループ ポリシーからの ACL の継承をディセーブルにし、NAC セッションでポストチャ検証ができなかったときに ACL を適用しません。

NAC はデフォルトでディセーブルになっているため、ASA を通過する VPN トラフィックは、NAC がイネーブルになるまで、NAC デフォルトの ACL の影響は受けません。

次の例では、ポストチャを検証できなかったときに、**acl-1** という ACL を適用するように指定しています。

```
hostname(config-group-policy) # nac-default-acl acl-1
hostname(config-group-policy) #
```

次の例では、デフォルト グループ ポリシーから ACL を継承しています。

```
hostname(config-group-policy) # no nac-default-acl
hostname(config-group-policy) #
```

次の例では、デフォルトグループポリシーからの ACL の継承をディセーブルにし、NAC セッションでポストチャを検証できなかったときに ACL を適用しません。

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

ステップ 4 VPN の NAC 免除を設定します。デフォルトでは、免除リストは空になっています。フィルタ属性のデフォルト値は **none** です。ポスチャ検証を免除するリモートホストのオペレーティングシステム（および ACL）ごとに **vpn-nac-exempt** コマンドを 1 回入力します。

ポスチャ検証を免除するリモートコンピュータのタイプのリストにエントリを追加するには、グループポリシー コンフィギュレーションモードで **vpn-nac-exempt** コマンドを使用します。

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

継承をディセーブルにし、すべてのホストをポスチャ検証の対象にするには、**vpn-nac-exempt** のすぐ後ろに **none** キーワードを入力します。

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

免除リストのエントリを削除するには、このコマンドの **no** 形式を使用し、削除するオペレーティングシステム（および ACL）を指定します。

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}] [disable]
hostname(config-group-policy)#
```

このグループポリシーに関連付けられている免除リストにある全エントリを削除し、デフォルトグループポリシーの免除リストを継承するには、キーワードを指定せずにこのコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

このコマンドの構文要素は次のとおりです。

- **acl-name** : ASA のコンフィギュレーションに存在する ACL の名前。
- **disable** : 免除リストのエントリを削除せずにディセーブルにします。
- **filter** : （オプション）コンピュータのオペレーティングシステムの名前が一致したときにトラフィックをフィルタリングするために ACL を適用します。
- **none** : このキーワードを **vpn-nac-exempt** のすぐ後ろに入力した場合は、継承がディセーブルになり、すべてのホストがポスチャ検証の対象になります。このキーワードを **filter** のすぐ後ろに入力した場合は、エントリで ACL を指定しないことを示します。
- **OS** : オペレーティングシステムをポスチャ検証から免除します。

- **os name** : オペレーティングシステムの名前です。名前にスペースが含まれている場合にのみ引用符が必要です（たとえば "Windows XP"）。

次の例では、継承がディセーブルにされ、すべてのホストがポスチャ検証の対象にされます。

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

次に、免除リストからすべてのエントリを削除する例を示します。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

ステップ 5 次のコマンドを入力して、ネットワーク アドミッション コントロールをイネーブルまたはディセーブルにします。

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

デフォルト グループ ポリシーから NAC の設定を継承するには、継承元の代替グループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

デフォルトでは、NAC はディセーブルになっています。NAC をイネーブルにすると、リモート アクセスでポスチャ検証が必要になります。リモート コンピュータのポスチャが正しいことが確認されると、ACS サーバーが ASA で使用するアクセス ポリシーをダウンロードします。NAC は、デフォルトではディセーブルになっています。

Access Control Server はネットワーク上に存在する必要があります。

次の例では、グループ ポリシーに対して NAC をイネーブルにします。

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)#
```

VPN クライアント ファイアウォール ポリシーの設定

ファイアウォールは、データの着信パケットと発信パケットをそれぞれ検査して、パケットのファイアウォール通過を許可するか、またはパケットをドロップするかどうかを決定することにより、コンピュータをインターネットから分離して保護します。ファイアウォールは、グループのリモートユーザーがスプリット トンネリングを設定している場合、セキュリティの向上をもたらします。この場合、ファイアウォールが、インターネットまたはユーザーのローカル LAN を経由する不正侵入からユーザーのコンピュータを保護し、ひいては企業ネットワー

クも保護します。VPN クライアントを使用して ASA に接続しているリモートユーザーは、適切なファイアウォール オプションを選択できます。

グループポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用して、ASA が IKE トンネル ネゴシエーション中に VPN クライアントに配信するパーソナルファイアウォールポリシーを設定します。ファイアウォールポリシーを削除するには、このコマンドの **no** 形式を入力します。

すべてのファイアウォールポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **client-firewall** コマンドを入力して作成したヌルポリシーがあればそれも含めて、設定済みのすべてのファイアウォールポリシーが削除されます。

ファイアウォールポリシーがなくなると、ユーザーはデフォルトまたはその他のグループポリシー内に存在するファイアウォールポリシーを継承します。ユーザーがこのようなファイアウォールポリシーを継承しないようにするには、**none** キーワードを指定して **client-firewall** コマンドを入力します。

[Client Firewall] タブの [Add or Edit Group Policy] ダイアログボックスでは、追加または変更するグループポリシーに対して VPN クライアントのファイアウォール設定を指定できます。



- (注) これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他（Windows 以外）のソフトウェア クライアントでは、これらの機能は使用できません。

最初のシナリオでは、リモートユーザーの PC 上にパーソナルファイアウォールがインストールされています。VPN クライアントは、ローカルファイアウォールで定義されているファイアウォールポリシーを適用し、そのファイアウォールが実行されていることを確認するためにモニターします。ファイアウォールの実行が停止すると、VPN クライアントは ASA への通信をドロップします（このファイアウォール適用メカニズムは **Are You There (AYT)** と呼ばれます。VPN クライアントが定期的に「are you there?」メッセージを送信することによってファイアウォールをモニターするからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしたため ASA への接続が終了したと認識します）。ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合がありますが、この方法を使用すれば、ユーザーは各自の設定をカスタマイズできます。

第2のシナリオでは、VPN クライアント PC のパーソナルファイアウォールに中央集中型ファイアウォールポリシーを適用することが選択されることがあります。一般的な例としては、スプリットトンネリングを使用してグループのリモート PC へのインターネットトラフィックをブロックすることが挙げられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、**プッシュポリシー**または **Central Protection Policy (CPP)** と呼ばれます。ASA では、VPN クライアントに適用するトラフィック管理ルールをセットを作成し、これらのルールをフィルタに関連付けて、そのフィルタをファイアウォールポリシーとして指定します。ASA はこのポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカルファイアウォールに渡し、そこでポリシーが適用されます。

セキュアクライアント ファイアウォールポリシーの設定

セキュアクライアントのファイアウォールルールでは、IPv4 アドレスおよび IPv6 アドレスを指定できます。

始める前に

IPv6 アドレスが指定された統合アクセス ルールを作成します。

手順

ステップ 1 webvpn 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。

webvpn

例 :

```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```

ステップ 2 プライベートまたはパブリック ネットワーク ルールのアクセス コントロール ルールを指定します。プライベート ネットワーク ルールが、クライアントの VPN 仮想アダプタ インターフェイスに適用されるルールです。

anyconnect firewall-rule client-interface {private | public} value [RuleName]

```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value
ClientFWRule
```

ステップ 3 グループ ポリシーのグループ ポリシー属性と webvpn ポリシー属性を表示します。

show runn group-policy [value]

例 :

```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
webvpn
    anyconnect firewall-rule client-interface private value ClientFWRule
```

ステップ 4 プライベート ネットワーク ルールからクライアント ファイアウォール ルールが削除されます。

no anyconnect firewall-rule client-interface private value [RuleName]

例 :

```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value
```

```
hostname (config-group-webvpn) #
```

Zone Labs Integrity サーバーの使用

この項では Zone Labs Integrity サーバー（Check Point Integrity サーバーとも呼ばれる）について説明し、Zone Labs Integrity サーバーをサポートするように ASA を設定する手順の例を示します。Integrity サーバーは、リモート PC 上でセキュリティ ポリシーを設定および実行するための中央管理ステーションです。リモート PC が Integrity サーバーによって指定されたセキュリティ ポリシーと適合しない場合、Integrity サーバーおよび ASA が保護するプライベートネットワークへのアクセス権が与えられません。

VPN クライアント ソフトウェアと Integrity クライアント ソフトウェアは、リモート PC 上に共に常駐しています。次の手順では、リモート PC と企業のプライベート ネットワーク間にセッションを確立する際のリモート PC、ASA、および Integrity サーバーのアクションをまとめます。

1. VPN クライアント ソフトウェア（Integrity クライアント ソフトウェアと同じリモート PC に常駐）は、ASA に接続し、それがどのタイプのファイアウォール クライアントであるかを ASA に知らせます。
2. ASA でクライアント ファイアウォールのタイプが承認されると、ASA から Integrity クライアントに Integrity サーバーのアドレス情報が返されます。
3. ASA はプロキシとして動作し、Integrity クライアントは Integrity サーバーとの制限付き接続を確立します。制限付き接続は、Integrity クライアントと Integrity サーバーの間だけで確立されます。
4. Integrity サーバーは、Integrity クライアントが指定されたセキュリティ ポリシーに準拠しているかどうかを特定します。Integrity クライアントがセキュリティ ポリシーに準拠している場合、Integrity サーバーから ASA に対して、接続を開いて接続の詳細をクライアントに提供するように指示されます。
5. リモート PC では、VPN クライアントから Integrity クライアントに接続の詳細が渡され、ポリシーの実施がただちに開始されること、また、Integrity クライアントがプライベートネットワークに接続できることが知らされます。
6. VPN 接続が確立すると、Integrity サーバーは、クライアント ハートビートメッセージを使用して Integrity クライアントの状態のモニターを続けます。



(注) ユーザー インターフェイスが最大 5 つの Integrity サーバーのコンフィギュレーションをサポートしている場合でも、現在のリリースの ASA が一度にサポートする Integrity サーバーは 1 つです。アクティブな Integrity サーバーに障害が発生した場合は、ASA 上に別の Integrity サーバーを設定してから、VPN クライアント セッションを再度確立します。

Integrity サーバーを設定するには、次の手順を実行します。

手順

ステップ 1 IP アドレス 10.0.0.5 を使用して Integrity サーバーを設定します。

```
zonelabs-integrity server-address {hostname1 | ip-address1}
```

例 :

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5
```

ステップ 2 ポート 300 を指定します (デフォルト ポートは 5054 です)。

```
zonelabs-integrity port port-number
```

例 :

```
hostname(config)# zonelabs-integrity port 300
```

ステップ 3 Integrity サーバーとの通信用に内部インターフェイスを指定します。

```
zonelabs-integrity interface interface
```

例 :

```
hostname(config)# zonelabs-integrity interface inside
```

ステップ 4 Integrity サーバーに障害があることを宣言して VPN クライアント接続を閉じる前に、ASA がアクティブまたはスタンバイ Integrity サーバーからの応答を 12 秒間待つようにします。

(注)

ASA と Integrity サーバーの間の接続で障害が発生した場合、エンタープライズ VPN が Integrity サーバーの障害によって中断されないように、デフォルトで VPN クライアント接続は開いたままになります。ただし、Zone Labs Integrity サーバーに障害が発生した場合、必要に応じて VPN 接続を閉じることができます。

```
zonelabs-integrity fail-timeout timeout
```

例 :

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

ステップ 5 ASA と Zone Labs Integrity サーバーとの接続に障害が発生した場合に VPN クライアントとの接続が閉じるよう、ASA を設定します。

```
zonelabs-integrity fail-close
```

例 :

```
hostname(config)# zonelabs-integrity fail-close
```

ステップ 6 設定された VPN クライアント接続の障害状態をデフォルトに戻して、クライアント接続が開いたままになるようにします。

`zonelabs-integrity fail-open`

例 :

`hostname(config)# zonelabs-integrity fail-open`

ステップ 7 Integrity サーバーが ASA のポート 300（デフォルトはポート 80）に接続して、サーバー SSL 証明書を要求するように指定します。

`zonelabs-integrity ssl-certificate-port cert-port-number`

例 :

`hostname(config)# zonelabs-integrity ssl-certificate-port 300`

ステップ 8 サーバーの SSL 証明書が常に認証される間、Integrity サーバーのクライアント SSL 証明書が認証されるように指定します。

`zonelabs-integrity ssl-client-authentication {enable | disable}`

例 :

`hostname(config)# zonelabs-integrity ssl-client-authentication enable`

ファイアウォール クライアント タイプの Zone Labs への設定

手順

	コマンドまたはアクション	目的
ステップ 1	ファイアウォール クライアント タイプを Zone Labs Integrity タイプに設定するには、次のコマンドを入力します。 例 : <code>hostname(config)# client-firewall req zonelabs-integrity</code>	client-firewall {opt req} zonelabs-integrity

次のタスク

詳細については、[VPN クライアント ファイアウォール ポリシーの設定（197 ページ）](#)を参照してください。ファイアウォールのタイプが **zonelabs-integrity** の場合、Integrity サーバーによってこれらのポリシーが決定されるため、ファイアウォールポリシーを指定するコマンド引数は使用されません。

クライアント ファイアウォールのパラメータの設定

次のコマンドを入力して、適切なクライアントファイアウォールのパラメータを設定します。各コマンドに設定できるインスタンスは1つだけです。詳細については、[VPN クライアント ファイアウォール ポリシーの設定 \(197 ページ\)](#) を参照してください。

- Cisco 統合ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated
acl-in ACL acl-out ACL
```

- Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

- ファイアウォールなし

```
hostname(config-group-policy)# client-firewall none
```

- カスタム ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num
product-id num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

- Zone Labs ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```



(注) ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバーによって決められます。

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm
policy {AYT | CPP acl-in ACL acl-out ACL}
```

```
hostname(config-group-policy)# client-firewall {opt | req}
zonelabs-zonealarmpro policy {AYT | CPP acl-in ACL acl-out ACL}
```

```
client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP
acl-in ACL acl-out ACL}
```

- Sygate Personal ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal
```

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro
```

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

- Network Ice、Black Ice ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

表 8: *client-firewall* コマンドのキーワードと変数

パラメータ	説明
acl-in ACL	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out ACL	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォールアプリケーションがファイアウォール ポリシーを制御することを指定します。ASA はファイアウォールが実行されていることを確認します。「Are You There?」という確認メッセージが表示されます。応答がない場合は、ASA によってトンネルが切断されます。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。
cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアントのファイアウォール ポリシーのソースとして Policy Pushed を指定します。
custom	カスタム ファイアウォール タイプを指定します。
description string	ファイアウォールの説明を示します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーにヌル値を設定して、ファイアウォールポリシーを拒否します。デフォルトのグループポリシーまたは指定されているグループ ポリシーからファイアウォールポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。

sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバー ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

次に、FirstGroup という名前のグループ ポリシーについて、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

クライアント アクセス ルールの設定

グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用して、ASA を介して IPsec で接続できるリモート アクセス クライアントのタイプとバージョンを制限するルールを設定します。次のガイドラインに従ってルールを作成します。

- ルールを定義しない場合、ASA はすべての接続タイプを許可します。
- クライアントがいずれのルールにも一致しない場合、ASA は接続を拒否します。拒否ルールを定義する場合は、許可ルールも1つ以上定義する必要があります。許可ルールを定義しないと、ASA はすべての接続を拒否します。
- ソフトウェアクライアントとハードウェアクライアントのどちらでも、タイプとバージョンは **show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。
- * 文字はワイルドカードです。ワイルドカードは各ルールで複数回入力することができます。たとえば、**client-access rul 3 deny type * version 3.*** では、バージョン 3.x のソフトウェアを実行しているすべてのクライアントタイプを拒否する、プライオリティ3のクライアント アクセス ルールが作成されます。
- 1つのグループ ポリシーにつき最大 25 のルールを作成できます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプまたはバージョン（あるいはその両方）を送信しないクライアントには、**n/a** を入力できます。

ルールを削除するには、このコマンドの **no** 形式を入力します。このコマンドは、次のコマンドと同等です。

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version 4.0
```

すべてのルールを削除するには、引数を指定せずに **no client-access-rule command** を入力します。これにより、**none** キーワードを指定して **client-access-rule** コマンドを発行して作成したヌルルールがあればそれも含めて、設定済みのすべてのルールが削除されます。

デフォルトでは、アクセスルールはありません。クライアントアクセスルールがない場合、ユーザーはデフォルトのグループ ポリシー内に存在するすべてのルールを継承します。

ユーザーがクライアントアクセスルールを継承しないようにするには、**none** キーワードを指定して **client-access-rule** コマンドを入力します。このコマンドの結果、すべてのタイプとバージョンのクライアントが接続できるようになります。

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type version {version | none}
```

```
hostname(config-group-policy)# no client-access rule [priority {permit | deny} type type version version]
```

次の表に、これらのコマンドのキーワードとパラメータの意味を示します。

表 9: *client-access rule* コマンドのキーワードと変数

パラメータ	説明
deny	特定のタイプとバージョンのデバイスの接続を拒否します。
none	クライアントアクセスルールを許可しません。client-access-rule をヌル値に設定します。これにより制限が許可されなくなります。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンのデバイスの接続を許可します。
<i>priority</i>	ルールのプライオリティを決定します。最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアントのタイプとバージョン（またはこのいずれか）に一致する最も小さい整数のルールが、適用されるルールとなります。値の小さいプライオリティルールに矛盾がある場合、ASA はそのルールを無視します。
type type	フリー形式の文字列を介してデバイスのタイプを識別します。文字列は、 show vpn-sessiondb remote で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。

パラメータ	説明
version version	7.0などの自由形式の文字列を使用して、デバイスバージョンを指定します。文字列は、 show vpn-sessiondb remote で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。

次に、FirstGroup という名前のグループ ポリシーのクライアント アクセス ルールを作成する例を示します。これらのルールは、バージョン 4.x のソフトウェアを実行する Cisco VPN Client を許可し、すべての Windows NT クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version
*
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client"
version 4.*
```



(注) 「type」フィールドは、任意の値が許可される自由形式の文字列ですが、その値は、接続時にクライアントから ASA に送信される固定値と一致している必要があります。

ユーザー属性の設定

この項では、ユーザー属性とその設定方法について説明します。

デフォルトでは、ユーザーは、割り当てられているグループポリシーからすべてのユーザー属性を継承します。また、ASA では、ユーザー レベルで個別に属性を割り当て、そのユーザーに適用されるグループポリシーの値を上書きすることができます。たとえば、すべてのユーザーに営業時間内のアクセスを許可し、特定のユーザーに24時間のアクセスを許可するグループポリシーを指定することができます。

ユーザー名のコンフィギュレーションの表示

グループポリシーから継承したデフォルト値も含めて、すべてのユーザー名のコンフィギュレーションを表示するには、次のように、**all** キーワードを指定して **show running-config username** コマンドを入力します。

```
hostname# show running-config all username
hostname#
```

このコマンドは、すべてのユーザーまたは特定のユーザー（ユーザー名を指定した場合）の暗号化されたパスワードと特権レベルを表示します。**all** キーワードを省略すると、明示的に設定された値だけがこのリストに表示されます。次の例は、このコマンドで **testuser** というユーザーを指定した場合の出力を示します。

```
hostname# show running-config all username testuse
username testuser password l2RsxXQnphyr/I9Z encrypted privilege 15
```

個々のユーザーの属性の設定

特定のユーザーを設定するには、**username** コマンドを使用してユーザー名モードに入り、ユーザーにパスワード（パスワードなしも可）と属性を割り当てます。指定しなかったすべての属性は、グループ ポリシーから継承されます。

内部ユーザー認証データベースは、**username** コマンドを使用して入力されたユーザーで構成されています。**login** コマンドでは、このデータベースを認証用に使用します。ユーザーを ASA データベースに追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザーを削除するには、削除するユーザー名を指定して、このコマンドの **no** バージョンを使用します。すべてのユーザー名を削除するには、ユーザー名を指定せずに、**clear configure username** コマンドを使用します。

ユーザーのパスワードと特権レベルの設定

ユーザーにパスワードと特権レベルを割り当てるには、**username** コマンドを入力します。**nopassword** キーワードを入力すると、このユーザーにパスワードが不要であることを指定できます。パスワードを指定する場合は、そのパスワードを暗号化形式で保存するかどうかを指定できます。

オプションの **privilege** キーワードにより、このユーザーの特権レベルを設定できます。特権レベルの範囲は 0（最低）～15 です。一般に、システム管理者は最高の特権レベルを持ちます。デフォルトのレベルは 2 です。

```
hostname(config)# username name {nopassword | password password [encrypted] }
[privilege priv_level]}
```

```
hostname(config)# no username [name]
```

下記の表に、このコマンドで使用するキーワードと変数の意味を示します。

username コマンドのキーワードと変数

キーワード/変数	意味
encrypted	パスワードの暗号化を指定します。
<i>name</i>	ユーザーの名前を指定します。
nopassword	このユーザーにパスワードが必要ないことを示します。
password password	このユーザーにパスワードが存在することを示し、パスワードを指定します。

キーワード/変数	意味
privilege priv_level	このユーザーの特権レベルを設定します。範囲は 0 ～ 15 です。この数値が低いほど、コマンドの使用や ASA の管理に関する機能が限定されます。デフォルトの特権レベルは 2 です。システム管理者の通常の特権レベルは 15 です。

デフォルトでは、このコマンドで追加した VPN ユーザーには属性またはグループポリシーが関連付けられません。すべての値を明示的に設定する必要があります。

次の例は、暗号化されたパスワードが pw_12345678 で、特権レベルが 12 の anyuser という名前のユーザーを設定する方法を示しています。

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege
12
hostname(config)#
```

ユーザー属性の設定

ユーザーのパスワード（存在する場合）と特権レベルの設定後は、その他の属性を設定します。これらは任意の順序で設定できます。任意の属性と値のペアを削除するには、このコマンドの **no** 形式を入力します。

attributes キーワードを指定して **username** コマンドを入力して、ユーザー名モードに入ります。

```
hostname(config)# username name attributes
hostname(config-username)#
```

プロンプトが変化し、新しいモードになったことが示されます。これで属性を設定できます。

VPN ユーザー属性の設定

VPN ユーザー属性は、次の項で説明するように、VPN 接続に固有の値を設定します。

継承の設定

ユーザーが、それまでにユーザー名レベルで設定されていない属性の値をグループポリシーから継承するようにできます。このユーザーが属性を継承するグループポリシーの名前を指定するには、**vpn-group-policy** コマンドを入力します。デフォルトでは、VPN ユーザーにはグループポリシーが関連付けられていません。

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

ユーザー名モードで利用できる属性の場合、ユーザー名モードで設定すると、特定のユーザーに関してグループポリシーにおける属性の値を上書きできます。

次に、FirstGroup という名前のグループ ポリシーから属性を使用するように anyuser という名前のユーザーを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

アクセス時間の設定

設定済みの time-range ポリシーの名前を指定して、このユーザーがシステムへのアクセスを許可される時間を関連付けます。

この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、他のグループ ポリシーから time-range 値を継承できます。値を継承しないようにするには、**vpn-access-hours none** コマンドを入力します。デフォルトでは、アクセスは無制限です。

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

次の例は、anyuser という名前のユーザーを 824 と呼ばれる time-range ポリシーに関連付ける方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

最大同時ログイン数の設定

このユーザーに許可される同時ログインの最大数を指定します。指定できる範囲は 0 ～ 2147483647 です。デフォルトの同時ログイン数は、3 です。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。ログインをディセーブルにしてユーザーのアクセスを禁止するには、0 を入力します。

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```



(注) 同時ログインの最大数の制限は非常に大きなものですが、複数の同時ログインを許可すると、セキュリティが低下し、パフォーマンスに影響を及ぼすことがあります。

次の例は、anyuser という名前のユーザーに最大 4 つの同時ログインを許可する方法を示しています。

```
hostname(config)# username anyuser attributes
```

```
hostname(config-username)# vpn-simultaneous-logins 4  
hostname(config-username)#
```

アイドル タイムアウトの設定

手順

ステップ 1 (任意) VPN アイドル タイムアウト期間を設定するには、グループ ポリシー コンフィギュレーションモードまたはユーザー名コンフィギュレーションモードで **vpn-idle-timeout minutes** コマンドを使用します。

この期間中に接続上で通信アクティビティがない場合、ASAは接続を終了します。最小時間は1分、最大時間は35791394分であり、デフォルトは30分です。

次の例は、FirstGroup という名前のグループ ポリシーに15分のVPN アイドル タイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes  
hostname(config-group-policy)# vpn-idle-timeout 15  
hostname(config-group-policy)#
```

[no] vpn-idle-timeout {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- VPN アイドル タイムアウトを無効にし、タイムアウト値を継承しないようにするには、**vpn-idle-timeout none** を入力します。

```
hostname(config)# group-policy FirstGroup attributes  
hostname(config-group-policy)# vpn-idle-timeout none  
hostname(config-group-policy)#
```

これにより、セキュアクライアント (SSL と IPsec/IKEv2 の両方) およびクライアントレス VPN がグローバル **webvpn default-idle-timeout seconds** 値を使用するようになります。このコマンドは、**webvpn** コンフィギュレーション モードで入力します。たとえば、**hostname(config-webvpn)# default-idle-timeout 300** のように入力します。デフォルトは1800秒 (30分) で、範囲は60 ~ 86400秒です。

すべての webvpn 接続において、**default-idle-timeout** 値が適用されるのは、グループ ポリシー/ユーザー名属性に **vpn-idle-timeout none** が設定されている場合のみです。すべてのセキュアクライアント 接続で、ASA によりゼロ以外のアイドルタイムアウト値が要求されます。

サイト間 (IKEv1、IKEv2) および IKEv1 リモートアクセス VPN の場合は、タイムアウトをディセーブルにし、無制限のアイドル期間を許可することを推奨します。

- このグループ ポリシーまたはユーザー ポリシーのアイドル タイムアウトを無効にするには、**no vpn-idle-timeout** を入力します。値は継承されます。
- **vpn-idle-timeout** をまったく設定しない場合、値は継承されます。デフォルトは30分です。

ステップ 2 (任意) オプションで、**vpn-idle-timeout alert-interval** {minutes} コマンドを使用して、アイドル タイムアウトのアラート メッセージがユーザーに表示される時間を設定できます。

このアラート メッセージは、VPN セッションが非アクティブ状態のため切断されるまでに何分あるかをユーザーに伝えます。デフォルトのアラート間隔は 1 分です。

次の例は、anyuser という名前のユーザーに 3 分の VPN アイドル タイムアウトのアラート間隔を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

[no] **vpn-idle-timeout alert-interval** {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- **none** パラメータは、ユーザーが通知を受信しないことを示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- このグループまたはユーザー ポリシーのアラート間隔を削除するには、**no vpn-idle-timeout alert-interval** を入力します。値は継承されます。
- このパラメータをまったく設定しない場合、デフォルトのアラート間隔は 1 分です。

最大接続時間の設定

手順

ステップ 1 (任意) グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **vpn-session-timeout** {minutes} コマンドを使用して、VPN 接続の最大時間を設定します。

最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。この期間が終了すると、ASA は接続を終了します。

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

次の例は、anyuser という名前のユーザーに 180 分の VPN セッション タイムアウトを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
```

```
hostname(config-username)#
```

[no] vpn-session-timeout {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- このポリシーから属性を削除し、継承を許可するには、このコマンドの **no vpn-session-timeout** 形式を入力します。
- 無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**vpn-session-timeout none** を入力します。

ステップ 2 vpn-session-timeout alert-interval {minutes | } コマンドを使用して、セッション タイムアウトのアラート メッセージがユーザーに表示される時間を設定します。

このアラート メッセージは、VPN セッションが自動的に切断されるまでに何分あるかをユーザーに伝えます。次に、VPN セッションが切断される 20 分前にユーザーに通知されるよう指定する例を示します。1 ～ 30 分の範囲を指定できます。

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

[no] vpn-session-timeout alert-interval {minutes | none} コマンドを使用したその他のアクションは次のとおりです。

- VPN セッションタイムアウトアラート間隔属性がデフォルト グループポリシーから継承されることを示すには、このコマンドの **no** 形式を使用します。

```
hostname(config-webvpn)# no vpn-session-timeout alert-interval
```

- **vpn-session-timeout alert-interval none** は、ユーザーが通知を受信しないことを示します。

ACL フィルタの適用

VPN 接続用のフィルタとして使用する、事前に設定されたユーザー固有の ACL の名前を指定します。ACL を拒否し、グループポリシーから ACL を継承しないようにするには、**none** キーワードを指定して **vpn-filter** コマンドを入力します。**vpn-filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、グループポリシーから値を継承できます。このコマンドには、デフォルトの動作や値はありません。

ACL を設定して、このユーザーについて、さまざまなタイプのトラフィックを許可または拒否します。VPN フィルタは初期接続にのみ適用されます。アプリケーション インспекションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。次に、**vpn-filter** コマンドを使用して、それらの ACL を適用します。

```
hostname(config-username)# vpn-filter {value ACL_name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```



(注) クライアントレス SSL VPN では、**vpn-filter** コマンドで定義された ACL は使用されません。

次に、anyuser という名前のユーザーの、acl_vpn という ACL を呼び出すフィルタを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

IPv4 アドレスとネットマスクの指定

特定のユーザーに割り当てる IP アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)#
```

次に、anyuser という名前のユーザーに IP アドレス 10.92.166.7 を設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)#
```

前の手順で指定した IP アドレスに使用するネットワーク マスクを指定します。

no vpn-framed-ip-address コマンドを使用した場合は、ネットワーク マスクを指定しないでください。サブネット マスクを削除するには、このコマンドの **no** 形式を入力します。デフォルトの動作や値はありません。

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)#
```

次の例は、anyuser という名前のユーザーに、サブネット マスク 255.255.255.254 を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)#
```

IPv6 アドレスとネットマスクの指定

特定のユーザーに割り当てる IPv6 アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
```



```
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

次に、**anyuser** という名前のユーザーに IP アドレスとネットマスク 2001::3000:1000:2000:1/64 を設定する例を示します。このアドレスは、プレフィックス値 2001:0000:0000:0000 および インターフェイス ID 3000:1000:2000:1 を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

トンネル プロトコルの指定

このユーザーが使用できる VPN トンネルのタイプ (IPsec またはクライアントレス SSL VPN) を指定します。デフォルトは、デフォルト グループ ポリシーから取得される値で、IPsec になります。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

このコマンドのパラメータの値は、次のとおりです。

- **IPsec**—2 つのピア (リモート アクセス クライアントまたは別のセキュア ゲートウェイ) 間の IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **webvpn**—HTTPS 対応 Web ブラウザ経由でリモート ユーザーにクライアントレス SSL VPN アクセスを提供します。クライアントは不要です。

このコマンドを入力して、1 つ以上のトンネリングモードを設定します。VPN トンネルを介して接続するユーザーには、少なくとも 1 つのトンネリングモードを設定する必要があります。

次の例は、**anyuser** という名前のユーザーにクライアントレス SSL VPN および IPsec トンネリングモードを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

リモート ユーザー アクセスの制限

value キーワードを指定して **group-lock** 属性を設定することにより、指定した既存の接続プロファイルだけを介してアクセスするようにリモート ユーザーを制限します。**group-lock** は、VPN クライアントで設定されたグループが、そのユーザーが割り当てられている接続プロファイルと同じかどうかをチェックすることによって、ユーザーを制限します。一致していない場

合、ASA はユーザーが接続できないようにします。グループロックを設定しない場合、ASA は、割り当てられたグループとは関係なく、ユーザーを認証します。

group-lock 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、値をグループポリシーから継承できます。**group-lock** をディセーブルにし、デフォルトまたは指定されたグループポリシーから **group-lock** の値を継承しないようにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

次の例は、**anyuser** という名前のユーザーにグループ ロックを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

ソフトウェア クライアント ユーザーのパスワード保存のイネーブル化

ユーザーがログインパスワードをクライアントシステム上に保存するかどうかを指定します。パスワード保存は、デフォルトでディセーブルになっています。セキュアサイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを入力します。**password-storage** 属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、**password-storage** の値をグループ ポリシーから継承できます。

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザー認証には関係ありません。

次の例は、**anyuser** という名前のユーザーでパスワード保存をイネーブルにする方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```

VPN フィルタ ACL の設定と調整に関するベストプラクティス

このセクションでは、トラフィックの中断なしに既存の VPN フィルタ ACL を更新する際に従うべきベストプラクティスを示します。

既存の VPN フィルタ ACL を更新する

ASA デバイスに適用されている vpn-filter ACL を更新するには、次の手順を実行します。

1. システムで新しい vpn-filter ACL を作成します（例：*new_acl.txt*）。
2. デバイスから現在の vpn-filter ACL をダウンロードします（例：*old_acl.txt*）。
3. 次のように、ACL の変更手順を作成します。

```
* Add update in-progress to ACL remark
echo ?access-list <name> line 1 ACL update in-progress? > push.txt
* Delete old rules
sed ?s/^/no /g? old_acl >> push.txt
* Add new rules
cat new_acl >> push.txt
* Remove update in-progress to ACL remark
echo ?no access-list <name> ACL update in-progress? >> push.txt
```

4. push.txt をデバイスにアップロードします。

既存の VPN フィルタ ACL を新しいものに置き換える

ASA デバイスに適用されている vpn-filter ACL を置き換えるには、次の手順を実行します。

1. 既存の vpn-filter ACL を置き換えるときは毎回新しいものを作成します。
2. 作成した vpn-filter ACL を使用してグループポリシーを更新します。
3. デバイスに適用されていた古い vpn-filter ACL を削除します。



第 6 章

VPN の IP アドレス

- [IP アドレス割り当てポリシーの設定 \(219 ページ\)](#)
- [ローカル IP アドレス プールの設定 \(221 ページ\)](#)
- [AAA アドレス指定の設定 \(223 ページ\)](#)
- [DHCP アドレス指定の設定 \(224 ページ\)](#)

IP アドレス割り当てポリシーの設定

ASA では、リモートアクセスクライアントに IP アドレスを割り当てる際に、次の 1 つ以上の方式を使用できます。複数のアドレス割り当て方式を設定すると、ASA は IP アドレスが見つかるまで各オプションを検索します。デフォルトでは、すべての方式がイネーブルになっています。

- **aaa** ユーザー単位で外部認証、認可、アカウンティング サーバーからアドレスを取得します。IP アドレスが設定された認証サーバーを使用している場合は、この方式を使用することをお勧めします。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
- **dhcp** DHCP サーバーから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバーを設定する必要があります。また、DHCP サーバーで使用可能な IP アドレスの範囲も定義する必要があります。この方法は IPv4 の割り当てポリシーに使用できます。
- **local** : 内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。ローカルを選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
 - **[Allow the reuse of an IP address so many minutes after it is released]** : IP アドレスがアドレス プールに戻された後に、IP アドレスを再利用するまでの時間を指定します。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、ASA は遅延時間を課しません。この設定要素は、IPv4 割り当てポリシーで使用できます。

次のいずれかの方式を使用して、IP アドレスをリモート アクセス クライアントに割り当てる方法を指定します。

IPv4 アドレス割り当ての設定

手順

ASA のアドレス割り当て方式を有効にして、IPv4 アドレスを VPN 接続に割り当てるときに使用します。IP アドレスを取得する使用可能な方式は、AAA サーバー、DHCP サーバー、またはローカルアドレス プールからの取得です。これらの方式はすべてデフォルトでイネーブルになっています。

```
vpn-addr-assign {aaa | dhcp | local [reuse-delay minutes]}
```

例：

たとえば、IP アドレスが解放された後に 0～480 分間の IP アドレスの再使用を設定できます。

```
hostname(config)#vpn-addr-assign aaa  
hostname(config)#vpn-addr-assign local reuse-delay 180
```

この例では、コマンドの **no** 形式を使用してアドレス割り当て方式を無効にします。

```
hostname(config)# no vpn-addr-assign dhcp
```

IPv6 アドレス割り当ての設定

手順

ASA のアドレス割り当て方式を有効にして、IPv6 アドレスを VPN 接続に割り当てるときに使用します。IP アドレスを取得する使用可能な方式は、AAA サーバーまたはローカルアドレス プールからの取得です。これら両方の方式はデフォルトでイネーブルになっています。

```
ipv6-vpn-addr-assign {aaa | local}
```

例：

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

この例では、コマンドの **no** 形式を使用してアドレス割り当て方式を無効にします。

```
hostname(config)# no ipv6-vpn-addr-assign local
```

アドレス割り当て方式の表示

手順

ASA で設定されているアドレス割り当て方式を表示するには、次のいずれかの方式を使用します。

- IPv4 アドレス割り当ての表示

設定されているアドレス割り当て方式を表示します。設定されているアドレス方式は、aaa、dhcp、または local です。

```
show running-config all vpn-addr-assign
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local
```

- IPv6 アドレス割り当ての表示

設定されているアドレス割り当て方式を表示します。設定されているアドレス方式は、aaa または local となります。

```
show running-config all ipv6-vpn-addr-assign
ipv6-vpn-addr-assign aaa
ipv6-vpn-addr-assign local reuse-delay 0
```

ローカル IP アドレス プールの設定

VPN リモート アクセス トンネルに使用する IPv4 アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを入力します。アドレス プールを削除するには、このコマンドの **no** 形式を入力します。

VPN リモート アクセス トンネルに使用する IPv6 アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ipv6 local pool** コマンドを入力します。アドレス プールを削除するには、このコマンドの **no** 形式を入力します。

ASA は、接続用の接続プロファイルまたはトンネル グループに基づいてアドレス プールを使用します。プールの指定順序は重要です。接続プロファイルまたはグループポリシーに複数のアドレス プールを設定すると、ASA は追加された順でそれらのプールを使用します。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。



(注) アクティブなトンネルグループ内で現在使用されている（つまり、接続のためにエンドユーザーが利用できる）既存のアドレスプールを変更する場合は、変更ウィンドウで変更を行う必要があります。その際、次のことを確認してください。

- 接続されているユーザーはログオフされます。
- トンネルグループからアドレスプールが削除され、必要に応じて変更されます。
- 変更されたアドレスプールがトンネルグループに再び追加されます。

これ以外の方法でアドレスプールを変更すると、ASA の動作に不整合が生じる可能性があります。

ローカル IPv4 アドレス プールの設定



(注) CLI で、アクティブなトンネルグループ内で現在使用されている（つまり、接続のためにエンドユーザーが利用できる）既存のアドレスプールを変更する場合は、変更ウィンドウでこの変更を行うことを推奨します。接続されたユーザーをログオフし、アドレスプールをトンネルグループから削除し、必要に応じて変更してから、トンネルグループに再度追加する必要があります。これ以外の方法でアドレスプールを変更すると、ASA の動作に不整合が生じる可能性があります。

手順

ステップ 1 アドレス割り当て方式として IP アドレス プールを設定します。**local** 引数を指定して **vpn-addr-assign** コマンドを入力します。

例：

```
hostname(config)# vpn-addr-assign local
```

ステップ 2 アドレス プールを設定します。このコマンドは、プールの名前を指定し、IPv4 アドレスとサブネット マスクの範囲を指定します。

ip local pool *poolname* *first_address-last_address* *mask* *mask*

例：

この例では、*firstpool* という IP アドレス プールを設定します。開始アドレスは 10.20.30.40、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

この例では、**firstpool** という IP アドレス プールを削除します。


```
hostname(config)# no ip local pool firstpool
```

ローカル IPv6 アドレス プールの設定

手順

- ステップ 1** アドレス割り当て方式として IP アドレス プールを設定します。**local** 引数を指定して **ipv6-vpn-addr-assign** コマンドを入力します。

例：

```
hostname(config)# ipv6-vpn-addr-assign local
```

- ステップ 2** アドレスプールを設定します。このコマンドは、プールに名前を指定し、開始 IPv6 アドレス、ビット単位のプレフィックス長、および範囲内で使用するアドレスの数を特定します。

ipv6 local pool pool_name starting_address prefix_length number_of_addresses

例：

この例では、*ipv6pool* という IP アドレス プールを設定します。開始アドレスは 2001:DB8::1、プレフィックス長は 32 ビット、プールで使用するアドレス数は 100 です。

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

この例では、*ipv6pool* という IP アドレス プールを削除します。

```
hostname(config)# no ipv6 local pool ipv6pool
```

AAA アドレス指定の設定

AAA サーバーを使用して VPN リモートアクセスクライアントにアドレスを割り当てるには、まず AAA サーバーまたは AAA サーバー グループを設定する必要があります。コマンドリファレンスで **aaa-server protocol** コマンドを参照してください。

また、ユーザーは RADIUS 認証用に設定された接続プロファイルと一致している必要があります。

次の例は、*firstgroup* という名前のトンネルグループに、*RAD2* という AAA サーバー グループを定義する方法を示しています。例の中に 1 つ余分な手順が入っていますが、これは以前にそのトンネルグループに名前を付け、トンネルグループタイプを定義していた場合のためです。この手順が次の例に記載されているのは、これらの値を設定しない限り、後続の **tunnel-group** コマンドにアクセスできないので、注意を促すためです。

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config)# authentication-server-group RAD2
```

IP アドレッシング用に AAA を設定するには、次の手順を実行します。

手順

- ステップ 1** アドレス割り当て方式として AAA を設定するには、**aaa** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

- ステップ 2** **firstgroup** というトンネルグループをリモートアクセスまたは LAN-to-LAN トンネルグループとして確立するには、**type** キーワードを指定して **tunnel-group** コマンドを入力します。次の例では、リモートアクセス トンネルグループを設定しています。

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

- ステップ 3** 一般属性コンフィギュレーションモードに入り、**firstgroup** というトンネルグループの AAA サーバーグループを定義するには、**general-attributes** 引数を指定して **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

- ステップ 4** 認証に使用する AAA サーバーグループを指定するには、**authentication-server-group** コマンドを入力します。

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

次のタスク

このコマンドには、この例で示すより多くの引数があります。詳細については、コマンドリファレンスを参照してください。

DHCP アドレス指定の設定

DHCP を使用して VPN クライアントのアドレスを割り当てるには、まず DHCP サーバー、およびその DHCP サーバーで使用可能な IP アドレスの範囲を設定する必要があります。その後、接続プロファイル単位で DHCP サーバーを定義します。また、オプションとして、該当の接続

プロファイルまたはユーザー名に関連付けられたグループポリシー内に、DHCP ネットワーク スコープも定義できます。

次の例では、**firstgroup** という名前の接続プロファイルに、172.33.44.19 の DHCP サーバーを定義しています。この例では、**remotegroup** というグループポリシーに対して、10.100.10.1 の DHCP ネットワーク スコープも定義しています。（**remotegroup** というグループポリシーは、**firstgroup** という接続プロファイルに関連付けられています）。ネットワーク スコープを定義しない場合、DHCP サーバーはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

始める前に

IPv4 アドレスを使用して、クライアント アドレスを割り当てる DHCP サーバーを識別できます。また、DHCP オプションはユーザーに転送されず、ユーザーはアドレス割り当てのみを受信します。

手順

ステップ 1 アドレス割り当て方式として IP アドレス プールを設定します。

vpn-addr-assign dhcp

ステップ 2 リモートアクセス接続プロファイルとして **firstgroup** という名前の接続プロファイルを設定します。

tunnel-group firstgroup type remote-access

ステップ 3 DHCP サーバーを設定できるように、接続プロファイルの一般属性コンフィギュレーション モードを開始します。

tunnel-group firstgroup general-attributes

ステップ 4 IPv4 アドレスで DHCP サーバーを定義し、トンネル グループ コンフィギュレーション モードを終了します。

dhcp-server IPv4_address_of_DHCP_server

IPv6 アドレスで DHCP サーバーを定義することはできません。接続プロファイルに複数の DHCP サーバー アドレスを指定できます。**dhcp-server** コマンドを入力します。このコマンドを使用すると、VPN クライアントの IP アドレスの取得を試みるときに、指定された DHCP サーバーに追加のオプションを送信するように ASA を設定できます。

例：

この例では、IP アドレス 172.33.44.19 の DHCP サーバーを設定しています。その後、トンネル グループ コンフィギュレーション モードを終了します。

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)#
```

ステップ 5 グループがまだ存在しない場合は、**remotegroup** という内部グループポリシーを作成します。

```
hostname(config)# group-policy remotegroup internal
```

ステップ 6 (オプション) グループポリシー属性コンフィギュレーションモードを開始し、DHCP ネットワークスコープを定義します。

```
dhcp-network-scope ip_address
```

接続プロファイルのアドレスプールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用する DHCP サーバーで定義されているアドレスプールのサブセットを選択できます。

ネットワーク スコープを定義しない場合、DHCP サーバーはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

(注)

スコープを指定するには、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを入力します。DHCP サーバーは、この IP アドレスが属するサブネットを判別し、そのプールからの IP アドレスを割り当てます。

ルーティングの目的で可能な場合は常に、インターフェイスの IP アドレスを使用することを推奨します。たとえば、プールが 10.100.10.2 ~ 10.100.10.254 で、インターフェイスアドレスが 10.100.10.1/24 の場合、DHCP スコープとして 10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP は IPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

例：

次の例では、**remotegroup** の属性コンフィギュレーション モードを開始し、DHCP スコープを 10.100.10.1 に設定します。

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

例

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type remote-access
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```



第 7 章

リモート アクセス IPsec VPN

- リモートアクセス IPsec VPN の概要 (227 ページ)
- Cisco Secure Client の AnyConnect VPN モジュールのライセンス要件 (229 ページ)
- リモートアクセス IPsec VPN の制限 (229 ページ)
- リモート アクセス IPsec VPN の設定 (230 ページ)
- リモート アクセス IPsec VPN の設定例 (238 ページ)
- マルチコンテキストモードでの標準ベース IPsec IKEv2 リモートアクセス VPN の設定例 (239 ページ)
- マルチコンテキストモードでのセキュアクライアント IPsec IKEv2 リモートアクセス VPN の構成例 (240 ページ)
- リモート アクセス VPN の機能履歴 (242 ページ)

リモートアクセス IPsec VPN の概要

リモートアクセス VPN を使用すると、TCP/IP ネットワーク上のセキュアな接続を介して、ユーザーを中央サイトに接続することができます。Internet Security Association and Key Management Protocol は IKE と呼ばれ、リモート PC の IPsec クライアントと ASA で、IPsec セキュリティアソシエーションの構築方法を一致させるためのネゴシエーションプロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 は、セキュアな接続を移動するデータを保護するトンネルを作成します。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。ここでは、次の項目について説明します。

- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code (HMAC) 方式。
- 暗号キーのサイズを設定する Diffie-Hellman グループ。

- 暗号キーを置き換える前に、ASA がその暗号キーを使用する時間の上限。

トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。特定のデータフローを保護する場合、ピアは、ISAKMP との IPsec セキュリティアソシエーションのネゴシエーション中に、特定のトランスフォームセットを使用することに同意します。トランスフォームセットは、両方のピアで同じである必要があります。

トランスフォームセットにより、関連付けられたクリプトマップエントリで指定された ACL のデータフローが保護されます。ASA 設定でトランスフォームセットを作成して、クリプトマップまたはダイナミック クリプトマップエントリでトランスフォームセットの最大数 11 を指定できます。有効な暗号化方式と認証方式をリストしたテーブルなど、さらに詳細な情報については、[IKEv1 トランスフォームセットまたは IKEv2 プロポーザルの作成 \(233 ページ\)](#) を参照してください。

セキュアクライアントに IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てるように ASA を設定できます。そのように設定するには、ASA 上で内部アドレスプールを作成するか、ASA 上のローカルユーザーに専用アドレスを割り当てます。

エンドポイントに両方のタイプのアドレスを割り当てるには、エンドポイントのオペレーティングシステムの中でデュアルスタックプロトコルが実装されている必要があります。どちらのシナリオでも、IPv6 アドレスプールは残っていないが IPv4 アドレスが使用できる場合や、IPv4 アドレスプールは残っていないが IPv6 アドレスが使用できる場合は、接続は行われます。ただし、クライアントには通知されないため、管理者は ASA ログで詳細を確認する必要があります。

クライアントへの IPv6 アドレスの割り当ては、SSL プロトコルに対してサポートされます。

Mobike およびリモートアクセス VPN について

モバイル IKEv2 (mobike) は、モバイルデバイスのローミングをサポートするために ASA RA VPN を拡張します。このサポートは、デバイスが現在の接続ポイントから別のポイントに移動するときに、モバイルデバイスの IKE/IPSEC セキュリティアソシエーション (SA) のエンドポイント IP アドレスが削除されるのではなく更新できることを意味します。

Mobike はバージョン 9.8(1) 以降は ASA でデフォルトにより利用可能です。つまり、Mobike は「常にオン」になります。Mobike は、クライアントがそれを提案し、ASA が受け入れるときにだけ、各 SA に対して有効になります。このネゴシエーションは、IKE_AUTH 交換の一部として行われます。

mobike サポートが有効な状態で SA が確立された後、クライアントはいつでもアドレスを変更して、新しいアドレスを示す UPDATE_SA_ADDRESS ペイロードを含む情報交換を使用して ASA に通知できます。ASA はこのメッセージを処理し、新しいクライアント IP アドレスで SA を更新します。



(注) show crypto ikev2 sa detail コマンドを使用して、現在のすべての SA で mobike が有効になっているかどうかを判別できます。

現在の Mobike の実装では、次の機能がサポートされています。

- IPv4 アドレスのみ
- NAT マッピングの変更
- オプションのリターン ルータビリティ チェックによるパス接続と停止検出
- アクティブ/スタンバイ フェールオーバー
- VPN ロード バランシング

RRC（リターン ルータビリティ チェック）機能が有効になっている場合、モバイル クライアントに RRC メッセージが送信され、SA が更新される前に新しい IP アドレスが確認されます。

Cisco Secure Client の AnyConnect VPN モジュールのライセンス要件



(注) この機能は、ペイロード暗号化機能のないモデルでは使用できません。

Secure Firewall ASA ヘッドエンドから Cisco Secure Client（AnyConnect を含む）を展開し、VPN および Secure Firewall ポスチャまたは HostScan モジュールを使用する場合は、Advantage または Premier ライセンスが必要です。トライアルライセンスも使用できます。『[Cisco Secure Client 発注ガイド](#)』を参照してください。モデルごとの最大値については、「[Cisco ASA Series Feature Licenses](#)」を参照してください。

リモート アクセス IPsec VPN の制限

- ファイアウォール モード ガイドライン：ルーテッド ファイアウォール モードでのみサポートされます。トランスペアレント モードはサポートされていません。
- フェールオーバー ガイドライン IPsec-VPN セッションは、アクティブ/スタンバイ フェールオーバー コンフィギュレーションでのみ複製されます。アクティブ/アクティブ フェールオーバー コンフィギュレーションはサポートされません。
- HA 同期中は設定の変更がブロックされます。この間にユーザーがログインしようとする、ファイアウォールでの DACL ルールのインストールが失敗する可能性があります。HA 同期が完了すると、ユーザーは正常にログインできます。
- ASA は、サードパーティ製クライアントが Null ユーザーエージェントを送信した場合、リモート アクセス VPN セッションを受け入れません。
- 複数の、頻繁に変更される IP アドレスに解決されるドメインに対して完全修飾ドメイン名（FQDN）アクセス制御リスト（ACL）を使用すると、リモート アクセス VPN 環境での

DHCP アドレスの解決に影響を与える可能性があります。この問題は、外部 DHCP サーバーが構成され、ネットワークアドレス変換 (NAT) のトランザクションコミットが有効になっている場合に発生する可能性があります。

- Advanced Endpoint Assessment を使用したポスチャアセスメントでは、SSL 接続の syslog メッセージが生成される場合がありますが、それらは VPN ログオンまたはログオフイベントと関連付けられません。
- ASA では EAP 方式を終了させないため、ローカル認証はできません。

ASA は、EAP をパススルーとしてのみサポートし、クライアントの EAP 認証には VPN クライアントの証明書認証を必要とします。リモート認証方式として EAP を構成する場合は、VPN クライアントの証明書認証を構成してください。EAP、PSK、証明書などの複数のリモート認証方式が EAP とともに設定されている場合でも、エラーが表示されます。

リモート アクセス IPsec VPN の設定

このセクションでは、リモート アクセス VPN の設定方法について説明します。

インターフェイスの設定

ASA には、少なくとも 2 つのインターフェイスがあり、これらをここでは外部および内部と言います。一般に、外部インターフェイスはパブリックインターネットに接続されます。一方、内部インターフェイスはプライベートネットワークに接続され、一般のアクセスから保護されます。

最初に、ASA の 2 つのインターフェイスを設定し、イネーブルにします。次に、名前、IP アドレス、およびサブネットマスクを割り当てます。オプションで、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重操作を設定します。

手順

ステップ 1 グローバル構成モードからインターフェイス構成モードに入ります。

```
interface {interface}
```

例 :

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

ステップ 2 インターフェイスに IP アドレスとサブネットマスクを設定します。

```
ip address ip_address [mask] [standby ip_address]
```

例 :


```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

ステップ3 インターフェイスの名前（最大 48 文字）を指定します。この名前は、設定した後での変更はできません。

nameif name

例：

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

ステップ4 インターフェイスをイネーブルにします。デフォルトでは、インターフェイスは無効です。

例：

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ISAKMPポリシーの設定と外部インターフェイスでのISAKMPのイネーブル化

手順

ステップ1 IKEv1 ネゴシエーション中に使用する認証方式とパラメータのセットを指定します。

Priority は、インターネット キー交換 (IKE) ポリシーを一意に識別し、ポリシーにプライオリティを割り当てます。1 ~ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

その後に続く手順では、プライオリティは 1 に設定されます。

ステップ2 IKE ポリシー内で使用する暗号化方式を指定します。

crypto ikev1 policy priority encryption {aes-192 | aes-256 || }

例：

ステップ3 IKE ポリシーのハッシュアルゴリズム (HMAC バリエントとも呼ばれます) を指定します。

crypto ikev1 policy priority hash { | sha }

例：

```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```

ステップ4 IKE ポリシーの Diffie-Hellman グループ (IPsec クライアントと ASA が共有秘密キーを確立できる暗号化プロトコル) を指定します。

```
crypto ikev1 policy priority group {14 ||| 19 | 20 | 21}
```

例 :

```
hostname (config) # crypto ikev1 policy 1 group 14
hostname (config) #
```

ステップ 5 暗号キーのライフタイム（各セキュリティアソシエーションが有効期限まで存在する秒数）を指定します。

```
crypto ikev1 policy priority lifetime {seconds}
```

限定されたライフタイムの範囲は、120 ～ 2147483647 秒です。無制限のライフタイムの場合は、0 秒を使用します。

例 :

```
hostname (config) # crypto ikev1 policy 1 lifetime 43200
hostname (config) #
```

ステップ 6 outside というインターフェイス上の ISAKMP を有効にします。

```
crypto ikev1 enable interface-name
```

例 :

```
hostname (config) # crypto ikev1 enable outside
hostname (config) #
```

ステップ 7 変更を構成に保存します。

```
write memory
```

アドレス プールの設定

ASA では、ユーザーに IP アドレスを割り当てる方式が必要です。この項では、例としてアドレス プールを使用します。

手順

IP アドレスの範囲を使用してアドレス プールを作成します。ASA は、このアドレス プールのアドレスをクライアントに割り当てます。

```
ip local pool poolname first-address—last-address [mask mask]
```

アドレス マスクはオプションです。ただし、VPN クライアントに割り当てられた IP アドレスが非標準のネットワークに属し、デフォルトのマスクを使用するとデータが誤ってルーティングされる可能性があるときは、マスク値を指定する必要があります。典型的な例が、IP ローカルプールに 10.10.10.0/255.255.255.0 アドレスが含まれている場合で、これはデフォルトではクラス A ネットワークです。これによって、VPN クライアントがさまざまなインターフェイス

で 10 のネットワーク内の異なるサブネットにアクセスする必要がある場合、ルーティングの問題が生じる可能性があります。

例：

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

ユーザーの追加

手順

ユーザー、パスワード、およびそのユーザーの特権レベルを作成します。

```
username name {nopassword | password password [mschap | encrypted | nt-encrypted]} [privilege priv_level]
```

例：

```
Hostname(config)# username testuser password 12345678
```

IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの作成

この項では、トランスフォーム セット (IKEv1) およびプロポーザル (IKEv2) を設定する方法について説明します。トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。

次の手順では、IKEv1 および IKEv2 プロポーザルを作成する方法を示します。

手順

ステップ 1 データ整合性を確保するために使用される IPsec IKEv1 暗号化とハッシュ アルゴリズムを指定する IKEv1 トランスフォーム セットを設定します。

```
crypto ipsec ikev1 transform-set transform-set-name encryption-method [authentication]
```

encryption には、次のいずれかの値を指定します。

- **esp-aes** : 128 ビット キーで AES を使用する場合。
- **esp-aes-192** : 192 ビット キーで AES を使用する場合。
- **esp-aes-256** : 256 ビット キーで AES を使用する場合。
- **esp-null** : 暗号化を使用しない場合。

authentication には、次のいずれかの値を指定します。

- esp-md5-hmac : ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合。
- esp-sha-hmac : ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合。
- esp-none : HMAC 認証を使用しない場合。

例 :

AES を使用して IKEv1 トランスフォームセットを設定するには、次のようにします。

```
hostname(config)# crypto ipsec transform set FirstSet esp-aes esp-sha-hmac
```

ステップ 2 IKEv2 プロポーザルセットを設定し、使用される IPsec IKEv2 プロトコル、暗号化、および整合性アルゴリズムを指定します。

esp は、カプセル化セキュリティ ペイロード (ESP) IPsec プロトコルを指定します (現在、唯一サポートされている IPsec のプロトコルです)。

crypto ipsec ikev2 ipsec-proposal proposal_name

protocol {esp} {encryption {|| aes | aes-192 | aes-256 ||} integrity {|| sha-1}}

encryption には、次のいずれかの値を指定します。

- aes : ESP に 128 ビットキー暗号化で AES (デフォルト) を使用する場合。
- aes-192 : ESP に 192 ビット キー暗号化で AES を使用する場合。
- aes-256 : ESP に 256 ビット キー暗号化で AES を使用する場合。

integrity には、次のいずれかの値を指定します。

- sha-1 (デフォルト) は、ESP の整合性保護のために米国連邦情報処理標準 (FIPS) で定義されたセキュア ハッシュ アルゴリズム (SHA) SHA-1 を指定します。

IKEv2 プロポーザルの設定手順

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal
```

```
hostname(config-ipsec-proposal)# protocol esp encryption aes integrity sha-1
```

トンネル グループの定義

トンネル グループは、トンネル接続ポリシーのコレクションです。AAA サーバーを識別するトンネル グループを設定し、接続パラメータを指定し、デフォルトのグループ ポリシーを定義します。ASA は、トンネル グループを内部的に保存します。

ASA システムには、2 つのデフォルト トンネル グループがあります。1 つはデフォルトのリモートアクセス トンネル グループである DefaultRAGroup で、もう 1 つはデフォルトの LAN-to-LAN トンネル グループである DefaultL2Lgroup です。これらのグループは変更できま

すが、削除はできません。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、ASA は、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

手順

- ステップ 1** IPsec リモート アクセス トンネル グループ（接続プロファイルとも呼ばれます）を作成します。

tunnel-group name type type

例：

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

- ステップ 2** トンネルグループ一般属性モードに入ります。このモードでは、認証方式を入力できます。

tunnel-group name general-attributes

例：

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#
```

- ステップ 3** トンネルグループに使用するアドレスプールを指定します。

address-pool [(interface name)] address_pool1 [...address_pool6]

例：

```
hostname(config-general)# address-pool testpool
```

- ステップ 4** トンネルグループ IPsec 属性モードに入ります。このモードでは、IKEv1 接続のための IPsec 固有の属性を入力できます。

tunnel-group name ipsec-attributes

例：

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

- ステップ 5** （任意） 事前共有キー（IKEv1 のみ）を設定します。キーには、1 ～ 128 文字の英数字文字列を指定できます。

適応型セキュリティアプライアンスとクライアントのキーは同じである必要があります。事前共有キーのサイズが異なる Cisco VPN Client が接続しようとする、ピアの認証に失敗したことを示すエラー メッセージがクライアントによってログに記録されます。

ikev1 pre-shared-key key

例：

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfxx
```

ダイナミック クリプト マップの作成

ダイナミック クリプト マップは、すべてのパラメータが設定されているわけではないポリシー テンプレートを定義します。これにより、ASA は、リモートアクセス クライアントなどの IP アドレスが不明なピアからの接続を受信することができます。

ダイナミック クリプト マップのエントリは、接続のトランスフォーム セットを指定します。また、逆ルーティングもイネーブルにできます。これにより、ASA は接続されたクライアントのルーティング情報を取得し、それを RIP または OSPF 経由でアドバタイズします。

手順

ステップ 1 ダイナミック クリプト マップを作成し、マップの IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを指定します。

- IKEv1 の場合は、このコマンドを使用します。

```
crypto dynamic-map dynamic-map-name seq-num set ikev1 transform-set transform-set-name
```

- IKEv2 の場合は、このコマンドを使用します。

```
crypto dynamic-map dynamic-map-name seq-num set ikev2 ipsec-proposal proposal-name
```

例 :

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)#
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal secure_proposal
hostname(config)#
```

ステップ 2 (オプション) このクリプト マップ エントリに基づく接続に対してリバース ルート インジェクションを有効にします。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set reverse-route
```

例 :

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse route
hostname(config)#
```

ダイナミック クリプト マップを使用するためのクリプト マップ エントリの作成

クリプトマップエントリを作成します。これにより、ASA は、ダイナミック クリプト マップを使用して IPsec セキュリティ アソシエーションのパラメータを設定することができます。

このコマンドに関する次の例では、クリプトマップ名は `mymap`、シーケンス番号は 1、ダイナミック クリプト マップ名は `dyn1` です。この名前は、「[ダイナミック クリプト マップの作成](#)」のトピックで作成したものです。

手順

ステップ 1 ダイナミック クリプト マップを使用するクリプトマップエントリを作成します。

crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name

例 :

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

ステップ 2 クリプトマップを外部インターフェイスに適用します。

crypto map map-name interface interface-name

例 :

```
hostname(config)# crypto map mymap interface outside
```

ステップ 3 変更を構成に保存します。

write memory

マルチコンテキストモードでの IPsec IKEv2 リモートアクセス VPN の設定

リモート アクセス IPsec VPN の設定の詳細については、次の項を参照してください。

- [インターフェイスの設定 \(230 ページ\)](#)
- [アドレス プールの設定 \(232 ページ\)](#)
- [ユーザーの追加 \(233 ページ\)](#)
- [IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの作成 \(233 ページ\)](#)
- [トンネル グループの定義 \(234 ページ\)](#)
- [ダイナミック クリプト マップの作成 \(236 ページ\)](#)

- [ダイナミック クリプトマップを使用するためのクリプトマップエントリの作成 \(237 ページ\)](#)

リモート アクセス IPsec VPN の設定例

次の例は、リモート アクセス IPsec/IKEv1 VPN を設定する方法を示しています。

```
hostname(config)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

次の例は、リモート アクセス IPsec/IKEv2 VPN を設定する方法を示しています。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```


マルチコンテキストモードでの標準ベース IPsec IKEv2 リモートアクセス VPN の設定例

次の例は、マルチコンテキストモードで標準ベースリモートアクセス IPsec/IKEv2 VPN 用の ASA を構成する方法を示しています。この例では、システム コンテキストおよびユーザー コンテキストの設定について、それぞれ情報を提供します。

システム コンテキストの設定：

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname(config)#context CTX2
hostname(config-ctx)#member default =====> License allotment for contexts
using class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

ユーザー コンテキストの設定：

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTOMAP
hostname/CTX2(config)#crypto map outside_map interface outside
```

デフォルトでは、標準ベースクライアントからの IPsec/IKEv2 リモートアクセス接続は、トンネルグループ DefaultRAGroup に分類されます。

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
```

```
hostname/CTX2 (config-tunnel-general) #authentication-server-group ISE
hostname/CTX2 (config-tunnel-general) #exit
hostname/CTX2 (config) #

hostname/CTX2 (config) #tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2 (config-tunnel-ipsec) #ikev2 remote-authentication eap query-identity
hostname/CTX2 (config-tunnel-ipsec) #ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2 (config-tunnel-ipsec) #exit
hostname/CTX2 (config) #
```

マルチコンテキストモードでのセキュアクライアント IPsec IKEv2 リモートアクセス VPN の構成例

次の例は、マルチコンテキストモードでセキュアクライアントリモートアクセス IPsec/IKEv2 VPN 用の ASA を構成する方法を示しています。この例では、システム コンテキストおよびユーザー コンテキストの設定について、それぞれ情報を提供します。

システム コンテキストの設定：

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname (config) #context CTX3
hostname (config-ctx) #member default =====> License allotment for contexts
using class
hostname (config-ctx) #allocate-interface Ethernet1/1.200
hostname (config-ctx) #allocate-interface Ethernet1/3.100
hostname (config-ctx) #config-url disk0:/CTX3.cfg
```

各コンテキストの仮想ファイルシステムの作成では、イメージ、プロファイルなどのセキュアクライアント ファイルを使用できます。

```
hostname (config-ctx) #storage-url shared disk0:/shared disk0
```

ユーザー コンテキストの設定：

```
hostname/CTX3 (config) #ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3 (config) #webvpn
hostname/CTX3 (config-webvpn) #enable outside
hostname/CTX3 (config-webvpn) # anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
hostname/CTX3 (config-webvpn) #anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3 (config-webvpn) #anyconnect enable
hostname/CTX3 (config-webvpn) #tunnel-group-list enable

hostname/CTX3 (config) #username cisco password *****
hostname/CTX3 (config) #ssl trust-point ASDM_TrustPoint0 outside
```

```
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes

hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user
```

次の例では、クライアントサービスを有効にするために、**crypto ikev2 enable outside client-services** コマンドを使用しています。

クライアントサービスサーバーは、HTTPS (SSL) アクセスを提供します。これにより、Secure Client ダウンローダは、ソフトウェアアップグレード、プロファイル、ローカリゼーションおよびカスタマイゼーションファイル、CSD、SCEP、およびクライアントが必要とするその他のファイルダウンロードを受信できます。このオプションを選択した場合は、クライアントサービスのポート番号を指定します。クライアント サービス サーバーを有効にしない場合、ユーザーは、Secure Client が必要とする可能性があるこれらのファイルをダウンロードできません。



- (注) 同じデバイスで実行する SSL VPN に対して同じポートを使用できます。SSL VPN を設定した場合でも、IPsec-IKEv2 クライアントで SSL を介してファイルをダウンロードするには、このオプションを選択する必要があります。

```
hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTOMAP
hostname/CTX3(config)#crypto map outside_map interface outside

hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

リモート アクセス VPN の機能履歴

機能名	リリース	機能情報
IPsec IKEv1 および SSL のリモート アクセス VPN	7.0	リモート アクセス VPN を使用すると、インターネットなどの TCP/IP ネットワーク上のセキュアな接続を介して、ユーザーを中央サイトに接続することができます。
IPsec IKEv2 のリモート アクセス VPN	8.4(1)	セキュアクライアントの IPsec IKEv2 サポートが追加されました。
リモート アクセス VPN の自動 mobike サポート。	9.8(1)	IPsec IKEv2 RA VPN に対するモバイル IKE (mobike) のサポートが追加されました。Mobike は常にオンになっています。 IKEv2 RA VPN 接続のための mobike 通信時のリターンルータビリティチェックを有効にできるよう、ikev2 mobike-rrc コマンドが追加されました。
マルチコンテキストモードでの IPsec IKEv2 のリモート アクセス VPN	9.9(2)	セキュアクライアントやサードパーティ製標準ベース IPsec IKEv2 VPN クライアントがマルチコンテキストモードで稼働する ASA へのリモートアクセス VPN セッションを確立できるように ASA を設定することをサポートします。 認証ペイロードに署名する <code>ikev2 rsa-sig-hash sha1</code> コマンドが追加されました。
認証ペイロードに署名するための SHA-1 ハッシュアルゴリズムを使用した RSA	9.12(1)	サードパーティの標準ベースの IPsec IKEv2 VPN クライアントを使用して、ASA へのリモートアクセス VPN セッションを確立する際の、SHA-1 ハッシュアルゴリズムによる認証ペイロードの署名をサポート。
IKE/IPsec 暗号化および整合性/PRF 暗号の廃止 DH グループ 14 での IKEv1 のサポート	9.13(1)	次の暗号化/整合性/PRF 暗号は廃止され、以降のリリース 9.14(1) で削除されます。 • 3DES 暗号化 • DES 暗号化 • MD5 の整合性 IKEv1 での DH グループ 14 (デフォルト) サポートが追加されました。グループ 2 およびグループ 5 コマンドオプションは廃止され、以降のリリース 9.14(1) で削除されます。



第 8 章

LAN-to-LAN IPsec VPN

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。

シスコのピアや、関連するすべての標準に準拠したサードパーティのピアとの LAN-to-LAN IPsec 接続を作成できます。これらのピアは、IPv4 と IPv6 のアドレッシングを使用して、内部アドレスと外部アドレスの任意の組み合わせを持つことができます。

ASA では、ping 以外のローカル発信トラフィックは VPN トンネルを通過できません。

この章では、LAN-to-LAN VPN 接続の構築方法について説明します。

- [コンフィギュレーションのまとめ \(243 ページ\)](#)
- [マルチコンテキスト モードでのサイトツーサイト VPN の設定 \(244 ページ\)](#)
- [インターフェイスの設定 \(245 ページ\)](#)
- [ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化 \(246 ページ\)](#)
- [IKEv1 トランスフォーム セットの作成 \(253 ページ\)](#)
- [IKEv2 プロポーザルの作成 \(254 ページ\)](#)
- [ACL の設定 \(255 ページ\)](#)
- [トンネル グループの定義 \(256 ページ\)](#)
- [クリプト マップの作成とインターフェイスへの適用 \(257 ページ\)](#)

コンフィギュレーションのまとめ

ここでは、この章で説明するサンプルの LAN-to-LAN コンフィギュレーションの概要を説明します。後の項で、手順の詳細を説明します。

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
```

```

hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# # encryption aes
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)# crypto ipsec ikev1 transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption aes
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list 121_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfxf
hostname(config)# crypto map abcmap 1 match address 121_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory

```

マルチコンテキストモードでのサイトツーサイトVPNの設定

マルチモードでサイトツーサイトVPNをサポートするには、次の手順を実行します。これらの手順を実行して、リソース割り当てがどのように分解されるのかを確認できます。

手順

- ステップ1** マルチモードのVPNを設定し、リソースクラスを設定し、許可されたリソースの一部としてVPNライセンスを選択します。「Configuring a Class for Resource Management」で、これらの設定手順を説明します。次に設定例を示します。

```

class ctx1
  limit-resource VPN Burst Other 100
  limit-resource VPN Other 1000

```

- ステップ2** コンテキストを設定し、VPNライセンスを許可する設定したクラスのメンバーにします。次に設定例を示します。

```

context context1
  member ctx1
  allocate-interface GigabitEthernet3/0.2
  allocate-interface GigabitEthernet3/1.2
  allocate-interface Management0/0
  config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
  join-failover-group 1

```

- ステップ3** 接続プロファイル、ポリシー、クリプトマップなどを、サイトツーサイト VPN のシングル コンテキストの VPN 設定と同様に設定します。

インターフェイスの設定

ASA には、少なくとも2つのインターフェイスがあり、これらをここでは外部および内部と言います。一般に、外部インターフェイスはパブリックインターネットに接続されます。一方、内部インターフェイスはプライベートネットワークに接続され、一般のアクセスから保護されます。

最初に、ASA の2つのインターフェイスを設定し、イネーブルにします。次に、名前、IP アドレス、およびサブネットマスクを割り当てます。オプションで、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重操作を設定します。



- (注) ASA の外部インターフェイスアドレス (IPv4 と IPv6 の両方) は、プライベート側のアドレス空間と重複してはなりません。

手順

- ステップ1** インターフェイス コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで、設定するインターフェイスのデフォルト名を指定して **interface** コマンドを入力します。次の例で、インターフェイスは **ethernet0** です。

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

- ステップ2** インターフェイスの IP アドレスとサブネットマスクを設定するには、**ip address** コマンドを入力します。次の例で、IP アドレスは 10.10.4.100、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

- ステップ3** インターフェイスに名前を付けるには、**nameif** コマンドを入力します。最大 48 文字です。この名前は、設定した後での変更はできません。次の例で、**ethernet0** インターフェイスの名前は **outside** です。

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

- ステップ4** インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** バージョンを入力します。デフォルトでは、インターフェイスはディセーブルです。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ステップ 5 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config-if)# write memory
hostname(config-if)#
```

ステップ 6 同じ手順で、2 番目のインターフェイスを設定します。

ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

ISAKMP は、2 台のホストで IPsec Security Association (SA; セキュリティ アソシエーション) の構築方法を一致させるためのネゴシエーション プロトコルです。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。これには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。ISAKMP のネゴシエーションは 2 つのフェーズ（フェーズ 1 とフェーズ 2）に分かれています。フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

IKE は、IPsec を使用するための SA の設定に ISAKMP を使用します。IKE は、ピアの認証に使用される暗号キーを作成します。

ASA は、レガシー Cisco VPN Client から接続するための IKEv1、および AnyConnect VPN クライアントの IKEv2 をサポートしています。

ISAKMP ネゴシエーションの条件を設定するには、IKE ポリシーを作成します。このポリシーには、次のものが含まれます。

- IKEv1 ピアに要求する認証タイプ。証明書を使用する RSA 署名または事前共有キー (PSK) です。
- データを保護し、プライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code (HMAC) 方式。
- 暗号キー決定アルゴリズムの強度を決定するデフィーヘルマン グループ。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。
- IKEv2 では、別個の Pseudo-Random Function (PRF; 疑似乱数関数) をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していました。
- ASA が暗号キーを使用する時間の制限。この時間が経過すると暗号キーを置き換えます。

IKEv1 ポリシーを使用して、パラメータごとに1つの値を設定します。IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

ここでは、IKEv1 およびIKEv2 ポリシーを作成して、インターフェイスでイネーブルにする手順について説明します。

- [IKEv1 接続の ISAKMP ポリシーの設定 \(247 ページ\)](#)
- [IKEv2 接続の ISAKMP ポリシーの設定 \(248 ページ\)](#)

IKEv1 接続の ISAKMP ポリシーの設定

IKEv1 接続の ISAKMP ポリシーを設定するには、**crypto ikev1 policy priority** コマンドを使用して IKEv1 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv1 のパラメータを設定できます。

手順

ステップ 1 IPsec IKEv1 ポリシー コンフィギュレーション モードを開始します。次に例を示します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

ステップ 2 認証方式を設定します。次の例では、事前共有キーを設定します。

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

ステップ 3 暗号方式を設定します。次に、 を設定する例を示します。

```
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)#
```

ステップ 4 HMAC 方式を設定します。次の例では、SHA-1 に設定します。

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

ステップ 5 Diffie-Hellman グループを設定します。次に、グループ 14 を設定する例を示します。

```
hostname(config-ikev1-policy)# group 14
```

```
hostname(config-ikev1-policy)#
```

ステップ 6 暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

ステップ 7 シングル コンテキスト モードまたはマルチ コンテキスト モードで、outside というインターフェイス上の IKEv1 をイネーブルにします。

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

ステップ 8 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 接続の ISAKMP ポリシーの設定

IKEv2 接続の ISAKMP ポリシーを設定するには、**crypto ikev2 policy priority** コマンドを使用して IKEv2 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv2 のパラメータを設定できます。

手順

ステップ 1 IPsec IKEv2 ポリシー コンフィギュレーション モードを開始します。次に例を示します。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

ステップ 2 暗号方式を設定します。次に、AES を設定する例を示します。

```
hostname(config-ikev2-policy)# encryption aes
hostname(config-ikev2-policy)#
```

ステップ 3 Diffie-Hellman グループを設定します。次に、グループ 15 を設定する例を示します。

```
hostname(config-ikev2-policy)# group 15
hostname(config-ikev2-policy)#
```

ステップ 4 アルゴリズムとして使用する疑似乱数関数（PRF）を設定し、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得します。次の例では、SHA-1（HMAC バリエント）を設定します。

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

ステップ 5 暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

ステップ 6 outside というインターフェイス上の IKEv2 をイネーブルにします。

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

ステップ 7 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 の複数キー交換

IKEv2 は、Diffie-Hellman (DH) グループを使用して、イニシエータとレスポンドの間で共有秘密を確立します。IKEv2 は、量子コンピュータ攻撃から IPsec 通信を保護するための追加のキー交換をサポートしています。各交換には異なる DH グループを使用します。SA セットアップ用に計算される共有秘密は、各交換から取得するすべてのキーの組み合わせです。IKE SA は、IKE ピア間での複数のキー交換後に確立されます。

ASA は、複数キー交換に 7 つの新しいトランスフォームタイプを使用します。

- 追加のキー交換 1 (IANA 値 6)
- 追加のキー交換 2 (IANA 値 7)
- 追加のキー交換 3 (IANA 値 8)
- 追加のキー交換 4 (IANA 値 9)
- 追加のキー交換 5 (IANA 値 10)
- 追加のキー交換 6 (IANA 値 11)
- 追加のキー交換 7 (IANA 値 12)

最大 7 つの複数キー交換を設定できます。設定する追加のキー交換ごとに DH グループを指定する必要があります。ASA は、以前の交換で得たキーを使用して中間キー交換を暗号化します。イニシエータピアとレスポンドピアが DH グループについて合意しない場合、ネゴシエーションは失敗し、**NO_PROPOSAL_CHOSEN** エラー通知がイニシエータに送信されます。トランスフォームを [なし (none)] に設定することもできます。[なし (none)] を選択すると、キー交換は行われません。

イニシエータについて、キー交換方式が追加のキー交換 n に対して **[なし (none)]** に設定されている場合：

- レスポンダは、追加のキー交換 n のキー交換方式として **[なし (None)]** を選択できます。
- 追加のキー交換はオプションです。

プロポーザルのネゴシエーションを成功させるには、イニシエータのプロポーザルのすべてのトランスフォームがレスポンダのトランスフォームと一致する必要があります。

次に、イニシエータの例を示します。

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 5
key-exchange-method none
```

レスポンダには、プロポーザルを一致させるために追加のキー交換 5 が必要です。

ピアが追加のキー交換をサポートしていない場合は、次のいずれかが発生します。

- イニシエータにレスポンダのプロポーザルと一致する別の IKEv2 プロポーザルがある場合、IKEv2 SA が確立されます。
- ピアは IKE_SA_INIT 交換メッセージ内の追加のキー交換のトランスフォームタイプを不明なトランスフォームタイプとして扱い、プロポーザルをスキップします。ネゴシエーションは失敗し、**NO_PROPOSAL_CHOSEN** エラー通知がイニシエータに送信されます。

この機能の詳細については、RFC 9242 を参照してください。

IKEv2 複数キー交換の注意事項と制限事項

- 最大 7 つの複数キー交換を持つことができます。
- 後続のキー交換で同じ DH グループを使用することはできません。

この機能について、ASA は次をサポートしません。

- IKEv1
- 従来のキー交換とポスト量子アルゴリズムベースのキー交換の組み合わせ。
- リモート アクセス VPN サイト間 VPN のみが IKEv2 複数キー交換をサポートします。
- クラスタ

IKEv2 の複数キー交換の設定

この設定はオプションです。量子コンピュータ攻撃から IPsec 通信を保護したい場合は、設定を実行できます。

始める前に

- 注意事項と制限事項を確認します。詳細については、[IKEv2 複数キー交換の注意事項と制限事項（250 ページ）](#)を参照してください。
- IKEv2 ポリシーの暗号化アルゴリズム、ハッシュアルゴリズム、認証方式、および SA ライフタイムを設定します。詳細については、[IKEv1 ポリシーと IKEv2 ポリシーの設定（8 ページ）](#)を参照してください。

手順

ステップ 1 IKEv2 ポリシーを作成します。

crypto ikev2 policy policy_index

プロンプトには、IKEv2 ポリシー設定モードが表示されます。

例：

```
hostname(config)# crypto ikev2 policy 1
```

ステップ 2 IKEv2 ポリシーの追加のキー交換トランスフォームを設定します。

additional-key-exchange <1-7>

プロンプトには、IKEv2 ポリシーの追加のキー交換設定モードが表示されます。1つのポリシーに最大7つのキー交換トランスフォームを設定できます。

例：

```
hostname(config-ikev2-policy)# additional-key-exchange 1
```

ステップ 3 追加のキー交換トランスフォームに1つ以上の DH グループを定義して、キー交換方式を設定します。

key-exchange-method <DH_group>

DH グループを 14、15、16、19、20、21、または 31 と指定します。トランスフォームを [なし (none)] に設定することもできます。[なし (none)] を選択すると、キー交換は行われません。

例：

```
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31
```

ステップ 4 IKEv2 ポリシーに複数のキー交換を設定するには、手順 2 と 3 を繰り返します。

```
hostname(config)# crypto ikev2 policy 1  
hostname(config-ikev2-policy)# additional-key-exchange 1  
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31  
hostname(config-ikev2-policy)# additional-key-exchange 2
```

```
hostname(config-ikev2-policy-ake)# key-exchange-method 20 21
hostname(config-ikev2-policy)# additional-key-exchange 3
hostname(config-ikev2-policy-ake)# key-exchange-method 19 20 none
...
```

次のタスク

設定を確認します。詳細については、[IKEv2 複数キー交換設定の確認（252 ページ）](#)を参照してください。

IKEv2 複数キー交換設定の確認

IKEv2 複数キー交換の設定を表示または確認するには、次の show コマンドを使用します。

- **show running-config crypto ikev2**

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 1
key-exchange-method 21 31
additional-key-exchange 2
key-exchange-method 20 21
...
```

- **show crypto ikev2 sa detail**

```
IKEv2 SAs:
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote fvrf/ivrf Status Role
41567725 192.168.15.1/500 192.168.15.2/500 READY INITIATOR
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify:
PSK
Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6:
15 AKE7: 14
Life/Active Time: 120/5 sec
Session-id: 4
Status Description: Negotiation done
Local spi: 6BB6B7BFA0BAADF4 Remote spi: 7030C7xxx xxxxxxE9DBDE77EB
Local id: 192.168.15.1
Remote id: 192.168.15.2
Local req mess id: 9 Remote req mess id: 0
Local next mess id: 9 Remote next mess id: 0
Local req queued: 9 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is not detected
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU:
548 bytes
Parent SA Extended Status:
Delete in progress: FALSE
Marked for delete: FALSE
Child sa: local selector 20.0.0.0/0 - 20.0.0.255/65535
remote selector 30.0.0.0/0 - 30.0.0.255/65535
ESP spi in/out: 0x4a7d5da2/0x56a28fa8
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IKEv1 トランスフォーム セットの作成

IKEv1 トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。特定のデータフローを保護する場合、ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエート中に、特定のトランスフォーム セットを使用することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットにより、関連付けられたクリプト マップ エントリで指定された ACL のデータ フローが保護されます。ASA 設定でトランスフォーム セットを作成して、クリプト マップまたはダイナミック クリプト マップ エントリでトランスフォーム セットの最大数 11 を指定できます。

次の表に、有効な暗号化方式と認証方式を示します。

表 10: 有効な暗号化方式と認証方式

有効な暗号化方式	有効な認証方式
	esp-sha-hmac (デフォルト)
esp-aes (128 ビット暗号化) (デフォルト)	
esp-aes-192	
esp-aes-256	
esp-null	

パブリック インターネットなどの非信頼ネットワークを介して接続された 2 つの ASA 間で IPsec を実装する通常の方法は、トンネル モードです。トンネル モードはデフォルトであり、設定は必要ありません。

トランスフォーム セットを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のサイト間タスクを実行します。

手順

- ステップ 1** グローバル コンフィギュレーション モードで、**crypto ipsec ikev1 transform-set** コマンドを入力します。次の例では、名前が FirstSet で、暗号化と認証に esp-aes と esp-sha-hmac を使用するトランスフォーム セットを設定しています。構文は次のようになります。

esp-sha-hmac (デフォルト)

crypto ipsec ikev1 transform-set transform-set-name encryption-method authentication-method

hostname(config)#

crypto ipsec transform-set FirstSet esp-aes esp-sha-hmac

```
hostname(config)#
```

ステップ2 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 プロポーザルの作成

IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

次の表に、有効な IKEv2 暗号化方式と認証方式を示します。

表 11: 有効な IKEv2 暗号化方式と整合性方式

有効な暗号化方式	有効な整合性方式
	sha (デフォルト)
aes (デフォルト) : 128 ビット キーを使用した AES。	
aes-192	
aes-256	

IKEv2 プロポーザルを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のタスクを実行します。

手順

ステップ1 グローバル コンフィギュレーション モードで **crypto ipsec ikev2 ipsec-proposal** コマンドを使用して、プロポーザルの複数の暗号化および整合性タイプを指定できる IPsec プロポーザル コンフィギュレーションモードを開始します。この例では、**secure** がプロポーザルの名前です。

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)#
```

ステップ2 次に、プロトコルおよび暗号化タイプを入力します。サポートされている唯一のプロトコルは ESP です。次に例を示します。


```
hostname(config-ipsec-proposal)# protocol esp encryption aes  
hostname(config-ipsec-proposal)#
```

ステップ3 整合性タイプを入力します。次に例を示します。

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1  
hostname(config-ipsec-proposal)#
```

ステップ4 変更を保存します。

ACL の設定

ASA は、アクセス コントロール リストを使用してネットワーク アクセスをコントロールします。デフォルトでは、適応型セキュリティ アプライアンスはすべてのトラフィックを拒否します。トラフィックを許可する ACL を設定する必要があります。詳細については、一般的操作用 コンフィギュレーション ガイドの「Information About Access Control Lists」を参照してください。

この LAN-to-LAN VPN 制御接続で設定する ACL は、送信元 IP アドレスと変換された宛先 IP アドレス、および任意指定のポートに基づいています。接続の両側に、互いにミラーリングする ACL を設定します。

VPN トラフィック用の ACL は、変換アドレスを使用します。



(注) VPN フィルタを使用した ACL の設定方法の詳細については、[リモートアクセスの VLAN の指定またはグループ ポリシーへの統合アクセス コントロール ルールの適用](#) (162 ページ) を参照してください。

手順

ステップ1 **access-list extended** コマンドを入力します。

```
access-list listname extended permit ip source-ipaddress source-netmask destination-ipaddress  
destination-netmask
```

次の例では、192.168.0.0 のネットワーク内にある IP アドレスから 150.150.0.0 のネットワークにトラフィックを送信する、l2l_list という名前の ACL を設定します。

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0  
150.150.0.0 255.255.0.0  
hostname(config)#
```

ステップ2 ACL をミラーリングする接続のもう一方の側の ASA に、ACL を設定します。

1つのクリプトマップのACLで定義されたサブネット、または同じクリプトマップに接続された2つの異なる暗号 ACLで定義されたサブネットは重複できません。

次の例では、該当ピアのプロンプトは `hostname2` です。

```
hostname2(config)# access-list 121_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname2(config)#
```

トンネル グループの定義

トンネルグループは、トンネル接続ポリシーを格納したレコードのセットです。AAAサーバーを識別するトンネルグループを設定し、接続パラメータを指定し、デフォルトのグループポリシーを定義します。ASAは、トンネルグループを内部的に保存します。

ASAには、2つのデフォルトトンネルグループがあります。1つはデフォルトのIPsecリモートアクセストンネルグループである `DefaultRAGroup` で、もう1つはデフォルトのIPsec LAN-to-LANトンネルグループである `DefaultL2Lgroup` です。これらは変更可能ですが、削除はできません。

IKEバージョン1および2の主な相違点は、使用できる認証方式にあります。IKEv1では、両方のVPNエンドで1つのタイプの認証のみが許可されます（つまり、事前共有キーまたは証明書）。しかし、IKEv2では、別のローカルおよびリモート認証CLIを使用して非対称認証方式を設定できます（つまり、送信元に対しては事前共有キー認証を設定し、応答側に対しては証明書認証を設定できます）。したがって、IKEv2を使用すると、両方の側がそれぞれ異なるクレデンシャルで認証する非対称認証を使用できます（事前共有キーまたは証明書）。

また、環境に合った新しいトンネルグループを1つ以上作成することもできます。トンネルネゴシエーションで識別された特定のトンネルグループがない場合は、ASAは、これらのグループを使用して、リモートアクセスおよびLAN-to-LANトンネルグループのデフォルトトンネルパラメータを設定します。

基本的なLAN-to-LAN接続を確立するには、次のように2つの属性をトンネルグループに設定する必要があります。

- 接続タイプをIPsec LAN-to-LANに設定します。
- IPアドレスの認証方式（つまり、IKEv1とIKEv2用の事前共有キー）を設定します。

手順

ステップ1 接続タイプをIPsec LAN-to-LANに設定するには、**tunnel-group** コマンドを入力します。

構文は、**tunnel-group *nametype* *type*** です。ここで、*name* はトンネルグループに割り当てる名前であり、*type* はトンネルのタイプです。CLIで入力するトンネルタイプは次のとおりです。

- **remote-access** (IPsec、SSL、およびクライアントレス SSL リモート アクセス)
- **ipsec-l2l** (IPsec LAN-to-LAN)

次の例では、トンネル グループの名前は、LAN-to-LAN ピアの IP アドレスである 10.10.4.108 です。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

(注)

IP アドレス以外の名前が付いている LAN-to-LAN トンネル グループは、トンネル認証方式がデジタル証明書である、またはピアが Aggressive モードを使用するように設定されている（あるいはその両方の）場合に限り使用できます。

ステップ 2 事前共有キーを使用するように認証方式を設定するには、**ipsec** 属性モードに入り、**ikev1pre-shared-key** コマンドを入力して事前共有キーを作成します。この LAN-to-LAN 接続の両方の ASA で、同じ事前共有キーを使用する必要があります。

キーは、1 ～ 128 文字の英数字文字列です。

次の例で、IKEv1 事前共有キーは 44kkaol59636jnfx です。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1-pre-shared-key 44kkaol59636jnfx
```

ステップ 3 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

トンネルが稼働中であることを確認するには、**show vpn-sessiondb summary**、**show vpn-sessiondb detail l2l**、または **show crypto ipsec sa** コマンドを使用します。

クリプト マップの作成とインターフェイスへの適用

クリプトマップエントリは、IPsecセキュリティアソシエーションの次のような各種要素をまとめたものです。

- IPsec で保護する必要のあるトラフィック (ACL で定義)
- IPsec で保護されたトラフィックの送信先 (ピアで指定)
- トラフィックに適用される IPsec セキュリティ (トランスフォームセットで指定)
- IPsec トラフィックのローカルアドレス (インターフェイスにクリプトマップを適用して指定)

IPsec が成功するためには、両方のピアに互換性のあるコンフィギュレーションを持つクリプトマップエントリが存在する必要があります。2つのクリプトマップエントリが互換性を持つためには、両者が少なくとも次の基準を満たす必要があります。

- クリプトマップエントリに、互換性を持つ暗号 ACL（たとえば、ミラーイメージ ACL）が含まれている。応答するピアがダイナミック クリプトマップを使用している場合は、ASA の暗号 ACL のエントリがピアの暗号 ACL によって「許可」されている必要があります。
- 各クリプトマップエントリが他のピアを識別する（応答するピアがダイナミック クリプトマップを使用していない場合）。
- クリプトマップエントリに、共通のトランスフォームセットが少なくとも1つ存在する。

所定のインターフェイスに対して複数のクリプトマップエントリを作成する場合は、各エントリのシーケンス番号（seq-num）を使用して、エントリにランクを付けます。seq-num が小さいほど、プライオリティが高くなります。クリプトマップセットを持つインターフェイスでは、ASA はまずトラフィックをプライオリティの高いマップエントリと照合して評価します。

リバースルートインジェクション（RRI）がクリプトマップに適用されている場合、そのマップは ASA 上のインターフェイスごとに一意である必要があります。つまり、同じクリプトマップは複数のインターフェイスに適用できないということです。複数のクリプトマップを複数のインターフェイスに適用すると、ルートが正しくクリーンアップされないことがあります。複数のインターフェイスに1つのクリプトマップが必要な場合は、一意に定義したマップを各ルートで使用する必要があります。

次の条件のいずれかに当てはまる場合は、所定のインターフェイスに対して複数のクリプトマップエントリを作成します。

- 複数のピアで異なるデータフローを処理する場合。
- 異なるタイプのトラフィック（同一または個別のピアへの）に異なる IPsec セキュリティを適用する場合。たとえば、あるサブネットセット間のトラフィックは認証し、別のサブネットセット間のトラフィックは認証および暗号化するような場合です。この場合は、異なるタイプのトラフィックを2つの個別の ACL で定義し、各暗号 ACL に対して個別にクリプトマップエントリを作成します。

複数のインターフェイスへの暗号マップの適用

デュアル ISP の場合、ASA の外部インターフェイスとバックアップ インターフェイスに暗号マップを適用できます。この設定を使用する場合、origin-only オプションは使用できません。この冗長性が必要な場合は、仮想トンネルインターフェイス（VTI）を使用する必要があります。

複数のインターフェイスで暗号マップを使用する場合：

- ルーティングプロトコルまたはルートトラッキングが必要です。
- リモート側もルーティングプロトコルを使用していることを確認してください。

- ASA は優先度の低いルートを持つインターフェイスでリモートサイトからの接続を許可するため、同じ暗号マップに対して複数のインターフェイスを慎重に選択する必要があります。

クリプト マップを作成してグローバル コンフィギュレーション モードで外部インターフェイスに適用するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次の手順を実行します。

手順

- ステップ 1** ACL をクリプト マップ エントリに割り当てるには、**crypto map match address** コマンドを入力します。

構文は、**crypto map map-name seq-num match address aclname** です。次の例では、マップ名は **abcmap**、シーケンス番号は 1、ACL 名は **121_list** です。

```
hostname(config)# crypto map abcmap 1 match address 121_list
hostname(config)#
```

- ステップ 2** IPsec 接続用のピアを指定するには、**crypto map set peer** コマンドを入力します。

構文は、**crypto map map-name seq-num set peer {ip_address1 | hostname1} [... ip_address10 | hostname10]** です。次の例では、ピア名は 10.10.4.108 です。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

- ステップ 3** クリプトマップエントリに IKEv1 トランスフォームセットを指定するには、**crypto map ikev1 set transform-set** コマンドを入力します。

構文は、**crypto map map-name seq-num ikev1 set transform-set transform-set-name** です。次の例では、トランスフォームセット名は FirstSet です。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

- ステップ 4** クリプト マップ エントリに IKEv2 プロポーザルを指定するには、**crypto map ikev2 set ipsec-proposal** コマンドを入力します。

構文は、**crypto map map-name seq-num set ikev2 ipsec-proposal proposal-name** です。次の例では、プロポーザル名は **secure** です。

crypto map コマンドでは、1 つのマップ インデックスに複数の IPsec プロポーザルを指定できます。この場合、複数のプロポーザルがネゴシエーションの一部として IKEv2 ピアに送信され、プロポーザルの順序はクリプト マップ エントリの順序付け時に管理者が決定します。

(注)

連結モード (AES-GCM/GMAC) および通常モード (その他すべて) のアルゴリズムが IPsec プロポーザルにある場合、ピアに単一のプロポーザルを送信できません。この場合、2 つのプ

ロポーザルが必要となります（連結モードのアルゴリズムに1つ、通常モードのアルゴリズムに1つ）。

```
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)#
```

クリプトマップのインターフェイスへの適用

クリプトマップセットは、IPsec トラフィックが通過する各インターフェイスに適用する必要があります。ASA は、すべてのインターフェイスで IPsec をサポートします。クリプトマップセットをインターフェイスに適用すると、ASA はすべてのインターフェイス トラフィックをクリプトマップセットと照合して評価し、接続時やセキュリティ アソシエーションのネゴシエート時に、指定されたポリシーを使用します。

また、クリプトマップをインターフェイスにバインドすると、セキュリティ アソシエーション データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期化されます。クリプトマップを後から変更すると、ASA は自動的にその変更を実行コンフィギュレーションに適用します。既存の接続はすべてドロップされ、新しいクリプトマップの適用後に再確立されます。

設定済みのクリプトマップを外部インターフェイスに適用するには、次の手順を実行します。

手順

ステップ 1 **crypto map interface** コマンドを入力します。構文は、**crypto map map-name interface interface-name** です。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

ステップ 2 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```



第 9 章

AnyConnect VPN Client 接続

この項では、AnyConnect VPN Client 接続を設定する方法について説明します。

- [セキュアクライアント VPN Client について \(261 ページ\)](#)
- [セキュアクライアントのライセンス要件 \(263 ページ\)](#)
- [セキュアクライアント 接続の設定 \(263 ページ\)](#)
- [SAML 2.0 \(284 ページ\)](#)
- [セキュアクライアント 接続のモニタリング \(296 ページ\)](#)
- [AnyConnect VPN セッションのログオフ \(298 ページ\)](#)
- [セキュアクライアント 接続機能の履歴 \(298 ページ\)](#)

セキュアクライアント VPN Client について

セキュアクライアントは、ASA へのセキュアな SSL および IKEv2 IPsec 接続をリモートユーザーに提供します。事前にクライアントがインストールされていない場合、リモートユーザーは、SSL または IPsec/IKEv2 VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。ASA が、`http://` 要求を `https://` にリダイレクトするように設定されていない限り、ユーザーは URL を `https://<address>` の形式で入力する必要があります。

URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面を表示します。ユーザーがログインと認証に成功し、そのユーザーがクライアントを要求していると ASA で識別されると、セキュリティ アプライアンスは、リモートコンピュータのオペレーティングシステムに合うクライアントをダウンロードします。ダウンロード後、クライアントは自分自身でインストールと設定を行い、セキュアな SSL または IPsec/IKEv2 接続を確立します。接続の終了時には、（設定に応じて）そのまま残るか、または自分自身をアンインストールします。

以前からインストールされているクライアントの場合は、ユーザーの認証時に、ASA によってクライアントのリビジョンが点検され、必要に応じてアップグレードされます。

クライアントが ASA と SSL VPN 接続をネゴシエートした場合は、Transport Layer Security (TLS) を使用して接続します。状況に応じて、Datagram Transport Layer Security (DTLS) が使用されます。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避さ

れ、パケット遅延の影響を受けやすいリアルタイムアプリケーションのパフォーマンスが向上します。

セキュアクライアントは、ASA からダウンロードできます。または、システム管理者が手動でリモートPCにインストールできます。クライアントの手動インストールの詳細については、『[Cisco AnyConnect Secure Mobility Configuration Guide](#)』の適切なリリースを参照してください。

ASA は、ユーザーが確立している接続のグループ ポリシーまたはユーザー名属性に基づきクライアントをダウンロードします。自動的にクライアントをダウンロードするように ASA を設定するか、またはクライアントをダウンロードするかをリモートユーザーに確認するように設定できます。後者の場合、ユーザーが応答しなかった場合は、タイムアウト時間が経過した後にクライアントをダウンロードするか、ログインページを表示するように ASA を設定できます。

セキュアクライアントの要件

セキュアクライアントを実行しているエンドポイントコンピュータの要件については、『[Cisco AnyConnect Secure Mobility Release Notes](#)』の適切なリリースを参照してください。

に関する注意事項と制限事項 セキュアクライアント

- ASA では、リモート HTTPS 証明書は確認されません。
- シングルまたはマルチコンテキストモードでサポートされます。AnyConnect Apex ライセンスは、マルチコンテキストモードのリモートアクセス VPN に必要です。ASA は AnyConnect Apex ライセンスを特異的に認識しませんが、プラットフォーム制限へのライセンス済み AnyConnect Premium、携帯電話用セキュアクライアント、Cisco VPN フォン用セキュアクライアント、および Advanced Endpoint Assessment など、Apex ライセンスのライセンス特性を適用します。共有ライセンス、AnyConnect Essentials、フェールオーバーライセンス集約、およびフレックス/時間ベースのライセンスはサポートされていません。
- RA VPN ヘッドエンドなどに対する `curl` などのコマンドの実行は直接サポートされていないため、望ましい結果が得られない可能性があります。たとえば、ヘッドエンドは HTTP HEAD リクエストに応答しません。
- Cisco 88xx シリーズなどのハードウェア VPN 電話機がセキュアクライアントを使用すると、DTLS がアップ状態で、Dead Peer Detection (DPD) が構成されていても、再接続が発生することがあります。
- クライアントがセキュアクライアントに接続すると、接続の前後でクライアントの IP アドレスが変わります。ASA は、この動作をサポートしています。

セキュアクライアントのライセンス要件



(注) この機能は、ペイロード暗号化機能のないモデルでは使用できません。

VPN ライセンスには、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。モデルごとの最大値については、「[Cisco ASA Series Feature Licenses](#)」を参照してください。

クライアントレス SSL VPN セッションを開始後、ポータルからセキュアクライアントクライアントセッションを開始した場合は、合計で1つのセッションが使用されます。これに対して、最初にセキュアクライアントを（スタンドアロンクライアントなどから）開始後、クライアントレス SSL VPN ポータルにログインした場合は、2つのセッションが使用されます。

セキュアクライアント 接続の設定

ここでは、ASA が AnyConnect VPN クライアント接続を受け入れるように設定するための前提条件、制限事項、および詳細なタスクについて説明します。

クライアントを Web 展開するための ASA の設定

この項では、セキュアクライアントを Web 展開するように ASA を設定する手順について説明します。

始める前に

TFTP や別の方法を使用して、クライアントイメージパッケージを ASA にコピーします。



(注) クライアントレス VPN 機能が ASA で無効になっている場合でも、Web ブラウザを使用して AnyConnect Web 展開 (<https://x.x.x.x<ASA IP address>>) にアクセスする際、ASA の VPN セッションはクライアントレスとしてカウントされます。

手順

ステップ 1 フラッシュ上のファイルをセキュアクライアント パッケージファイルとして指定します。

ASA は、リモート PC にダウンロードするために、キャッシュ メモリのファイルを展開します。複数のクライアントがある場合は、order 引数を使用して、クライアントイメージに順序を割り当てます。

ASA は、リモート PC のオペレーティングシステムと一致するまで、指定されている順序で各クライアントの一部をダウンロードします。そのため、最も一般的に使用されているオペレーティングシステム用のイメージには、最も低い数値を割り当てます。

anyconnect image filename order

例：

```
hostname(config-webvpn)# anyconnect image
anyconnect-win-2.3.0254-k9.pkg 1
hostname(config-webvpn)# anyconnect image
anyconnect-macosx-i386-2.3.0254-k9.pkg 2
hostname(config-webvpn)# anyconnect image
anyconnect-linux-2.3.0254-k9.pkg 3
```

(注)

anyconnect image コマンドでセキュアクライアントイメージを設定した後に **anyconnect enable** コマンドを発行する必要があります。セキュアクライアントをイネーブルにしない場合、AnyConnect の動作は不完全になり、**show webvpn anyconnect** コマンドは SSL VPN クライアントがイネーブルにされていないと見なし、インストールされたセキュアクライアントパッケージのリストは表示されません。

ステップ 2 クライアントレス接続またはセキュアクライアント SSL 接続のインターフェイスの SSL をイネーブルにします。

enable interface

例：

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

ステップ 3 このコマンドを発行しないと、セキュアクライアントは想定したとおりに機能せず、**show webvpn anyconnect** コマンドは、インストールされたセキュアクライアントパッケージのリストを表示する代わりに、「SSL VPN is not enabled」というメッセージを返します。

AnyConnect のイネーブル

ステップ 4 (任意) アドレスプールを作成します。DHCP やユーザーによる割り当てのアドレスの指定など、別のアドレス割り当ての方法を使用することもできます。

ip local pool poolname startaddr-endaddr mask mask

例：

```
hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

ステップ 5 アドレスプールをトンネルグループに割り当てます。

address-pool poolname

例：

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

ステップ 6 デフォルトのグループ ポリシーをトンネル グループに割り当てます。

default-group-policy name

```
hostname(config-tunnel-general)# default-group-policy sales
```

ステップ 7 クライアントレスポータルおよびセキュアクライアント GUI のログインページでのトンネルグループリストの表示をイネーブルにします。エイリアスのリストは、*group-alias name enable* コマンドによって定義されます。

group-alias name enable

例：

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

ステップ 8 グループまたはユーザーの許可された VPN トンネリングプロトコルとしてセキュアクライアントを指定します。

tunnel-group-list enable

例：

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

ステップ 9 グループまたはユーザーの許可された VPN トンネリングプロトコルとして SSL を指定します。その他のプロトコルを追加して指定することもできます。詳細については、コマンドリファレンスの *vpn-tunnel-protocol* コマンドを参照してください。

vpn-tunnel-protocol

例：

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol
```

次のタスク

グループ ポリシーに対するユーザーの割り当ての詳細については、第 6 章「接続プロファイル、グループ ポリシー、およびユーザーの設定」を参照してください。

永続的なクライアント インストールのイネーブル化

永続的なクライアント インストールをイネーブルにすると、クライアントの自動アンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモートコンピュータにインストールされたままなので、リモートユーザーの接続時間が短縮されます。

特定のグループまたはユーザーに対する永続的なクライアントインストールをイネーブルにするには、グループ ポリシー **webvpn** モードまたはユーザー名 **webvpn** モードで **anyconnect keep-installer** コマンドを使用します。

デフォルトでは、クライアントの永続的なインストールはイネーブルになっています。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。次の例では、セッションの終了時点でリモート コンピュータのクライアントを削除するように既存のグループ ポリシー **sales** を設定します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

DTLS の設定

Datagram Transport Layer Security (DTLS) を使用すると、SSL VPN 接続を確立しているセキュアクライアントで、2つのトンネル (SSL トンネルと DTLS トンネル) を同時に使用できます。DTLS を使用すると、SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

始める前に

このヘッドエンドで DTLS を設定し、使用する DTLS のバージョンを確認するには、[SSL の詳細設定 \(100 ページ\)](#) を参照してください。

DTLS を TLS 接続にフォールバックさせるには、デッドピア検知 (DPD) をイネーブルにする必要があります。DPD をイネーブルにしない場合、DTLS 接続で問題が発生すると、TLS にフォールバックする代わりに接続は終了します。DPD の詳細については、[デッドピア検出の設定 \(279 ページ\)](#) を参照してください。

手順

ステップ 1 セキュアクライアント VPN 接続に対して DTLS オプションを指定します。

a) **webvpn** モードのインターフェイスで SSL と DTLS を有効にします。

デフォルトでは、DTLS がイネーブルになるのは、インターフェイスで SSL VPN アクセスをイネーブルにした場合です。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

webvpn コンフィギュレーション モードで、**enable interface tls-only** コマンドを使用し、すべてのセキュアクライアントユーザーに対して DTLS をディセーブルにします。

DTLS をディセーブルにすると、SSL VPN 接続は SSL VPN トンネルだけに接続します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only
```

- b) **port** および **dtls port** コマンドを使用して SSL および DTLS のポートを設定します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

ステップ 2 特定のグループ ポリシーに対して DTLS オプションを指定します。

- a) グループ ポリシー **webvpn** コンフィギュレーション モードまたはユーザー名 **webvpn** コンフィギュレーション モードで、**anyconnect ssl dtls** コマンドを使用して特定のグループまたはユーザーに対して DTLS をイネーブルにします。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl dtls enable
```

- b) 必要に応じて、**anyconnect dtls compression** コマンドを使用して DTLS 圧縮をイネーブルにします。

```
hostname(config-group-webvpn)# anyconnect dtls compression lzs
```

リモート ユーザーに対するプロンプト

手順

ASA で、リモート SSL VPN クライアント ユーザーがクライアントをダウンロードするためのプロンプトをイネーブルにするには、グループ ポリシー **webvpn** コンフィギュレーション モードまたはユーザー名 **webvpn** コンフィギュレーション モードで **anyconnect ask** コマンドを使用します。

[no] anyconnect ask {none | enable [default {webvpn | } timeout value]}

- **anyconnect enable** を指定すると、クライアントをダウンロードするか、クライアントレス ポータルページに移動するかを尋ねるプロンプトをリモート ユーザーに表示し、ユーザーの応答を無期限に待機します。
- **anyconnect ask enable default** を指定すると、すぐにクライアントがダウンロードされます。
- **anyconnect ask enable default webvpn** を指定すると、すぐにポータル ページに移動します。
- **anyconnect ask enable default timeoutvalue** を指定すると、クライアントをダウンロードするか、またはクライアントレス ポータルページに移動するかを尋ねるプロンプトをリモート ユーザーに表示し、デフォルト アクション（クライアントのダウンロード）を実行する前に、**value** の間待機します。

- **anyconnect ask enable default clientless timeoutvalue** を指定すると、クライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかを尋ねるプロンプトをリモート ユーザーに表示し、デフォルト アクション（クライアントレス ポータル ページの表示）を実行する前に、**value** の間待機します。

次の図に、**default anyconnect timeout value** または **default webvpn timeout value** が設定された場合にリモート ユーザーに表示されるプロンプトを示します。

図 6: リモート ユーザーに表示される **SSL VPN** クライアントのダウンロードを求めるプロンプト



例

次の例では、ASA でクライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかをユーザーに尋ねるプロンプトを表示して、クライアントをダウンロードする前に応答を 10 秒待機するように設定しています。

```
hostname(config-group-webvpn) # anyconnect ask enable default anyconnect timeout
10
```

セキュアクライアント プロファイルダウンロードのイネーブル化

セキュアクライアント プロファイル（コアクライアントとその VPN 機能のコンフィギュレーション設定、およびオプションのクライアント モジュールのコンフィギュレーション設定を含む XML ファイル）でセキュアクライアント 機能をイネーブルにします。ASA はセキュアクライアントのインストールおよび更新中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

クライアントにダウンロードされるファイルのフォーマットは、**<profile_name>.xml** です。

プロファイルは、セキュアクライアント プロファイル エディタを使用して設定できます。このエディタは、ASDM または ISE から起動できる便利な GUI ベースの構成ツールです。Windows 用セキュアクライアント ソフトウェア パッケージにはエディタが含まれています。このエディタは、クライアント パッケージを選択したヘッドエンド デバイスにロードし、セキュアクライアント イメージとして指定するとアクティブになります。

ASDM または ISE に統合されたプロファイル エディタの代わりに、Windows 用プロファイル エディタのスタンドアロンバージョンも使用できます。クライアントを事前展開する場合は、

ソフトウェア管理システムを使用してコンピュータに展開する、VPNサービス用のプロファイルおよびその他のモジュールを、スタンドアロンのプロファイルエディタを使用して作成できます。

セキュアクライアント およびプロファイルエディタの詳細については、『[Cisco AnyConnect Secure Mobility Configuration Guide](#)』の適切なリリースを参照してください。



- (注) セキュアクライアント プロトコルのデフォルトはSSLです。IPsec IKEv2をイネーブルにするには、ASAでIKEv2設定を設定し、また、クライアントプロファイルのプライマリプロトコルとしてIKEv2を設定する必要があります。IKEv2enabledプロファイルは、エンドポイントコンピュータに展開する必要があります。それ以外の場合、クライアントはSSLを使用して接続を試行します。

手順

- ステップ 1** ASDM/ISEのプロファイルエディタまたはスタンドアロンプロファイルエディタを使用して、プロファイルを作成します。
- ステップ 2** tftp または別の方式を使用して、ASAのフラッシュメモリにプロファイルファイルをロードします。
- ステップ 3** webvpn コンフィギュレーションモードで **anyconnect profiles** コマンドを使用して、キャッシュメモリにロードするクライアントプロファイルとしてこのファイルを識別します。

例：

次に、プロファイルとしてファイル sales_hosts.xml と engineering_hosts.xml を指定する例を示します。

```
asa1(config-webvpn)# anyconnect profiles sales
disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering
disk0:/engineering_hosts.xml
```

これで、プロファイルをグループポリシーに利用できます。

dir cache:stc/profiles コマンドを使用して、キャッシュメモリにロードされたプロファイルを表示します。

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774          11:54:41 Nov 22 2006  engineering.xml
0      ----  774          11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

ステップ 4 グループ ポリシー webvpn コンフィギュレーション モードを開始し、**anyconnect profiles** コマンドを使用して、グループ ポリシーのクライアント プロファイルを指定します。

例：

使用可能なプロファイルを表示するには、**client profiles value** コマンドに続けて、疑問符 (?) を入力します。次に例を示します。

```
asal(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages: engineering sales
```

次の例では、クライアントプロファイルタイプが **vpn** のプロファイル **sales** を使用するようにグループ ポリシーを設定します。

```
asal(config-group-webvpn)# anyconnect profiles value sales type vpn
asal(config-group-webvpn)#
```

セキュアクライアント 遅延アップグレードのイネーブル化

セキュアクライアント ユーザーは、遅延アップグレードを使用して、クライアントアップグレードのダウンロードを遅らせることができます。クライアントアップデートが使用できる場合、セキュアクライアントは、更新するか、またはアップグレードを延期するかを尋ねるダイアログを開きます。セキュアクライアント プロファイル設定で [自動更新 (AutoUpdate)] が [有効 (Enabled)] に設定されていない限り、このアップグレードダイアログは表示されません。

遅延アップグレードをイネーブルにするには、カスタム属性タイプと名前付きの値を ASA に追加して、グループ ポリシーでこれらの属性を参照および設定します。

次のカスタム属性は遅延アップグレードをサポートします。

表 12: 遅延アップグレードのカスタム属性

カスタム属性タイプ	有効な値	デフォルト値	注記
DeferredUpdateAllowed	true false	false	true は遅延アップデートを有効にします。遅延アップデートが無効 (false) の場合、次の設定は無視されます。

カスタム属性タイプ	有効な値	デフォルト値	注記
DeferredUpdateMinimumVersion	x.y.z	0.0.0	アップデートを遅延できるようにインストールする必要がある セキュアクライアント の最小バージョン。 最小バージョンのチェックは、ヘッドエンドで有効になっているすべてのモジュールに適用されます。有効になっているモジュール（VPN を含む）がインストールされていないか、最小バージョンを満たしていない場合、接続は遅延アップデートの対象になりません。 この属性が指定されていない場合、エンドポイントにインストールされているバージョンに関係なく、遅延プロンプトが表示されます（または自動消去されます）。
DeferredUpdateDismissTimeout	0 ～ 300（秒）	none（ディセーブル）	遅延アップデート プロンプトが表示され、自動的に消去されるまでの秒数。この属性は、遅延アップデート プロンプトが表示される場合に限り適用されます（最小バージョン属性が最初に評価されます）。 この属性がない場合、自動消去機能が無効になり、ユーザが応答するまでダイアログが表示されます（必要な場合）。 この属性を 0 に設定すると、次に基づいて強制的に自動遅延またはアップグレードが実施されます。 - インストールされているバージョンおよび DeferredUpdateMinimumVersion の値。 - DeferredUpdateDismissResponse の値。
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout が発生した場合に実行するアクション。

手順

ステップ 1 webvpn コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用してカスタム属性タイプを作成します。

[no] anyconnect-custom-attr attr-type [description description]

例：

次に、カスタム属性タイプ `DeferredUpdateAllowed` および `DeferredUpdateDismissTimeout` を追加する例を示します。

```
hostname(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
hostname(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout
```

ステップ 2 グローバル コンフィギュレーション モードで **`anyconnect-custom-data`** コマンドを使用してカスタム属性の名前付きの値を追加します。長い値を持つ属性の場合は、重複するエントリを指定でき、連結が可能です。ただし、設定エントリが重複している場合、[Defer Update] ダイアログは表示されず、ユーザーはアップグレードを保留できません。代わりに、アップグレードが自動的に行われます。

[no] **`anyconnect-custom-data attr-type attr-name attr-value`**

例：

次に、カスタム属性タイプ `DeferredUpdateDismissTimeout` の名前付きの値と、`DeferredUpdateAllowed` をイネーブルにするための名前付きの値を追加する例を示します。

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimeout
def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed
def-allowed true
```

ステップ 3 **`anyconnect-custom`** コマンドを使用して、カスタム属性の名前付きの値をグループ ポリシーに追加するか、グループ ポリシーから削除します。

- **`anyconnect-customattr-type value attr-name`**
- **`anyconnect-custom attr-type none`**
- **`no anyconnect-custom attr-type`**

例：

次に、`sales` という名前のグループ ポリシーで延期アップデートを有効にしてタイムアウトを 150 秒に設定する例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

DSCP の保存の有効化

Windows または OS X プラットフォームでは、DTLS 接続の場合にのみ別のカスタム属性を設定することで DiffServ コード ポイント (DSCP) を制御できます。DSCP の保存を有効にする

と、デバイスは遅延の影響を受けやすいトラフィックを優先することができます。ルータでは、これが設定されているかどうかが反映され、アウトバウンド接続品質の向上のために優先トラフィックがマークされます。

手順

ステップ 1 webvpn コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用してカスタム属性タイプを作成します。

[no] anyconnect-custom-attr DSCP Preservation Allowed description Set to control Differentiated Services Code Point (DSCP) on Windows or OS X platforms for DTLS connections only.

ステップ 2 グローバル コンフィギュレーション モードで **anyconnect-custom-data** コマンドを使用してカスタム属性の名前付きの値を追加します。

[no] anyconnect-custom-data DSCP Preservation Allowed true

(注)

デフォルトでは、セキュアクライアントは DSCP の保存を実行します (true)。無効にするには、ヘッドエンドでカスタム属性を false に設定し、接続を再実行します。

追加 セキュアクライアント 機能のイネーブル化

ダウンロード時間を最小限に抑えるために、クライアントは必要なコア モジュールのダウンロード (ASA または ISE から) だけを要求します。追加機能が セキュアクライアント で使用可能になったら、それらの機能を使用できるようにするためにリモートクライアントを更新する必要があります。

新しい機能をイネーブルにするには、グループ ポリシー webvpn またはユーザー名 webvpn コンフィギュレーション モードで **anyconnect modules** コマンドを使用して、新しいモジュール名を指定する必要があります。

[no]anyconnect modules {none | value string}

複数のストリングを指定する場合は、カンマで区切ります。

Start Before Logon のイネーブル化

Start Before Logon (SBL) を使用すると、Windows PC にインストールされている セキュアクライアントに対するログインスクリプト、パスワードキャッシング、ドライブマッピングなどが使用できるようになります。SBL では、セキュアクライアントの Graphical Identification and Authentication (GINA) をイネーブルにするモジュールをダウンロードするように ASA をイネーブルにする必要があります。次の手順は、SBL をイネーブルにする方法を示しています。

手順

ステップ 1 グループ ポリシー **webvpn** またはユーザー名 **webvpn** コンフィギュレーション モードで **anyconnect modules vpngina** コマンドを使用して、特定のグループまたはユーザーへの VPN 接続のための GINA モジュールを ASA でダウンロードする機能を有効にします。

例：

次の例では、ユーザーはグループ ポリシー **telecommuters** でグループ ポリシー属性モードを開始し、そのグループポリシーで **webvpn** コンフィギュレーションモードを開始し、ストリング **vpngina** を指定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect modules value vpngina
```

ステップ 2 クライアント プロファイル ファイル (AnyConnectProfile.tmpl) のコピーを取得します。

ステップ 3 プロファイル ファイルを編集して SBL がイネーブルであることを指定します。次の例では、Windows 用のプロファイル ファイル (AnyConnectProfile.tmpl) の関係部分を示しています。

```
<Configuration>
  <ClientInitialization>
    <UseStartBeforeLogon>false</UseStartBeforeLogon>
  </ClientInitialization>
```

<UseStartBeforeLogon>タグによって、クライアントが SBL を使用するかどうかが決まります。SBL をオンにするには、**false** を **true** で置き換えます。次の例は、SBL がオンになっているタグを示しています。

```
<ClientInitialization>
  <UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

ステップ 4 AnyConnectProfile.tmpl に対する変更を保存し、webvpn コンフィギュレーションモードで **profile** コマンドを使用して、ASA のグループまたはユーザーに対するプロファイル ファイルをアップデートします。次に例を示します。

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

セキュアクライアント ユーザーメッセージの言語の変換

ASA には、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザーに表示されるポータルと画面、および Cisco AnyConnect VPN Client ユーザーに表示されるインターフェイスの言語変換機能があります。

この項では、これらのユーザー メッセージを変換するために ASA を設定する方法について説明します。

言語変換について

リモートユーザーに可視である機能エリアとそれらのメッセージは、変換ドメイン内にまとめられています。すべての Cisco AnyConnect VPN Client のユーザーインターフェイスに表示されるメッセージは、セキュアクライアント ドメイン内にあります。

ASA のソフトウェア イメージ パッケージには、セキュアクライアント ドメインの変換テーブル テンプレートが含まれています。このテンプレートはエクスポートでき、入力する URL にテンプレートの XML ファイルが作成されます。このファイルのメッセージ フィールドは空です。メッセージを編集して、テンプレートをインポートし、フラッシュ メモリに置かれる新しい変換テーブル オブジェクトを作成できます。

既存の変換テーブルをエクスポートすることもできます。作成した XML ファイルに事前に編集したメッセージが表示されます。この XML ファイルを同じ言語名で再インポートすると、変換テーブル オブジェクトの新しいバージョンが作成され、以前のメッセージが上書きされます。セキュアクライアント ドメインの変換テーブルに対する変更は、ただちにセキュアクライアント クライアントユーザーに表示されます。

変換テーブルの作成

次の手順では、セキュアクライアント ドメインの変換テーブルを作成する方法について説明します。

手順

ステップ 1 特権 EXEC モードで **export webvpn translation-table** コマンドを使用して、コンピュータに変換テーブル テンプレートをエクスポートします。

次の例では、**show import webvpn translation-table** コマンドによって、使用可能な変換テーブル テンプレートとテーブルを表示しています。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect

PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

次に、セキュアクライアント変換ドメイン用の変換テーブルをエクスポートします。作成された XML ファイルのファイル名は *client* という名前が付けられ、空のメッセージ フィールドが含まれています。

```
hostname# export webvpn translation-table AnyConnect
template tftp://209.165.200.225/client
```

次の例では、テンプレートからインポートした **zh** という名前の変換テーブルをエクスポートします。zh は Microsoft Internet Explorer における中国語の省略形です。

```
hostname# export webvpn translation-table customization
language zh tftp://209.165.200.225/chinese_client
```

ステップ 2 変換テーブルの XML ファイルを編集します。次の例は、セキュアクライアントテンプレートの一部を示しています。この出力の最後には、**Connected** メッセージのメッセージ ID フィールド (msgid) とメッセージ文字列フィールド (msgstr) が含まれています。このメッセージは、クライアントが VPN 接続を確立するときにセキュアクライアント GUI に表示されます。完全なテンプレートには、多くのメッセージフィールドのペアが含まれています。

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

msgid には、デフォルト変換が含まれています。msgid に続く msgstr が変換を提供します。変換を作成するには、msgstr 文字列の引用符の間に変換対象のテキストを入力します。たとえば、メッセージ「Connected」をスペイン語で変換するには、引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

ファイルは必ず保存してください。

ステップ3 特権 EXEC モードで **import webvpn translation-table** コマンドを使用して、変換テーブルをインポートします。ブラウザと互換性がある言語の省略形を付けて新しい変換テーブルの名前を指定します。

次の例では、米国スペイン語用の Microsoft Internet Explorer で使用される省略形である *es-us* で XML ファイルがインポートされます。

```
hostname# import webvpn translation-table AnyConnect
language es-us tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

変換テーブルの削除

変換テーブルがなくなっただけの場合は、削除できます。

手順

ステップ1 既存の変換テーブルを一覧表示します。

次の例では、**show import webvpn translation-table** コマンドによって、使用可能な変換テーブル テンプレートとテーブルを表示しています。フランス語 (fr)、日本語 (ja)、ロシア語 (ru) のさまざまなテーブルが用意されています。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder
banners
csd
customization
url-list
webvpn
Translation Tables:
fr          PortForwarder
fr          AnyConnect
fr          customization
fr          webvpn
```

ja	PortForwarder
ja	AnyConnect
ja	customization
ja	webvpn
ru	PortForwarder
ru	customization
ru	webvpn

ステップ 2 不要な変換テーブルを削除します。

revert webvpn translation-table translationdomain language language

translationdomain は上記に示す変換テーブルの右側に記載されているドメインで、*language* は 2 文字の言語名です。

各テーブルを個別に削除する必要があります。1 つのコマンドを使用して、特定の言語のテーブルをすべて削除することはできません。

たとえば、セキュアクライアントのフランス語の変換テーブルを削除するには、次のコマンドを使用します。

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

高度な セキュアクライアント SSL 機能の設定

次の項では、セキュアクライアント SSL VPN 接続を調整する高度な機能について説明します。

キー再生成の有効化

ASA とセキュアクライアントが SSL VPN 接続でキー再生成を行うときは、暗号キーと初期化ベクトルを再ネゴシエーションして、接続のセキュリティを高めます。

特定のグループまたはユーザーの SSL VPN 接続で、クライアントによるキー再生成の実行を有効にするには、グループポリシー webvpn モードまたはユーザー名 webvpn モードで **anyconnect ssl rekey** コマンドを使用します。

[no]anyconnect ssl rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time minutes**}

- **method new-tunnel** キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
- **method ssl** キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
- **method none** キーの再生成を無効にします。
- **timeminutes** は、セッションの開始からまたは前回のキー再生成から、キーの再生成が行われるまでの時間を 1 から 10080（1 週間）の分数で指定します。



- (注) キーの再生成方法を **ssl** または **new-tunnel** に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。anyconnect ssl rekey コマンドの履歴については、コマンドリファレンスを参照してください。

次の例では、セッション開始の 30 分後に実施されるキー再生成中に、既存のグループ ポリシー **sales** に対する SSL との再ネゴシエーションを実施するようにクライアントを設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

デッドピア検出の設定

Dead Peer Detection (DPD) により、ピアの応答がなく接続が失敗している場合には、ASA (ゲートウェイ) またはクライアント側で瞬時に検出できます。デッドピア検出 (DPD) を有効にし、セキュアクライアントまたは ASA ゲートウェイが DPD を実行する頻度を設定するには、以下の手順を実行します。

始める前に

- この機能は、ASA ゲートウェイとセキュアクライアント SSL VPN クライアント間の接続のみに適用されます。DPD は、埋め込みが許可されない標準実装に基づくため、IPsec とは併用できません。
- DTLS をイネーブルにすると、Dead Peer Detection (DPD) もイネーブルになります。DPD により、失敗した DTLS 接続の TLS へのフォールバックがイネーブルになります。それ以外の場合、接続は終了します。
- ASA で DPD が有効になっているとき、Optimal MTU (OMTU) 機能を使用すると、クライアントが DTLS パケットを正常に渡すことができる最大のエンドポイント MTU を見つけることができます。最大 MTU までパディングされた DPD パケットを送信することによって、OMTU を実装します。ペイロードの正しいエコーをヘッドエンドから受信すると、MTU サイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されます。

手順

- ステップ 1** 目的のグループ ポリシーに移動します。
グループ ポリシーまたはユーザー名 webvpn モードを開始します。

```
hostname(config)# group-policy group-policy-name attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

または

```
hostname# username username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn)#
```

ステップ2 ゲートウェイ側の検出を設定します。

[no] anyconnect dpd-interval {[gateway {seconds | none}]} コマンドを使用します。

gateway は、ASA のことです。DPD を有効にし、ASA がクライアントからのパケットを待機する時間を 30 秒（デフォルト）から 3600 秒（1 時間）の範囲で指定します。値 300 が推奨されます。その間隔内にパケットが受信されない場合、ASA は同じ間隔で DPD テストを 3 回試行します。ASA はクライアントからの応答がない場合、TLS/DTLS トンネルを切断します。

（注）

none を指定すると、ASA が実行する DPD テストはディセーブルになります。このコマンドを構成から削除するには、**no anyconnect dpd-interval** を使用します。

none を指定すると、ASA が実行する DPD テストはディセーブルになります。このコマンドを設定から削除するには、**no anyconnect dpd-interval** を使用します。

ステップ3 クライアント側の検出を設定します。

[no] anyconnect dpd-interval {[client {seconds | none}]} コマンドを使用します。

client はセキュアクライアント のことです。DPD を有効にし、クライアントが DPD テストを実行する頻度を 30 秒（デフォルト）から 3600 秒（1 時間）の範囲で指定します。30 秒が推奨されます。

client none を指定すると、クライアントにより実行される DPD はディセーブルになります。このコマンドを設定から削除するには、**no anyconnect dpd-interval** を使用します。

例

次の例では、ASA による DPD の実行頻度が 30 秒に設定され、クライアントによる既存のグループ ポリシー *sales* に対する DPD の実行頻度が 10 秒に設定されています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

キープアライブの有効化

キープアライブメッセージの頻度を調整することで、接続がアイドルでいられる時間がデバイスによって制限されている場合でも、プロキシ、ファイアウォール、または NAT デバイス経由の SSL VPN 接続をオープンのまま維持します。また、頻度を調整すると、リモートユーザー

が Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバーの際に、SSL VPN クライアントセッションはスタンバイ デバイスに引き継がれません。

キープアライブ メッセージの頻度を設定するには、グループ ポリシー **webvpn** またはユーザー名 **webvpn** コンフィギュレーション モードから **keepalive** コマンドを使用します。設定からコマンドを削除して値が継承されるようにするには、このコマンドの **no** 形式を使用します。

[no] anyconnect ssl keepalive {none | seconds}

- **none** は、クライアントのキープアライブ メッセージを無効にします。
- **seconds** は、クライアントによるキープアライブ メッセージの送信をイネーブルにし、メッセージの頻度を 15 ～ 600 秒の範囲で指定します。

次の例では、既存のグループ ポリシー **sales** に対して、クライアントがキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるように ASA を設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
```

圧縮の使用

圧縮により、低帯域幅の接続に転送されるパケットのサイズが減少し、ASA とクライアント間の通信パフォーマンスが向上します。デフォルトでは、ASA では、グローバル レベルと特定のグループまたはユーザーの両方において、すべての SSL VPN 接続に対する圧縮がイネーブルになっています。



- (注) ブロードバンド接続の圧縮を実装する場合は、圧縮が損失が少ない接続に依存していることを慎重に考慮する必要があります。これが、ブロードバンド接続ではデフォルトで圧縮がイネーブルになっていない主な理由です。

圧縮は、グローバル コンフィギュレーション モードで **compression** コマンドを使用してグローバルにオンにする必要があります。そうすることで、グループ ポリシーおよびユーザー名 **webvpn** モードで **anyconnect ssl compression** コマンドを使用して、特定のグループまたはユーザーに圧縮を設定することができます。

圧縮のグローバルな変更

グローバルな圧縮の設定を変更するには、グローバル コンフィギュレーション モードで **anyconnect ssl compression** コマンドを使用します。設定からコマンドを削除するには、コマンドの **no** 形式を使用します。

次の例では、すべての SSL VPN 接続の圧縮は、グローバルにディセーブルになっています。

```
hostname(config)# no compression
```

グループおよびユーザーに対する圧縮の変更

特定のグループまたはユーザーに対する圧縮を変更するには、グループ ポリシーおよびユーザー名 webvpn モードで **anyconnect ssl compression** コマンドを使用します。

[no] anyconnect ssl compression {deflate | none}

デフォルトでは、グループおよびユーザーに対する SSL 圧縮は *deflate* (イネーブル) に設定されています。

コンフィギュレーションから **anyconnect ssl compression** コマンドを削除し、グローバル設定から値が継承されるようにするには、このコマンドの **no** 形式を使用します。

次に、グローバル ポリシー **sales** の圧縮をディセーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

MTU サイズの調整

クライアントによって確立された SSL VPN 接続の MTU サイズ (576 ~ 1406 バイト) は、グループ ポリシー webvpn またはユーザー名 webvpn コンフィギュレーションモードで **anyconnect mtu** コマンドを使用して調整できます。

[no] anyconnect mtu size

このコマンドは、セキュアクライアントのみに影響します。レガシー Cisco SSL VPN クライアント (SVC) は、さまざまな MTU サイズに調整できません。また、SSL で確立されたクライアント接続と DTLS による SSL で確立された接続は、このコマンドの影響を受けます。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、**no anyconnect mtu** です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

たとえば、ISE Posture AnyConnect モジュールの実行時に、「MTU configuration sent from the secure gateway is too small」というメッセージが表示されることがあります。**anyconnect ssl df-bit-ignore disable** と一緒に **anyconnect mtu 1200** を入力すると、これらのシステム スキャンエラーを回避できます。

例

次の例では、グループ ポリシー **telecommuters** の MTU サイズを 1200 バイトに設定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

セキュアクライアントイメージの更新

ASA のクライアント イメージは、次の手順を使用していつでもアップデートできます。

手順

- ステップ 1 特権 EXEC モードで **copy** コマンドを使用して、または別の方法で新しいクライアント イメージを ASA にコピーします。
- ステップ 2 新しいクライアント イメージ ファイルの名前が、すでにロードされているファイルと同じ場合は、設定内の **anyconnect image** コマンドを再入力します。新しいファイル名が異なっている場合は、**[no]anyconnect image image** コマンドを使用して古いファイルをアンインストールします。次に、**anyconnect image** コマンドを使用して、イメージに順序を割り当て、ASA が新しいイメージをロードするようにします。

IPv6 VPN アクセスのイネーブル化

IPv6 アクセスを設定する場合は、コマンドライン インターフェイスを使用します。ASA のリリース 9.0 (x) では、外部インターフェイスへの IPv6 VPN 接続 (SSL および IKEv2/IPsec プロトコルを使用) のサポートが追加されています。

IPv6 アクセスをイネーブルにするには、SSL VPN 接続のイネーブル化の一部として **ipv6 enable** コマンドを使用します。次は、外部インターフェイスで IPv6 をイネーブルにする IPv6 接続の例です。

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

IPv6 SSL VPN をイネーブルにするには、次の一般的なアクションを実行します。

1. 外部インターフェイスで IPv6 をイネーブルにする。
2. 内部インターフェイスで IPv6 および IPv6 アドレスをイネーブルにする。
3. クライアント割り当て IP アドレス用に IPv6 アドレス ローカル プールを設定する。
4. IPv6 トンネルのデフォルト ゲートウェイを設定する。

手順

- ステップ 1 インターフェイスを設定します。

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
```

```

ip address 192.168.0.1 255.255.255.0
ipv6 enable          ; Needed for IPv6.
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.0.1 255.255.0.0
 ipv6 address 2001:DB8::1/32      ; Needed for IPv6.
 ipv6 enable                    ; Needed for IPv6.

```

ステップ 2 「ipv6 local pool」（IPv6 アドレスの割り当てに使用）を設定します。

```

ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100      ; Use your IPv6 prefix here

```

（注）

セキュアクライアントに IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てるように ASA を設定できます。そのように設定するには、ASA 上で内部アドレスプールを作成するか、ASA 上のローカルユーザーに専用アドレスを割り当てます。

ステップ 3 ipv6 アドレス プールをトンネルグループ ポリシー（またはグループ ポリシー）に追加します。

```

tunnel-group YourTunGrp1 general-attributes ipv6-address-pool ipv6pool

```

（注）

ここでは「address-pool」コマンドを使用して IPv4 アドレス プールも設定する必要があります。

ステップ 4 IPv6 トンネルのデフォルト ゲートウェイを設定します。

```

ipv6 route inside ::/0 X:X:X:X::X tunneled

```

SAML 2.0

ASA は SAML 2.0 をサポートしているので、VPN のエンドユーザーは、クレデンシャルを 1 回入力するだけで、プライベートネットワーク外の他の SAAS アプリケーションを切り替えることができるようになります。

たとえば、企業の顧客の場合は、SAML アイデンティティプロバイダー (IdP) として PingIdentity をイネーブルにして、SAML 2.0 SSO 対応の Rally、Salesforce、Oracle OEM、Microsoft ADFS、onelogin、または Dropbox のアカウントを持ちます。サービスプロバイダー (SP) として 2.0 SAML SSO をサポートするように ASA を設定すると、エンドユーザーは、一度サインインするだけであらゆるサービスにアクセスできるようになります。

AnyConnect 4.4 クライアントが SAML 2.0 を使用して SAAS ベースのアプリケーションにアクセスできるように、AnyConnect SAML サポートが追加されました。AnyConnect 4.6 では、以前のリリースのネイティブ（外部）ブラウザ統合が、組み込みブラウザとの SAML 統合の拡張バージョンに置き換えられました。組み込みブラウザを搭載した新しい拡張バージョンを使用

するには、AnyConnect 4.6（またはそれ以降）および ASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）へのアップグレードが必要です。

ASA リリース 9.17.1/ASDM リリース 7.17.1 では、AnyConnect 4.10.04065（またはそれ以降）を使用した AnyConnect VPN SAML 外部ブラウザのサポートが導入されました。AnyConnect VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、Web 認証の実行時にセキュアクライアントがセキュアクライアント組み込みブラウザではなくローカルブラウザを使用する設定を選択できます。この機能により、セキュアクライアントは WebAuthN および他の SAML ベースの Web 認証オプション（シングルサインオン、生体認証、または組み込みブラウザでは利用できないその他の拡張方法など）をサポートします。SAML 外部ブラウザを使用するには、「[SAML 認証用のデフォルト OS ブラウザの設定（292 ページ）](#)」で説明する設定を実行する必要があります。

トンネルグループやデフォルト トンネルグループなどの認証方式として SAML が設定されている場合、ASA は SP に対応します。VPN のユーザーは、イネーブルになっている ASA または SAML IdP にアクセスして、シングルサインオンを開始します。以下では、これらの各シナリオについて説明します。

SAML SP によって開始される SSO

ユーザーが ASA にアクセスしてログインを開始した場合、サインオン動作は次のように進行します。

1. VPN のユーザーが SAML 対応のトンネルグループにアクセスするか、またはグループを選択すると、そのユーザーは認証のために SAML IdP にリダイレクトされます。グループ URL に直接アクセスしない限り、ユーザーは入力を要求されます。直接アクセスした場合、リダイレクトは行われません。

ASA は、ブラウザによって SAML IdP にリダイレクトされる SAML 認証要求を生成します。

2. IdP がエンドユーザーのクレデンシャルを確認し、エンドユーザーがログインします。入力されたクレデンシャルは IdP の認証設定に合致していなければなりません。
3. IdP の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

SAML IdP によって開始される SSL

エンドユーザーが IdP にアクセスしてログインを開始した場合、サインオン動作は次のように進行します。

1. エンドユーザーが IdP にアクセスします。IdP は、独自の認証設定に従ってエンドユーザーのクレデンシャルを確認します。エンドユーザーはクレデンシャルを入力し、IdP にログインします。
2. 一般的には、エンドユーザーは、IdP で設定された SAML 対応サービスのリストを取得します。エンドユーザーが ASA を選択します。

3. SAML の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

信頼の輪

ASA と SAML アイデンティティプロバイダーとの信頼関係は、設定されている証明書（ASA トラストポイント）によって確立されます。

エンドユーザーと SAML アイデンティティプロバイダーとの信頼関係は、IdP に設定されている認証によって確立されます。

SAML のタイムアウト

SAML アサーションには、次のような NotBefore と NotOnOrAfter があります：<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

ASA で設定されている SAML のタイムアウトと NotBefore の合計が NotOnOrAfter よりも早い場合は、そのタイムアウトが NotOnOrAfter よりも優先されます。NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。

タイムアウト後にアサーションによって再利用されないように、タイムアウトにはごく短い時間を設定してください。SAML 機能を使用するためには、ASA の Network Time Protocol (NTP) サーバーを IdP NTP サーバーと同期する必要があります。

プライベート ネットワークでのサポート

SAML 2.0 ベースのサービス プロバイダー IdP は、プライベート ネットワークでサポートされます。SAML IdP がプライベート クラウドに展開されると、ASA およびその他の SAML 対応サービスはピアの位置になり、すべてプライベート ネットワーク内になります。ASA をユーザーとサービス間のゲートウェイとして、IdP の認証は制限された匿名の webvpn セッションで処理され、IdP とユーザー間のすべてのトラフィックは変換されます。ユーザーがログインすると、ASA は対応する属性のセッションを修正し、IdP セッションを保存します。その後は、クレデンシャルを再度入力することなくプライベート ネットワークのサービス プロバイダーを使用できます。

SAML IdP NameID 属性は、ユーザーのユーザー名を特定し、認証、アカウントिंग、および VPN セッション データベースに使用されます。



- (注) プライベート ネットワークとパブリック ネットワーク間で認証情報を交換することはできません。内部および外部の両方のサービスプロバイダーに同じ IdP を使用する場合は、個別に認証する必要があります。内部専用の IdP を外部サービスで使用することはできません。外部専用の IdP は、プライベート ネットワーク内のサービス プロバイダーでは使用できません。

SAML 2.0 に関する注意事項と制約事項

- ASA は、SAML 認証用に次のシグニチャをサポートしています。

- RSA および HMAC を使用する SHA1
- RSA および HMAC を使用する SHA2
- ASA は、すべての SAML IdP でサポートされる SAML 2.0 Redirect-POST バインディングをサポートしています。
- ASA は SAML SP としてのみ機能します。ゲートウェイ モードやピア モードでアイデンティティプロバイダーとして動作することはできません。
- この SP SAML SSO 機能は相互排他認証方式です。この方式は、AAA や証明書と併用できません。
- ユーザー名/パスワード認証、証明書認証、および KCD に基づく機能はサポートされません。たとえば、ユーザー名/パスワードの事前フィルタリング機能、フォーム ベースの自動サインオン、マクロ置換ベースの自動サインオン、KCD SSO などです。
- ASA は、AnyConnect SAML 認証を使用した VPN ロードバランシングをサポートするようになりました。
- SAML 認証に Safari を使用している場合は、Safari アップデート 14.1.2 以降がインストールされていることを確認してください。
- 認証アサーションが適切に処理され、タイムアウトが適切に機能するように、ASA の管理者は、ASA と SAML IdP とのクロック同期を確保する必要があります。
- ASA の管理者は、次の点を考慮して、ASA と IdP の両方で有効な署名証明書を保持する責任があります。
 - ASA に IdP を設定する際には、IdP の署名証明書が必須です。
 - ASA は、IdP から受け取った署名証明書に対して失効チェックを行いません。
- SAML アサーションには、NotBefore と NotOnOrAfter 条件があります。ASA SAML に設定されている**タイムアウト**と、これらの条件との相関関係は次のとおりです。
 - NotBefore とタイムアウトの合計が NotOnOrAfter よりも早い場合は、タイムアウトが NotOnOrAfter に優先します。
 - NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。
 - NotBefore 属性が存在しない場合、ASA はログイン要求を拒否します。NotOnOrAfter 属性が存在せず、SAML タイムアウトが設定されていない場合、ASA はログイン要求を拒否します。
- 二要素認証（プッシュ、コード、パスワード）のチャレンジ/応答中に FQDN が変更されるため、ASA がクライアントとのプロキシを強制的に認証する、内部 SAML を使用した展開では ASA は Duo と連携しません。
- 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。

- 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
- Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに AnyConnect がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、ASA の Network Time Protocol (NTP) サーバを IdP NTP サーバと同期する必要があります。
- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- 内部 IdP を使用してログインした後に SSO で内部サーバーにアクセスすることはできません。
- SAML IdP NameID 属性は、ユーザーのユーザー名を特定し、認証、アカウントティング、および VPN セッション データベースに使用されます。
- マルチコンテキストモードで SAML はサポートされません。
- SAML アサーションで受信した複数の属性はサポートされていません。
- Chromebook は、外部ブラウザ認証を備えた Secure Client SAML をサポートしていません。
- IdP が、SAML 応答に、対応する SAML 要求で受信したのと同じ Relay state パラメータを含めていることを確認します。

SAML 2.0 アイデンティティ プロバイダー (IdP) の設定

始める前に

SAML (IdP) プロバイダーのサインイン URL とサインアウト URL を取得します。URL はプロバイダーの Web サイトから取得できます。また、プロバイダーがメタデータ ファイルで情報を提供していることもあります。

手順

- ステップ 1** webvpn コンフィギュレーション モードで SAML アイデンティティ プロバイダーを作成し、webvpn で saml-idp サブモードを開始します。

```
[no] saml idp idp-entityID
```

idp-entityID : SAML IdP の entityID には 4 ～ 128 文字を指定します。

SAML IdP 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 2 IdP URL を設定します。**url** [sign-in | sign-out] *value*

value : IdP にサインインするための URL、または IdP からサインアウトするときにリダイレクトされる URL です。**sign-in** URL は必須ですが、**sign-out** URL はオプションです。url の値には 4 ～ 500 文字を指定します。

ステップ 3 (任意) クライアントレス VPN のベース URL を設定します。**base-url** *URL*

この URL は、エンドユーザーを ASA にリダイレクトするために、サードパーティ製 IdP に提供されます。

base-url が設定されている場合、その URL は **show saml metadata** の AssertionConsumerService と SingleLogoutService 属性のベース URL として使用されます。

base-url が設定されていない場合、URL は ASA のホスト名とドメイン名から決定されます。たとえば、ホスト名が `ssl-vpn`、ドメイン名が `cisco.com` の場合は、`https://ssl-vpn.cisco.com` が使用されます。

base-url もホスト名/ドメイン名も設定されていない場合は、**show saml metadata** を入力するとエラーが発生します。

ステップ 4 IdP と SP (ASA) 間のトラストポイントを設定します。**trustpoint idp** *trustpoint-name1* [*trustpoint-name2*]**trustpoint sp** *trustpoint-name1*

idp : ASA が SAML アサーションを検証するための IdP 証明書を含むトラストポイントを指定します。

デバイスの SAML IdP に 2 つのトラストポイントを構成できるようになりました。この機能を使用すると、サービスを失うことなく、新しいアイデンティティ プロバイダー (IdP) 証明書にグレースフルに移行できます。同じ証明書ですべての ASA と IdP を同時に更新するためにメンテナンスウィンドウを開く必要はありません。新しい IdP 証明書が IdP で有効になると、デバイスは新しい証明書を自動的に検出します。元のトラストポイントは移行後に安全に削除できます。

sp : IdP が ASA (SP) の署名や暗号化 SAML アサーションを検証するための ASA (SP) 証明書を含むトラストポイントを指定します。

trustpoint-name : 設定されているトラストポイントを指定します。

ステップ 5 (任意) ローカルベース URL を設定します。**local base-url** *URL*

DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるベース URL を指定できます。

ステップ 6 (任意) SAML タイムアウトを設定します。**timeout assertion** *timeout-in-seconds*

指定した場合、NotBefore と timeout-in-seconds の合計が NotOnOrAfter よりも早い場合は、この設定が NotOnOrAfter に優先します。

指定しない場合は、セッションの NotBefore と NotOnOrAfter が有効期間の確認に使用されます。

(注)

既存の SAML IdP が設定済みのトンネル グループの場合、webvpn での saml idp CLI に対するすべての変更は、SAML がその特定のトンネル グループに再度有効にされたときにのみトンネルグループに適用されます。タイムアウトを設定すると、更新されたタイムアウトはトンネルグループの webvpn 属性の saml アイデンティティ プロバイダー CLI 再発行後にのみ有効になります。

ステップ 7 (任意) SAML 要求の署名をイネーブルまたはディセーブル (デフォルト設定) にします。

signature <value>

(注)

SSO 2.5.1 へのアップグレードに伴い、デフォルトの署名方法は SHA1 から SHA256 に変更します。value に rsa-sha1、rsa-sha256、rsa-sha384、または rsa-sha512 を入力すると、希望する署名方法のオプションを設定できます。

ステップ 8 (オプション) IdP が内部ネットワークであることを特定するフラグを設定するには、**internal** コマンドを使用します。ASA はゲートウェイ モードで機能するようになります。

ステップ 9 **show webvpn saml idp** を使用してコンフィギュレーションを表示します。

ステップ 10 SAML 認証要求が発生したときに、以前のセキュリティ コンテキストに依存するのではなくアイデンティティ プロバイダーが直接認証するようにするには、**force re-authentication** を使用します。この設定はデフォルトなので、ディセーブルにする場合は **no force re-authentication** を使用します。

例

次の例では、salesforce_idp という名前の IdP を設定し、事前設定されたトラストポイントを使用します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
salesforce_trustpoint2
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
```

```
trustpoint idp salesforce_trustpoint salesforce_trustpoint2
trustpoint sp asa_trustpoint
```

次の Web ページには、OneLogin の URL の取得方法について例が示されています。

<https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen>

次の Web ページには、メタデータを使用して OneLogin から URL を検索する方法について、例が示されています。

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

次のタスク

[SAML 2.0 サービス プロバイダー \(SP\) としての ASA の設定 \(291 ページ\)](#) の説明に従って、SAML 認証を接続プロファイルに適用します。

SAML 2.0 サービス プロバイダー (SP) としての ASA の設定

始める前に

事前に IdP を設定しておく必要があります。[SAML 2.0 アイデンティティ プロバイダー \(IdP\) の設定 \(288 ページ\)](#) を参照してください。

手順

- ステップ 1** tunnel-group webvpn サブモードで、saml identify-provider コマンドを使用して IdP を割り当てます。

saml identity-provider *idp-entityID*

idp-entityID : 設定されている既存の IdP のいずれかを指定します。

SAML SP をディセーブルにするには、このコマンドの **no** 形式を使用します。

- ステップ 2** SAML 認証方式を有効化します。

authentication saml

- ステップ 3** (オプション) トンネルグループの SAML IdP トラストポイントを構成します。

saml idp-trustpoint *trustpoint-name* [*trustpoint-name2*]

Azure IdP など、IdP で複数のアプリケーションがある場合も同じ SAML エンティティ ID を共有しますが、アプリケーションごとに独自の証明書を使用します。特定のアプリケーションに関連付けられた上記のコマンドを使用して、メインの webvpn saml 構成を上書きできます。

例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

トンネルグループの IdP トラストポイントを構成します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group partner-saml type remote-access
ciscoasa(config)# tunnel-group partner-saml webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://sts.windows.net/123-3456-7890/
ciscoasa(config-tunnel-webvpn)# saml idp-trustpoint azure-partner-idp-tp
```

SAML 認証用のデフォルト OS ブラウザの設定

AnyConnect が、プラットフォームのネイティブブラウザ（オペレーティングシステムのデフォルトブラウザ）または AnyConnect に組み込まれているブラウザを使用して SSO 認証プロセスを処理するかどうかを指定します。

AnyConnect 外部ブラウザパッケージ（*external-ssso-4.10.04065-webdeploy-k9.pkg* など）をダウンロードして、ASA にアップロードする必要があります。次に、SAML 認証用の SAML ログイン方法（AnyConnect の組み込みブラウザまたはオペレーティングシステムのデフォルトブラウザ）を選択できます。このバンドルは、認証目的で VPN クライアントがデフォルトの OS Web ブラウザを起動できるようにするスクリプトです。このバンドルは、オペレーティングシステム、ブラウザ、および VPN クライアントのバージョンに依存してはいません。この機能が有効になっていれば、VPN クライアントのバージョンと外部ブラウザのパッケージのバージョンファイルが一致している必要はありません。

オペレーティングシステムのデフォルトブラウザを選択すると、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）が有効になります。VPN クライアントの組み込みブラウザでは実行できない Web 認証方式（生体認証など）をサポートしたい場合も、このオプションを選択します。オペレーティングシステムのブラウザを選択する前に、ブラウザで実行できるパッケージをアップロードして Web 認証を有効にする必要があります。

手順

- ステップ 1** オペレーティングシステムのデフォルトブラウザを使用して AnyConnect SAML 認証を有効にするには、webvpn サブモードで `anyconnect external-browser-pkg` コマンドを使用します。

anyconnect external-browser-pkg path

SAML 認証用のオペレーティングシステムのデフォルトブラウザを無効にするには、このコマンドの **no** 形式を使用します。

ステップ 2 オペレーティングシステムのデフォルトブラウザを使用して AnyConnect SAML 認証を有効にするには、`tunnel-group webvpn` サブモードで `external-browser` コマンドを使用します。

external-browser enable idp-entityID

SAML 認証用のオペレーティングシステムのデフォルトブラウザを無効にするには、このコマンドの **no** 形式を使用します。

例

この例では、AnyConnect 外部ブラウザパッケージのパスを選択し、SAML 認証用に外部ブラウザ（オペレーティングシステムのデフォルトブラウザ）を有効にします。

```
asa(config-webvpn)# anyconnect external-browser-pkg flashshow :
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

証明書と SAML 認証の設定

SAML ベースの接続プロファイル用の証明書と SAML 認証を設定して、特定のファイル/レジストリキーのプロファイルを作成せずに、お客様が所有するアセットを検証できます。SAML ベースの認証は、承認済みのアセットおよび/またはユーザーに関連付けることができます。認証には、SAML による単一の証明書または複数の証明書を使用できます。

セキュアクライアントが接続を開始すると、ASA または FTD は、SAML 認証が実行される前に、エンドポイントからの 1 つ以上の証明書を要求して認証します。

SAML 認証が完了すると、SAML と証明書のユーザー名に対して以下を実行できます。

SAML 認証が完了すると、承認フェーズに進む前に SAML と証明書のユーザー名を比較できます。

始める前に

証明書と SAML 認証を設定する前に、必要な SAML 設定を構成してください。

- SAML (IdP) プロバイダーのサインイン URL とサインアウト URL を取得します。URL はプロバイダーの Web サイトから取得できます。また、プロバイダーがメタデータ ファイルで情報を提供していることもあります。
- SAML ID プロバイダーとトラストポイントの設定を構成します。[証明書と SAML 認証の設定 \(293 ページ\)](#) を参照してください

手順

- ステップ 1** 証明書と SAML 認証を設定するには、次のコマンドを入力して `tunnel-group webvpn-attributes` モードを開始します。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name webvpn-attributes
hostname(config-tunnel-webvpn)#
```

- ステップ 2** 使用する認証方法を指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)#authentication authentication_method
```

たとえば、次のコマンドは SAML と証明書認証の両方を許可します。

```
hostname(config-tunnel-webvpn)#authentication saml certificate
```

次のコマンドは、証明書と SAML 認証を許可します。

```
hostname(config-tunnel-webvpn)#authentication certificate saml
```

次のコマンドは、複数の証明書と SAML 認証の両方を許可します。

```
hostname(config-tunnel-webvpn)#authentication multiple-certificate saml
```

- ステップ 3** 接続プロファイルを追加または編集してから、[基本 (Basic)] 接続プロファイル属性設定を選択します。

- ステップ 4** 証明書と SAML 認証の認証方法を指定するには、ドロップダウンから SAML と証明書、または複数の証明書と SAML を選択します。

例

次の例では、`sales_group` 接続プロファイルに複数の証明書と SAML 認証を設定しています。

```
ciscoasa(config)# tunnel-group sales_group webvpn
ciscoasa(config-tunnel-webvpn)#authentication multiple-certificate saml
```

SAML 2.0 と Onelogin の例

以下の例を実行する際は、Onelogin の情報とネーミングの代わりにサードパーティ製の SAML 2.0 IdP を使用してください。

1. IdP と ASA (SP) 間での時刻の同期を設定します。

```
ciscoasa(config)# ntp server 209.244.0.4
```


2. サードパーティ製 IdP で指定されている手順に従って、IdP から IdP の SAML メタデータを取得します。

3. トラストポイントに IdP の署名証明書をインポートします。

```
ciscoasa(config)# crypto ca trustpoint onelogin
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
quit
INFO: Certificate has the following attributes:
Fingerprint:      85de3781 07388f5b d92d9d14 1e22a549
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. トラストポイントに SP (ASA) 署名 PKCS12 をインポートします

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. SAML IdP を追加します。

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. saml-idp サブモードで属性を設定します。

IdP サインイン URL とサインアウト URL を設定します。

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

IdP トラストポイントと SP トラストポイントを設定します

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

クライアントレス VPN ベース URL、SAML 要求の署名、および SAML アサーション タイムアウトを設定します。

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. トンネル グループの IdP を設定し、SAML 認証をイネーブルにします。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. ASA の SAML SP メタデータを表示します。

ASA の SAML SP メタデータは、
https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin から取得できます。この URL の `cloud_idp_onelogin` は、トンネルグループ名です。

9. サードパーティ製 IdP で指定されている手順に従って、その IdP で SAML SP を設定します。

SAML 2.0 のトラブルシューティング

SAML 2.0 の動作をデバッグするには、**debug webvpn samlvalue** を使用します。*value* に応じて次の SAML メッセージが表示されます。

- 8 : エラー
- 16 : 警告およびエラー
- 128 または 255 : デバッグ、警告、およびエラー

セキュアクライアント 接続のモニタリング

アクティブなセッションに関する情報を表示するには、**show vpn-sessiondb** コマンドを使用します。

コマンド	目的
show vpn-sessiondb	アクティブなセッションに関する情報を表示します。
vpn-sessiondb logoff	VPN セッションをログオフします。
show vpn-sessiondb anyconnect	VPN セッションの要約を拡張して、OSPFv3 セッション情報を含めます。
show vpn-sessiondb ratio encryption	Suite-B のアルゴリズム（AES-GCM-128、AES-GCM-192、AES-GCM-256、AES-GMAC-128 など）用のトンネル数と割合のパーセンテージを表示します。

**(注) AnyConnect 親トンネル**

AnyConnect 親トンネルには IP アドレスが割り当てられません。

これは、ネットワーク接続の問題またはハイバネーションが原因で再接続が必要な場合に必要となるセッショントークンをセットアップするために、ネゴシエーション中に作成されるメインセッションです。接続メカニズムに基づいて、Cisco 適応型セキュリティアプライアンス (ASA) は、セッションをクライアントレス (ポータル経由の Weblaunch) または親 (スタンドアロン AnyConnect) として一覧表示します。

AnyConnect 親は、クライアントがアクティブに接続されていない場合のセッションを表します。事実上、これは特定のクライアントからの接続にマッピングされる ASA のデータベースエントリであるという点で、Cookie と同様に機能します。クライアントがスリープ/ハイバネーション状態になると、トンネル (IPsec/インターネット キー エクスチェンジ (IKE) /Transport Layer Security (TLS) /Datagram Transport Layer Security (DTLS) プロトコル) が切断されますが、親は、アイドルタイマーまたは最大接続時間が有効になるまで機能し続けます。これにより、ユーザーは再認証しないで再接続できます。

例

Inactivity フィールドに、セキュアクライアントセッションが接続を失ってから経過時間が表示されています。セッションがアクティブな状態の場合、このフィールドには 00:00m:00s が表示されます。

```
hostname# show vpn-sessiondb
```

```
Session Type: SSL VPN Client
```

```
Username      : lee
Index         : 1
Protocol      : SSL VPN Client
Hashing       : SHA1
TCP Dst Port  : 443
Bytes Tx      : 20178
Pkts Tx       : 27
Client Ver    : Cisco STC 1.1.0.117
Client Type   : Internet Explorer
Group         : DfltGrpPolicy
Login Time    : 14:32:03 UTC Wed Mar 20 2007
Duration      : 0h:00m:04s
Inactivity    : 0h:00m:04s
Filter Name   :
```

```
hostname# vpn-sessiondb logoff
```

```
INFO: Number of sessions of type "" logged off : 1
```

```
hostname# vpn-sessiondb logoff name tester
```

```
Do you want to logoff the VPN session(s)? [confirm]
```

```
INFO: Number of sessions with name "tester" logged off : 1
```

AnyConnect VPN セッションのログオフ

すべての VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

次に、すべての VPN セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1
```

name 引数または index 引数のいずれかを使用して、個々のセッションをログオフできます。

```
vpn-sessiondb logoff name name
vpn-sessiondb logoff index index
```

ライセンス容量に達して新しいユーザーがログインできなくなることがないように、非アクティブの状態が最長時間続いたセッションはアイドル状態になります（自動的にログオフされます）。後でセッションが再開されると、非アクティブ リストから削除されます。

ユーザー名とインデックス番号（クライアント イメージの順序で設定される）は、両方とも **show vpn-sessiondb anyconnect** コマンドの出力で確認できます。次の例は、ユーザー名 *lee* とインデックス番号 *1* を示しています。

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : lee                      Index      : 1
Assigned IP   : 192.168.246.1           Public IP   : 10.139.1.2
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : RC4 AES128              Hashing     : SHA1
Bytes Tx      : 11079                   Bytes Rx    : 4942
Group Policy  : EngPolicy                Tunnel Group : EngGroup
Login Time    : 15:25:13 EST Fri Jan 28 2011
Duration      : 0h:00m:15s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                     VLAN        : none
```

次の例は、**vpn-session-db logoff** コマンドの **name** オプションを使用してセッションを終了しています。

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "lee" logged off : 1

hostname#
```

セキュアクライアント 接続機能の履歴

次の表に、この機能のリリース履歴を示します。

表 13: セキュアクライアント 接続機能の履歴

機能名	リリース	機能情報
セキュアクライアント 接続	7.2(1)	authentication eap-proxy、authentication ms-chap-v1、authentication ms-chap-v2、authentication pap、l2tp tunnel hello、および vpn l2tp-ipsec コマンドが導入または変更されました。
IPsec IKEv2	8.4(1)	セキュアクライアントおよび LAN-to-LAN の IPsec IKEv2 接続を行う IKEv2 が追加されました。



第 10 章

セキュアクライアント HostScan

AnyConnect ポスチャモジュールにより、セキュアクライアントは、ホストにインストールされているオペレーティングシステム、アンチマルウェア、ファイアウォールの各ソフトウェアを識別できます。この情報は、HostScan アプリケーションによって収集されます。ポスチャアセスメントでは、ホストに HostScan がインストールされている必要があります。

- [HostScan/Secure Firewall ポスチャの前提条件](#) (301 ページ)
- [HostScan のライセンス](#) (302 ページ)
- [HostScan パッケージ](#) (302 ページ)
- [HostScan/Secure Firewall ポスチャのインストールまたはアップグレード](#) (302 ページ)
- [HostScan の有効化または無効化](#) (303 ページ)
- [ASA で有効になっている HostScan/Secure Firewall ポスチャバージョンの表示](#) (304 ページ)
- [HostScan/Secure Firewall ポスチャのアンインストール](#) (305 ページ)
- [グループポリシーへの セキュアクライアント 機能モジュールの割り当て](#) (306 ページ)
- [HostScan/Secure Firewall ポスチャ関連資料](#) (307 ページ)

HostScan/Secure Firewall ポスチャの前提条件

セキュアクライアントを Secure Firewall Posture/HostScan モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

SCEP 認証機能を使用するには、Secure Firewall Posture/HostScan をインストールする必要があります。

Secure Firewall Posture/HostScan のインストールでサポートされるオペレーティングシステムについては、『[Supported VPN Platforms, Cisco ASA Series](#)』を参照してください。

HostScan のライセンス

次に、HostScan のセキュアクライアント ライセンス要件を示します。

- AnyConnect Apex
- AnyConnect VPN Only

HostScan パッケージ

HostScan パッケージを ASA にスタンドアロン パッケージ **hostscan-version.pkg** としてロードすることができます。このファイルには、HostScan ソフトウェアとともに、HostScan ライブラリおよびサポート表が含まれています。

HostScan/Secure Firewall ポスチャのインストールまたはアップグレード

この手順では、ASA のコマンドライン インターフェイスを使用して HostScan または Secure Firewall ポスチャパッケージをインストールまたはアップグレードし、有効にします。

始める前に



- (注) HostScan バージョン 4.3.x 以前から 4.6.x 以降にアップグレードしようとしている場合、以前に確立した既存の AV/AS/FW DAP ポリシーおよび LUA スクリプトがすべて HostScan 4.6.x 以降と非互換であるという事実に起因するエラー メッセージが表示されます。

設定を適応させるために実行する必要があるワントタイム移行手順が存在します。この手順では、このダイアログボックスを閉じて、この設定を保存する前に HostScan 4.4.x と互換になるように設定を移行します。この手順を中止し、『[セキュアクライアント HostScan 4.3.x to 4.6.x Migration Guide](#)』で詳細な手順を参照してください。つまり、移行するには ASDM DAP のポリシー ページに移動して、互換性のない AV/AS/FW 属性を確認して手動で削除してから、LUA スクリプトを確認し、書き換える必要があります。

- ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。
- `secure-firewall-posture-version-k9.pkg` を ASA にアップロードします。HostScan 4.x バージョンを使用している場合は、`hostscan_version-k9.pkg` ファイルをアップロードする必要があります。

手順

ステップ 1 webvpn コンフィギュレーション モードを開始します。

例 :

```
hostname(config)# webvpn
```

ステップ 2 ASDM を開いて [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [Cisco Secure Firewall用ポスチャ (Posture (for Secure Firewall))] > [ポスチャイメージ (Posture Image)] を選択します。HostScan 4.x バージョンを使用している場合、パスは [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [Secure Desktop Manager] > [ホストスキャンイメージ (Host Scan Image)] になります。

ステップ 3 HostScan/Secure Firewall ポスチャイメージとして指定するパッケージのパスを指定します。スタンドアロンのパッケージ、またはセキュアクライアント パッケージを指定することができます。

hostscan image path

例 :

HostScan 4.x バージョンを使用している場合は、

```
ASAName(webvpn)#hostscan image disk0:/hostscan_4.10.06081.pkg
```

Secure Firewall ポスチャ 5.x バージョンを使用している場合は、

```
ASAName(webvpn)#hostscan image disk0:/secure-firewall-posture5.0.00556.pkg
```

ステップ 4 前の手順で指定した HostScan/Secure Firewall ポスチャイメージを有効にします。

例 :

```
ASAName(webvpn)#hostscan enable
```

ステップ 5 実行コンフィギュレーションをフラッシュメモリに保存します。新しいコンフィギュレーションがフラッシュメモリに正常に保存されると、[OK] メッセージが表示されます。

例 :

```
hostname(webvpn)# write memory
```

ステップ 6

HostScan の有効化または無効化

これらのコマンドは、ASA のコマンドライン インターフェイスを使用して、インストール済みの HostScan イメージを有効または無効にします。

始める前に

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。

手順

ステップ 1 `webvpn` コンフィギュレーション モードを開始します。

例 :

`webvpn`

ステップ 2 ASA からスタンドアロンの HostScan イメージがアンインストールされていない場合、このイメージを有効にします。

`hostscan enable`

ステップ 3 インストールされているすべての HostScan パッケージの HostScan を無効にします。

(注)

有効になっている HostScan イメージをアンインストールする前に、このコマンドを使用して、HostScan を無効にする必要があります。

`no hostscan enable`

ASA で有効になっている HostScan/Secure Firewall ポスチャバージョンの表示

この手順では、ASA のコマンドライン インターフェイスを使用して、有効になっている HostScan/Secure Firewall ポスチャのバージョンを特定します。

始める前に

ASA にログインし、特権 EXEC モードを開始します。ASA の特権 EXEC モードでは、表示されるプロンプトは `hostname#` となります。

手順

ASA で有効になっている HostScan/Secure Firewall ポスチャバージョンを表示します。

`show webvpn hostscan`

HostScan/Secure Firewall ポスチャのアンインストール

HostScan/Secure Firewall ポスチャパッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、HostScan/Secure Firewall ポスチャが有効になっている場合でも ASA による HostScan/Secure Firewall ポスチャパッケージの展開が回避されます。HostScan/Secure Firewall ポスチャをアンインストールしても、HostScan/Secure Firewall ポスチャパッケージはフラッシュドライブから削除されません。

始める前に

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。

手順

ステップ 1 webvpn コンフィギュレーション モードを開始します。

webvpn

ステップ 2 アンインストールする HostScan/Secure Firewall ポスチャイメージを無効にします。

no hostscanenable

ステップ 3 アンインストールする HostScan/Secure Firewall ポスチャイメージのパスを指定します。スタンドアロンのパッケージが HostScan/Secure Firewall ポスチャパッケージとして指定されている場合があります。

no hostscan image path

例 :

HostScan 4.x バージョンを使用している場合は、

`ASAName (webvpn) #hostscan image disk0:/hostscan_4.10.06081-k9.pkg`

Secure Firewall ポスチャ 5.x バージョンを使用している場合は、

`ASAName (webvpn) #hostscan image disk0:/secure-firewall-posture-5.0.00556-k9.pkg`

ステップ 4 実行コンフィギュレーションをフラッシュメモリに保存します。新しいコンフィギュレーションがフラッシュメモリに正常に保存されると、[OK] メッセージが表示されます。

write memory

グループポリシーへの セキュアクライアント 機能モジュールの割り当て

次の手順で、セキュアクライアント機能モジュールとグループポリシーを関連付けます。VPN ユーザーが ASA に接続するときに、ASA はこれらのセキュアクライアント機能モジュールをエンドポイントコンピュータにダウンロードしてインストールします。

始める前に

ASA にログオンし、グローバル コンフィギュレーションモードを開始します。グローバル コンフィギュレーション モードでは、ASA は `hostname(config)#` プロンプトを表示します。

手順

ステップ 1 ネットワーク クライアント アクセス用の内部グループ ポリシーを追加します。

group-policy name internal

例 :

```
hostname(config)# group-policy PostureModuleGroup internal
```

ステップ 2 新しいグループ ポリシーを編集します。このコマンドを入力した後は、グループ ポリシー コンフィギュレーション モードのプロンプト `hostname(config-group-policy)#` が表示されます。

group-policy name attributes

例 :

```
hostname(config)# group-policy PostureModuleGroup attributes
```

ステップ 3 グループポリシー webvpn コンフィギュレーションモードを開始します。このコマンドを入力した後は、次に示す ASA のプロンプトが表示されます。 `hostname(config-group-webvpn)#`

webvpn

ステップ 4 グループ内のすべてのユーザーに セキュアクライアント 機能モジュールがダウンロードされるように、グループポリシーを設定します。

anyconnect modules value Secure Firewall モジュール 名

`anyconnect module` コマンドの `value` には、次の値の 1 つ以上を指定することができます。複数のモジュールを指定する場合は、値をカンマで区切ります。

値	Secure Firewall モジュール/機能名
dart	Secure Client DART (診断およびレポートツール)
vpngina	Secure Client SBL (ログイン前の起動)

値	Secure Firewall モジュール/機能名
ポスチャ	Secure Firewall ポスチャ/HostScan
nam	Secure Client ネットワーク アクセス マネージャ
none	グループ ポリシーからすべての AnyConnect モジュールを削除する場合に使用します。
profileMgmt	Secure Client 管理トンネル VPN

例：

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

モジュールの1つを削除するには、保持したいモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドは Web セキュリティ モジュールを削除します。

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

ステップ5 実行コンフィギュレーションをフラッシュ メモリに保存します。

新しいコンフィギュレーションが正常にフラッシュ メモリに保存されると、[OK] というメッセージが表示され、次に示す ASA のプロンプトが表示されます。hostname(config-group-webvpn)# write memory

HostScan/Secure Firewall ポスチャ関連資料

HostScan/Secure Firewall ポスチャがエンドポイントコンピュータからポスチャクレデンシャルを収集した後は、情報を活用するために、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらのトピックの詳細については、『[Cisco Adaptive Security Device Manager Configuration Guides](#)』を参照してください。また、セキュアクライアントでの HostScan/Secure Firewall ポスチャの動作の詳細については、『[Cisco Secure Client \(including AnyConnect\) Administrator Guide](#)』を参照してください。



第 11 章

仮想トンネル インターフェイス

この章では、VTI トンネルの設定方法について説明します。

- [仮想トンネル インターフェイスについて \(309 ページ\)](#)
- [仮想トンネル インターフェイスの注意事項 \(310 ページ\)](#)
- [VTI トンネルの作成 \(313 ページ\)](#)
- [仮想トンネル インターフェイスの機能履歴 \(324 ページ\)](#)

仮想トンネル インターフェイスについて

ASA は、仮想トンネル インターフェイス (VTI) と呼ばれる論理インターフェイスをサポートします。ポリシーベースの VPN の代わりに、VTI を使用してピア間に VPN トンネルを作成できます。VTI は、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。動的ルートまたは静的ルートを使用できます。VTI からの出力トラフィックは暗号化されてピアに送信され、VTI への入力トラフィックは関連付けされた SA によって復号化されます。

VTI を使用することにより、静的暗号マップのアクセスリストを設定してインターフェイスにマッピングすることが不要になります。すべてのリモートサブネットを追跡し、暗号マップのアクセスリストに含める必要がなくなります。展開が簡単になるほか、ダイナミックルーティングプロトコルのルートベースの VPN をサポートするステティック VTI があると、仮想プライベートクラウドの多くの要件を満たすこともできます。

スタティック VTI

2 つのサイト間でトンネルが常にオンになっているサイト間接続用に、スタティック VTI 設定を使用できます。スタティック VTI インターフェイスの場合、物理インターフェイスをトンネルソースとして定義する必要があります。デバイスごとに最大 1024 の VTI を関連づけることができます。スタティック VTI インターフェイスを作成するには、[VTI インターフェイスの追加 \(318 ページ\)](#) を参照してください。

Dynamic VTI

ダイナミック VTI は、サイト間 VPN に高度に安全でスケーラブルな接続を提供します。ダイナミック VTI は、大規模な企業向けハブアンドスポーク展開でのピアの構成を容易にします。

ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。ダイナミック VTI テクノロジーは、ダイナミック クリプト マップとトンネルを確立するためのダイナミック ハブアンドスポーク方式にとって代わるものです。管理センターでは、ダイナミック VTI はハブアンドスポークトポロジのみをサポートします。

ダイナミック VTI では、IPsec インターフェイスの動的なインスタンス化および管理のために、仮想テンプレートが使用されます。仮想テンプレートは、VPN セッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。ダイナミック VTI はダイナミック (DHCP) スポークもサポートします。ダイナミック VTI インターフェイスを作成するには、[ダイナミック VTI インターフェイスの追加 \(321 ページ\)](#) を参照してください。

ASA で VPN セッションのダイナミック VTI トンネルを作成する方法

1. ASA で仮想テンプレートを作成します (インターフェイス `virtual-Template template_number type tunnel`) 。
このテンプレートは、複数の VPN セッションに使用できます。
2. このテンプレートをトンネルグループに適用します。1 つの仮想テンプレートを複数のトンネルグループに適用することができます。
3. スポークは、ハブとのトンネル要求を開始します。
4. ハブはスポークを認証します。
5. ASA は、仮想テンプレートを使用して、スポークとの VPN セッション用にハブ上に仮想アクセスインターフェイスを動的に作成します。
6. ハブは、仮想アクセスインターフェイスを使用して、スポークとのダイナミック VTI トンネルを確立します。
7. IKEv2 交換で VTI インターフェイス IP をアドバタイズするように、IKEv2 `route set interface` コマンドを設定します。このオプションにより、トンネルを介して機能する BGP またはパスマニタリングの VTI インターフェイス間のユニキャスト到達可能性が有効になります。
8. VPN セッションが終了すると、トンネルは切断され、ハブは対応する仮想アクセスインターフェイスを削除します。

仮想トンネル インターフェイスの注意事項

コンテキストモードとクラスタリング

- シングル モードでだけサポートされています。
- クラスタリングはサポートされません。

ファイアウォール モード

ルーテッド モードのみでサポートされます。

BGP IPv4 および IPv6 のサポート

VTI を介した IPv4 および IPv6 BGP ルーティングをサポートします。

EIGRP サポート

VTI を介した IPv4 および IPv6 EIGRP ルーティングをサポートします。

OSPF IPv4 および IPv6 のサポート

VTI を介した IPv4 および IPv6 OSPF ルーティングをサポートします。

IPv6 のサポート

- IPv6 アドレスが指定された VTI を設定できます。
- VTI のトンネル送信元とトンネル接続先の両方に IPv6 アドレスを設定できます。
- パブリック IP バージョンを介した VTI IP（または内部ネットワーク IP バージョン）の次の組み合わせがサポートされています。
 - IPv6 over IPv6
 - IPv4 over IPv6
 - IPv4 over IPv4
 - IPv6 over IPv4
- トンネルの送信元および接続先としてサポートされるのは、静的 IPv6 アドレスだけです。
- トンネル送信元インターフェイスには IPv6 アドレスを設定できます。トンネルエンドポイントとして使用するアドレスを指定できます。指定しない場合、デフォルトでは、リスト内の最初の IPv6 グローバルアドレスがトンネルエンドポイントとして使用されます。
- トンネルモードを IPv6 として指定できます。指定した場合、VTI を介して IPv6 トラフィックをトンネリングできます。ただし、単一 VTI のトンネルモードは IPv4 または IPv6 のいずれかになります。

一般的な設定時の注意事項

- LAN-to-LAN VPN でダイナミッククリプトマップとダイナミック VTI を使用する場合は、ダイナミック VTI トンネルのみが起動します。この動作は、クリプトマップとダイナミック VTI の両方がデフォルトのトンネルグループを使用しようとするために発生します。

次のいずれかを実行することを推奨します。

 - LAN-to-LAN VPN をダイナミック VTI に移行します。

- 独自のトンネルグループを持つ静的クリプトマップを使用します。
- VTI は IPsec モードのみで設定可能です。ASA で GRE トンネルを終了することはサポートされていません。
- トンネルインターフェイスを使用するトラフィックには、静的、BGP、OSPF、または EIGRP IPv4 ルートを使用できます。
- スタティックおよびダイナミック VTI の場合は、借用 IP インターフェイスを VTI インターフェイスのトンネルソース IP アドレスとして使用しないでください。
- VTI の MTU は、基盤となる物理インターフェイスに応じて自動的に設定されます。ただし、VTI を有効にした後で物理インターフェイス MTU を変更した場合は、新しい MTU 設定を使用するために VTI を無効にしてから再度有効にする必要があります。
- ダイナミック VTI の場合、仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスから MTU を継承します。トンネル送信元インターフェイスを指定しない場合、仮想アクセスインターフェイスは、ASA が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。
- デバイスには最大 1024 の VTI を設定できます。VTI 数を計算する際は、次の点を考慮してください。
 - nameif サブインターフェイスを含めて、デバイスに設定できる VTI の総数を導き出します。
 - ポートチャネルのメンバーインターフェイスに nameif を設定することはできません。したがって、トンネル数は実際のメイン ポートチャネルインターフェイスの数だけ減少し、そのメンバーインターフェイスの数は減少しません。
 - プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、500 の VLAN をサポートしているモデルの場合、トンネル数は 500 から設定された物理インターフェイスの数を引いた数になります。
- VTI は IKE のバージョン v1 および v2 をサポートしており、トンネルの送信元と宛先の間でのデータ送受信に IPsec を使用します。
- NAT を適用する必要がある場合、IKE および ESP パケットは、UDP ヘッダーにカプセル化されます。
- IKE および IPsec のセキュリティアソシエーションには、トンネル内のデータトラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。
- トンネルグループ名は、ピアが自身の IKEv1 または IKEv2 識別情報として送信するものと一致する必要があります。
- サイト間トンネルグループの IKEv1 では、トンネルの認証方式がデジタル証明書である場合、かつ/またはピアがアグレッシブモードを使用するように設定されている場合、IP アドレス以外の名前を使用できます。

- 暗号マップに設定されるピア アドレスと VTI のトンネル宛先が異なる場合、VTI 設定と暗号マップの設定を同じ物理インターフェイスに共存させることができます。
- VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセスルールを適用することができます。
- ICMP ping は、VTI インターフェイス間でサポートされます。
- IKEv2 サイト間 VPN トンネルのピアデバイスが IKEv2 設定要求ペイロードを送信した場合、ASA はデバイスとの IKEv2 トンネルを確立できません。ASA がピアデバイスとの VPN トンネルを確立するには、ピアデバイスで **config-exchange** 要求を無効にする必要があります。
- ダイナミック VTI は HA および IKEv2 をサポートします。

デフォルト設定

- デフォルトでは、VTI 経由のトラフィックは、すべて暗号化されます。
- VTI インターフェイスのデフォルトのセキュリティレベルは 0 です。セキュリティレベルを設定することはできません。

VTI の制限事項

ASA は、VTI 復号の後にセキュリティグループタグ (SGT) フレームとパケットをドロップします。

ダイナミック VTI は以下をサポートしていません。

- ECMP と VRF
- クラスタリング
- IKEv1
- QoS

ダイナミック VTI では、トンネル送信元が指定されていないと、管理専用インターフェイスとフェールオーバーインターフェイスを除くデバイスのすべてのインターフェイスで、IKEv2 が有効になります。

VTI トンネルの作成

VTI トンネルを設定するには、IPsec プロポーザル（トランスフォームセット）を作成します。IPsec プロポーザルを参照する IPsec プロファイルを作成した後で、IPsec プロファイルを持つ VTI インターフェイスを作成します。リモートピアには、同じ IPsec プロポーザルおよび IPsec プロファイルパラメータを設定します。SA ネゴシエーションは、すべてのトンネルパラメータが設定されると開始します。



(注) VPN および VTI ドメインの両方に属し、物理インターフェイス上で BGP 隣接関係を持つ ASA では、次の動作が発生します。

インターフェイスヘルスチェックによって状態の変更がトリガーされると、物理インターフェイスでのルートは、新しいアクティブなピアとの BGP 隣接関係が再確立されるまで削除されます。この動作は、論理 VTI インターフェイスには該当しません。

VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセス制御リストを適用することができます。IPsec トンネルから送信されるすべてのパケットに対して、ACL で発信元インターフェイスと宛先インターフェイスをチェックせずに許可するには、グローバルコンフィギュレーション モードで `sysopt connection permit-vpn` コマンドを入力します。

ACL をチェックせずに ASA を通過する IPsec トラフィックをイネーブлにするための次のコマンドを使用できます。

hostname(config)# sysopt connection permit-vpn

外部インターフェイスと VTI インターフェイスのセキュリティレベルが 0 の場合、VTI インターフェイスに ACL が適用されていても、`same-security-traffic` が設定されていなければヒットしません。

この機能を設定するには、グローバルコンフィギュレーションモードで **intra-interface** 引数を指定して **same-security-traffic** コマンドを実行します。

詳細については、[インターフェイス内トラフィックの許可（ヘアピニング）](#)（81 ページ）を参照してください。

手順

ステップ 1 IPsec プロポーザル（トランスフォームセット）を追加します。

ステップ 2 IPsec プロファイルを追加します。

ステップ 3 VTI トンネルを追加します。

IPsec プロポーザル（トランスフォームセット）の追加

トランスフォームセットは、VTI トンネル内のトラフィックを保護するために必要です。これは、VPN 内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムのセットであり、IPsec プロファイルの一部として使用されます。

始める前に

- VTI に関連付けられた IKE セッションを認証するには、事前共有キーまたは証明書のいずれかを使用できます。IKEv2 では、非対称認証方式とキーが使用できます。IKEv1 と IKEv2

のどちらも、VTIに使用するトンネルグループの下に事前共有キーを設定する必要があります。

- IKEv1 を使用した証明書ベースの認証には、イニシエータで使用されるトラストポイントを指定する必要があります。レスポндаについては、`tunnel-group` コマンドでトラストポイントを設定する必要があります。IKEv2 では、イニシエータとレスポндаの両方について、認証に使用するトラストポイントを `tunnel-group` コマンドで設定する必要があります。

手順

セキュリティアソシエーションを確立するための IKEv1 トランスフォームセットまたは IKEv2 IPsec プロポーザルを追加します。

IKEv1 トランスフォーム セットを追加します。

crypto ipsec ikev1 transform-set {transform-set-name | encryption | authentication}

例：

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

encryption では、IPsec データ フローを保護するための暗号化方式を指定します。

- `esp-aes` : AES と 128 ビット キーを使用します。
- `esp-aes-192` : AES と 192 ビット キーを使用します。
- `esp-aes-256` : AES と 256 ビット キーを使用します。
- `esp-null` : 暗号化なし。

authentication では、IPsec データ フローを保護するための暗号化方式を指定します

- `esp-md5-hmac` : ハッシュ アルゴリズムとして MD5/HMAC-128 を使用します。
- `esp-sha-hmac` : ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。
- `esp-none` : HMAC 認証なし。

IKEv2 IPsec プロポーザルを追加します。

(注)

IOS プラットフォームについては、IKEv2 プロファイル コンフィギュレーション モードで **no config-exchange request** コマンドを使用し、設定の交換のオプションをディセーブルにします。

詳細については、「<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280>」を参照してください。

- IPsec プロポーザルの名前を指定します。

crypto ipsec ikev2 ipsec-proposal IPsec proposal name

例：

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- crypto IPsec ikev2 ipsec-proposal コンフィギュレーションモードで、セキュリティパラメータを指定します。

```
protocol esp {encryption {aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null} |
integrity {sha-1 | sha-256 | sha-384 | sha-512 | null}}
```

例：

```
ciscoasa(config-ipsec-proposal)#protocol esp encryption aes aes-192
```

IPsec プロファイルの追加

IPsec プロファイルには、その参照先の IPsec プロポーザルまたはトランスフォームセット内にある必要なセキュリティプロトコルおよびアルゴリズムが含まれています。これにより、2つのサイト間 VTI VPN ピアの間でセキュアな論理通信パスが確保されます。

手順

ステップ1 プロファイル名を設定します。

```
crypto ipsec profile name
```

例：

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

ステップ2 IKEv1 または IKEv2 プロポーザルを設定します。IKEv1 トランスフォームセットまたは IKEv2 IPsec プロポーザルのいずれかを選択できます。

a) IKEv1 トランスフォームセットを設定します。

- IKEv1 プロポーザルを設定するには、crypto ipsec profile コマンドサブモードで次のコマンドを入力します。

```
set ikev1 transform set set_name
```

この例の SET1 は、以前に作成された IKEv1 プロポーザルセットです。

```
ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
```

b) IKEv2 プロポーザルを設定します。

- IKEv2 プロポーザルを設定するには、crypto ipsec profile コマンドサブモードで次のコマンドを入力します。

```
set ikev2 ipsec-proposal IPsec_proposal_name
```

この例では、SET1 は、以前に作成された IKEv2 IPsec プロポーザルです。

```
ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
```

ステップ3 (任意) セキュリティ アソシエーションの期間を指定します。

```
set security-association lifetime { seconds number | kilobytes {number | unlimited}}
```

例 :

```
ciscoasa(config-ipsec-profile)#set security-association lifetime  
seconds 120 kilobytes 10000
```

ステップ4 (任意) VTI トンネルの一端をレスポндаとしてのみ動作するように設定します。

responder-only

- VTI トンネルの一端をレスポндаとしてのみ動作するように設定できます。レスポндаのみの端は、トンネルまたはキー再生成を開始しません。
- IKEv2 を使用する場合、セキュリティ アソシエーションのライフタイム期間は、イニシエータ側の IPsec プロファイルのライフタイム値より大きく設定します。こうすることで、イニシエータ側での正常なキー再生成が促進され、トンネルのアップ状態が保たれます。
- IKEv1 を使用すると、IOS が継続的なチャネル モードをサポートしていないため、IOS は常にレスポндаのみのモードになります。ASA は、イニシエータ、セッション、キーの再生成になります。
- イニシエータ側のキー再生成の設定が不明の場合、レスポндаのみのモードを解除して SA の確立を双方向にするか、レスポндаのみの端の IPsec ライフタイム値を無期限にして期限切れを防ぎます。

ステップ5 (任意) PFS グループを指定します。Perfect Forward Secrecy (PFS) は、暗号化された各交換に対し、一意のセッション キーを生成します。この一意のセッション キーにより、交換は、後続の復号化から保護されます。PFS を設定するには、PFS セッション キーを生成する際に使用する Diffie-Hellman キー導出アルゴリズムを選択する必要があります。キー導出アルゴリズムは、IPsec セキュリティ アソシエーション (SA) キーを生成します。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。Diffie-Hellman グループは、両方のピアで一致させる必要があります。

```
set pfs { group14 }
```

例 :

```
ciscoasa(config-ipsec-profile)# set pfs group14
```

ステップ6 (任意) VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

```
set trustpoint name
```

例 :

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

ステップ7 (任意) この IPsec プロファイルのリバース ルート インジェクション (RRI) を有効にし、リバースルートをダイナミックに設定します。

```
set reverse-route [ dynamic]
```

例 :

```
ciscoasa(config-ipsec-profile)#set reverse-route dynamic
```

VTI インターフェイスの追加

新しい VTI インターフェイスを作成して VTI トンネルを確立するには、次の手順を実行します。



(注) アクティブなトンネル内のルータが使用できないときにトンネルをアップした状態に保つため、IP SLA を実装します。<http://www.cisco.com/go/asa-config> の『ASA General Operations Configuration Guide』の「Configure Static Route Tracking」を参照してください。

手順

ステップ 1 新しいトンネル インターフェイスを作成します。

```
interface tunnel tunnel_interface_number
```

トンネル ID を 0 ～ 10413 の範囲で指定します。最大 10413 の VTI インターフェイスがサポートされます。

例：

```
ciscoasa(config)#interface tunnel 100
```

ステップ 2 VTI インターフェイス の名前を入力します。

interface tunnel コマンド サブモードで、次のコマンドを入力します。

```
nameif interface name
```

例：

```
ciscoasa(config-if)#nameif vti
```

ステップ 3 VTI インターフェイスの IP アドレスを入力します。

```
ip address IP addressmask
```

例：

```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```

ステップ 4 仮想テンプレートが継承するインターフェイスの IPv4 アドレスまたは IPv6 アドレスを入力します。

デバイスに設定されている任意の物理インターフェイスからループバックアドレスを選択できます。仮想テンプレートから複製されたすべての仮想アクセスインターフェイスは、同じ IP アドレスを持つことになります。

```
ip unnumbered interface-name
```


ipv6 unnumbered *interface-name*

例 :

```
ciscoasa(config-if)#ip unnumbered loopback1
```

ステップ 5 トンネル送信元のインターフェイスを指定します。

tunnel source interface *interface_name*

送信元インターフェイスとして、物理インターフェイスかループバック インターフェイスを使用できます。

例 :

```
ciscoasa(config-if)#tunnel source interface outside
```

ステップ 6 トンネル宛先の IP アドレスを指定します。

tunnel destination *ip_address*

例 :

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

ステップ 7 トンネルにトンネル モード IPsec IPv4 を設定します。

tunnel mode ipsec ipv4

例 :

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

ステップ 8 トンネルに IPsec プロファイルを割り当てます。

tunnel protection ipsec *IPsec profile*

例 :

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

ステップ 9 スタティック VTI インターフェイスのトラフィックセクタを割り当てます。

tunnel protection policy *acl_name*

アクセスリストには、1 つまたは複数のリストセクタを含めることができます。このコマンドを設定しない場合、スタティック VTI インターフェイスは any-any セクタを提案します。これがデフォルトの動作です。

例 :

```
ciscoasa(config)# access-list Spoke-to-Hub extended permit ip 209.165.200.225  
255.255.255.224 any  
ciscoasa(config-if)# tunnel protection ipsec policy Spoke-to-Hub
```

例

ASA と IOS デバイスの間の VTI トンネル (IKEv2 を使用) の設定例

ASA □

```
crypto ikev2 policy 1
  encryption aes-gcm-256
  integrity null
  group 21
  prf sha512
  lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal gcm256
  protocol esp encryption aes-gcm-256
  protocol esp integrity null
!
crypto ipsec profile asa-vti
  set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
  nameif vti
  ip address 10.10.10.1 255.255.255.254
  tunnel source interface [asa-source-nameif]
  tunnel destination [router-ip-address]
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
  ikev2 remote-authentication pre-shared-key cisco
  ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]
```

IOS □

```
!
crypto ikev2 proposal asa-vti
  encryption aes-gcm-256
  prf sha512
  group 21
!
crypto ikev2 policy asa-vti
  match address local [router-ip-address]
  proposal asa-vti
!
crypto ikev2 profile asa-vti
  match identity remote address [asa-ip-address] 255.255.255.255
  authentication local pre-share key cisco
  authentication remote pre-share key cisco
  no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
  set ikev2-profile asa-vti
  set transform-set gcm256
!
interface tunnel 100
```

```
ip address 10.10.10.0 255.255.255.254
tunnel mode ipsec ipv4
tunnel source [router-interface]
tunnel destination [asa-ip-address]
tunnel protection ipsec profile asa-vti
!
```

ダイナミック VTI インターフェイスの追加

ダイナミック VTI の仮想テンプレートを作成するには、次の手順を行います。



- (注) アクティブなトンネル内のルータが使用できないときにトンネルをアップした状態に保つため、IP SLA を実装します。<http://www.cisco.com/go/asa-config> の『ASA General Operations Configuration Guide』の「Configure Static Route Tracking」を参照してください。

始める前に

IPsec プロファイルと IP アンナumberド インターフェイスが設定されていることを確認します。

手順

ステップ 1 新しい仮想テンプレートを作成します。

interface virtual-Template *template_number* type tunnel

template_number は、仮想テンプレート固有の番号です。範囲は 0 ～ 10413 です。

インターフェイス テンプレートはシャットダウン状態ではない必要があります。仮想テンプレートの必須パラメータは次のとおりです。

- インターフェイス名
- トンネル IPsec モード
- トンネル IPsec プロファイル

例：

```
ciscoasa(config)#interface virtual-Template 101 type tunnel
```

ステップ 2 ダイナミック VTI 仮想テンプレート インターフェイスの名前を指定します。

interface コンフィギュレーション モードで、次のコマンドを使用します。

nameif *interface_name*

ASA は、仮想アクセスインターフェイスを <Virtual_Template_name>_va<n> として動的に作成します。たとえば、仮想テンプレートの名前が dVTI101 の場合、仮想アクセスインターフェイス

スは dVTI101_va1、dVTI101_va2 などになります。仮想テンプレートを変更する場合は、**shutdown** コマンドを使用して仮想テンプレートをシャットダウンする必要があります。

例：

```
ciscoasa(config-if)#nameif dVTI101
```

ステップ 3 仮想テンプレートが継承するインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。

ip unnumbered interface-name

ipv6 unnumbered interface-name

仮想テンプレートは、任意の物理インターフェイスの IP アドレスまたはデバイスに設定されたループバックアドレスを継承できます。仮想テンプレートから複製されたすべての仮想アクセスインターフェイスは、同じ IP アドレスを持つことになります。

例：

```
ciscoasa(config-if)#ip unnumbered loopback1
```

ステップ 4 （任意）トンネル送信元インターフェイスを指定します。

tunnel source interface interface_name

発信元インターフェイスは、物理インターフェイスかループバック インターフェイスです。

ASA は、トンネル送信元 IP アドレスとして設定されたインターフェイスからのみ VPN セッション要求を受け入れます。このインターフェイスを指定しない場合、ASA は任意のインターフェイスから受信した VPN セッション要求を受け入れます。仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスから MTU を継承します。上記のオプションを有効にしない場合、仮想アクセスインターフェイスは、ASA が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。

例：

```
ciscoasa(config-if)#tunnel source interface outside1
```

ステップ 5 トンネル保護モードを IPv4 または IPv6 として指定します。

tunnel mode ipsec {ipv4 | ipv6}

例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

ステップ 6 トンネルに IPsec プロファイルを割り当てます。

tunnel protection ipsec profile ipsec_profile

この IPsec プロファイルは、交換のネゴシエーションに必要な IPSec/IKE パラメータを設定します。

例：

```
ciscoasa(config-if)#tunnel protection ipsec profile Profile1
```

ステップ 7 仮想テンプレートをトンネルグループに適用します。

tunnel-group tunnel_group_name type type

```
tunnel-group tunnel_group_name ipsec-attributes
```

```
virtual-template template_number
```

同じ仮想テンプレートを複数のトンネルグループに適用することができます。ASA は、仮想テンプレートを使用して、VPN セッションごとに個別の仮想アクセスインターフェイスを作成します。

例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 type ipsec-l2l  
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes  
ciscoasa(config-tunnel-ipsec)#virtual-template 101
```

ステップ 8 トンネルグループのダイナミックルーティングを有効にします。

```
tunnel-group tunnel_group_name ipsec-attributes
```

```
ikev2 route accept any
```

```
ikev2 route set interface
```

ikev2 route accept any コマンドを使用すると、ASA は、IKEv2 交換中に受信したすべてのトンネルインターフェイス IP アドレスを受け入れることが可能になります。デフォルトで、このオプションは有効になっています。

ikev2 route set interface コマンドを使用すると、ASA は、IKEv2 交換中にトンネルインターフェイスの IP アドレスを送信できるようになります。このオプションにより、BGP がトンネル経由で機能するための VTI インターフェイス間のユニキャスト到達可能性が有効になります。

BGP/OSPF/EIGRP を使用して、トンネルグループに対して動的ルーティングが有効になります。仮想テンプレートを設定した後、VTI トンネルを介してデバイス間のダイナミック VTI トラフィックをルーティングするようにルーティングポリシーを設定する必要があります。また、暗号化されたトラフィックを許可するアクセスコントロールルールを設定する必要があります。

例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes  
ciscoasa(config-tunnel-ipsec)#ikev2 route set interface  
ciscoasa(config-tunnel-ipsec)#ikev2 route accept any
```

仮想トンネルインターフェイスの機能履歴

機能名	リリース	機能情報
ダイナミック仮想トンネルインターフェイスのサポート	9.19(1)	ダイナミック VTI を作成し、それを使用して、ハブアンドスポークトポロジでルートベースのサイト間 VPN を設定できます。ダイナミック VTI は、大規模な企業向けハブアンドスポーク展開でのピアの構成を容易にします。ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。 新規/変更されたコマンド : interface virtual-Template、ip unnumbered、ipv6 unnumbered、tunnel protection ipsec policy
OSPF IPv4 および IPv6 のサポート	9.19(1)	VTI 経由の OSPF IPv4 および IPv6 ルーティングプロトコルをサポートします。
EIGRP のサポート	9.19(1)	VTI 経由の EIGRP IPv4 および IPv6 ルーティングプロトコルをサポートします。
スタティックおよびダイナミック VTI のループバックインターフェイスのサポート	9.19(1)	ループバック インターフェイスを VTI の送信元インターフェイスとして設定できるようになりました。静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。 新規/変更されたコマンド : tunnel source interface、ip unnumbered、ipv6 unnumbered
ローカルトンネル ID のサポート	9.17(1)	ASA は、ASA が NAT の背後に複数の IPsec トンネルを持ち、Cisco Umbrella Secure Internet Gateway (SIG) に接続できるようにする、一意のローカルトンネル ID をサポートしています。ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。 新規/変更されたコマンド : local-identity-from-cryptomap、
スタティック VTI での IPv6 のサポート	9.16(1)	ASA は、仮想トンネルインターフェイス (VTI) の設定で IPv6 アドレスをサポートしています。 VTI トンネル送信元インターフェイスには、トンネルエンドポイントとして使用するように設定できる IPv6 アドレスを設定できます。トンネル送信元インターフェイスに複数の IPv6 アドレスがある場合は、使用するアドレスを指定できます。指定しない場合は、リストの最初の IPv6 グローバルアドレスがデフォルトで使用されます。 トンネルモードは、IPv4 または IPv6 のいずれかです。ただし、トンネルをアクティブにするには、VTI で設定されている IP アドレスタイプと同じである必要があります。IPv6 アドレスは、VTI のトンネル送信元インターフェイスまたはトンネル宛先インターフェイスに割り当てることができます。 新規/変更されたコマンド : tunnel source interface、tunnel destination、tunnel mode

機能名	リリース	機能情報
デバイスあたり 1024 個の VTI インターフェイスのサポート	9.16(1)	デバイスに設定できる VTI の最大数が、100 個から 1024 個に増加しました。 プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、ASA 5510 は 100 個の VLAN をサポートしているため、トンネル数は 100 から設定された物理インターフェイスの数を引いた数になります。 新規/変更されたコマンド：なし
VTI での DHCP リレーサーバーのサポート	9.14(1)	ASA は、インターフェイスを接続する DHCP リレーサーバーとして VTI インターフェイスを設定することを可能にします。 次のコマンドが変更されました。 dhcprelay server ip_address vti_ifc_name。
VTI での IKEv2、証明書ベース認証、および ACL のサポート	9.8(1)	仮想トンネルインターフェイス (VTI) は、BGP (静的 VTI) をサポートするようになりました。スタンドアロンモードとハイアベイラビリティモードで、IKEv2 を使用できます。IPsec プロファイルにトラストポイントを設定することにより、証明書ベースの認証を使用できます。また、入力トラフィックをフィルタリングする access-group コマンドを使用して、VTI 上でアクセスリストを適用することもできます。 IPsec プロファイルのコンフィギュレーションモードに次のコマンドが導入されました。 set trustpoint
仮想トンネルインターフェイス (VTI) のサポート	9.7.(1)	ASA が、仮想トンネルインターフェイス (VTI) と呼ばれる新しい論理インターフェイスによって強化されました。VTI はピアへの VPN トンネルを表すために使用されます。これは、トンネルの各終端に接続されている IPsec プロファイルを利用したルートベースの VPN をサポートします。VTI を使用することにより、静的暗号マップのアクセスリストを設定してインターフェイスにマッピングすることが不要になります。 次のコマンドが導入されました。 crypto ipsec profile、interface tunnel、responder-only、set ikev1 transform-set、set pfs、set security-association lifetime、tunnel destination、tunnel mode ipsec、tunnel protection ipsec profile、tunnel source interface。



第 12 章

VPN の外部 AAA サーバーの設定

- [外部 AAA サーバーについて \(327 ページ\)](#)
- [外部 AAA サーバーを使用する際のガイドライン \(328 ページ\)](#)
- [複数証明書認証の設定 \(328 ページ\)](#)
- [VPN の LDAP 許可の設定 \(330 ページ\)](#)
- [Active Directory/LDAP VPN リモート アクセス許可の例 \(346 ページ\)](#)

外部 AAA サーバーについて

この ASA は、外部の LDAP、RADIUS、TACACS+ サーバーを使用して、ASA の認証、認可、アカウントिंग (AAA) をサポートするように設定できます。外部 AAA サーバーは、設定されたアクセス許可と属性を適用します。外部サーバーを使用するように ASA を設定する前に、適切な ASA 許可属性を指定して外部 AAA サーバーを設定し、それらの属性のサブセットから特定のアクセス許可を個々のユーザーに割り当てる必要があります。

許可属性のポリシー適用の概要

ASA は、ユーザー認可属性（ユーザー権利またはユーザー権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ASA を設定して、次のいずれかの組み合わせからユーザー属性を取得できます。

- ASA のダイナミック アクセス ポリシー (DAP)
- 外部 RADIUS または LDAP 認証および許可サーバー（およびその両方）
- ASA のグループ ポリシー

ASA がすべてのソースから属性を受信すると、それらの属性は評価されて集約され、ユーザーポリシーに適用されます。属性の間で衝突がある場合、DAP 属性が優先されます。

ASA は次の順序で属性を適用します。

1. ASA 上の DAP 属性：バージョン 8.0(2) で導入されたこの属性は、他のどの属性よりも優先されます。DAP 内でブックマークまたは URL リストを設定した場合は、グループポリシーで設定されているブックマークや URL リストよりも優先されます。

2. AAA サーバー上のユーザー属性：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。これらの属性を、ASA のローカル AAA データベースで個々のユーザーに設定されている属性（ASDM のユーザー アカウント）と混同しないようにしてください。
3. ASA で設定されているグループポリシー：RADIUSサーバーからユーザーに対してRADIUS CLASS 属性 IETF-Class-25（OU=*group-policy*）の値が返された場合、ASA はそのユーザーを同じ名前のグループポリシーに配置し、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。

LDAPサーバーでは、任意の属性名を使用してセッションのグループポリシーを設定できます。ASA 上に設定された LDAP 属性マップによって、LDAP 属性が Cisco 属性 IETF-Radius-Class にマッピングされます。
4. 接続プロファイル（CLIでは「トンネルグループ」と呼ばれます）によって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。ASA に接続しているすべてのユーザーは、最初にこのグループに所属します。このグループで、DAP、サーバーから返されるユーザー属性、ユーザーに割り当てられているグループポリシーにはない属性が提供されます。
5. ASA で割り当てられたデフォルトのグループポリシー（DfltGrpPolicy）：システムのデフォルト属性は、DAP、ユーザー属性、グループポリシー、接続プロファイルで不足している値を提供します。

外部 AAA サーバーを使用する際のガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を適用します。RADIUS 属性は、名前ではなく数値 ID によって適用されます。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ASDM バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 属性は、RADIUS の章に記載されている RADIUS 属性のサブセットです。

複数証明書認証の設定

セキュアクライアント SSL クライアントプロトコルと IKEv2 クライアントプロトコルを使用して、セッションごとに複数の認証を検証できるようになりました。たとえば、マシン証明書の発行元が特定の CA と一致することでデバイスが企業から支給されたデバイスであることを確認できます。

複数証明書オプションを使用すると、証明書を通じたマシンとユーザー両方の証明書認証が可能になります。このオプションがなければ、両方ではなく一方のみの証明書認証しか行うことができません。



- (注) 複数の証明書認証にはマシン証明書とユーザー証明書（または2つのユーザー証明書）が必要であるため、この機能ではセキュアクライアント Start Before Logon (SBL) を使用できません。

ユーザー名の事前入力フィールドでは、2つ目の（ユーザー）証明書のフィールドを解析し、AAA および証明書認証済みの接続で以降の AAA 認証に使用することができます。プライマリとセカンダリの両方の事前入力のユーザー名は、常にクライアントから受信した2つ目の（ユーザー）証明書から取得されます。

9.14(1) 以降、ASA では、複数証明書認証を設定し、認証または許可にユーザー名の事前入力オプションを使用する場合に、プライマリユーザー名およびセカンダリユーザー名を取得する証明書を指定できます。詳細については、[複数証明書ユーザー名の設定 \(329 ページ\)](#) を参照してください。

複数証明書認証では、2つの証明書が認証されます。クライアントから受信した2つ目の（ユーザー）証明書は、事前入力および証明書由来のユーザー名のプライマリおよびセカンダリユーザー名による解析対象です。

SAML による複数証明書認証も設定できます。

既存の認証 webvpn 属性は、複数証明書認証のオプションを含めるように変更されます。

```
tunnel-group <name> webvpn-attributes
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml] | saml [certificate | multiple-certificate]}
```

複数証明書認証では、その接続試行を認証するために使用された証明書のフィールドに基づいてポリシー決定を行うことができます。複数証明書認証中にクライアントから受信したユーザーおよびマシンの証明書は DAP にロードされ、証明書のフィールドに基づいてポリシーを設定することができます。接続試行を許可または拒否するルールを設定できるようにダイナミックアクセス ポリシー (DAP) を使用して複数証明書認証を追加するには、『[ASA VPN ASDM Configuration Guide](#)』の適切なリリースの「Add Multiple Certificate Authentication to DAP」を参照してください。

複数証明書ユーザー名の設定

ASA 9.14(1) では、認証または許可のプライマリユーザー名およびセカンダリユーザー名として ASA で使用する必要がある証明書を設定するための新しいコマンドが導入されました。認証または許可パラメータを取得するために、SSL または IKE で送信されたマシン証明書（1 つ目の証明書）を使用するか、クライアントからのユーザー証明書（2 つ目の証明書）を使用するかを指定できます。このオプションは、認証タイプ（aaa、certificate、または multiple-certificate）に関係なく、任意のトンネルグループに使用および設定できます。ただし、構成は、複数証明書認証（multiple-certificate または aaa multiple-certificate）に対してのみ有効となります。このオプションが複数証明書認証に使用されない場合は、2 つ目の証明書がデフォルトとして認証または許可に使用されます。

手順

ステップ 1 1つ目の証明書と2つ目の証明書のどちらのプライマリユーザー名を使用するかを指定します。

username-from-certificate-choice {first-certificate | second-certificate}

ステップ 2 1つ目の証明書と2つ目の証明書のどちらのセカンダリユーザー名を使用するかを指定します。

secondary-username-from-certificate-choice {first-certificate | second-certificate}

例 :

```
tunnel-group tgl webvpn-attributes
authentication aaa multiple-certificate
pre-fill-username client
secondary-pre-fill-username client
tunnel-group tgl type remote-access
tunnel-group tgl general-attributes
secondary-authentication-server-group LOCAL
username-from-certificate-choice first-certificate
secondary-username-from-certificate-choice first-certificate
```

VPN の LDAP 許可の設定

VPN アクセスのための LDAP 認証が成功すると、ASA は LDAP 属性を返す LDAP サーバーに対してクエリーを実行します。通常これらの属性には、VPNセッションに適用される認可データが含まれます。

この許可メカニズムとは別の異なる許可を LDAP ディレクトリ サーバーから取得することが必要な場合があります。たとえば、認証に SDI または証明書サーバーを使用している場合、認可情報は返されません。この場合、ユーザー認可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と認可は2つのステップで行われます。

LDAP を使用した VPN ユーザー許可を設定するには、次の手順を実行します。

手順

ステップ 1 AAA サーバー グループを作成します。

aaa-server server_group protocol {ldap | nt | radius | sdi | tacacs+}

例 :

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

ステップ 2 remotegrp という名前の IPsec リモート アクセス トンネル グループを作成します。

tunnel-group groupname

例 :

```
hostname(config)# tunnel-group remotegrp
```

ステップ 3 サーバー グループとトンネル グループを関連付けます。

tunnel-group groupname general-attributes

例 :

```
hostname(config)# tunnel-group remotegrp general-attributes
```

ステップ 4 以前作成した認証のための AAA サーバー グループに新しいトンネル グループを割り当てます。

authorization-server-group group-tag

例 :

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

例

次に、LDAP を使用したユーザー許可を有効にするコマンドの例を示します。この例では、RAVPN という名前の IPsec リモート アクセス トンネル グループを作成し、すでに作成してある許可用の LDAP AAA サーバー グループにその新しいトンネルグループを割り当てています。

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# authorization-server-group (inside) LDAP
hostname(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリパスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを設定できます。

```
hostname(config)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
```

```
hostname(config-aaa-server-host) # server-type microsoft
```

ASA LDAP 構成の定義

このセクションでは、LDAP AV-pair 属性のシンタックスの定義方法について説明します。次の情報が含まれています。

- [LDAP 許可でサポートされている Cisco 属性 \(332 ページ\)](#)
- [Cisco-AV-Pair 属性の構文 \(345 ページ\)](#)
- [Cisco-AV-Pair の ACL 例 \(346 ページ\)](#)



(注) ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を適用します。一方、RADIUS 属性には、名前ではなく数値の ID が使用されます。

認可では、権限または属性を使用するプロセスを参照します。認証または認可サーバーとして定義されている LDAP サーバーは、権限または属性（設定されている場合）を適用します。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ソフトウェア バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 許可でサポートされている Cisco 属性

このセクションでは、ASA 5500、VPN 3000 コンセントレータ、および PIX 500 シリーズ ASA で使用される全属性のリストを示します。この表には、VPN 3000 コンセントレータおよび PIX 500 シリーズ ASA での属性サポート情報も含まれています。これは、このようなデバイスの組み合わせを使用するネットワークを設定するために役立ちます。

表 14: ASA が LDAP 許可でサポートする Cisco 属性

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Access-Hours	Y	Y	対応	文字列	シングル	time-range の名前 (Business-Hours など)
Allow-Network-Extension-Mode	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	Y	Y	対応	整数	シングル	1 ~ 35791394 分

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Authorization-Required	対応			整数	シングル	0 = しない 1 = する
Authorization-Type	対応			整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	Y	対応	文字列	シングル	クライアントレス SSL VPN、クライアント SSL VPN、および IPSec クライアントのバナー文字列。
Banner2	Y	Y	対応	文字列	シングル	クライアントレス SSL VPN、クライアント SSL VPN、および IPSec クライアントのバナー文字列。
Cisco-AV-Pair	Y	Y	対応	文字列	[マルチ (Multi)]	次の形式のオクテット文字列 : [Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port] 詳細については、「 Cisco AV ペア属性のシンタックス 」のセクションを参照してください。
Cisco-IP-Phone-Bypass	Y	Y	対応	整数	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	Y	対応	整数	シングル	0 = ディセーブル 1 = イネーブル
Client-Intercept-DHCP-Configure-Msg	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
Client-Type-Version-Limiting	Y	Y	対応	文字列	シングル	IPsec VPN クライアントのバージョン番号を示す文字列
Confidence-Interval	Y	Y	対応	整数	シングル	10 ~ 300 秒
DHCP-Network-Scope	Y	Y	対応	文字列	シングル	IP アドレス

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
DN-Field	Y	Y	対応	文字列	シングル	有効な値 : UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name。
Firewall-ACL-In		Y	対応	文字列	シングル	アクセス リスト ID
Firewall-ACL-Out		Y	対応	文字列	シングル	アクセス リスト ID
Group-Policy		Y	対応	文字列	シングル	リモート アクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の 3 つの形式のいずれかを使用できます。 • グループ ポリシー名 • OU= グループ ポリシー名 • OU= グループ ポリシー名 :
IE-Proxy-Bypass-Local				ブール	シングル	0 = ディセーブル 1 = イネーブル
IE-Proxy-Exception-List				文字列	シングル	DNS ドメインのリスト。エントリは改行文字シーケンス (\n) で区切る必要があります。
IE-Proxy-Method	Y	Y	対応	整数	シングル	1 = プロキシ設定を変更しない 2 = プロキシを使用しない 3 = 自動検出 4 = ASA 設定を使用する
IE-Proxy-Server	Y	Y	対応	整数	シングル	IP アドレス

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
IETF-Radius-Class	Y	Y	対応		シングル	リモート アクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の 3 つの形式のいずれかを使用できます。 - グループ ポリシー名 - OU= グループ ポリシー名 - OU= グループ ポリシー名 :
IETF-Radius-Filter-Id	Y	Y	対応	文字列	シングル	ASA で定義されたアクセスリスト名。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETF-Radius-Framed-IP-Address	Y	Y	対応	文字列	シングル	IP アドレス。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETF-Radius-Framed-IP-Netmask	Y	Y	対応	文字列	シングル	IP アドレス マスク。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETF-Radius-Idle-Timeout	Y	Y	対応	整数	シングル	Seconds
IETF-Radius-Service-Type	Y	Y	対応	整数	シングル	1 = Login 2 = Framed 5 = リモート アクセス 6 = Administrative 7 = NAS プロンプト
IETF-Radius-Session-Timeout	Y	Y	対応	整数	シングル	Seconds
IKE-Keep-Alives	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
IPsec-Allow-Passwd-Stor	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Authentication	Y	Y	対応	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP (認可のみ) 3 = NT ドメイン 4 = SDI (RSA) 5 = 内部 6 = RADIUS with Expiry 7 = Active Directory
IPsec-Auth-On-Rekey	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Backup-Server-List	Y	Y	対応	文字列	シングル	サーバー アドレス (スペース区切り)
IPsec-Backup-Servers	Y	Y	対応	文字列	シングル	1 = クライアントが設定したリストを使用する 2 = クライアント リストをディセーブルにして消去する 3 = バックアップ サーバー リストを使用する
IPsec-Client-Firewall-Filter-Name	対応			文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	Y	対応	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	Y	対応	文字列	シングル	クライアントに送信する1つのデフォルト ドメイン名を指定します (1 ~ 255 文字)。
IPsec-ExtAuth-On-Rekey		Y	対応	文字列	シングル	文字列

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
IPsec-IKE-Peer-ID-Check	Y	Y	対応	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	Y	対応	整数	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Mode-Config	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP-Port	Y	Y	対応	整数	シングル	4001 ~ 49151、デフォルトは 10000。
IPsec-Remote-Auth-Client-Auth-Mode	Y	Y	対応	整数	シングル	0 = なし 1 = リモート FW Are-You-There (AYT) で定義されているポリシー 2 = Policy pushed CPP 4 = サーバーからのポリシー
IPsec-Sec-Association	対応			文字列	シングル	セキュリティ アソシエーションの名前
IPsec-Split-DNS-Names	Y	Y	対応	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します (1 ~ 255 文字)。
IPsec-Split-Tunneling-Policy	Y	Y	対応	整数	シングル	0 = すべてをトンネリング 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	Y	対応	文字列	シングル	スプリット トンネルの包含リストを記述したネットワークまたはアクセス リストの名前を指定します。
IPsec-Tunnel-Type	Y	Y	対応	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
L2TP-Encryption	対応			整数	シングル	ビットマップ : 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MP-Compression	対応			整数	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	Y	Y	対応	文字列	シングル	IP アドレス
PFS-Required	Y	Y	対応	ブール	シングル	0 = しない 1 = する
Port-Forwarding-Name	Y	対応		文字列	シングル	名前の文字列 (例 : 「Corporate-Apps」)
PPTP-Encryption	はい			整数	シングル	ビットマップ : 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 例 : 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MP-Compression	対応			整数	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	Y	Y	対応	文字列	シングル	IP アドレス
Primary-WINS	Y	Y	対応	文字列	シングル	IP アドレス
Privilege-Level				整数	シングル	ユーザー名の場合、0 ~ 15

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Required-Client-Firewall-Vendor-Code	Y	Y	対応	整数	シングル	1 = シスコ (Cisco Integrated Client を使用) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ (Cisco Intrusion Prevention Security Agent を使用)
Required-Client-Firewall-Description	Y	Y	対応	文字列	シングル	—
Required-Client-Firewall-Product-Code	Y	Y	対応	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client (CIC) Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Require-HW-Client-Auth	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
Require-Individual-User-Auth	Y	Y	対応	整数	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	Y	Y	対応	文字列	シングル	IP アドレス
Secondary-WINS	Y	Y	対応	文字列	シングル	IP アドレス
SEP-Card-Assignment				整数	シングル	未使用

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Simultaneous-Logins	Y	Y	対応	整数	シングル	0 ～2147483647
Strip-Realm	Y	Y	対応	ブール	シングル	0 = ディセーブル 1 = イネーブル
TACACS-AuthType	Y	Y	対応	整数	シングル	—
TACACSPrivilegeLevel	Y	Y	対応	整数	シングル	—
Tunnel-Group-Lock		Y	対応	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	Y	対応	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN. 32 = SVC 64 = IPsec (IKEv2) 8 および 4 は相互排他値 (0～11、16～27、32～43、48～59 は有効値)。
Use-Client-Address	対応			ブール	シングル	0 = ディセーブル 1 = イネーブル
User-Auth-Server-Name	対応			文字列	シングル	IPアドレス/ホスト名
User-Auth-Server-Port	Y	Y	対応	整数	シングル	サーバー プロトコルのポート番号
User-Auth-Server-Secret	対応			文字列	シングル	サーバーのパスワード
WebVPN-ACL-Filters		対応		文字列	シングル	Webtype アクセス リスト名
WebVPNApplyACLFilter	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル バージョン 8.0 以降では、この属性は必須ではありません。

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
WebVPNClientSupportEnable	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル バージョン 8.0 以降では、この属性は必須ではありません。
WebVPNEnableFunctions				整数	シングル	使用しない (廃止)
WebVPNExchangeServerAddress				文字列	シングル	使用しない (廃止)
WebVPNExchangeServerNETBIOS-Name				文字列	シングル	使用しない (廃止)
WebVPNFileAccessEnable	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNFileServerBrowseEnable	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNFileServerEntry-Enable	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNForwardedPorts		対応		文字列	シングル	ポート転送リスト名
WebVPN-Homepage	Y	対応		文字列	シングル	URL (たとえば http://www.example.com)
WebVPNMacShim1Url	Y	対応		文字列	シングル	例については、次の URL にある『SSL VPN Deployment Guide』を参照してください。 http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPNMacShim1Url2	Y	対応		文字列	シングル	例については、次の URL にある『SSL VPN Deployment Guide』を参照してください。 http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPNPortForwarding-Auto-Download-Enable	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
WebVPN-PortForwarding-Enable	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-PortForwarding-Exchange-Proxy-Enable	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-PortForwarding-HTTP-Proxy-Enable	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Single-Sign-On-Server-Name	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCCleanDPI	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCCompression	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Enable	Y	対応		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCGatewayDPI	Y	対応		整数	シングル	0 = ディセーブル n = デッドピア検出値 (30 ~ 3600 秒)
WebVPN-SVC-Keepalive	Y	対応		整数	シングル	0 = ディセーブル n = キープアライブ値 (15 ~ 600 秒)
WebVPNSVCKeepEnable	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCRetryMethod	Y	対応		整数	シングル	0 = なし 1 = SSL 2 = 新規トンネル 3 = 任意 (SSL に設定)

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
WebVPN-SVC-Require-Port	Y	対応		整数	シングル	0 = ディセーブル n = 分単位の再試行間隔 (4 ~ 10080 分)
WebVPN-SVC-Require-Auth	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-Require-Auth	Y	対応		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-List		対応		文字列	シングル	URL リスト名

ACL でサポートされる URL タイプ

URL は部分的な URL でもかまいません。また、サーバーを表すワイルドカードや、ポートが含まれていてもかまいません。

次の URL タイプがサポートされています。

すべての URL	https://	post://	ssh://
cifs://	ica://	rdp://	telnet://
citrix://	imap4://	rdp2://	vnc://
citrixs://	ftp://	smart-tunnel://	
http://	pop3://	smtp://	

Cisco-AV-Pair (ACL) 使用のガイドライン

- リモート IPsec トンネルおよび SSL VPN Client (SVC) トンネルにアクセス リストを適用するには、Cisco-AV-Pair エントリにプレフィックス `ip:inac1#` を追加して使用してください。
- SSL VPN クライアントレス (ブラウザモード) トンネルにアクセス リストを適用するには、Cisco-AV-Pair エントリにプレフィックス `webvpn:inac1#` を追加して使用してください。
- Webtype ACL では、ASA が送信元となるため、送信元を指定しないでください。

表 15: ASA でサポートされるトークン

トークン	構文のフィールド	説明
ip:inacl# Num =	該当なし (識別子)	(ここで、Num は一意の整数です) すべての AV ペアアクセス制御リストを開始します。リモート IPsec トンネルと SSLVPN (SVC) トンネルにアクセス リストを適用します。
webvpn:inacl# Num =	該当なし (識別子)	(ここで、Num は一意の整数です) すべてのクライアントレス SSL AV ペアアクセス制御リストを開始します。クライアントレス (ブラウザモード) トンネルにアクセス リストを適用します。
deny	アクション	アクションを拒否します。(デフォルト)。
許可	アクション	アクションを許可します。
icmp	プロトコル	インターネット制御メッセージプロトコル (ICMP)
1	プロトコル	インターネット制御メッセージプロトコル (ICMP)
IP	プロトコル	インターネットプロトコル (IP)
0	プロトコル	インターネットプロトコル (IP)
[TCP]	プロトコル	伝送制御プロトコル (TCP)
[6]	プロトコル	伝送制御プロトコル (TCP)
UDP	プロトコル	User Datagram Protocol (UDP)
17	プロトコル	User Datagram Protocol (UDP)
任意	ホストネーム	すべてのホストにルールを適用します。
host	ホストネーム	ホスト名を示す任意の英数字文字列。
log	ログ	イベントが発生すると、フィルタ ログ メッセージが表示されます。(permit and log または deny and log の場合と同様)。
lt	演算子	値より小さい
gt	演算子	値より大きい
eq	演算子	値と等しい
neq	演算子	値と等しくない
range	演算子	この範囲に含まれる。range の後に 2 つの値を続けます。

Cisco-AV-Pair 属性の構文

Cisco Attribute Value (AV) ペア (ID 番号 26/9/1) を使用すると、アクセス リストを RADIUS サーバー (たとえば Cisco ACS) から、または LDAP サーバーから LDAP 属性マップ経由で適用できます。

Cisco-AV-Pair ルールの構文は次のとおりです。

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]

表 16: AV-Pair 属性の構文ルール

フィールド	説明
操作	ルールに一致する場合に実行するアクション (deny または permit)。
接続先 (Destination)	パケットを受信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード any で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。
Destination Wildcard Mask	宛先アドレスに適用されるワイルドカードマスク。
ログ	FILTER ログメッセージを生成します。重大度レベル9のイベントを生成するには、このキーワードを使用する必要があります。
演算子	論理演算子: greater than、less than、equal to、not equal to。
[ポート (Port)]	TCP または UDP ポートの番号 (0 ~ 65535)。
[プレフィックス (Prefix)]	AV ペアの固有識別子。(例: ip:inac1#1= (標準アクセス リスト用) または webvpn:inac1# (クライアントレス SSL VPN アクセスリスト用))。このフィールドは、フィルタが AV ペアとして送信された場合にだけ表示されます。
プロトコル	IP プロトコルの番号または名前。0 ~ 255 の整数値、または icmp 、 igmp 、 ip 、 tcp 、 udp のいずれかのキーワード。
ソース (Source)	パケットを送信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード any で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。ASA がソースまたはプロキシの役割を果たすため、このフィールドはクライアントレス SSL VPN には適用されません。
Source Wildcard Mask	送信元アドレスに適用されるワイルドカードマスク。ASA がソースまたはプロキシの役割を果たすため、このフィールドはクライアントレス SSL VPN には適用されません。

Cisco-AV-Pair の ACL 例

このセクションでは、Cisco AV ペアの例を示し、その結果の許可または拒否のアクションについて説明します。



(注) `inacl#` の各 ACL # は固有である必要があります。ただし、これらは連続している（たとえば 1、2、3、4）必要はありません。たとえば、5、45、135 でもかまいません。

表 17: Cisco AV ペアとそのアクション許可/拒否の例

Cisco-AV-Pair の例	アクションの許可または拒否
<code>ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log</code>	フルトンネル IPsec または SSL VPN クライアントを使用した、2 つのホスト間の IP トラフィックを許可します。
<code>ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log</code>	フルトンネル IPsec または SSL VPN クライアントのみを使用した、すべてのホストから特定のホストのポート 80 への TCP トラフィックを許可します。
<code>webvpn:inacl#1=permit url http://www.example.comwebvpn:inacl#2=deny url smtp://serverwebvpn:inacl#3=permit url cifs://server/share</code>	指定 URL へのクライアントレス SSL VPN トラフィックを許可し、特定サーバーへの SMTP トラフィックを拒否し、指定サーバーへのファイル共有アクセス (CIFS) を許可します。
<code>webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log</code>	クライアントレス SSL VPN について、非デフォルト ポート 2323 および 2222 で Telnet アクセスを拒否し、SSH アクセスを許可します。これらのポートを使用して通過する他のアプリケーション トラフィックも同様に許可または拒否します。
<code>webvpn:inacl#1=permit url ssh://10.86.1.2webvpn:inacl#35=permit tcp 10.86.1.5 eq 22 logwebvpn:inacl#48=deny url telnet://10.86.1.2webvpn:inacl#100=deny tcp 10.86.1.6 eq 23</code>	クライアントレス SSL VPN でのデフォルト ポート 22 への SSH アクセスを許可し、ポート 23 への Telnet アクセスを拒否します。この例は、これらの ACL で適用される Telnet または SSH Java プラグインを使用していることを前提とします。

Active Directory/LDAP VPN リモート アクセス許可の例

この項では、Microsoft Active Directory サーバーを使用している ASA で認証および認可を設定するための手順の例を示します。説明する項目は次のとおりです。

- [ユーザー ベースの属性のポリシー適用 \(347 ページ\)](#)
- [セキュアクライアントトンネルのスタティック IP アドレス割り当ての適用 \(349 ページ\)](#)
- [ダイヤルイン許可または拒否アクセスの適用 \(351 ページ\)](#)
- [ログオン時間と Time-of-Day ルールの適用 \(353 ページ\)](#)

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- 『ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example』
- 『PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login』

ユーザー ベースの属性のポリシー適用

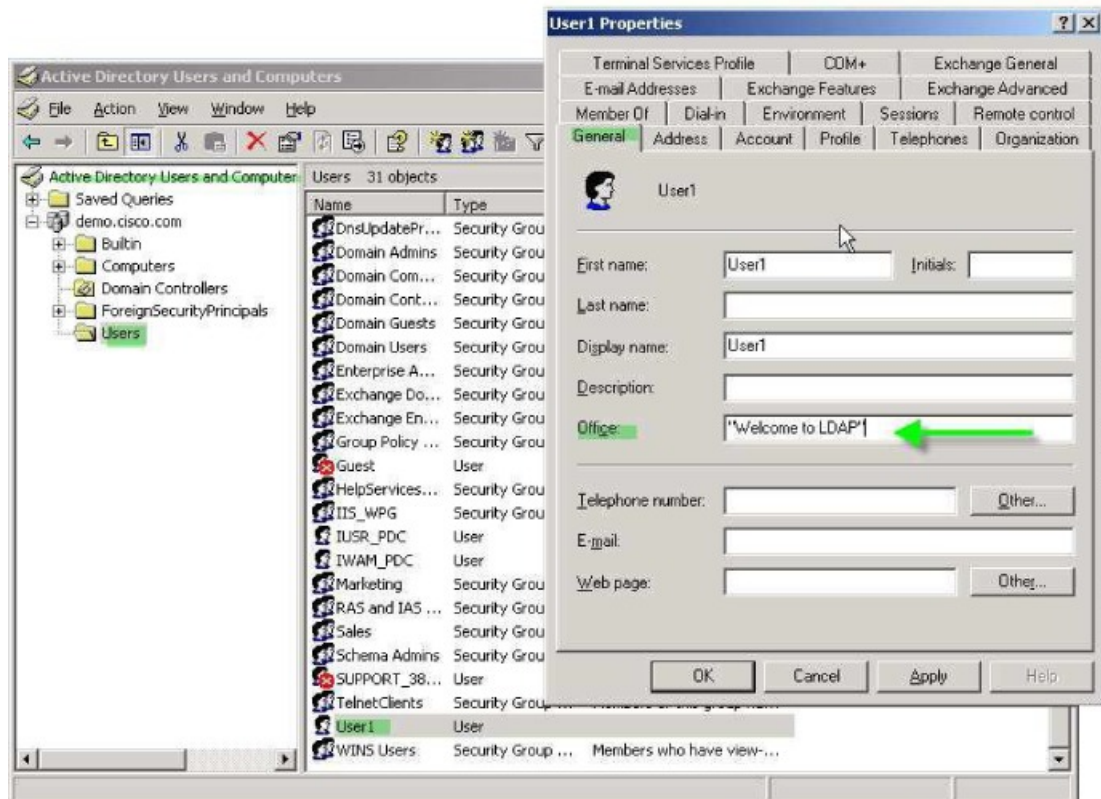
この例では、ユーザー向けの簡易バナーを表示して、標準の LDAP 属性を既知のベンダー固有属性（VSA）にマッピングする方法と 1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングする方法を示します。IPsec VPN クライアントやセキュアクライアントなど、どの接続タイプにも適用されます。

AD LDAP サーバー上で設定されたユーザーに簡易バナーを適用するには、[General] タブの [Office] フィールドを使用してバナー テキストを入力します。このフィールドでは、physicalDeliveryOfficeName という名前の属性を使用します。ASA で、physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングする属性マップを作成します。

認証時、ASA はサーバーから physicalDeliveryOfficeName の値を取得し、その値を Cisco 属性 Banner1 にマッピングしてユーザーにバナーを表示します。

手順

-
- ステップ 1** ユーザー名を右クリックして、[Properties] ダイアログボックスの [General] タブを開き、AD/LDAP 属性 physicalDeliveryOfficeName を使用する [Office] フィールドにバナー テキストを入力します。



ステップ 2 ASA で LDAP 属性マップを作成します。

Banner というマップを作成し、AD/LDAP 属性 physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングします。

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバー ホスト コンフィギュレーション モードを開始し、以前作成した属性マップ Banner を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

ステップ 4 バナーの適用をテストします。

セキュアクライアント トンネルのスタティック IP アドレス割り当ての適用

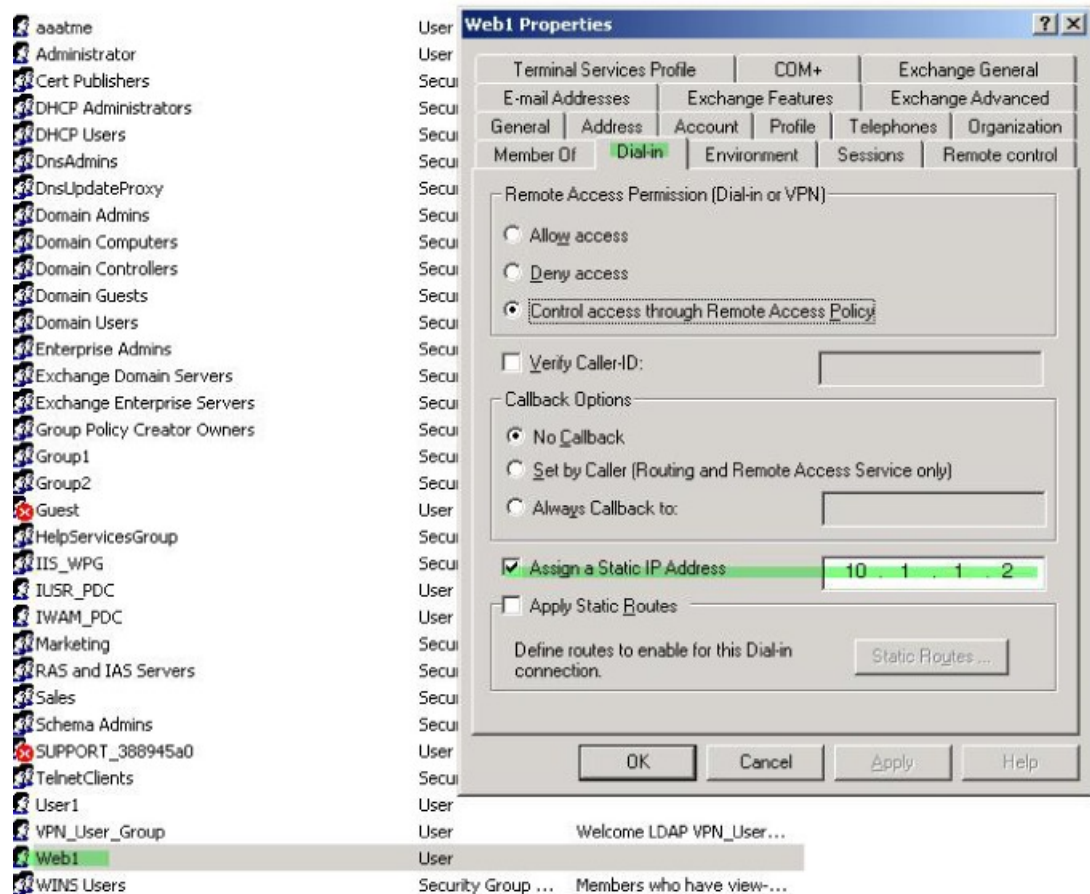
この例は、IPsec クライアントや SSL VPN クライアントなどのフルトンネルクライアントに適用されます。

スタティック セキュアクライアント スタティック IP 割り当てを適用するには、セキュアクライアントユーザー Web1 をスタティック IP アドレスを受信するように設定して、そのアドレスを AD LDAP サーバーの [ダイヤルイン (Dialin)] タブの [スタティック IP アドレスの割り当て (Assign Static IP Address)] フィールド (このフィールドで msRADIUSFramedIPAddress 属性が使用される) に入力し、この属性を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする属性マップを作成します。

認証時に、ASA はサーバーから msRADIUSFramedIPAddress の値を取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングして、User1 にスタティック アドレスを渡します。

手順

-
- ステップ 1** ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Assign Static IP Address] チェックボックスをオンにして、10.1.1.2 という IP アドレスを入力します。



ステップ 2 図に示す LDAP コンフィギュレーションの属性マップを作成します。

[Static Address] フィールドで使用される AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングします。

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、作成した属性マップ static_address を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

ステップ 4 vpn-address-assignment コマンドが AAA を指定するように設定されているかどうかを確認するために、コンフィギュレーションのこの部分を表示します。


```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

ステップ 5 ASA とセキュアクライアントとの接続を確立します。サーバーで設定され、ASA にマッピングされた IP アドレスをユーザーが受信することを確認します。

ステップ 6 `show vpn-sessiondb svc` コマンドを使用してセッションの詳細を表示し、割り当てられたアドレスを確認します。

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username       : web1                      Index       : 31
Assigned IP    : 10.1.1.2                  Public IP    : 10.86.181.70
Protocol       : Clientless SSL-Tunnel     DTLS-Tunnel
Encryption     : RC4 AES128                Hashing      : SHA1
Bytes Tx       : 304140                    Bytes Rx     : 470506
Group Policy   : VPN_User_Group             Tunnel Group : Group1_TunnelGroup
Login Time     : 11:13:05 UTC Tue Aug 28 2007
Duration      : 0h:01m:48s
NAC Result     : Unknown
VLAN Mapping   : N/A                      VLAN         : none
```

ダイヤルイン許可または拒否アクセスの適用

この例では、ユーザーによって許可されるトンネリングプロトコルを指定する LDAP 属性マップを作成します。[Dialin] タブの許可アクセスと拒否アクセスの設定を Cisco 属性 Tunneling-Protocol にマッピングします。この属性は次のビットマップ値をサポートします。

値	トンネリング プロトコル
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec
16	クライアントレス SSL
32	SSL クライアント : セキュアクライアント または SSL VPN クライアント
64	IPsec (IKEv2)

¹ (1) IPsec と L2TP over IPsec は同時にはサポートされません。そのため、値 4 と 8 は相互排他値となります。

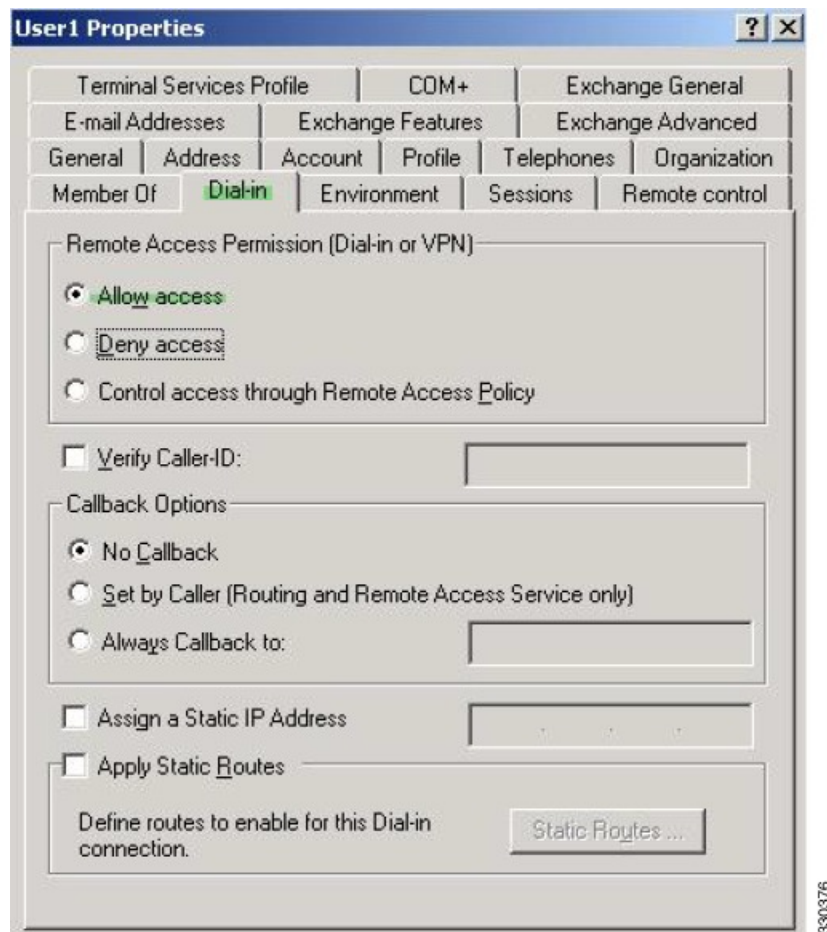
² (2) 注 1 を参照。

この属性を使用して、プロトコルの [Allow Access] (TRUE) または [Deny Access] (FALSE) の条件を作成し、ユーザーがアクセスを許可される方法を適用します。

ダイヤルイン許可アクセスまたは拒否アクセスの適用に関するその他の例については、テクニカル ノート『[ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example](#)』を参照してください。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Allow Access] オプション ボタンをクリックします。



(注)

[Control access through the Remote Access Policy] オプションを選択した場合は、サーバーから値が返されず、適用される権限は ASA の内部グループ ポリシー設定に基づいて決定されます。

ステップ 2 IPsec とセキュアクライアントの両方の接続を許可する一方で、クライアントレス SSL 接続を拒否する属性マップを作成します。

- a) マップ `tunneling_protocols` を作成します。

```
hostname(config)# ldap attribute-map tunneling_protocols
```

- b) [Allow Access] 設定で使用する AD 属性 `msNPAllowDialin` を Cisco 属性 `Tunneling-Protocols` にマッピングします。

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

- c) マップ値を追加します。

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48  
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

- a) AAA サーバー グループ `MS_LDAP` でホスト `10.1.1.2` の AAA サーバー ホスト コンフィギュレーション モードを開始します。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

- b) 作成した属性マップ `tunneling_protocols` を関連付けます。

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

ステップ 4 属性マップが設定したとおりに機能することを確認します。

クライアントレス SSL を使用して接続を試みます。ユーザーには、許可されていない接続メカニズムが接続の失敗の原因であることが通知されます。IPsec クライアントの接続は成功します。これは、属性マップに従って IPsec にトンネリング プロトコルが許可されるためです。

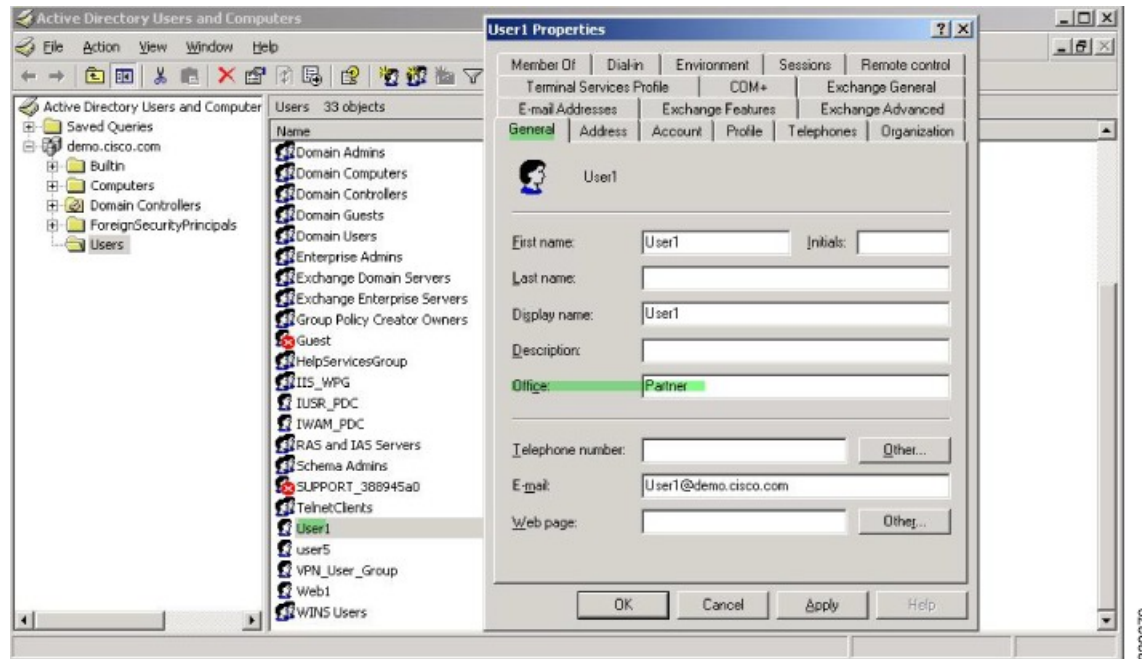
ログオン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザー（たとえばビジネス パートナー）にネットワークへのアクセスを許可する時間帯を設定して適用する方法を示します。

AD サーバー上で、[Office] フィールドを使用してパートナーの名前を入力します。このフィールドでは、`physicalDeliveryOfficeName` 属性が使用されます。次に、ASA で属性マップを作成し、その属性を Cisco 属性 `Access-Hours` にマッピングします。認証時に、ASA は `physicalDeliveryOfficeName` の値を取得して `Access-Hours` にマッピングします。

手順

ステップ 1 ユーザーを選択して、[Properties] を右クリックし、[General] タブを開きます。



ステップ 2 属性マップを作成します。

属性マップ `access_hours` を作成し、[Office] フィールドで使用する AD 属性 `physicalDeliveryOfficeName` を Cisco 属性 `Access-Hours` にマッピングします。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ `MS_LDAP` のホスト `10.1.1.2` に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、作成した属性マップ `access_hours` を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

ステップ 4 各値にサーバーで許可された時間範囲を設定します。

パートナー アクセス時間を月曜日から金曜日の午前 9 時から午後 5 時に設定します。

```
hostname(config)# time-range Partner
```

```
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

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。