



ASDM ブック 3 : Cisco ASA シリーズ VPN ASDM 7.12 コンフィギュレーションガイド

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)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

はじめに :	このマニュアルについて xix
	本書の目的 xix
	関連資料 xix
	表記法 xix
	通信、サービス、およびその他の情報 xxi

第 1 部 :	サイト間 VPN およびクライアント VPN 23
---------	----------------------------------

第 1 章	VPN ウィザード 1
	VPN の概要 1
	IPsec Site-to-Site VPN Wizard 3
	AnyConnect VPN Wizard 5
	Clientless SSL VPN Wizard 8
	IPsec IKEv1 Remote Access Wizard 9
	IPsec IKEv2 Remote Access Wizard 15

第 2 章	IKE 19
	IKE の設定 19
	IKE の有効化 19
	サイト間 VPN の IKE パラメータ 20
	IKE ポリシー 24
	IKEv1 ポリシーの追加または編集 25
	IKEv2 ポリシーの追加または編集 27
	IPsec の設定 29
	暗号マップ 31

[Create/Edit an IPsec Rule] : [Tunnel Policy (Crypto Map) - Basic] タブ	33
[Create/Edit IPsec Rule] : [Tunnel Policy (Crypto Map) - Advanced] タブ	35
[Create/Edit IPsec Rule] : [Traffic Selection] タブ	37
IPsec 事前フラグメンテーション ポリシー	40
IKEv2 フラグメンテーション オプションの設定	42
IPsec Proposals (Transform Sets)	43

第 3 章

ハイアベイラビリティ オプション	47
ハイアベイラビリティ オプション	47
EXOS シャーシ上の VPN とクラスタリング	47
VPN ロード バランシング	48
フェールオーバー	48
VPN ロード バランシング	49
VPN ロードバランシングについて	49
VPN ロードバランシングのアルゴリズム	50
VPN ロードバランシンググループ構成	50
VPN ロードバランシングについてよく寄せられる質問 (FAQ)	51
VPN ロードバランシングのライセンス	52
VPN ロードバランシングの前提条件	52
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	53
VPN ロード バランシングの設定	55
High Availability and Scalability Wizard を使用した VPN ロード バランシングの設定	55
VPN ロード バランシングの設定 (ウィザードを使用しない場合)	56

第 4 章

一般的な VPN 設定	61
システム オプション	62
最大 VPN セッション数の設定	63
DTLS の設定	64
DNS サーバグループの設定	65
暗号化コアのプールの設定	65
SSL VPN 接続用のクライアント アドレス指定	66

グループ ポリシー	68
外部グループ ポリシー	70
AAA サーバによるパスワード管理	70
内部グループ ポリシー	72
内部グループ ポリシー、一般属性	72
内部グループ ポリシーの設定、サーバ属性	76
内部グループ ポリシー、ブラウザ プロキシ	77
AnyConnect クライアントの内部グループ ポリシー	79
内部グループ ポリシー、詳細、AnyConnect クライアント	79
AnyConnect トラフィックに対するスプリット トンネリングの設定	82
ダイナミック スプリット トンネリングの設定	86
ダイナミック スプリット除外トンネリングの設定	87
ダイナミック スプリット インクルード トンネリングの設定	88
管理 VPN トンネルの設定	89
サブネットの除外をサポートするための Linux の設定	90
内部グループ ポリシー、AnyConnect クライアント属性	91
内部グループ ポリシー、AnyConnect ログイン設定	94
クライアント ファイアウォールによる VPN でのローカル デバイス サポートの有効化	95
内部グループ ポリシー、AnyConnect クライアント キーの再生成	100
内部グループ ポリシー、AnyConnect クライアント、デッドピア検出	100
内部グループ ポリシー、クライアントレス ポータルの AnyConnect カスタマイズ	101
内部グループ ポリシーの AnyConnect クライアント カスタム属性の設定	102
IPsec (IKEv1) クライアントの内部グループ ポリシー	103
内部グループ ポリシー、IPsec (IKEv1) クライアントの一般属性	103
内部グループ ポリシーの IPsec (IKEv1) クライアントのアクセスルールについて	104
内部グループ ポリシー、IPsec (IKEv1) クライアントのクライアント ファイアウォール	105
内部グループ ポリシー、IPsec (IKEv1) のハードウェア クライアント属性	108
クライアントレス SSL VPN の内部グループ ポリシー	111
内部グループ ポリシー、クライアントレス SSL VPN 一般属性	111
内部グループ ポリシー、クライアントレス SSL VPN アクセス ポータル	114

内部グループ ポリシーの設定、クライアントレス SSL VPN のポータルのカスタマイズ	116
内部グループ ポリシー、クライアントレス SSL VPN のログイン設定	116
内部グループ ポリシー、クライアントレス SSL VPN アクセス用のシングルサインオン サーバと自動サインオン サーバ	116
サイト間内部グループ ポリシー	116
ローカル ユーザの VPN ポリシー属性の設定	118
接続プロファイル	121
AnyConnect 接続プロファイル、メイン ペイン	121
デバイス証明書の指定	123
接続プロファイル、ポート設定	123
AnyConnect 接続プロファイル、基本属性	124
接続プロファイル、詳細属性	125
AnyConnect 接続プロファイル、一般属性	126
接続プロファイル、クライアント アドレス指定	127
接続プロファイル、クライアント アドレス指定、追加または編集	128
接続プロファイル、アドレス プール	129
接続プロファイル、詳細、IP プールの追加または編集	129
AnyConnect 接続プロファイル、認証属性	129
接続プロファイル、2 次認証属性	131
AnyConnect 接続プロファイル、認可属性	135
AnyConnect 接続プロファイル、認可、ユーザ名を選択するためのスクリプトの内容の 追加	136
クライアントレス SSL VPN 接続プロファイル、インターフェイスへの認可サーバ グ ループの割り当て	139
接続プロファイル、アカウントティング	139
接続プロファイル、グループエイリアスとグループ URL	139
接続プロファイル、クライアントレス SSL VPN	140
クライアントレス SSL VPN 接続プロファイル、基本属性	142
クライアントレス SSL VPN 接続プロファイル、一般属性	143
クライアントレス SSL VPN 接続プロファイル、認証	143
クライアントレス SSL VPN 接続プロファイル、認証、サーバ グループの追加	144

クライアントレス SSL VPN 接続プロファイル、2 次認証	144
クライアントレス SSL VPN 接続プロファイル、認可	144
クライアントレス SSL VPN 接続プロファイル、NetBIOS サーバ	144
クライアントレス SSL VPN 接続プロファイル、クライアントレス SSL VPN	145
IKEv1 接続プロファイル	145
IPsec リモート アクセス接続プロファイル、[Basic] タブ	146
[Add/Edit Remote Access Connections] > [Advanced] > [General]	147
IKEv1 クライアントアドレス指定	149
IKEv1 接続プロファイル、認証	149
IKEv1 接続プロファイル、認可	150
IKEv1 接続プロファイル、アカウントティング	150
IKEv1 接続プロファイル、IPsec	150
IKEv1 接続プロファイル、IPsec、IKE 認証	150
IKEv1 接続プロファイル、IPsec、クライアント ソフトウェアの更新	151
IKEv1 接続プロファイル、PPP	151
IKEv2 接続プロファイル	152
IPsec IKEv2 接続プロファイル：[Basic] タブ	152
IPsec リモート アクセス接続プロファイル：[Advanced] > [IPsec] タブ	154
IPsec または SSL VPN 接続プロファイルへの証明書のマッピング	154
証明書/接続プロファイル マップ、ポリシー	154
証明書/接続プロファイル マップのルール	155
証明書/接続プロファイル マップ、証明書照合ルール基準の追加	155
証明書照合ルール基準の追加/編集	156
Site-to-Site 接続プロファイル	158
Site-to-Site 接続プロファイル、追加または編集	159
Site-to-Site トンネル グループ	161
Site-to-Site 接続プロファイル、暗号マップ エントリ	164
CA 証明書の管理	165
Site-to-Site 接続プロファイル、証明書のインストール	166
AnyConnect VPN クライアント イメージ	166
AnyConnect VPN クライアント接続の設定	168

AnyConnect クライアント プロファイルの設定	168
AnyConnect トラフィックに対するネットワーク アドレス変換の免除	169
AnyConnect HostScan	176
HostScan の前提条件	177
AnyConnect HostScan のライセンス	177
HostScan パッケージ	177
HostScan のインストールまたはアップグレード	177
HostScan のアンインストール	179
グループ ポリシーへの AnyConnect フィーチャ モジュールの割り当て	179
HostScan の関連マニュアル	181
AnyConnect セキュア モビリティ ソリューション	181
Add or Edit MUS Access Control	183
AnyConnect のカスタマイズとローカリゼーション	183
AnyConnect のカスタマイズとローカリゼーション、リソース	184
AnyConnect のカスタマイズとローカリゼーション、バイナリとスクリプト	184
AnyConnect のカスタマイズとローカリゼーション、GUI テキストとメッセージ	185
AnyConnect のカスタマイズとローカリゼーション、カスタマイズされたインストーラ ランスフォーム	186
AnyConnect のカスタマイズとローカリゼーション、ローカライズされたインストーラ ランスフォーム	186
AnyConnect カスタム属性	186
IPsec VPN クライアント ソフトウェア	189
Zone Labs Integrity Server	189
ISE ポリシーの適用	190
ISE 許可変更の設定	191

第 5 章

VPN の IP アドレス 195

IP アドレス割り当てポリシーの設定	195
IP アドレス割り当てオプションの設定	196
アドレス割り当て方式の表示	197
ローカル IP アドレス プールの設定	197
ローカル IPv4 アドレス プールの設定	197

ローカル IPv6 アドレス プールの設定	198
グループ ポリシーへの内部アドレス プールの割り当て	199
DHCP アドレス指定の設定	200
ローカルユーザへの IP アドレスの割り当て	201

第 6 章

ダイナミック アクセス ポリシー 203

ダイナミック アクセス ポリシーについて	203
DAP によるリモート アクセス プロトコルおよびポスチャ評価ツールのサポート	204
DAP によるリモート アクセス接続のシーケンス	205
ダイナミック アクセス ポリシーのライセンス	206
ダイナミック アクセス ポリシーの設定	206
ダイナミック アクセス ポリシーの追加または編集	208
ダイナミック アクセス ポリシーのテスト	209
DAP の AAA 属性選択基準の設定	209
Active Directory グループの取得	212
AAA 属性の定義	212
DAP のエンドポイント属性選択基準の設定	213
DAP へのマルウェア対策エンドポイント属性の追加	215
DAP へのアプリケーション属性の追加	215
DAP への AnyConnect エンドポイント属性の追加	216
DAP へのファイルエンドポイント属性の追加	217
DAP へのデバイス エンドポイント属性の追加	218
DAP への NAC エンドポイント属性の追加	219
DAP へのオペレーティング システム エンドポイント属性の追加	219
DAP へのパーソナル ファイアウォール エンドポイント属性の追加	220
DAP へのポリシー エンドポイント属性の追加	220
DAP へのプロセス エンドポイント属性の追加	221
DAP へのレジストリ エンドポイント属性の追加	221
DAP への複数証明書認証属性の追加	222
DAP とマルウェア対策およびパーソナル ファイアウォール プログラム	223
エンドポイント属性の定義	223

LUA を使用した DAP における追加の DAP 選択基準の作成	228
LUA EVAL 式を作成する構文	228
HostScan 4.6 以降の LUA 手順	229
'ANY' のウイルス対策 (endpoint.am) 用 LUA スクリプト (最終更新済み)	229
'ANY' のパーソナル ファイアウォール用 LUA スクリプト	230
追加の LUA 関数	230
DAP EVAL 式の例	232
DAP アクセスと許可ポリシー属性の設定	234
DAP トレースの実行	239
DAP の例	240
DAP を使用したネットワーク リソースの定義	240
DAP を使用した WebVPN ACL の適用	241
DAP による CSD チェックの強制とポリシーの適用	241

第 7 章

電子メール プロキシ	243
電子メール プロキシの設定	244
電子メール プロキシの要件	244
AAA サーバグループの設定	244
電子メール プロキシを使用するインターフェイスの識別	246
電子メール プロキシの認証の設定	247
プロキシ サーバの識別	248
デリミタの設定	249

第 8 章

VPN の監視	251
VPN 接続グラフの監視	251
VPN 統計の監視	251

第 9 章

SSL 設定	259
SSL 設定	259

第 10 章

Easy VPN	265
-----------------	------------

Easy VPN について	265
Easy VPN リモートの設定	269
Easy VPN サーバの設定	272
Easy VPN の機能の履歴	273

第 11 章

仮想トンネル インターフェイス	275
仮想トンネル インターフェイスについて	275
仮想トンネル インターフェイスの注意事項	275
VTI トンネルの作成	277
IPsec プロポーザル (トランスフォーム セット) の追加	278
IPsec プロファイルの追加	279
VTI インターフェイスの追加	280

第 12 章

VPN の外部 AAA サーバの設定	283
外部 AAA サーバについて	283
許可属性のポリシー適用の概要	283
外部 AAA サーバを使用する際のガイドライン	284
複数証明書認証の設定	284
Active Directory/LDAP VPN リモート アクセス許可の例	285
ユーザ ベースの属性のポリシー適用	285
特定のグループ ポリシーへの LDAP ユーザの配置	287
AnyConnect トンネルのスタティック IP アドレス割り当ての適用	289
ダイヤルイン許可または拒否アクセスの適用	291
ログオン時間と Time-of-Day ルールの適用	293

第 11 部 :

クライアントレス SSL VPN	295
-------------------------	------------

第 13 章

クライアントレス SSL VPN の概要	297
クライアントレス SSL VPN の概要	297
クライアントレス SSL VPN の前提条件	298
クライアントレス SSL VPN に関する注意事項と制約事項	298

クライアントレス SSL VPN のライセンス 300

第 14 章

基本的なクライアントレス SSL VPN のコンフィギュレーション 301

各 URL の書き換え 301

クライアントレス SSL VPN アクセスの設定 302

信頼できる証明書のプール 303

HTTP サーバ検証の有効化 304

証明書のバンドルのインポート 304

trustpool のエクスポート 305

証明書の削除 305

信頼できる証明書プールのポリシーの編集 306

trustpool の更新 306

証明書のバンドルの削除 306

信頼できる証明書プールのポリシーの編集 307

Java Code Signer 307

プラグインへのブラウザ アクセスの設定 308

プラグインに伴う前提条件 309

プラグインの使用上の制限 309

プラグインのためのセキュリティ アプライアンスの準備 310

シスコによって再配布されたプラグインのインストール 310

Citrix XenApp Server へのアクセスの提供 314

Citrix プラグインの作成とインストール 314

ポート転送の設定 315

ポート転送の前提条件 316

ポート転送に関する制限事項 316

ポート転送用の DNS の設定 317

ポート転送エントリの追加と編集 320

ポート フォワーディング リストの割り当て 320

ポート フォワーディングのイネーブル化と切り替え 321

ファイル アクセスの設定 321

CIFS ファイル アクセスの要件と制限事項 322

ファイルアクセスのサポートの追加	323
SharePoint アクセスのためのクロックの正確性の確保	323
Virtual Desktop Infrastructure (VDI)	323
VDI の制限事項	323
Citrix モバイルのサポート	324
Citrix の制限	324
Citrix Mobile Receiver のユーザ ログオンについて	325
Citrix サーバをプロキシするための ASA の設定	325
VDI サーバまたは VDI プロキシサーバの設定	326
グループ ポリシーへの VDI サーバの割り当て	326
クライアント/サーバプラグインへのブラウザ アクセスの設定	327
ブラウザプラグインのインストールについて	327
ブラウザプラグインのインストールに関する要件	329
RDP プラグインのセットアップ	329
プラグインのためのセキュリティ アプライアンスの準備	330

第 15 章

高度なクライアントレス SSL VPN のコンフィギュレーション	331
Microsoft Kerberos Constrained Delegation ソリューション	331
KCD の機能	332
KCD の認証フロー	332
制約付き委任用の Kerberos サーバグループの作成	334
Kerberos Constrained Delegation (KCD) の設定	336
Kerberos Constrained Delegation の監視	337
外部プロキシサーバの使用法の設定	337
クライアントレス SSL VPN セッションでの HTTPS の使用	339
アプリケーション プロファイル カスタマイゼーション フレームワークの設定	340
APCF プロファイルの管理	341
APCF パッケージのアップロード	342
APCF パケットの管理	343
APCF 構文	344
セッションの設定	347

エンコーディング	348
文字エンコーディングの表示または指定	349
コンテンツ キャッシングの設定	350
Content Rewrite	352
リライト ルールの作成	353
コンテンツ リライト ルールの設定例	354
クライアントレス SSL VPN を介した電子メールの使用	355
Web 電子メールの設定 : MS Outlook Web App	355
ブックマークの設定	355
GET または Post メソッドによる URL のブックマークの追加	357
定義済みアプリケーションテンプレートに対する URL の追加	358
自動サインオンアプリケーションのブックマークの追加	360
ブックマーク リストのインポートおよびエクスポート	362
Import and Export GUI Customization Objects (Web Contents)	362
POST パラメータの追加および編集	363
外部ポートのカスタマイズ	369
第 16 章	ポリシー グループ 371
スマート トンネル アクセス	371
スマート トンネルについて	372
スマート トンネルの前提条件	373
スマート トンネルのガイドライン	373
スマート トンネルの設定 (Lotus の例)	375
トンネリングするアプリケーションの設定の簡略化	376
スマート トンネル アクセスに適切なアプリケーションの追加	377
スマート トンネル リストについて	381
スマート トンネル自動サインオン サーバリストの作成	381
スマート トンネル自動サインオン サーバリストへのサーバの追加	382
スマート トンネル アクセスのイネーブル化とオフへの切り替え	383
スマート トンネルからのログオフの設定	384
親プロセスが終了した場合のスマート トンネルからのログオフの設定	384

通知アイコンを使用したスマート トンネルからのログオフの設定	384
クライアントレス SSL VPN キャプチャ ツール	385
ポータル アクセス ルール の設定	385
クライアントレス SSL VPN のパフォーマンスの最適化	387
コンテンツ変換の設定	387
プロキシバイパスの使用	387

第 17 章

クライアントレス SSL VPN リモート ユーザ	389
クライアントレス SSL VPN リモート ユーザ	389
ユーザ名とパスワード	389
セキュリティ ヒントの通知	390
クライアントレス SSL VPN の機能を使用するためのリモート システムの設定	391
クライアントレス SSL VPN データのキャプチャ	400
キャプチャ ファイルの作成	401
ブラウザによるキャプチャ データの表示	401

第 18 章

クライアントレス SSL VPN ユーザ	403
パスワードの管理	403
クライアントレス SSL VPN でのシングル サインオンの使用	405
SAML 2.0 による SSO	405
SSO および SAML 2.0 について	405
SAML 2.0 に関する注意事項と制約事項	407
SAML 2.0 アイデンティティ プロバイダー (IdP) の設定	409
SAML 2.0 サービス プロバイダー (SP) としての ASA の設定	410
自動サインオンの使用	411
ユーザ名とパスワードの要件	413
セキュリティ ヒントの通知	414
クライアントレス SSL VPN の機能を使用するためのリモート システムの設定	414
クライアントレス SSL VPN について	414
クライアントレス SSL VPN の前提条件	415
クライアントレス SSL VPN フローティング ツールバーの使用	415

Web のブラウズ	416
ネットワークのブラウズ (ファイル管理)	416
Remote File Explorer の使用	417
ポート転送の使用	418
ポート転送を介した電子メールの使用	419
Web アクセスを介した電子メールの使用	420
電子メール プロキシを介した電子メールの使用	420
スマート トンネルの使用	420

第 19 章

モバイル デバイスでのクライアントレス SSL VPN 423

モバイル デバイスでのクライアントレス SSL VPN の使用	423
モバイルでのクライアントレス SSL VPN の制限	423

第 20 章

クライアントレス SSL VPN のカスタマイズ 425

クライアントレス SSL VPN ユーザ エクスペリエンスのカスタマイズ	425
Customization Editor によるログイン ページのカスタマイズ	425
独自のフル カスタマイズしたページへのログイン ページの置き換え	427
カスタム ログイン画面ファイルの作成	428
ファイルおよびイメージのインポート	430
カスタム ログイン画面を使用するセキュリティ アプライアンスの設定	430
クライアントレス SSL VPN エンド ユーザの設定	430
エンド ユーザ インターフェイスの定義	431
クライアントレス SSL VPN ホーム ページの表示	431
クライアントレス SSL VPN の [Application Access] パネルの表示	431
フローティング ツールバーの表示	431
クライアントレス SSL VPN ページのカスタマイズ	432
カスタマイゼーションについて	433
カスタマイゼーション テンプレートの編集	433
ログイン画面の高度なカスタマイゼーション	438
HTML ファイルの変更	441
ポータル ページのカスタマイズ	442

カスタム ポータル タイムアウト アラートの設定	444
カスタマイゼーションオブジェクトファイルでのカスタム タイムアウト アラートの指 定	445
ログアウト ページのカスタマイズ	446
カスタマイゼーション オブジェクトの追加	447
カスタマイゼーション オブジェクトのインポートおよびエクスポート	448
XML カスタマイゼーション ファイルの構成について	448
カスタマイゼーションの設定例	454
カスタマイゼーション テンプレートの使用	456
カスタマイゼーション テンプレート	456
ヘルプのカスタマイズ	464
シスコが提供するヘルプ ファイルのカスタマイズ	465
シスコが提供していない言語用のヘルプ ファイルの作成	467
アプリケーションのヘルプ コンテンツのインポートおよびエクスポート	467
ブックマーク ヘルプのカスタマイズ	468
言語変換について	469
変換テーブルの編集	471
変換テーブルの追加	471

第 21 章

クライアントレス SSL VPN のトラブルシューティング	473
Application Access 使用時の hosts ファイル エラーからの回復	473
Hosts ファイルの概要	474
クライアントレス SSL VPN による hosts ファイルの自動再設定	475
手動による hosts ファイルの再設定	476
WebVPN 条件付きデバッグ	477
管理者によるクライアントレス SSL VPN ユーザへのアラートの送信	478
クライアントレス SSL VPN セッション クッキーの保護	478



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](#) (xix ページ)
- [関連資料](#) (xix ページ)
- [表記法](#) (xix ページ)
- [通信、サービス、およびその他の情報](#) (xxi ページ)

本書の目的

このマニュアルは、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、適応型セキュリティ アプライアンス (ASA) に VPN を設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

このマニュアルは、Cisco 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。
[]	角カッコの中の要素は、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。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)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、[シスコ サポート](#)にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) 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

[Cisco 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 部

サイト間 VPN およびクライアント VPN

- VPN ウィザード (1 ページ)
- IKE (19 ページ)
- ハイアベイラビリティ オプション (47 ページ)
- 一般的な VPN 設定 (61 ページ)
- VPN の IP アドレス (195 ページ)
- ダイナミック アクセス ポリシー (203 ページ)
- 電子メール プロキシ (243 ページ)
- VPN の監視 (251 ページ)
- SSL 設定 (259 ページ)
- Easy VPN (265 ページ)
- 仮想トンネル インターフェイス (275 ページ)
- VPN の外部 AAA サーバの設定 (283 ページ)



第 1 章

VPN ウィザード

- [VPN の概要](#) (1 ページ)
- [IPsec Site-to-Site VPN Wizard](#) (3 ページ)
- [AnyConnect VPN Wizard](#) (5 ページ)
- [Clientless SSL VPN Wizard](#) (8 ページ)
- [IPsec IKEv1 Remote Access Wizard](#) (9 ページ)
- [IPsec IKEv2 Remote Access Wizard](#) (15 ページ)

VPN の概要

ASA は、ユーザがプライベート接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、バーチャルプライベート ネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

セキュアな接続はトンネルと呼ばれ、ASA はトンネリングプロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを介したパケットの送受信、パケットのカプセル化解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーンパケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

VPN ウィザードを使用すると、基本的な LAN-to-LAN とリモートアクセス VPN 接続を設定して、事前共有キーまたはデジタル証明書を認証用に割り当てることができます。ASDM を使用して拡張機能を編集および設定してください。

ここでは、次の 4 つの VPN ウィザードについて説明します。

- [Clientless SSL VPN Wizard](#) (8 ページ)

ASA クライアントレス SSL VPN は、ほぼすべてのインターネット対応環境から Web ブラウザとそのネイティブ SSL 暗号化機能だけを使用して、Secure Socket Layer (SSL) リモートアクセス接続できるようにします。このブラウザベースの VPN により、適応型セキュリティアプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。

認証されると、ユーザにはポータルページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザにリソースへのアクセス権限を付与します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

• AnyConnect VPN Wizard (5 ページ)

Cisco AnyConnect VPN クライアントは ASA へのセキュアな SSL 接続または IPsec (IKEv2) 接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN トンネリングが可能になります。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 ユーザは、クライアントレス VPN 接続を受け入れるように設定された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 は、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロードが完了すると、クライアントが自動的にインストールされて設定され、セキュアな接続が確立されます。接続が終了すると、ASA の設定に応じて、クライアントはそのまま残るか、またはアンインストールされます。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。

AnyConnect VPN ウィザードは、ASA がマルチコンテキスト モードのときにユーザ コンテキストのみで利用可能になります。必要なコンテキストのストレージとリソースクラスは、システム コンテキストから設定する必要があります。

Cisco AnyConnect パッケージとプロファイルファイルを使用するには、コンテキストごとのストレージが必要です。各コンテキストのライセンスの割り当てには、リソースクラスが必要です。使用するライセンスは、AnyConnect Premium です。



(注) このウィザードの残りの設定は、シングルコンテキストの場合と同じです。

• IPsec IKEv2 Remote Access Wizard (15 ページ)

IKEv2 によって、他のベンダーの VPN クライアントが ASA に接続できます。これにより、セキュリティが強化されるとともに、国や地方自治体が規定している IPsec リモートアクセス要件を満たすことができます。

IPsec IKEv2 リモートアクセス ウィザードは、ASA がマルチコンテキスト モードのときにユーザ コンテキストのみで利用可能になります。必要なコンテキストのリソースクラスは、ライセンス割り当て用のシステムコンテキストから設定する必要があります。使用するライセンスは、AnyConnect Premium です。



(注) このウィザードの残りの設定は、シングルコンテキストの場合と同じです。

- [IPsec IKEv1 Remote Access Wizard \(9 ページ\)](#)
- [IPsec Site-to-Site VPN Wizard \(3 ページ\)](#)

LAN-to-LAN 接続で IPv4 と IPv6 の両方のアドレッシングが使用されている場合、ASA で VPN トンネルがサポートされるのは、両方のピアが ASA であり、かつ両方の内部ネットワークのアドレッシング方式が一致している（両方とも IPv4 または IPv6）ときです。これは、両方のピアの内部ネットワークが IPv6 で外部ネットワークが IPv6 の場合にも当てはまります。

IPsec Site-to-Site VPN Wizard

2 台の ASA デバイス間のトンネルは「サイトツーサイト トンネル」と呼ばれ、双方向です。サイトツーサイト VPN トンネルでは、IPsec プロトコルを使用してデータが保護されます。

Peer Device Identification

- [Peer IP Address] : 他のサイト（ピア デバイス）の IP アドレスを設定します。
- [VPN Access Interface] : サイトツーサイト トンネルに使用するインターフェイスを選択します。
- [Crypto Map Type] : このピアに使用されるマップのタイプ（スタティックまたはダイナミック）を指定します。

Traffic to Protects

このステップでは、ローカル ネットワークおよびリモート ネットワークを指定します。これらのネットワークでは、IPsec 暗号化を使用してトラフィックが保護されます。

- [Local Networks] : IPsec トンネルで使用されるホストを指定します。
- [Remote Networks] : IPsec トンネルで使用されるネットワークを指定します。

セキュリティ

このステップでは、ピアデバイスとの認証の方法を設定します。単純な設定を選択するか、事前共有キーを指定できます。またさらに詳細なオプションについては、以下に説明する [Customized Configuration] を選択できます。

- [IKE Version] : どちらのバージョンを使用するかに応じて、[IKEv1] または [IKEv2] チェックボックスをオンにします。
- IKE version 1 Authentication Methods
 - [Pre-shared Key] : 事前共有キーを使用すると、リモートピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション

ン情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモートサイトの管理者と事前共有キーを交換してください。

- [Device Certificate] : ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。

デジタル証明書による IPSec トンネルの確立に使用するセキュリティキーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

2つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

- IKE version 2 Authentication Methods

- [Local Pre-shared Key] : IPsec IKEv2 認証方式と暗号化アルゴリズムを指定します。
- [Local Device Certificate] : VPN アクセスの認証を、セキュリティアプライアンスを通して行います。
- [Remote Peer Pre-shared Key] : ローカル ASA とリモート IPsec ピア間の認証で事前共有キーを使用する場合にクリックします。
- [Remote Peer Certificate Authentication] : このチェックボックスがオンのときは、ピアデバイスが証明書を使用してこのデバイスに対して自身の認証を行うことができます。

- [Encryption Algorithms] : このタブでは、データの保護に使用する暗号化アルゴリズムのタイプを選択します。

- [IKE Policy] : IKEv1/IKEv2 認証方式を指定します。
- [IPsec Proposal] : IPsec 暗号化アルゴリズムを指定します。

- Perfect Forward Secrecy

- [Enable Perfect Forwarding Secrecy (PFS)] : フェーズ 2 IPsec キーの生成において、Perfect Forward Secrecy を使用するかどうか、および使用する番号のサイズを指定します。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

PFS は、接続の両側でイネーブルにする必要があります。

- [Diffie-Hellman Group] : Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトの Group 2 (1024 ビット Diffie-Hellman) は、Group 5 (1536 ビット) と比較して、CPU の実行時間は短いですが、安全性は低くなります。

NAT Exempt

- [Exempt ASA side host/network from address translation] : ドロップダウンリストを使用して、アドレス変換から除外するホストまたはネットワークを選択します。

AnyConnect VPN Wizard

このウィザードは、AnyConnect VPN クライアントからの VPN 接続を受け入れるように ASA を設定するときに使用します。このウィザードでは、フル ネットワーク アクセスができるように IPsec (IKEv2) プロトコルまたは SSL VPN プロトコルを設定します。VPN 接続が確立したときに、ASA によって自動的に AnyConnect VPN クライアントがエンド ユーザのデバイスにアップロードされます。

Connection Profile Identification

[Connection Profile Identification] では、リモート アクセス ユーザに対する ASA を指定します。

- [Connection Profile Name] : リモート アクセス ユーザが VPN 接続のためにアクセスする名前を指定します。
- [VPN Access Interface] : リモート アクセス ユーザが VPN 接続のためにアクセスするインターフェイスを選択します。

VPN Protocols

この接続プロファイルに対して許可する VPN プロトコルを指定します。

AnyConnect クライアントのデフォルトは SSL です。接続プロファイルの VPN トンネル プロトコルとして IPsec をイネーブルにした場合は、IPsec をイネーブルにしたクライアント プロファイルを作成して展開することも必要になります (作成するには、ASDM のプロファイル エディタを使用します)。

WebLaunch の代わりに AnyConnect クライアントを事前展開する場合は、最初のクライアント接続に SSL を使用し、セッション中に ASA からクライアント プロファイルを受け取ります。以降の接続では、クライアントはそのプロファイルで指定されたプロトコル (SSL または IPsec) を使用します。IPsec が指定されたプロファイルをクライアントとともに事前展開した場合は、最初のクライアント接続で IPsec が使用されます。IPsec をイネーブルにした状態のクライアント プロファイルを事前展開する方法の詳細については、『*AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。

- SSL
- IPsec (IKE v2)
- [Device Certificate] : リモート アクセス クライアントに対する ASA を指定します。AnyConnect の機能の中には、Always on や IPsec/IKEv2 のように、有効なデバイス証明書が ASA に存在することを要件とするものがあります。
- [Manage] : [Manage] を選択すると [Manage Identity Certificates] ウィンドウが開きます。
 - [Add] : ID 証明書とその詳細情報を追加するには、[Add] を選択します。
 - [Show Details] : 特定の証明書を選択して [Show Details] をクリックすると、[Certificate Details] ウィンドウが開き、その証明書の発行対象者と発行者が表示されるほか、シリアル番号、使用方法、対応するトラストポイント、有効期間などが表示されます。
 - [Delete] : 削除する証明書を強調表示して [Delete] をクリックします。
 - [Export] : 証明書を強調表示して [Export] をクリックすると、その証明書をファイルにエクスポートできます。このときに、暗号化パスフレーズを付けるかどうかを指定できます。
 - [Enroll ASA SSL VPN with Entrust] : Entrust からの SSL Advantage デジタル証明書を使用すると、すぐに Cisco ASA SSL VPN アプライアンスの稼働を開始できます。

Client Images

ASA は、クライアントデバイスがエンタープライズ ネットワークにアクセスするときに、最新の AnyConnect パッケージをそのデバイスに自動的にアップロードすることができます。ブラウザのユーザ エージェントとイメージとの対応を、正規表現を使用して指定できます。また、接続の設定に要する時間を最小限にするために、最もよく使用されるオペレーティングシステムをリストの先頭に移動できます。

認証方法

この画面では、認証情報を指定します。

- [AAA server group] : ASA がリモート AAA サーバグループにアクセスしてユーザを認証できるようにします。AAA サーバグループを、事前設定されたグループのリストから選択するか、[New] をクリックして新しいグループを作成します。
- [Local User Database Details] : ASA に格納されているローカル データベースに新しいユーザを追加します。
 - [Username] : ユーザのユーザ名を作成します。
 - [Password] : ユーザのパスワードを作成します。
 - [Confirm Password] : 確認のために同じパスワードを再入力します。
 - [Add/Delete] : ローカル データベースにユーザを追加またはデータベースから削除します。

Client Address Assignment

リモート AnyConnect ユーザのための IP アドレス範囲を指定します。

- [IPv4 Address Pools] : SSL VPN クライアントは、ASA に接続したときに新しい IP アドレスを受け取ります。クライアントレス接続では新しい IP アドレスは不要です。アドレスプールでは、リモート クライアントが受け取ることができるアドレス範囲が定義されます。既存の IP アドレスプールを選択するか、[New] をクリックして新しいプールを作成します。

[New] を選択した場合は、開始と終了の IP アドレスおよびサブネット マスクを指定する必要があります。

- [IPv6 Address Pool] : 既存の IP アドレスプールを選択するか、[New] をクリックして新しいプールを作成します。



(注) IPv6 アドレスプールは、IKEv2 接続プロファイル用には作成できません。

Network Name Resolution Servers

リモートユーザが内部ネットワークにアクセスするときにどのドメイン名を解決するかを指定します。

- [DNS Servers] : DNS サーバの IP アドレスを入力します。
- [WINS Servers] : WINS サーバの IP アドレスを入力します。
- [Domain Name] : デフォルトのドメイン名を入力します。

NAT Exempt

ASA 上でネットワーク変換がイネーブルに設定されている場合は、VPN トラフィックに対してこの変換を免除する必要があります。

AnyConnect Client Deployment

次の 2 つの方法のいずれかを使用して、AnyConnect クライアントプログラムをクライアントデバイスにインストールできます。

- [WebLaunch] : AnyConnect クライアント パッケージは、Web ブラウザを使用して ASA にアクセスしたときに自動的にインストールされます。



(注) Web launch はマルチ コンテキスト モードではサポートされません。

- [Pre-deployment] : 手動で AnyConnect クライアント パッケージをインストールします。

[Allow Web Launch] は、すべての接続に影響が及ぶグローバル設定です。このチェックボックスがオフ（許可しない）の場合は、AnyConnect SSL 接続とクライアントレス SSL 接続は機能しません。

事前展開の場合は、disk0:/test2_client_profile.xml プロファイルバンドルの中に .msi ファイルがあり、このクライアント プロファイルを ASA から AnyConnect パッケージに入れておく必要があります。これは、IPsec 接続を期待したとおりに確実に動作させるためです。

Clientless SSL VPN Wizard

このウィザードでは、サポートされる特定の内部リソースに対する、ポータルページからのクライアントレス ブラウザ ベース接続をイネーブルにします。

SSL VPN Interface

接続プロファイルと、SSL VPN ユーザの接続先となるインターフェイスを指定します。

- [Connection Profile Name] : 接続プロファイルの名前を指定します。
- [SSL VPN Interface] : SSL VPN 接続のためにユーザがアクセスするインターフェイスです。
- [Digital Certificate] : ASA の認証のために ASA からリモート Web ブラウザに送信するものを指定します。
 - [Certificate] : ドロップダウン リストから選択します。
- Accessing the Connection Profile
 - [Connection Group Alias/URL] : グループエイリアスはログイン時に [Group] ドロップダウン リストから選択されます。この URL が Web ブラウザに入力されます。
 - [Display Group Alias list at the login page] : ログイン ページにグループエイリアスのリストを表示する場合にオンにします。

User Authentication

このペインでは、認証情報を指定します。

- [Authenticate using a AAA server group] : ASA がリモート AAA サーバグループにアクセスしてユーザを認証できるようにします。
 - [AAA Server Group Name] : 事前設定されたグループのリストから AAA サーバグループを選択するか、[New] をクリックして新しいグループを作成します。
- [Authenticate using the local user database] : ASA に保存されているローカル データベースに新しいユーザを追加します。
 - [Username] : ユーザのユーザ名を作成します。

- [Password] : ユーザのパスワードを作成します。
- [Confirm Password] : 確認のために同じパスワードを再入力します。
- [Add/Delete] : ローカル データベースにユーザを追加またはデータベースから削除します。

Group Policy

グループ ポリシーによって、ユーザ グループの共通属性を設定します。新しいグループ ポリシーを作成するか、または既存のポリシーを選択して修正します。

- [Create new group policy] : 新しいグループ ポリシーを作成できます。新しいポリシーの名前を入力します。
- [Modify existing group policy] : 修正する既存のグループ ポリシーを選択します。

Bookmark List

グループ イン트라ネット Web サイトのリストを設定します。これらのサイトは、ポータル ページにリンクとして表示されます。例としては、<https://intranet.acme.com>、<rdp://10.120.1.2>、<vnc://100.1.1.1> などがあります。

- [Bookmark List] : ドロップダウン リストから選択します。
- [Manage] : [Configure GUI Customization Object] ダイアログボックスを開く場合にクリックします。

IPsec IKEv1 Remote Access Wizard



- (注) Cisco VPN Client は耐用年数末期で、サポートが終了しています。AnyConnect セキュア モバイル クライアントにアップグレードする必要があります。

IPsec IKEv1 Remote Access Wizard を使用して、モバイル ユーザなどの VPN クライアントに安全なリモート アクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

- [VPN Tunnel Interface] : リモート アクセス クライアントで使用するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを実行する前に ASA でインターフェイスを設定します。
- [Enable inbound IPsec sessions to bypass interface access lists] : IPsec 認証済みの着信セッションを ASA によって常に許可するようにします (つまり、インターフェイスの access-list 文をチェックしないようにします)。着信セッションがバイパスするのは、インターフェイス ACL だけです。設定されたグループ ポリシー、ユーザ、およびダウンロードされた ACL は適用されます。

リモート アクセス クライアント

さまざまなタイプのリモート アクセス ユーザが、この ASA への VPN トンネルを開くことができます。このトンネルの VPN クライアントのタイプを選択します。

• VPN Client Type

- [Easy VPN Remote product]

- [Microsoft Windows client using L2TP over IPsec] : PPP 認証プロトコルを指定します。選択肢は、PAP、CHAP、MS-CHAP-V1、MS-CHAP-V2、および EAP-PROXY です。

[PAP] : 認証中にクリアテキストのユーザ名とパスワードを渡すので、安全ではありません。

[CHAP] : サーバ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。

[MS-CHAP, Version 1] : CHAP と似ていますが、サーバは、CHAP のようなクリアテキストのパスワードではなく、暗号化したパスワードだけを保存および比較するので安全です。

[MS-CHAP, Version 2] : MS-CHAP, Version 1 以上のセキュリティ強化機能が含まれています。

[EAP-Proxy] : EAP をイネーブルにします。これによって ASA は、PPP 認証プロセスを外部の RADIUS 認証サーバに代行させることができます。

リモートクライアントでプロトコルが指定されていない場合は、指定しないでください。

- 指定するのは、クライアントからトンネルグループ名が `username@tunnelgroup` として送信される場合です。

VPN クライアント認証方式とトンネルグループ名

認証方式を設定し、接続ポリシー（トンネルグループ）を作成するには、[VPN Client Authentication Method and Name] ペインを使用します。

- [Authentication Method] : リモートサイトピアは、事前共有キーか証明書のいずれかを使用して認証します。
- [Pre-shared Key] : ローカル ASA とリモート IPsec ピア間の認証で事前共有キーを使用する場合にクリックします。

事前共有キーを使用すると、リモートピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモートサイトの管理者と事前共有キーを交換してください。

- [Pre-shared Key] : 1~128 文字の英数字文字列を入力します。
- [Certificate] : ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、事前に CA に登録し、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

デジタル証明書による IPsec トンネルの確立に使用するセキュリティキーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

デジタル証明書を使用するには、デジタル証明書を発行する認証局 (CA) に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

[Certificate Signing Algorithm] : デジタル証明書署名アルゴリズムを表示します (RSA の場合は rsa-sig) 。

- [Tunnel Group Name] : 名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウントティングサーバ、デフォルトグループポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーは、認証方式を指定し、ASA のデフォルトのグループポリシーを使用します。

クライアント認証

[Client Authentication] ペインでは、ASA がリモートユーザを認証するときに使用する方法を選択します。次のオプションのいずれかを選択します。

- [Authenticate using the local user database] : ASA の内部の認証方式を使用する場合にクリックします。この方式は、ユーザの数が少なく安定している環境で使用します。次のペインでは、ASA に個々のユーザのアカウントを作成できます。
- [Authenticate using an AAA server group] : リモート ユーザ認証で外部サーバグループを使用する場合にクリックします。
 - [AAA Server Group Name] : 先に構成された AAA サーバグループを選択します。
 - [New ...] : 新しい AAA サーバグループを設定する場合にクリックします。

User Accounts

[User Accounts] ペインでは、認証を目的として、ASA の内部ユーザデータベースに新しいユーザを追加します。

Address Pool

[Address Pool] ペインでは、ASA がリモート VPN クライアントに割り当てるローカル IP アドレスのプールを設定します。

- [Tunnel Group Name] : このアドレス プールが適用される接続プロファイル (トンネルグループ) の名前が表示されます。この名前は、[VPN Client Name and Authentication Method] ペイン (ステップ 3) で設定したものです。
- [Pool Name] : アドレス プールの記述 ID を選択します。
- [New...] : 新しいアドレス プールを設定します。
- [Range Start Address] : アドレス プールの開始 IP アドレスを入力します。
- [Range End Address] : アドレス プールの終了 IP アドレスを入力します。
- [Subnet Mask] : (任意) これらの IP アドレスのサブネット マスクを選択します。

Attributes Pushed to Client (任意)

[Attributes Pushed to Client (Optional)] ペインでは、DNS サーバと WINS サーバに関する情報およびデフォルト ドメイン名をリモート アクセスクライアントに渡すように、ASA を設定します。

- [Tunnel Group] : アドレス プールが適用される接続ポリシーの名前を表示します。この名前は、[VPN Client Name and Authentication Method] ペインで設定したものです。
- [Primary DNS Server] : プライマリ DNS サーバの IP アドレスを入力します。
- [Secondary DNS Server] : セカンダリ DNS サーバの IP アドレスを入力します。
- [Primary WINS Server] : プライマリ WINS サーバの IP アドレスを入力します。
- [Secondary WINS Server] : セカンダリ WINS サーバの IP アドレスを入力します。
- [Default Domain Name] : デフォルトのドメイン名を入力します。

IKE Policy

Internet Security Association and Key Management Protocol (ISAKMP) と呼ばれる IKE は、2 台のホストで 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 IKE 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 IKE 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 Policy] ペインでは、フェーズ 1 IKE ネゴシエーションの条件を設定します。この条件には、データを保護し、プライバシーを守る暗号化方式、ピアの ID を確認する認証方式、およ

び暗号キー判別アルゴリズムを強化する Diffie-Hellman グループが含まれます。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。

- [Encryption] : フェーズ 2 ネゴシエーションを保護するフェーズ 1 SA を確立するために ASA が使用する、対称暗号化アルゴリズムを選択します。ASA は、次の暗号化アルゴリズムをサポートしています。

アルゴリズム	説明
DES	データ暗号規格。56 ビット キーを使用します。
3DES	Triple DES。56 ビット キーを使用して暗号化を 3 回実行します。
AES-128	高度暗号化規格。128 ビット キーを使用します。
aes-192	192 ビット キーを使用する AES。
AES-256	256 ビット キーを使用する AES。

デフォルトの 3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。同様に、AES オプションによるセキュリティは強力ですが、必要な処理量も増大します。

- [Authentication] : 認証や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選択します。デフォルトは SHA です。MD5 のダイジェストは小さく、SHA よりもわずかに速いとされています。MD5 は、(きわめて困難ですが) 攻撃により破れることが実証されています。しかし、ASA で使用される Keyed-Hash Message Authentication Code (HMAC) バージョンはこの攻撃を防ぎます。
- [Diffie-Hellman Group] : Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトの Group 2 (1024 ビット Diffie-Hellman) は、Group 5 (1536 ビット) と比較して、CPU の実行時間は短いですが、安全性は低くなります。

IPsec Settings (任意)

[IPsec Settings (Optional)] ペインでは、アドレス変換が不要なローカル ホスト/ネットワークを指定します。デフォルトでは、ASA は、ダイナミックまたはスタティックなネットワーク アドレス変換 (NAT) を使用して、内部のホストおよびネットワークの実 IP アドレスを外部ホストから隠します。NAT は、信頼できない外部ホストによる攻撃の危険性を最小限に抑えますが、VPN によって認証および保護されているホストに対しては不適切な場合があります。

たとえば、ダイナミック NAT を使用する内部ホストは、プールから無作為に選択したアドレスと照合することにより、その IP アドレスを変換させます。外部ホストからは、変換されたアドレスだけが見えるようになります。本当の IP アドレスにデータを送信することによって

これらの内部ホストに到達しようとするリモート VPN クライアントは、NAT 免除ルールを設定しない限り、これらのホストには接続できません。



(注) すべてのホストとネットワークを NAT から免除する場合は、このペインでは何も設定しません。エントリが1つでも存在すると、他のすべてのホストとネットワークはNATに従います。

- **[Interface]** : 選択したホストまたはネットワークに接続するインターフェイスの名前を選択します。
- **[Exempt Networks]** : 選択したインターフェイス ネットワークから免除するホストまたはネットワークの IP アドレスを選択します。
- **[Enable split tunneling]** : リモートアクセスクライアントからのパブリックインターネット宛のトラフィックを暗号化せずに送信する場合に選択します。スプリットトンネリングにより、保護されたネットワークのトラフィックが暗号化され、保護されていないネットワークのトラフィックは暗号化されません。スプリットトンネリングをイネーブルにすると、ASA は、認証後に IP アドレスのリストをリモート VPN クライアントにプッシュします。リモート VPN クライアントは、ASA の背後にある IP アドレスへのトラフィックを暗号化します。他のすべてのトラフィックは暗号化されずに直接インターネットに送り出され、ASA は関与しません。
- **[Enable Perfect Forwarding Secrecy (PFS)]** : フェーズ 2 IPsec キーの生成において、Perfect Forward Secrecy を使用するかどうか、および使用する番号のサイズを指定します。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでは、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

PFS は、接続の両側でイネーブルにする必要があります。

- **[Diffie-Hellman Group]** : Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトの Group 2 (1024 ビット Diffie-Hellman) は、Group 5 (1536 ビット) と比較して、CPU の実行時間は短いですが、安全性は低くなります。

Summary

設定に問題なければ、**[Finish]** をクリックします。ASDM によって LAN-to-LAN のコンフィギュレーションが保存されます。**[Finish]** をクリックした後は、この VPN ウィザードを使用してこのコンフィギュレーションを変更することはできません。ASDM を使用して拡張機能を編集および設定してください。

IPsec IKEv2 Remote Access Wizard

IPsec IKEv2 Remote Access Wizard を使用して、モバイル ユーザなどの VPN クライアントに安全なリモートアクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

Connection Profile Identification

[Connection Profile Name] に接続プロファイルの名前を入力し、[VPN Access Interface] で IPsec IKEv2 リモートアクセスに使用する VPN アクセス インターフェイスを選択します。

- [Connection Profile Name] : 名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウントिंगサーバ、デフォルトグループポリシー、およびIKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーは、認証方式を指定し、ASA のデフォルトのグループポリシーを使用します。
- [VPN Access Interface] : リモート IPsec ピアとのセキュアなトンネルを確立するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを実行する前に VPN コンフィギュレーションを計画し、セキュアな接続を確立する予定のリモート IPsec ピアごとに、使用するインターフェイスを特定しておく必要があります。

標準規格に基づく IPsec (IKEv2) 認証ページ

[IKE Peer Authentication] : リモート サイト ピアは、事前共有キー、証明書、または EAP を使用したピア認証のいずれかを使用して認証します。

- [Pre-shared Key] : 1~128 文字の英数字文字列を入力します。

事前共有キーを使用すると、リモートピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモートサイトの管理者と事前共有キーを交換してください。

- [Enable Certificate Authentication] : オンにすると、認証に証明書を使用できます。
- [Enable peer authentication using EAP] : オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
- [Send an EAP identity request to the client] : リモートアクセス VPN クライアントに EAP 認証要求を送信できます。

Mobike RRC

- [Enable Return Routability Check for mobike] : Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレスの変更をチェックする Return Routability を有効にします。

[IKE Local Authentication]

- ローカル認証をイネーブルにして、事前共有キーまたは証明書のいずれかを選択します。
 - [Preshared Key] : 1 ~ 128 文字の英数字文字列を入力します。
 - [Certificate] : ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、事前に CA に登録し、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

デジタル証明書による IPsec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

デジタル証明書を使用するには、デジタル証明書を発行する認証局 (CA) に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

認証方法

IPsec IKEv2 リモート アクセスでは RADIUS 認証のみがサポートされています。

- [AAA Server Group] : 先に構成された AAA サーバグループを選択します。
- [New] : 新しい AAA サーバグループを設定する場合にクリックします。
- [AAA Server Group Details] : この領域を使用して、AAA サーバグループを必要に応じて変更します。

Client Address Assignment

IPv4 および IPv6 のアドレス プールを作成するか、選択します。リモート アクセス クライアントには、IPv4 または IPv6 のプールのアドレスが割り当てられます。両方を設定した場合は、IPv4 アドレスが優先されます。詳細については、「ローカル IP アドレス プールの設定」を参照してください。

Network Name Resolution Servers

リモートユーザが内部ネットワークにアクセスするときどのようにドメイン名を解決するかを指定します。

- [DNS Servers] : DNS サーバの IP アドレスを入力します。

- [WINS Servers] : WINS サーバの IP アドレスを入力します。
- [Default Domain Name] : デフォルトのドメイン名を入力します。

NAT Exempt

- [Exempt VPN traffic from Network Address Translation] : ASA で NAT がイネーブルになっている場合は、このチェックボックスをオンにする必要があります。



第 2 章

IKE

- [IKE の設定 \(19 ページ\)](#)
- [IPsec の設定 \(29 ページ\)](#)

IKE の設定

IKE は ISAKMP と呼ばれ、2 台のホストで 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。バーチャルプライベートネットワーク用に ASA を設定するには、システム全体に適用するグローバル IKE パラメータを設定し、さらに、VPN 接続を確立するためにピアがネゴシエートする IKE ポリシーも作成します。

手順

- ステップ 1 [IKE の有効化 \(19 ページ\)](#) を使用して無効にすることができます。
 - ステップ 2 [サイト間 VPN の IKE パラメータ \(20 ページ\)](#) を設定します。
 - ステップ 3 [IKE ポリシー \(24 ページ\)](#) を設定します。
-

IKE の有効化

手順

- ステップ 1 VPN 接続に対して IKE を有効にする方法
 - a) ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。
 - b) [Access Interfaces] 領域で、IKE を使用するインターフェイスに対して、[IPsec (IKEv2) Access] の下にある [Allow Access] をオンにします。
- ステップ 2 サイト間 VPN に対して IKE を有効にする方法

- a) ASDM で、[Configuration] > [Site-to-Site VPN] > [Connection Profiles] を選択します。
- b) IKEv1 および IKEv2 を使用するインターフェイスを選択します。

サイト間 VPN の IKE パラメータ

ASDM で、[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Parameters] を選択します。

NAT の透過性

- [Enable IPsec over NAT-T]

IPsec over NAT-T により IPsec ピアは、リモートアクセスと LAN-to-LAN の両方の接続を NAT デバイスを介して確立できます。NAT-T は UDP データグラムの IPsec トラフィックをカプセル化し、ポート 4500 を使用して、NAT デバイスにポート情報を提供します。NAT-T はすべての 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。この機能は、デフォルトでイネーブルにされています。

- 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。
- NAT-T と IPsec over UDP の両方がイネーブルになっている場合、NAT-T が優先されます。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

ASA による NAT-T の実装では、次の場合において、単一の NAT/PAT デバイスの背後にある IPsec ピアをサポートします。

- LAN-to-LAN 接続。
- LAN-to-LAN 接続または複数のリモートアクセスクライアントのいずれか。ただし、両方を混在させることはできません。

NAT-T を使用するには、次の手順を実行する必要があります。

- ポート 4500 を開くために使用するインターフェイスの ACL を作成します ([Configuration] > [Firewall] > [Access Rules]) 。
- このペインで、IPsec over NAT-T をイネーブルにします。
- [Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Prefragmentation Policies] ペインの [Fragmentation Policy] パラメータで、[Enable IPsec Pre-fragmentation] で使用するインターフェイスを編集します。これが設定されている場合、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移動できます。これによって、IP フラグメンテーションをサポートする NAT デバイスの動作が妨げられることはありません。

• Enable IPsec over TCP

IPsec over TCP を使用すると、標準 ESP や標準 IKE が機能できない環境、または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、VPN クライアントが動作可能になります。IPsec over TCP は TCP パケット内で IKE プロトコルと IPsec プロトコルをカプセル化し、NAT と PAT の両方のデバイスおよびファイアウォールにより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。



(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。また、すべての物理インターフェイスと VLAN インターフェイスでも動作します。これは、ASA 機能に対応しているクライアントに限られます。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。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

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。

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) などのウェルノウン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機能しなくなることを示す警告がシステムに表示されます。その結果、ブラウザを使用して IKE 対応インターフェイスから ASA を管理できなくなります。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。

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。

ピアに送信される ID

IKE ネゴシエーションでピアが相互に相手を識別する [Identity] を選択します。

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。
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	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 [Key Id String] を指定します。

<p>Automatic</p>	<p>接続タイプによって IKE ネゴシエーションを決定します。</p> <ul style="list-style-type: none"> • 事前共有キーの IP アドレス • 証明書認証の cert DN。
-------------------------	---

セッション制御

- [Disable Inbound Aggressive Mode Connections]

フェーズ 1 の IKE ネゴシエーションでは、Main モードと Aggressive モードのいずれかを使用できます。どちらのモードも同じサービスを提供しますが、Aggressive モードの場合にピア間で必要とされる交換処理は、3つではなく2つだけです。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。そのため、情報を暗号化するセキュアな 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。この機能はデフォルトで無効に設定されています。

- [Alert Peers Before Disconnecting]

- ASA のシャットダウンやリブート、セッションアイドルタイムアウト、最大接続時間の超過、管理者による停止など、いくつかの理由でクライアントセッションまたは LAN-to-LAN セッションがドロップされることがあります。
- ASA は、切断される直前のセッションについて（LAN 間設定内の）限定されたピアに通知し、それらに理由を伝達します。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。
- このペインでは、ASA がそれらのアラートを送信して接続解除の理由を伝えることができるように、通知機能をイネーブルにできます。

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
- バージョン 4.0 以降のソフトウェアを実行している VPN クライアント（設定は不要）

- [Wait for All Active Sessions to Voluntarily Terminate Before Rebooting]

すべてのアクティブセッションが自動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。

- [Number of SAs Allowed in Negotiation for IKEv1]

一時点でのネゴシエーション中 SA の総数を制限します。

IKE v2 特有の設定

追加のセッション制御は、オープン SA の数を制限する IKE v2 で使用できます。デフォルトでは、ASA はオープン SA の数を制限しません。

- **[Cookie Challenge]** : SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
 - **[% threshold before incoming SAs are cookie challenged]** : ASA に対して許容される合計 SA のうち、ネゴシエーション中の SA の割合。この数値に達すると、以降の SA ネゴシエーションに対してクッキー チャレンジが行われます。範囲は 0 ~ 100% です。デフォルトは 50% です。
- **[Number of Allowed SAs in Negotiation]** : 一時点でのネゴシエーション中 SA の総数を制限します。クッキー チャレンジと併用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこの制限よりも低くしてください。
- **[Maximum Number of SAs Allowed]** : ASA 上で許可される IKEv2 接続の数を制限します。デフォルトでは、ライセンスで指定されている最大接続数が上限です。
- **[Notify Invalid Selector]** : SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合に、管理者はピアへの IKE 通知の送信を有効または無効にできます。この通知の送信はデフォルトでは、無効になっています。

IKE v2 特有の設定による DoS 攻撃の防止

着信セキュリティ アソシエーション (SA) 識別のチャレンジを行うクッキー チャレンジを設定するか、オープンな SA の数を制限することにより、IPsec IKEv2 接続に対するサービス拒否 (DoS) 攻撃を防止できます。デフォルトでは、ASA はオープンな SA の数を制限せず、SA のクッキー チャレンジを行うこともありません。許可される SA の数を制限することもできます。これによって、それ以降は接続のネゴシエーションが行われなくなるため、クッキー チャレンジ機能では阻止できず現在の接続を保護できない可能性がある、メモリや CPU への攻撃を防止できます。

DoS 攻撃では、攻撃者は、ピア デバイスが SA 初期パケットを送信し、ASA がその応答を送信すると攻撃を開始しますが、ピア デバイスはこれ以上応答しません。ピア デバイスがこれを継続的に行うと、応答を停止するまで ASA で許可されるすべての SA 要求を使用できます。

クッキー チャレンジのしきい値 (%) をイネーブルにすると、オープン SA ネゴシエーションの数が制限されます。たとえば、デフォルト設定の 50% では、許可される SA の 50% がネゴシエーション中 (オープン) のときに、ASA は、到着した追加の SA 初期パケットのクッキー チャレンジを行います。10,000 個の IKEv2 SA が許可される Cisco ASA 5585-X では、5,000 個の SA がオープンになると、それ以降の着信 SA に対してクッキー チャレンジが行われます。

[Number of SAs Allowed in Negotiation] または **[Maximum Number of SAs Allowed]** とともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこれらの設定よりも低くしてください。

[Configuration] > **[Site-to-Site VPN]** > **[Advanced]** > **[System Options]** を選択して、IPsec レベルのすべての SA の寿命を制限することもできます。

IKE ポリシー

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Policies]

このペインは、IKEv1 ポリシーと IKEv2 ポリシーを追加、編集、または削除するために使用します。

IKE ネゴシエーションの条件を設定するには、次に示す項目を含む IKE ポリシーを 1 つ以上作成します。

- 一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。
- 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。
- HMAC 方式。送信者の身元を保証し、搬送中にメッセージが変更されていないことを保証します。
- 暗号キー判別アルゴリズムを強化する Diffie-Hellman 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。
- 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。

各 IKE 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 IKE 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。

IKEv1 の場合は、各パラメータに対して 1 つの設定だけをイネーブルにできます。IKEv2 の場合は、1 つのプロポーザルで複数の設定 ([Encryption]、[D-H Group]、[Integrity Hash]、および [PRF Hash]) を指定できます。

IKE ポリシーが設定されていない場合、ASA はデフォルトのポリシーを使用します。デフォルトポリシーには各パラメータのデフォルト値が含まれており、ポリシーのプライオリティは常に最下位に設定されます。特定のパラメータの値を指定しない場合、デフォルト値が適用されます。

IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモートピアに送信します。リモートピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。

暗号化、ハッシュ、認証、および Diffie-Hellman の値が同じで、SA ライフタイムが送信されたポリシーのライフタイム以下の場合には、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、（リモートピアポリシーからの）短い方のライフタイムが適用されます。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、IKE SA は確立されません。

フィールド

- [IKEv1 Policies] : 設定済み IKE ポリシーそれぞれのパラメータ設定を表示します。
 - [Priority #] : ポリシーのプライオリティを示します。

- [Encryption] : 暗号化方式を示します。
 - [Hash] : ハッシュ アルゴリズムを示します。
 - [D-H Group] : Diffie-Hellman グループを示します。
 - [Authentication] : 認証方式を示します。
 - [Lifetime (secs)] : SA ライフタイムを秒数で示します。
- [IKEv2 Policies] : 設定済み IKEv2 ポリシーそれぞれのパラメータ設定を表示します。
 - [Priority #] : ポリシーのプライオリティを示します。
 - [Encryption] : 暗号化方式を示します。
 - [Integrity Hash] : ハッシュ アルゴリズムを示します。
 - [PRF Hash] : 疑似乱数関数 (PRF) ハッシュ アルゴリズムを示します。
 - [D-H Group] : Diffie-Hellman グループを示します。
 - [Lifetime (secs)] : SA ライフタイムを秒数で示します。

IKEv1 ポリシーの追加または編集

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Policies] > [Add/Edit IKE Policy]

[Priority #] : IKE ポリシーのプライオリティを設定する数字を入力します。範囲は 1 ~ 65535 で、1 が最高のプライオリティです。

[Encryption] : 暗号化方式を選択します。これは、2つの IPSec ピア間で伝送されるデータを保護する対称暗号化アルゴリズムです。次の中から選択できます。

des	56 ビット DES-CBC。安全性は低いですが、他の選択肢より高速です。デフォルト。
3des	168 ビット Triple DES。
aes	128 ビット AES。
aes-192	192 ビット AES。
aes-256	256 ビット AES。

[Hash] : 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。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。

sha	SHA-1	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと思われています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリエーションがこの攻撃を防ぎます。
md5	MD5	

[Authentication] : 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選択します。事前共有キーは拡大するネットワークに対応した拡張が困難ですが、小規模ネットワークではセットアップが容易です。次の選択肢があります。

pre-share	事前共有キー。
rsa-sig	RSA シグニチャ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。

[D-H Group] : Diffie-Hellman グループ ID を選択します。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。

1	グループ 1 (768 ビット)	「デフォルト」のグループ 2 (1024 ビット Diffie-Hellman) は、グループ 1 または 5 と比較して、CPU の実行時間は短いものの、安全性は低くなります。
2	グループ 2 (1024 ビット)	
5	グループ 5 (1536 ビット)	

[Lifetime (secs)] : [Unlimited] をオンにするか、SA ライフタイムを整数で入力します。デフォルトは 86,400 秒、つまり 24 時間です。ライフタイムを長くするほど、ASA は後の IPSec セキュリティアソシエーションをより緩やかにセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2～3 分ごと）にしながらもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

[Time Measure] : 時間基準を選択します。ASA では次の値を使用できます。

120 ~ 86,400 秒
2 ~ 1,440 分
1 ~ 24 時間
1 日

IKEv2 ポリシーの追加または編集

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Policies] > [Add/Edit IKEv2 Policy]

[Priority #] : IKEv2 ポリシーのプライオリティを設定する数字を入力します。範囲は 1 ~ 65535 で、1 が最高のプライオリティです。

[Encryption] : 暗号化方式を選択します。これは、2 つの IPSec ピア間で伝送されるデータを保護する対称暗号化アルゴリズムです。次の中から選択できます。

des	56 ビット DES-CBC 暗号化を ESP に対して指定します。
3des	(デフォルト) トリプル DES 暗号化アルゴリズムを ESP に対して指定します。
aes	AES と 128 ビット キー暗号化を ESP に対して指定します。
aes-192	AES と 192 ビット キー暗号化を ESP に対して指定します。
aes-256	AES と 256 ビット キー暗号化を ESP に対して指定します。
aes-gcm	AES-GCM/GMAC 128 ビットのサポートを対称暗号化と整合性に対して指定します。
aes-gcm-192	AES-GCM/GMAC 192 ビットのサポートを対称暗号化と整合性に対して指定します。
aes-gcm-256	AES-GCM/GMAC 256 ビットのサポートを対称暗号化と整合性に対して指定します。
NULL	暗号化が行われないことを示します。

[D-H Group] : Diffie-Hellman グループ ID を選択します。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。

1	グループ 1 (768 ビット)	これがデフォルトです。Group 2 (1024 ビット Diffie-Hellman) では、実行に必要な CPU 時間が少なくなりますが、Group 2 または 5 より安全性が劣ります。
2	グループ 2 (1024 ビット)	
5	グループ 5 (1536 ビット)	
14	グループ 14	

19	グループ 19	
20	グループ 20	
21	グループ 21	
24	グループ 24	

[Integrity Hash] : ESP プロトコルのデータ整合性を保証するためのハッシュ アルゴリズムを選択します。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。

sha	SHA 1	デフォルトは SHA 1 です。
md5	MD5	MD5 の方がダイジェストが小さく、SHA 1 よりもやや速い と見なされています。しかし、MD5 に対する攻撃が成功 (これは非常に困難) しても、IKE が使用する HMAC バ リエントがこの攻撃を防ぎま 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-bit digest	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-bit digest	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 または AES-GMAC が暗号化アルゴリズムとして 設定されていることを示しま す。AES-GCM 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。

[Pseudo-Random Function (PRF)] : SA で使用されるすべての暗号化アルゴリズムのためのキー
関連情報の組み立てに使用される PRF を指定します。

sha	SHA-1	デフォルト値は SHA-1 です。
md5	MD5	MD5 のダイジェストの方が小さく、SHA-1 よりもやや速い と見なされています。しかし、MD5 に対する攻撃が成功 (これは非常に困難) しても、IKE が使用する HMAC バ リエントがこの攻撃を防ぎま 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。

[Lifetime (secs)] : [Unlimited] をオンにするか、SA ライフタイムを整数で入力します。デフォルトは 86,400 秒、つまり 24 時間です。ライフタイムを長くするほど、ASA は以後の IPsec セキュリティアソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く (約 2 ~ 3 分ごと) にしなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

ASA では次の値を使用できます。

120 ~ 86,400 秒
2 ~ 1,440 分
1 ~ 24 時間
1 日

IPsec の設定

ASA では、LAN-to-LAN VPN 接続に IPsec が使用され、client-to-LAN VPN 接続に IPsec を使用することも選択できます。IPsec の用語では、「ピア」は、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を指します。ASA は、シスコピア (IPv4 または IPv6) と、関連するすべての標準に準拠したサードパーティピアとの LAN-to-LAN IPsec 接続をサポートします。

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。

ASA は、次の IPsec 属性をサポートしています。

- 認証でデジタル証明書を使用するときに、フェーズ 1 ISAKMP セキュリティアソシエーションをネゴシエートする場合の Main モード
- 認証で事前共有キーを使用するときに、フェーズ 1 ISAKMP セキュリティアソシエーション (SA) をネゴシエートする場合の Aggressive モード
- 認証アルゴリズム :
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- 認証モード :
 - 事前共有キー
 - X.509 デジタル証明書
- Diffie-Hellman グループ 1、2、および 5。
- 暗号化アルゴリズム :
 - AES-128、-192、および -256
 - 3DES-168
 - DES-56
 - ESP-NULL
- 拡張認証 (XAuth)
- モード コンフィギュレーション (別名 ISAKMP コンフィギュレーション方式)
- トンネル カプセル化モード
- LZS を使用した IP 圧縮 (IPCOMP)

手順

- ステップ1 [暗号マップ \(31 ページ\)](#) を設定します。
- ステップ2 [IPsec 事前フラグメンテーションポリシー \(40 ページ\)](#) を設定します。
- ステップ3 [IPsec Proposals \(Transform Sets\) \(43 ページ\)](#) を設定します。

暗号マップ

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps]

このペインには、IPSec ルールに定義されている、現在設定されているクリプト マップが表示されます。ここでは、IPSec ルールを追加、編集、削除、切り取り、および貼り付けしたり、上下に移動させたりできます。



- (注) 暗黙のルールは、編集、削除、またはコピーできません。ASA は、ダイナミック トンネル ポリシーが設定されている場合、リモートクライアントからトラフィックの選択提案を暗黙的に受け入れます。特定のトラフィックを選択することによって、その提案を無効化できます。

[Interface]、[Source]、[Destination]、[Destination Service]、または [Rule Query] を選択、[is] または [contains] を選択、あるいはフィルタ パラメータを入力することによって、ルールを検索 (ルールの表示をフィルタ処理) することもできます。[...] をクリックして、選択可能なすべての既存エントリが示された参照ダイアログボックスを開きます。ダイアグラムは、ルールを図で表示するために使用します。

IPsec ルールでは以下を指定します。

- [Type: Priority] : ルールのタイプ (Static または Dynamic) とそのプライオリティを表示します。
- Traffic Selection
 - [#] : ルール番号を示します。
 - [Source] : トラフィックを [Remote Side Host/Network] カラムのリストにある IP アドレス宛てに送信するときに、このルールに従う IP アドレスを示します。詳細モード ([Show Detail] ボタンを参照) では、アドレス カラムに、「any」という語が含まれるインターフェイス名が表示される場合があります (例: 「inside:any」)。any は、内部インターフェイスのすべてのホストがルールの影響を受けることを意味します。
 - [Destination] : トラフィックが [Security Appliance Side Host/Network] カラムのリストにある IP アドレスから送信されるときに、このルールに従う IP アドレスを一覧表示します。詳細モード ([Show Detail] ボタンを参照) では、アドレス カラムに、「any」という語が含まれるインターフェイス名が表示される場合があります (例: 「outside:any」)。any は、外部インターフェイスのすべてのホストがルールの影響を受けることを意味します。さらに詳細モードでは、アドレスカラムに角カッコで囲

まれた IP アドレスが含まれることもあります ([209.165.201.1-209.165.201.30] など)。これらのアドレスは、変換済みアドレスです。内部ホストによって外部ホストへの接続が作成されると、ASA は内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、ASA はこのアドレス マッピングを保持します。このアドレス マッピング構造は `xlate` と呼ばれ、一定期間メモリに保持されます。

- [Service] : ルールによって指定されるサービスとプロトコルを指定します (TCP、UDP、ICMP、または IP)。
- [Action] : IPsec ルールのタイプ (保護する、または保護しない) を指定します。
- [Transform Set] : ルールのトランスフォーム セットを表示します。
- [Peer] : IPsec ピアを識別します。
- [PFS] : ルールの完全転送秘密設定値を表示します。
- [NAT-T Enabled] : ポリシーで NAT Traversal が有効になっているかどうかを示します。
- [Reverse Route Enabled] : ポリシーでリバースルートインジェクション (RRI) がイネーブルになっているかどうかを示します。RRI は設定で行われ、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。
- [Dynamic] : ダイナミックに指定されている場合、RRI 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。

- [Connection Type] : (スタティック トンネルポリシーでのみ有効)。このポリシーの接続タイプを `bidirectional`、`originate-only`、または `answer-only` として識別します。
- [SA Lifetime] : ルールの SA ライフタイムを表示します。
- [CA Certificate] : ポリシーの CA 証明書を表示します。これは、スタティック接続にだけ適用されます。
- [IKE Negotiation Mode] : IKE ネゴシエーションで、Main モードまたは Aggressive モードを使用するかどうかを表示します。
- [Description] : (任意) このルールの簡単な説明を指定します。既存ルールの場合、ルールの追加時に入力した説明になります。暗黙のルールには、「Implicit rule」という記述が含まれています。暗黙のルール以外のルールの説明を編集するには、このカラムを右クリックして [Edit Description] を選択するか、このカラムをダブルクリックします。

- [Enable Anti-replay window size] : リプレイ攻撃防止ウィンドウのサイズを、64 ~ 1028 の範囲の 64 の倍数で設定します。階層型 QoS ポリシーでのトラフィックシェーピングによるプライオリティキューイング（「[Rule Actions] > [QoS] タブ」を参照）の副次的影響は、パケットの順番が変わることです。IPsec パケットでは、アンチリプレイウィンドウ内にはない不連続パケットにより、警告 syslog メッセージが生成されます。これらの警告は、プライオリティキューイングの場合は誤報です。アンチリプレイのパネルサイズを設定すると、誤報を回避することができます。
- [Enable IPsec Inner Routing Lookup] : デフォルトでは、IPsec トンネル経由で送信されるパケットに対してルックアップは実行されません。パケット単位の隣接関係ルックアップは外部 ESP パケットに対してのみ行われます。一部のネットワークトポロジでは、ルーティングの更新によって内部パケットのパスが変更されても、IPsec トンネルがまだアップ状態の場合、トンネルを介したパケットは正常にルーティングされず、宛先に到達できません。これを防止するには、IPsec 内部パケットのパケットごとのルーティングルックアップをイネーブルにします。

[Create/Edit an IPsec Rule] : [Tunnel Policy (Crypto Map) - Basic] タブ

このペインでは、IPsec ルールの新しいトンネルポリシーを定義します。ここで定義する値は、[OK] をクリックした後に [IPsec Rules] テーブルに表示されます。すべてのルールは、デフォルトで [IPsec Rules] テーブルに表示されるとすぐにイネーブルになります。

[Tunnel Policy] ペインでは、IPsec（フェーズ2）セキュリティアソシエーション（SA）のネゴシエートで使用するトンネルポリシーを定義できます。ASDMは、ユーザのコンフィギュレーション編集結果を取り込みますが、[Apply] をクリックするまでは実行中のコンフィギュレーションに保存しません。

すべてのトンネルポリシーでは、トランスフォームセットを指定し、適用するセキュリティアプライアンスインターフェイスを特定する必要があります。トランスフォームセットでは、IPsec の暗号化処理と復号化処理を実行する暗号化アルゴリズムおよびハッシュアルゴリズムを特定します。すべての IPsec ピアが同じアルゴリズムをサポートするとは限らないため、多くのポリシーを指定して、それぞれに1つのプライオリティを割り当てるようにすることもできます。その後セキュリティアプライアンスは、リモートの IPsec ピアとネゴシエートして、両方のピアがサポートするトランスフォームセットを一致させます。

トンネルポリシーは、スタティックまたはダイナミックにすることができます。スタティックトンネルポリシーでは、セキュリティアプライアンスで IPsec 接続を許可する1つ以上のリモート IPsec ピアまたはサブネットワークを特定します。スタティックポリシーを使用して、セキュリティアプライアンスで接続を開始するか、またはリモートホストから接続要求を受信するかどうかを指定できます。スタティックポリシーでは、許可されるホストまたはネットワークを識別するために必要な情報を入力する必要があります。

ダイナミックトンネルポリシーは、セキュリティアプライアンスとの接続を開始することを許可されるリモートホストについての情報を指定できないか、または指定しない場合に使用します。リモート VPN 中央サイトデバイスとの関係で、セキュリティアプライアンスを VPN クライアントとしてしか使用しない場合は、ダイナミックトンネルポリシーを設定する必要はありません。ダイナミックトンネルポリシーが最も効果的なのは、リモートアクセスクライアントが、VPN 中央サイトデバイスとして動作するセキュリティアプライアンスからユー

がネットワークへの接続を開始できるようにする場合です。ダイナミック トンネル ポリシーは、リモートアクセスクライアントにダイナミックに割り当てられた IP アドレスがある場合、または多くのリモートアクセスクライアントに別々のポリシーを設定しないようにする場合に役立ちます。

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] > [Create / Edit IPsec Rule] > [Tunnel Policy (Crypto Map) - Basic]

- [Interface] : このポリシーを適用するインターフェイス名を選択します。
- [Policy Type] : このトンネル ポリシーのタイプとして、[Static] または [Dynamic] を選択します。
- [Priority] : ポリシーのプライオリティを入力します。
- [IKE Proposals (Transform Sets)] : IKEv1 および IKEv2 の IPsec プロポーザルを指定します。
 - [IKEv1 IPsec Proposal] : ポリシーのプロポーザル（トランスフォーム セット）を選択して [Add] をクリックすると、アクティブなトランスフォームセットのリストに移動します。[Move Up] または [Move Down] をクリックして、リストボックス内でのプロポーザルの順番を入れ替えます。クリプト マップ エントリまたはダイナミック クリプト マップ エントリには、最大で 11 のプロポーザルを追加できます。
 - [IKEv2 IPsec Proposal] : ポリシーのプロポーザル（トランスフォーム セット）を選択して [Add] をクリックすると、アクティブなトランスフォームセットのリストに移動します。[Move Up] または [Move Down] をクリックして、リストボックス内でのプロポーザルの順番を入れ替えます。クリプト マップ エントリまたはダイナミック クリプト マップ エントリには、最大で 11 のプロポーザルを追加できます。
- [Peer Settings - Optional for Dynamic Crypto Map Entries] : ポリシーのピア設定値を設定します。
 - [Connection Type] : (スタティック トンネル ポリシーでのみ有効)。bidirectional、originate-only、または answer-only を選択して、このポリシーの接続タイプを指定します。LAN-to-LAN 接続の場合は、bidirectional または answer-only (originate-only ではない) を選択します。LAN-to-LAN 冗長接続の場合は、answer-only を選択します。originate only を選択した場合は、最大 10 個の冗長ピアを指定できます。単方向に対してだけ、originate only または answer only を指定できます。どちらもデフォルトでイネーブルになっていません。
 - [IP Address of Peer to Be Added] : 追加する IPSec ピアの IP アドレスを入力します。
- [Enable Perfect Forwarding Secrecy] : ポリシーの PFS をイネーブルにする場合にオンにします。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPsec ネゴシエーションでのフェーズ 2 キーは、PFS を指定しない限りフェーズ 1 に基づいて生成されます。
- [Diffie-Hellman Group] : PFS をイネーブルにする場合は、ASA がセッションキーの生成に使用する Diffie-Hellman グループも選択する必要があります。次の選択肢があります。

- [Group 1 (768 ビット)] : PFS を使用し、Diffie-Hellman Group 1 を使用して IPsec セッション キーを生成します。このときの素数と generator 数は 768 ビットです。このオプションは高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
- [Group 2 (1024 ビット)] : PFS を使用し、Diffie-Hellman Group 2 を使用して IPsec セッション キーを生成します。このときの素数と generator 数は 1024 ビットです。このオプションは Group 1 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
- [Group 5 (1536 ビット)] : PFS を使用し、Diffie-Hellman Group 5 を使用して IPsec セッション キーを生成します。このときの素数と generator 数は 1536 ビットです。このオプションは Group 2 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
- [Group 14 (2048-bits)] : 完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 14 を使用します。
- [Group 19] : 完全転送秘密を使用し、IKEv2 に対する Diffie-Hellman グループ 19 を使用して、ECDH をサポートします。
- [Group 20] : 完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 20 を使用して、ECDH をサポートします。
- [Group 21] : 完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 21 を使用して、ECDH をサポートします。
- [Group 24] : 完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 24 を使用します。

[Create/Edit IPsec Rule] : [Tunnel Policy (Crypto Map) - Advanced] タブ

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] > [Create / Edit IPsec Rule] > [Tunnel Policy (Crypto Map) - Advanced]

- [Enable NAT-T] : このポリシーの NAT Traversal (NAT-T) をイネーブルにします。
- [Enable Reverse Route Injection] : このポリシーの逆ルート注入をイネーブルにします。リバース ルート インジェクション (RRI) は、ダイナミック ルーティング プロトコルを使用する内部ルータのルーティング テーブルにデータを入力するために使用されます。ダイナミック ルーティング プロトコルの例としては、Open Shortest Path First (OSPF)、Enhanced Interior Gateway Routing Protocol (EIGRP) (ASA を実行する場合)、ルーティング情報 プロトコル (RIP) (リモート VPN クライアントや LAN-to-LAN セッションに使用) があります。RRI は設定で行われ、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。

- [Dynamic] : ダイナミックに指定されている場合、RRI 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。通常、RRI ルートは、ルートが存在せず、トラフィックを暗号化する必要がある場合に、トンネルを開始するために使用されます。ダイナミック RRI がサポートされると、トンネルが確立されるまでルートが存在しません。したがって、ダイナミック RRI が設定された ASA は通常、レスポンドとしてのみ動作します。



(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。

- [Security Association Lifetime Settings] : セキュリティ アソシエーション (SA) の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
 - [Time] : 時 (hh) 、分 (mm) 、および秒 (ss) 単位で SA のライフタイムを指定します。
 - [Traffic Volume] : キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロードデータのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。
- [Static Type Only Settings] : スタティック トンネル ポリシーのパラメータを指定します。
 - [Device Certificate] : 使用する証明書を選択します。デフォルトの [None] (事前共有キーを使用) 以外の値を選択する場合。[None] 以外を選択すると、[Send CA certificate chain] チェックボックスがオンになります。
 - [Send CA certificate chain] : トラスト ポイント チェーン全体の伝送をイネーブルにします。
 - [IKE Negotiation Mode] : IKE ネゴシエーションモード (Main または Aggressive) を選択します。このパラメータにより、キー情報の交換と SA のセットアップを行う場合のモードを設定します。ネゴシエーションの発信側が使用するモードを設定し、応答側は自動ネゴシエーションします。Aggressive モードは高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。[Aggressive] を選択すると、[Diffie-Hellman Group] リストがアクティブになります。
 - [Diffie-Hellman Group] : 適用する Diffie-Hellman グループを選択します。Group 1 (768 ビット) 、 Group 2 (1024 ビット) Group 5 (1536 ビット) の中から選択します。
- [ESP v3] : 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、セキュリティ単位のアソシエーションポリシーを設定するか、トラフィック フロー パケットをイネーブルにします。

- [Validate incoming ICMP error messages] : IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先のこれらの ICMP エラー メッセージを検証するかどうかを選択します。
- [Enable Do Not Fragment (DF) policy] : IP ヘッダーに Do-Not-Fragment (DF) ビットセットを持つ大きなパケットを IPSec サブシステムがどのように処理するかを定義します。次のいずれかを選択します。
 - [Clear DF bit] : DF ビットを無視します。
 - [Copy DF bit] : DF ビットを維持します。
 - [Set DF bit] : DF ビットを設定して使用します。
- [Enable Traffic Flow Confidentiality (TFC) packets] : トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットをイネーブルにします。



(注) TFC をイネーブルにする前に、[Tunnel Policy (Crypto Map)] の [Basic] タブで IKE v2 IPsec プロポーザルが設定されていなければなりません。

バースト、ペイロードサイズ、およびタイムアウトパラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

[Create/Edit IPsec Rule] : [Traffic Selection] タブ

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] > [Create / Edit IPsec Rule] > [Traffic Selection]

このペインでは、保護する（許可）トラフィックまたは保護しない（拒否）トラフィックを定義できます。

- [Action] : このルールで実行するアクションを指定します。選択肢は、[protect] と [do not protect] です。
- [Source] : 送信元ホストまたはネットワークの IP アドレス、ネットワーク オブジェクトグループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。[...] をクリックして、次のフィールドを含む [Browse Source] ダイアログボックスを開きます。
 - [Add/Edit] : 送信元アドレスまたはグループを追加するには、[IP Address] または [Network Object Group] を選択します。
 - [Delete] : エントリを削除します。
 - [Filter] : 表示される結果をフィルタリングする IP アドレスを入力します。
 - [Name] : 続くパラメータが、送信元ホストまたはネットワークの名前を指定することを示します。

- [IP Address] : 続くパラメータが、送信元ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。
- [Netmask] : IP アドレスに適用する標準サブネットマスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
- [Description] : 説明を入力します。
- [Selected Source] : 選択したエントリを送信元として含めるには [Source] をクリックします。
- [Destination] : 宛先ホストまたはネットワークの IP アドレス、ネットワーク オブジェクトグループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。[...] をクリックして、次のフィールドを含む [Browse Destination] ダイアログを開きます。
 - [Add/Edit] : [IP Address] または [Network Object Group] を選択して、宛先アドレスまたはグループを追加します。
 - [Delete] : エントリを削除します。
 - [Filter] : 表示される結果をフィルタリングする IP アドレスを入力します。
 - [Name] : 続くパラメータが、宛先ホストまたはネットワークの名前を指定することを示します。
 - [IP Address] : 続くパラメータが、宛先ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。
 - [Netmask] : IP アドレスに適用する標準サブネットマスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
 - [Description] : 説明を入力します。
 - [Selected Destination] : 選択したエントリを宛先として含めるには [Destination] をクリックします。
- [Service] : サービスを入力するか、または [...] をクリックして [Browse Service] ダイアログボックスを開き、サービスのリストから選択できます。
- [Description] : [Traffic Selection] のエントリの説明を入力します。
- More Options
 - [Enable Rule] : このルールをイネーブルにします。
 - [Source Service] : サービスを入力するか、[...] をクリックしてサービス参照ダイアログボックスを開き、サービスのリストから選択します。
 - [Time Range] : このルールを適用する時間範囲を定義します。
 - [Group] : 続くパラメータが、送信元ホストまたはネットワークのインターフェイスとグループ名を指定することを示します。

- **[Interface]** : IP アドレスのインターフェイス名を選択します。このパラメータは、**[IP Address]** オプション ボタンを選択するときに表示されます。
 - **[IP address]** : このポリシーが適用されるインターフェイスの IP アドレスを指定します。このパラメータは、**[IP Address]** オプション ボタンを選択するときに表示されます。
 - **[Destination]** : 送信元、宛先のホストまたはネットワークについて、IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。これらのフィールドのいずれかで [...] をクリックし、次のフィールドを含む **[Browse]** ダイアログ ボックスを開きます。
 - **[Name]** : 送信元または宛先のホストまたはネットワークとして使用するインターフェイス名を選択します。このパラメータは、**[Name]** オプション ボタンを選択するときに表示されます。これは、このオプションに関連付けられる唯一のパラメータです。
 - **[Interface]** : IP アドレスのインターフェイス名を選択します。このパラメータは、**[Group]** オプション ボタンをクリックするときに表示されます。
 - **[Group]** : 送信元または宛先のホストまたはネットワークに指定されたインターフェイスに存在するグループの名前を選択します。リストにエントリが何もない場合は、既存グループの名前を入力できます。このパラメータは、**[Group]** オプション ボタンをクリックするときに表示されます。
- **[Protocol and Service]** : このルールに関連するプロトコルパラメータとサービスパラメータを指定します。



(注) 「Any-any」 IPsec ルールは使用できません。このタイプのルールにより、デバイスおよびそのピアが複数の LAN-to-LAN トンネルをサポートできなくなります。

- **[TCP]** : このルールを TCP 接続に適用することを指定します。これを選択すると、**[Source Port]** グループ ボックスと **[Destination Port]** グループ ボックスも表示されます。
- **[UDP]** : ルールを UDP 接続に適用することを指定します。これを選択すると、**[Source Port]** グループ ボックスと **[Destination Port]** グループ ボックスも表示されます。
- **[ICMP]** : ルールを ICMP 接続に適用することを指定します。これを選択すると、**[ICMP Type]** グループ ボックスも表示されます。
- **[IP]** : このルールを IP 接続に適用することを指定します。これを選択すると、**[IP Protocol]** グループ ボックスも表示されます。
- **[Manage Service Groups]** : **[Manage Service Groups]** ペインを表示します。このパネルでは、TCP/UDP サービス/ポートのグループを追加、編集、または削除できます。

- [Source Port] および [Destination Port] : [Protocol and Service] グループ ボックスで選択したオプション ボタンに応じて、TCP または UDP ポート パラメータが表示されます。
 - [Service] : 個々のサービスのパラメータを指定しようとしていることを示します。フィルタの適用時に使用するサービス名とブーリアン演算子を指定します。
 - [Boolean operator] (ラベルなし) : [Service] ボックスで指定したサービスを照合するときに使用するブーリアン条件 (等号、不等号、大なり、小なり、または範囲) を一覧表示します。
 - [Service] (ラベルなし) : 照合対象のサービス (https、kerberos その他) を特定します。range サービス演算子を指定すると、このパラメータは2つのボックスに変わります。ボックスに、範囲の開始値と終了値を入力します。
 - [...] : サービスのリストが表示され、ここで選択したサービスが [Service] ボックスに表示されます。
 - [Service Group] : 送信元ポートのサービス グループの名前を指定しようとしていることを示します。
 - [Service] (ラベルなし) : 使用するサービス グループを選択します。
 - [ICMP Type] : 使用する ICMP タイプを指定します。デフォルトは any です。[...] ボタンをクリックすると、使用可能なタイプのリストが表示されます。
- Options
 - [Time Range] : 既存の時間範囲の名前を指定するか、または新しい範囲を作成します。
 - [...] : [Add Time Range] ペインが表示され、ここで新しい時間範囲を定義できます。
 - [Please enter the description below (optional)] : ルールについて簡単な説明を入力するためのスペースです。

IPsec 事前フラグメンテーション ポリシー

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Prefragmentation Policies]

IPsec Pre-Fragmentation ポリシーでは、パブリック インターフェイスを介してトラフィックをトンネリングするときに、最大伝送単位 (MTU) の設定を超えるパケットの処理方法を指定します。この機能により、ASA とクライアント間のルータまたは NAT デバイスが IP フラグメントを拒否またはドロップする状況に対処できます。たとえば、クライアントが ASA の背後の FTP サーバに対して FTP get コマンドを実行するとします。FTP サーバから送信されるパケットは、カプセル化された場合にパブリック インターフェイス上の ASA の MTU サイズを超過する可能性があります。ASA でのこれらのパケットの処理方法は、選択されたオプションに応じて決まります。事前フラグメンテーション ポリシーは、ASA のパブリック インターフェイスから送出されるすべてのトラフィックに適用されます。

ASA は、トンネリングされたすべてのパケットをカプセル化します。このカプセル化の後、ASA は MTU の設定値を超えるパケットをフラグメント化して、パブリック インターフェイスから送信します。これがデフォルトのポリシーです。このオプションは、フラグメント化されたパケットが、障害なしでトンネル通過を許可される状況で機能します。FTP の例では、大きなパケットがカプセル化されてから、IP レイヤでフラグメント化されます。中間デバイスは、フラグメントをドロップするか、または異常なフラグメントだけをドロップします。ロードバランシング デバイスが、異常フラグメントを取り入れる可能性があります。

事前フラグメンテーションをイネーブルにすると、カプセル化の前に、MTU の設定値を超えるトンネリングされたパケットがフラグメント化されます。これらのパケットに DF ビットが設定されている場合、ASA は DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。ここでの例では、ASA は MTU を無効化し、DF ビットをクリアすることによってフラグメンテーションを許可します。



- (注) いずれのインターフェイスにおいても、MTU または事前フラグメンテーションのオプションを変更すると、すべての既存の接続が切断されます。たとえば、パブリック インターフェイスで 100 件のアクティブなトンネルが終了し、そのときに外部インターフェイスで [MTU] または [Pre-Fragmentation] オプションを変更すると、パブリック インターフェイスのすべてのアクティブなトンネルがドロップされます。

このペインでは、親ペインで選択したインターフェイスの既存の IPsec 事前フラグメンテーション ポリシーと Do-Not-Fragment (DF) ビット ポリシーを表示または編集します。

フィールド

- [Interface] : 選択されたインターフェイスを識別します。このダイアログボックスを使用しても、このパラメータは変更できません。
- [Enable IPsec pre-fragmentation] : IPsec の事前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します。ASA は、カプセル化する前に、MTU の設定を超えるトンネリングされたパケットをフラグメント化します。これらのパケットに DF ビットが設定されている場合、ASA は DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。
- [DF Bit Setting Policy] : Do-Not-Fragment ビット ポリシー : [Copy]、[Clear]、または [Set]

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、管理者は次の画面で、優先するフラグメンテーション方式を設定できます。

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE parameters]

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 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 AnyConnect 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。

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。

手順

- ステップ 1 ASDM で、**[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE parameters]** に移動します。
- ステップ 2 **[Enable fragmentation]** フィールドを選択または選択解除します。
- ステップ 3 **[Fragmentation MTU]** でサイズを指定します。
- ステップ 4 **[Preferred fragmentation method]** で優先する方式を指定します。

IPsec Proposals (Transform Sets)

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)]

トランスフォームは、データフローで実行される操作のセットで、データ認証、データ機密性、およびデータ圧縮を実現します。たとえば、1 つのトランスフォームは、3DES 暗号化と HMAC-MD5 認証アルゴリズム (ESP-3DES-MD5) による ESP プロトコルです。

このペインは、後述する IKEv1 および IKEv2 トランスフォームセットを表示、追加、編集、または削除するために使用します。各テーブルには、設定済みのトランスフォームセットの名前と詳細が表示されます。

[IKEv1 IPsec Proposals (Transform Sets)]

- **[Mode]** : ESP 暗号化と認証を適用するモード。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。
 - **[Tunnel mode]** (デフォルト) : 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]** : 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になります。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。transport 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。
- **[ESP Encryption]** : トランスフォームセットのカプセル化セキュリティプロトコル（ESP）暗号化アルゴリズム。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESPは、保護されているデータをカプセル化します。
- **[ESP Authentication]** : トランスフォームセットの ESP 認証アルゴリズム。

[IKEv2 IPsec Proposals]

- **[Mode]** : ESP 暗号化と認証を適用するモード。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。

- **[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。transport 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。



(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。
- [Encryption] : IKEv2 IPsec プロポーザルのカプセル化セキュリティプロトコル (ESP) 暗号化アルゴリズムを示します。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESP は、保護されているデータをカプセル化します。
 - [Integrity Hash] : ESP プロトコルのデータ整合性を保証するためのハッシュアルゴリズムを示します。パケットが想定した発信元から発信されたこと、また搬送中に変更されていることを保証します。パケットが想定した発信元から発信されたこと、また搬送中に変更されていることを保証します。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。



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](#) (47 ページ)
- [VPN ロード バランシング](#) (49 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 ASDM 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。

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伝送します。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回目のトランザクション（ユーザに対しては透過的）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、整数の割合（アクティブセッション数）として計算されます。AnyConnect の非アクティブセッションは、VPN ロードバランシングの SSL VPN 負荷に数えられません。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、AnyConnect、およびクライアントレス SSL VPN クライアントとクライアントレス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 または同じリリースの ASA を含む VPN ロードバランシンググループは、IPsec セッションおよびクライアントレス SSL 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最大 10 のノードはテスト済みです。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実装するには、異なる ASA 上の AnyConnect 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 ユーザの SSL VPN ライセンスを持つ 2 つの ASA 5525-X 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 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を使用するには、Security Plus ライセンスを備えた ASA モデル 5512-X、または ASA モデル 5515-X 以降が必要です。VPN ロードバランシングには、アクティブな 3DES または AES ライセンスが必要です。ASA は、VPN ロードバランシングをイネーブルにする前に、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。

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 (53 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ディセーブルになっています。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。
これを行うには、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に移動します。
- 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 にしかできません。
- ロード バランシング ユニットもフェールオーバー用に設定されている場合は、内部および外部インターフェイスのスタンバイ IP アドレスを設定する必要があります。設定しないと、VPN ロードバランシング構成がセカンダリノードに正しく同期されず、フェールオーバー後にセカンダリユニットが VPN ロードバランシンググループに参加しません。

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

[VPN ロードバランシングの前提条件 \(52 ページ\)](#) も参照してください。

適格なプラットフォーム

VPN ロードバランシンググループには、ASA モデルの ASA 5512-X (Security Plus ライセンスあり) および Model 5515-X 以降を含めることができます。混合構成は可能ですが、通常は、同種グループにする方が容易に管理できます。

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。

- AnyConnect Secure Mobility 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)
- クライアントレス SSL VPN

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 クライアントおよびクライアントレス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、AnyConnect 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。

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。

証明書の確認

AnyConnect 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、クライアントにより、この IP アドレスを通してその名前チェックがすべて実行されます。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は、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 ロードバランシング構成が AnyConnect との組み合わせで適切に機能するには、ASA の名前からアドレスへのマッピングが、その 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、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。

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。

High Availability and Scalability Wizard を使用した VPN ロード バランシングの設定

手順

- ステップ 1** [Wizards] > [High Availability and Scalability] を選択します。
- ステップ 2** [Configuration Type] 画面で、[Configure VPN Cluster Load Balancing] をクリックしてから、[Next] をクリックします。
- ステップ 3** VPN ロードバランシンググループ全体を表す 1 つの IP アドレスを選択します。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 アドレスを指定します。
- ステップ 4** 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、VPN 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。
- ステップ 5** IPsec 暗号化をイネーブルにして、デバイス間で通信されるすべての VPN 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、[Enable IPsec Encryption] チェックボックスをオンにします。
- ステップ 6** IPsec 共有秘密を指定して確認します。入力した値は、連続するアスタリスク文字として表示されます。
- ステップ 7** グループ内でこのデバイスに割り当てる優先順位を指定します。値の範囲は 1 ~ 10 です。優先順位は、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）、このデバイスがディレクタになる可能性が高くなります。

(注) VPN ロードバランシンググループ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、ディレクタの役割を果たすと想定されます。グループ内の各デバイスは起動するとチェックを行い、グループにディレクタがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、グループに追加されたデバイスは、グループメンバーになります。グループ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスがディレクタになります。グループ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスがディレクタになります。

ステップ 8 [Public Interface of This Device] を選択します。

ステップ 9 [Private Interface of This Device] を選択します。

ステップ 10 VPN クライアント接続をデバイスにリダイレクトするとき、外部 IP アドレスの代わりにデバイスのホスト名とドメイン名を使用して、ディレクタによって完全修飾ドメイン名が送信されるようにするには、[Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにします。

ステップ 11 [Next] をクリックします。[Summary] 画面でコンフィギュレーションを確認します。

ステップ 12 [Finish] をクリックします。

VPN ロードバランシンググループの構成が ASA に送信されます。

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、AnyConnect 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。

Group URL は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] > *connection profile name* > [Add or Edit] > [Advanced] > [Group Alias / Group URL] ペインで設定します。

VPN ロード バランシングの設定 (ウィザードを使用しない場合)

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Load Balancing] を選択します。

ステップ 2 [Participate in Load Balancing] をオンにして、この ASA がロードバランシング クラスタに参加していることを指定します。

ロード バランシングに参加するすべての ASA に対してこの方法でロード バランシングをイネーブルにする必要があります。

ステップ 3 [VPN Cluster Configuration] エリアで、次のフィールドを設定します。これらの値は、仮想クラスター全体で同じである必要があります。すべてのクラスターに同一のクラスター設定を行う必要があります。

- [Cluster IPv4 Address] : IPv4 仮想クラスター全体を表す単一の IPv4 アドレスを指定します。仮想クラスター内のすべての ASA が共有するパブリックサブネットのアドレス範囲内から、IP アドレスを選択します。
- [UDP Port] : このデバイスが参加する仮想クラスターの 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。
- [Cluster IPv6 Address] : IPv6 仮想クラスター全体を示す単一の IPv6 アドレスを指定します。仮想クラスター内のすべての ASA が共有するパブリックサブネットのアドレス範囲内から、IP アドレスを選択します。IPv6 アドレスを使用したクライアントは、ASA クラスターの公開されている IPv6 アドレス経由または GSS サーバ経由で AnyConnect 接続を行うことができます。同様に、IPv6 アドレスを使用したクライアントは、ASA クラスターの公開されている IPv4 アドレス経由または GSS サーバ経由で AnyConnect VPN 接続を行うことができます。どちらのタイプの接続も ASA クラスター内でロードバランシングできます。

(注) 少なくとも 1 台の DNS サーバに DNS サーバグループが設定されており、ASA インターフェイスの 1 つで DNS ルックアップがイネーブルにされている場合、[Cluster IPv4 Address] および [Cluster IPv6 Address] フィールドでは、仮想クラスターの完全修飾ドメイン名も指定できます。
- [Enable IPsec Encryption] : IPsec 暗号化をイネーブルまたはディセーブルにします。このボックスをオンにして、共有秘密情報を指定して確認します。仮想クラスター内の 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、このチェックボックスをオンにします。
- [IPsec Shared Secret] : IPsec 暗号化がイネーブルになっているときに、IPsec ピア間の共有秘密情報を指定します。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。
- [Verify Secret] : 共有秘密情報を再入力します。[IPsec Shared Secret] ボックスに入力された共有秘密情報の値を確認します。

ステップ 4 特定の ASA の [VPN Server Configuration] エリアのフィールドを設定します。

- [Public Interface] : このデバイスのパブリック 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。
- [Private Interface] : このデバイスのプライベート 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。

- **[Priority]** : クラスタ内でこのデバイスに割り当てるプライオリティを指定します。値の範囲は 1 ~ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタマスターになる可能性を表します。優先順位を高く設定すれば (10 など)、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

(注) 仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタマスターの役割を果たすと想定されます。仮想クラスタにはマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、バックアップデバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタマスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

- **[NAT Assigned IPv4 Address]** : このデバイスの IP アドレスを NAT によって変換した結果の IP アドレスを指定します。NAT を使用しない場合 (またはデバイスが NAT を使用するファイアウォールの背後にはない場合) は、このフィールドを空白のままにしてください。
- **[NAT Assigned IPv6 Address]** : このデバイスの IP アドレスを NAT によって変換した後の IP アドレスを指定します。NAT を使用しない場合 (またはデバイスが NAT を使用するファイアウォールの背後にはない場合) は、このフィールドを空白のままにしてください。
- **[Send FQDN to client]** : このチェックボックスをオンにすると、VPN クラスタ マスターが VPN クライアント接続をクラスタ デバイスにリダイレクトするときに、外部 IP アドレスの代わりにクラスタデバイスのホスト名とドメイン名を使用して完全修飾ドメイン名が送信されるようになります。

デフォルトで、ASA はロードバランシング リダイレクションの 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、その証明書はバックアップデバイスにリダイレクトされたときに無効になります。

VPN クライアント接続を別のクラスタ デバイス (クラスタ内の別の ASA) にリダイレクトするときに、この ASA は VPN クラスタ マスターとして、DNS 逆ルックアップを使用し、そのクラスタデバイスの (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。

クラスタ内の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。

(注) IPv6 を使用し、FQDNS をクライアントに送信するときに、これらの名前は DNS を通じて ASA で解決できる必要があります。

詳細については、「[FQDN を使用したクライアントレス SSL VPN ロード バランシングのイネーブル化 \(59 ページ\)](#)」を参照してください。

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クラスタ化され、AnyConnect 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 ノードは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 バランシング仮想クラスタ 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。

Group URL は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] > *connection profile name* > [Add or Edit] > [Advanced] > [Group Alias / Group URL] ペインで設定します。

FQDN を使用したクライアントレス SSL VPN ロード バランシングのイネーブル化

手順

-
- ステップ 1** [Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにして、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。
 - ステップ 2** DNS サーバに、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** [Configuration] > [Device Management] > [DNS] > [DNS Client] ダイアログボックスで、DNS サーバへのルートを持つインターフェイスについて、ASA での DNS ルックアップをイネーブルにします。
 - ステップ 4** ASA で DNS サーバの IP アドレスを定義します。これを行うには、このダイアログボックスで [Add] をクリックします。[Add DNS Server Group] ダイアログボックスが開きます。追加する DNS サーバの IPv4 または IPv6 アドレスを入力します。たとえば、192.168.1.1 または 2001:DB8:2000::1 です。
 - ステップ 5** [OK] および [Apply] をクリックします。
-



第 4 章

一般的な VPN 設定

- システム オプション (62 ページ)
- 最大 VPN セッション数の設定 (63 ページ)
- DTLS の設定 (64 ページ)
- DNS サーバ グループの設定 (65 ページ)
- 暗号化コアのプールの設定 (65 ページ)
- SSL VPN 接続用のクライアント アドレス指定 (66 ページ)
- グループ ポリシー (68 ページ)
- 接続プロファイル (121 ページ)
- 接続プロファイル、クライアントレス SSL VPN (140 ページ)
- IKEv1 接続プロファイル (145 ページ)
- **IKEv2 接続プロファイル** (152 ページ)
- IPsec または SSL VPN 接続プロファイルへの証明書のマッピング (154 ページ)
- Site-to-Site 接続プロファイル (158 ページ)
- AnyConnect VPN クライアント イメージ (166 ページ)
- AnyConnect VPN クライアント接続の設定 (168 ページ)
- AnyConnect HostScan (176 ページ)
- HostScan のインストールまたはアップグレード (177 ページ)
- HostScan のアンインストール (179 ページ)
- グループ ポリシーへの AnyConnect フィーチャ モジュールの割り当て (179 ページ)
- HostScan の関連マニュアル (181 ページ)
- AnyConnect セキュア モビリティ ソリューション (181 ページ)
- AnyConnect のカスタマイズとローカリゼーション (183 ページ)
- AnyConnect カスタム属性 (186 ページ)
- IPsec VPN クライアント ソフトウェア (189 ページ)
- Zone Labs Integrity Server (189 ページ)
- ISE ポリシーの適用 (190 ページ)

システムオプション

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [System Options] ペイン（または [Configuration] > [Site-to-Site VPN] > [Advanced] > [System Options] を使用して到達）を使用すると、ASA 上の IPsec セッションと VPN セッションに固有の機能を設定できます。

- [Limit maximum number of active IPsec VPN sessions] : アクティブな IPsec VPN セッションの最大数の制限をイネーブルまたはディセーブルにします。範囲は、ハードウェアプラットフォームとソフトウェアライセンスによって異なります。
- [Maximum IPsec Sessions] : アクティブな IPsec VPN セッションの最大許可数を指定します。このフィールドは、上記のチェックボックスをオンにして、アクティブな IPsec VPN セッションの最大数を制限した場合にだけアクティブになります。
- [L2TP Tunnel Keep-alive Timeout] : キープアライブ メッセージの頻度を秒単位で指定します。範囲は 10 ~ 300 秒です。デフォルトは 60 秒です。これは、Network (Client) Access 専用の高度なシステム オプションです。
- VPN トンネルの確立時に、既存のフローを再分類します。
- [Preserve stateful VPN flows when the tunnel drops] : ネットワーク拡張モード (NEM) での IPsec トンネルフローの保持をイネーブルまたはディセーブルにします。永続的な IPsec トンネルフロー機能をイネーブルにすると、[Timeout] ダイアログボックスで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がステート情報にアクセスできるため、データは正常にフローを続行します。このオプションは、デフォルトで無効です。



(注) 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。

- [IPsec Security Association Lifetime] : セキュリティアソシエーション (SA) の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
 - [Time] : 時 (hh) 、分 (mm) 、および秒 (ss) 単位で SA のライフタイムを指定します。
 - [Traffic Volume] : キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロードデータのキロバイト数を入力します。または [unlimited] をオンにします。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。

- [Enable PMTU (Path Maximum Transmission Unit) Aging] : 管理者が PMTU のエージングをイネーブルにすることができます。
 - [Interval to Reset PMTU of an SA (Security Association)] : PMTU 値が元の値にリセットされる秒数を入力します。
- [Enable inbound IPSec sessions to bypass interface access-lists]. [Group policy and per-user authorization ACLs still apply to the traffic] : ASA は、VPN トラフィックが ASA インターフェイスで終了することをデフォルトで許可するので、IKE または ESP (またはその他のタイプの VPN パケット) をアクセスルールで許可する必要はありません。このオプションをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセスルールは不要です。VPN トンネルは VPN セキュリティメカニズムを使用して正常に終端されたので、この機能によって、構成が簡略化され、セキュリティリスクを負うことなく、デバイスのパフォーマンスが最大化されます。(グループポリシーおよびユーザ単位の許可 ACL は、引き続きトラフィックに適用されます)。

このオプションをオフにすることにより、アクセスルールをローカル IP アドレスに適用することを強制的に適用できます。アクセスルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。
- [Permit communication between VPN peers connected to the same interface] : この機能をイネーブルまたはディセーブルにします。

同じインターフェイスを介して着信クライアント VPN トラフィックを暗号化せずに、または暗号化してリダイレクトすることもできます。同じインターフェイスを介して VPN トラフィックを暗号化せずに送信する場合は、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)。
- [Compression Settings] : 圧縮をイネーブルにする機能 (WebVPN および SSL VPN クライアント) を指定します。圧縮はデフォルトでイネーブルになっています。

最大 VPN セッション数の設定

VPN セッションまたは AnyConnect クライアント VPN セッションで許可される最大数を指定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Advanced] > [Maximum VPN Sessions] を選択します。

ステップ 2 [Maximum AnyConnect Sessions] フィールドにセッションの最大許容数を入力します。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 3 [Maximum Other VPN Sessions] フィールドで、許可する最大の VPN セッション数を入力します。これには、Cisco VPN クライアント (IPsec IKEv1) と LAN-to-LAN VPN セッションが含まれます。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 4 [適用 (Apply)] をクリックします。

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 AnyConnect 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 設定 \(259 ページ\)](#) 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、[内部グループ ポリシー、AnyConnect クライアント、デッドピア検出 \(100 ページ\)](#) を参照してください。

手順

ステップ 1 AnyConnect VPN 接続に対して DTLS オプションを指定します。

- a) [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] の [Access Interfaces] セクションに移動します。
- b) [Interface] テーブルの AnyConnect 接続に設定するインターフェイスの行で、インターフェイスでイネーブルにするプロトコルをオンにします。
 - [SSL Access / Allow Access] をオンにするかイネーブルにした場合、[Enable DTLS] はデフォルトでオンまたはイネーブルになります。
 - DTLS を無効にするには、[Enable DTLS] をオフにします。SSL VPN 接続は SSL VPN トンネルのみに接続します。
- c) [Port Settings] を選択し、**SSL ポート**を設定します。
 - [HTTPS Port] : HTTPS (ブラウザベース) SSL 接続用にイネーブルにするポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。

- [DTLS Port] : DTLS 接続用にイネーブルにする UDP ポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。

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) [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] に移動します。
- b) [Datagram Transport Layer Security (DTLS)] の [Inherit] (デフォルト)、[Enable]、または [Disable] を選択します。
- c) [DTLS Compression] の [Inherit] (デフォルト)、[Enable]、または [Disable] を選択し、DTLS の圧縮を設定します。

DNS サーバグループの設定

[Configuration] > [Remote Access VPN] > [DNS] ダイアログボックスでは、サーバグループ名、サーバ、タイムアウトの秒数、許容リトライ回数、およびドメイン名を含む、設定済みの DNS サーバがテーブルに表示されます。このダイアログボックスで、DNS サーバグループを追加、編集、または削除できます。

- [Add or Edit] : [Add or Edit DNS Server Group] ダイアログボックスが開きます。別の場所にあるヘルプ
- [Delete] : 選択した行をテーブルから削除します。確認されず、やり直しもできません。
- [DNS Server Group] : この接続の DNS サーバグループとして使用するサーバを選択します。デフォルトは DefaultDNS です。
- [Manage] : [Configure DNS Server Group] ダイアログボックスが開きます。

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、AnyConnect 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、AnyConnect、スマートトンネル、およびポート転送において、ユーザ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

ステップ 1 [Configuration] > [Remote Access VPN] > [Advanced] > [Crypto Engine] を選択します。

ステップ 2 [Accelerator Bias] ドロップダウンリストから、暗号アクセラレータプロセッサの割り当て方法を選択します。

(注) このフィールドは、機能がデバイスで使用可能な場合にだけ表示されます。

- [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)。これは、ASA 5500-X シリーズデバイスのデフォルトバイアスです。
- [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 AnyConnect 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。

ステップ 3 [Apply] をクリックします。

SSL VPN 接続用のクライアントアドレス指定

このダイアログボックスを使用して、グローバルクライアントアドレスの割り当てポリシーを指定し、インターフェイスに固有のアドレスプールを設定します。このダイアログボックスを使用して、インターフェイスに固有のアドレスプールを追加、編集、または削除することもできます。ダイアログボックス下部のテーブルには、設定されているインターフェイス固有のアドレスプールの一覧が表示されます。

- [Global Client Address Assignment Policy] : すべての IPsec 接続と SSL VPN Client 接続 (AnyConnect クライアント接続を含む) に影響するポリシーを設定します。ASA は、アドレスを見つけるまで、選択されたソースを順番に使用します。
 - [Use authentication server] : クライアントアドレスのソースとして、ASA が認証サーバの使用を試みるように指定します。
 - [Use DHCP] : クライアントアドレスのソースとして、ASA が DHCP の使用を試みるように指定します。
 - [Use address pool] : クライアントアドレスのソースとして、ASA がアドレスプールの使用を試みるように指定します。
- [Interface-Specific IPv4 Address Pools] : 設定されているインターフェイス固有のアドレスプールの一覧を表示します。
- [Interface-Specific IPv6 Address Pools] : 設定されているインターフェイス固有のアドレスプールの一覧を表示します。
- [Add] : [Assign Address Pools to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスおよび割り当てるアドレスプールを選択できます。

- [Edit] : インターフェイスとアドレス プールのフィールドに値が取り込まれた状態で、[Assign Address Pools to Interface] ダイアログボックスが開きます。
- [Delete] : 選択したインターフェイスに固有のアドレス プールを削除します。確認されず、やり直しもできません。

Assign Address Pools to Interface

このダイアログボックスを使用して、インターフェイスを選択し、そのインターフェイスにアドレス プールを 1 つ以上割り当てます。

- [Interface] : アドレス プールの割り当て先インターフェイスを選択します。デフォルトは DMZ です。
- [Address Pools] : 指定したインターフェイスに割り当てるアドレス プールを指定します。
- [Select] : [Select Address Pools] ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てるアドレス プールを 1 つ以上選択できます。選択内容は、[Assign Address Pools to Interface] ダイアログボックスの [Address Pools] フィールドに表示されます。

Select Address Pools

[Select Address Pools] ダイアログボックスには、クライアントアドレスの割り当てで選択可能なプール名、開始アドレスと終了アドレス、およびアドレスプールのサブネットマスクが表示され、リストのエントリを追加、編集、削除できます。

- [Add] : [Add IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、新しい IP アドレス プールを設定できます。
- [Edit] : [Edit IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、選択した IP アドレス プールを変更できます。
- [Delete] : 選択したアドレス プールを削除します。確認されず、やり直しもできません。
- [Assign] : インターフェイスに割り当てられているアドレス プール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。

Add or Edit an IP Address Pool

IP アドレス プールを設定または変更します。

- [Name] : IP アドレス プールに割り当てられている名前を指定します。
- [Starting IP Address] : プールの最初の IP アドレスを指定します。
- [Ending IP Address] : プールの最後の IP アドレスを指定します。
- [Subnet Mask] : プール内のアドレスに適用するサブネット マスクを選択します。

グループポリシー

グループポリシーは、ASA の内部（ローカル）または外部の RADIUS または LDAP サーバに格納されているユーザ指向の属性と値のペアのセットです。VPN 接続を確立する際に、グループポリシーによってクライアントに属性が割り当てられます。デフォルトでは、VPN ユーザにはグループポリシーが関連付けられません。グループポリシー情報は、VPN 接続プロファイル（トンネルグループ）およびユーザアカウントで使用されます。

ASA には、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。デフォルトグループパラメータは、すべてのグループおよびユーザに共通であると考えられるパラメータで、コンフィギュレーションタスクの効率化に役立ちます。新しいグループはこのデフォルトグループからパラメータを「継承」でき、ユーザは自身のグループまたはデフォルトグループからパラメータを「継承」できます。これらのパラメータは、グループおよびユーザを設定するときに上書きできます。

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。内部グループポリシーはローカルに保存され、外部グループは RADIUS サーバまたは LDAP サーバに外部で保存されます。

[Group Policy] ダイアログボックスで、次の種類のパラメータを設定します。

- 一般属性：名前、バナー、アドレスプール、プロトコル、フィルタリング、および接続の設定。
- サーバ：DNS および WINS サーバ、DHCP スコープ、およびデフォルトドメイン名。
- 詳細属性：スプリットトンネリング、IE ブラウザプロキシ、AnyConnect クライアント、および IPsec クライアント。

これらのパラメータを設定する前に、次の項目を設定する必要があります。

- アクセス時間 ([General] > [More Options] > [Access Hours]) 。
- フィルタ ([General] > [More Options] > [Filters]) 。
- IPsec セキュリティアソシエーション ([Configuration] > [Policy Management] > [Traffic Management] > [Security Associations]) 。
- フィルタリングおよびスプリットトンネリング用のネットワークリスト ([Configuration] > [Policy Management] > [Traffic Management] > [Network Lists]) 。
- ユーザ認証サーバと内部認証サーバ ([Configuration] > [System] > [Servers] > [Authentication]) 。

次のタイプのグループポリシーを設定できます。

- **外部グループポリシー (70 ページ)**：外部グループポリシーは、RADIUS または LDAP サーバを ASA に示し、内部グループポリシーに設定されているようなポリシー情報の大部分を取得できるようにします。外部グループポリシーは、ネットワーク（クライアント）アクセス VPN 接続、クライアントレス SSL VPN 接続、およびサイト間 VPN 接続に対して同じ方法で設定されます。

- [内部グループポリシー \(72 ページ\)](#) : これらの接続は、エンドポイントにインストールされている VPN クライアントによって開始されます。AnyConnect セキュア モビリティ クライアントおよび Cisco IPsec VPN クライアントは、VPN クライアントの使用例です。VPN クライアントが認証されると、オンサイトの場合、リモートユーザは企業ネットワークまたはアプリケーションにアクセスできます。リモートユーザと企業ネットワーク間のデータトラフィックは、暗号化によってインターネットを通過する際に保護されます。
- [AnyConnect クライアントの内部グループポリシー \(79 ページ\)](#)
- [クライアントレス SSL VPN の内部グループポリシー \(111 ページ\)](#) : これは、ブラウザベースの VPN アクセスとも呼ばれます。ASA のポータルページに正常にログインすると、リモートユーザは Web ページに表示されるリンクから企業ネットワークとアプリケーションにアクセスできます。リモートユーザと企業ネットワーク間のデータトラフィックは、SSL トンネルを通過する際に保護されます。
- [サイト間内部グループポリシー \(116 ページ\)](#)

[Group Policy] ペイン フィールド

ASDM の [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] ペインには、設定済みのグループポリシーが一覧表示されます。VPN グループポリシーを管理するための [Add]、[Edit]、および [Delete] ボタンを以下に示します。

- [Add] : ドロップダウンリストが表示され、内部または外部のグループポリシーを追加するかどうかを選択できます。単に [Add] をクリックする場合は、デフォルトにより内部グループポリシーを作成することになります。[Add] をクリックすると、[Add Internal Group Policy] ダイアログボックスまたは [Add External Group Policy] ダイアログボックスが開きます。これらのダイアログボックスを使用して、新しいグループポリシーを一覧に追加できます。このダイアログボックスには、3つのメニューセクションがあります。それぞれのメニュー項目をクリックすると、その項目のパラメータが表示されます。項目間を移動するとき、ASDM は設定を保持します。すべてのメニューセクションでパラメータの設定が終了したら、[Apply] または [Cancel] をクリックします。
- [Edit] : [Edit Group Policy] ダイアログボックスを表示します。このダイアログボックスを使用して、既存のグループポリシーを編集できます。
- [Delete] : AAA グループポリシーをリストから削除します。確認されず、やり直しもできません。
- [Assign] : 1つ以上の接続プロファイルにグループポリシーを割り当てることができます。
- [Name] : 現在設定されているグループポリシーの名前を一覧表示します。
- [Type] : 現在設定されている各グループポリシーのタイプを一覧表示します。
- [Tunneling Protocol] : 現在設定されている各グループポリシーが使用するトンネリングプロトコルを一覧表示します。
- [Connection Profiles/Users Assigned to] : このグループポリシーに関連付けられた ASA に直接設定された接続プロファイルとユーザを示します。

外部グループポリシー

外部グループポリシーは、外部サーバから認可および認証の属性値を取得します。このグループポリシーによって、ASA が属性を照会できる RADIUS または LDAP サーバグループを特定し、それらの属性を取得するときに使用するパスワードを指定します。

ASA での外部グループ名は、RADIUS サーバのユーザ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 サーバはクエリをユーザ 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 サーバ上のユーザ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と同じ RADIUS サーバに存在する場合、それらの間で名前を重複させることはできません。

外部サーバを使用するように ASA を設定する前に、適切な ASA 認可属性を指定してサーバを設定し、それらの属性のサブセットから個々のユーザに対する特定の許可を割り当てる必要があります。外部サーバを設定するには、「認可および認証用の外部サーバ」の説明に従ってください。

これらの RADIUS 設定には、ローカル認証の RADIUS、Active Directory/Kerberos Windows DC の RADIUS、NT/4.0 ドメインの RADIUS、LDAP の RADIUS が含まれます。

外部グループポリシーのフィールド

- [Name] : 追加または変更するグループポリシーを特定します。[Edit External Group Policy] の場合、このフィールドは表示専用です。
- [Server Group] : このポリシーの適用先として利用できるサーバグループを一覧表示します。
- [New] : 新しい RADIUS サーバグループまたは新しい LDAP サーバグループを作成するかどうかを選択できるダイアログボックスを開きます。どちらの場合も [Add AAA Server Group] ダイアログボックスが開きます。
- [Password] : このサーバグループポリシーのパスワードを指定します。

AAA サーバの作成および設定については、『Cisco ASA Series General Operations ASDM Configuration Guide』の「AAA Servers and Local Database」の章を参照してください。

AAA サーバによるパスワード管理

ASA は、RADIUS および LDAP プロトコルのパスワード管理をサポートしています。

「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。その他のパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。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。



- (注) 現在のところ MS-CHAP をサポートしていても、MS-CHAPv2 はサポートしていない RADIUS サーバもあります。この機能には MS-CHAPv2 が必要なため、ベンダーに確認してください。

ASA では、通常、LDAP による認証時または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPsec VPN クライアント
- IPsec IKEv2 クライアント
- クライアントレス SSL VPN

Kerberos/Active Directory (Windows パスワード) または NT 4.0 ドメインでは、パスワード管理はサポートされません。一部の RADIUS サーバ (Cisco ACS など) は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバとだけ通信しているように見えます。



(注) LDAP でパスワードを変更するには、市販の LDAP サーバ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。

AnyConnect でのパスワードのサポート

ASA では、AnyConnect の次のパスワード管理機能をサポートします。

- ユーザが接続しようとしたときのパスワード期限切れの通知。
- パスワードの期限が切れる前のパスワード期限切れのリマインダ。
- パスワード期限切れの無効化。ASA は AAA サーバからのパスワード期限切れの通知を無視し、ユーザの接続を許可します。

パスワード管理を設定すると、ASA は、リモートユーザがログインしようとしたときに、現在のパスワードの期限が切れていること、または期限切れが近づいていることを通知します。それから ASA は、ユーザ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、ユーザはその古いパスワードを使用してログインし続けて、後でパスワードを変更することができます。

AnyConnect クライアントはパスワードの変更を開始できず、AAA サーバからの変更要求に ASA を介して応答することしかできません。AAA サーバは、AD にプロキシする RADIUS サーバ、または LDAP サーバにする必要があります。

ASA は、次の条件下ではパスワード管理をサポートしません。

- ローカル (内部) 認証を使用する場合

- LDAP 認証を使用する場合
- RADIUS 認証のみを使用しており、ユーザが RADIUS サーバ データベースに存在する場合

パスワード期限切れの無効化を設定すると、ASA は AAA サーバからの `account-disabled` インジケータを無視するようになります。これは、セキュリティ上のリスクになる可能性があります。たとえば、管理者のパスワードを変更しないようにする場合があります。

パスワード管理をイネーブルにすると、ASA は AAA サーバに MS-CHAPv2 認証要求を送信します。

内部グループポリシー

内部グループポリシー、一般属性

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] ペインで、[Add or Edit Group Policy] ダイアログボックスを使用すると、追加または変更するグループポリシーのトンネリングプロトコル、フィルタ、接続設定、およびサーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルトグループポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

ASDM で [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] を選択して、内部グループポリシーの一般属性を設定します。次の属性は、SSL VPN セッションと IPsec セッションに適用されます。そのため、いくつかの属性は、1 つのタイプのセッションに表示され、他のタイプには表示されません。

- [Name] : このグループポリシーの名前を最大 64 文字で指定します (スペースの使用可)。Edit 機能の場合、このフィールドは読み取り専用です。
- [Banner] : ログイン時にユーザに対して表示するバナーテキストを指定します。長さは最大 4000 文字です。デフォルト値はありません。

IPsec VPN クライアントは、バナー用の完全な HTML をサポートしています。ただし、クライアントレスポータルおよび AnyConnect クライアントは部分的な HTML をサポートしています。バナーがリモートユーザに適切に表示されるようにするには、次のガイドラインに従います。

- IPsec クライアント ユーザの場合は、`\n` タグを使用します。
- AnyConnect クライアント ユーザの場合は、`
` タグを使用します。
- [SCEP forwarding URL] : CA のアドレス。クライアントプロファイルで SCEP プロキシを設定する場合に必要です。
- [Address Pools] : このグループポリシーで使用する 1 つ以上の IPv4 アドレスプールの名前を指定します。[Inherit] チェックボックスがオンの場合、グループポリシーはデフォルト

トグループポリシーで指定されている IPv4 アドレスプールを使用します。IPv4 アドレスプールを追加または編集する方法の詳細については、を参照してください。



(注) 内部グループポリシーで IPv4 と IPv6 両方のアドレスプールを指定できます。

[Select]—このボタンをアクティブにするには、[Inherit] チェックボックスをオフにします。[Select] をクリックして、[Address Pools] ダイアログボックスを開きます。このダイアログボックスには、クライアントアドレス割り当てで選択可能なアドレスプールのプール名、開始アドレスと終了アドレス、およびサブネットマスクが表示され、そのリストからエントリを選択、追加、編集、削除、および割り当てできます。

- [IPv6 Address Pools] : このグループポリシーで使用する 1 つ以上の IPv6 アドレスプールの名前を指定します。

[Select]—このボタンをアクティブにするには、[Inherit] チェックボックスをオフにします。[Select] をクリックすると、前述のような [Select Address Pools] ダイアログボックスが開きます。IPv6 アドレスプールを追加または編集する方法の詳細については、を参照してください。

- [More Options] : フィールドの右側にある下矢印をクリックすると、このグループポリシーのその他の設定可能なオプションが表示されます。
- [Tunneling Protocols] : このグループが使用できるトンネリングプロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。
 - [Clientless SSL VPN] : SSL/TLS による VPN の使用を指定します。この VPN では、ソフトウェアやハードウェアのクライアントは必要なく、Web ブラウザを使用して ASA へのセキュアなリモートアクセストンネルが確立されます。クライアントレス SSL VPN を使用すると、HTTPS インターネットサイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有 (Web 対応)、電子メール、およびその他の TCP ベースアプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
 - [SSL VPN Client] : Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して Mobile User Security (MUS) がサポートされるようにする必要があります。
 - [IPsec IKEv1] : IP セキュリティプロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site (ピアツーピア) 接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
 - [IPsec IKEv2] : AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェアアップデート、クライアントプロファイル、GUI のローカリゼーション (翻訳) とカ

スタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。

- [L2TP over IPsec] : 一部の一般的 PC やモバイル PC のオペレーティングシステムで提供される VPN クライアントを使用しているリモートユーザは、L2TP over IPSec によって、パブリック IP ネットワーク経由でセキュリティアプライアンスやプライベート企業ネットワークへのセキュアな接続を確立できます。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。セキュリティアプライアンスは、IPsec 転送モード用に設定する必要があります。
- [Filter] : IPv4 または IPv6 接続で使用するアクセスコントロールリストを指定するか、グループポリシーから値を継承するかどうかを指定します。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。フィルタおよびルールを設定するには、[Manage] をクリックします。
- [NAC Policy] : このグループポリシーに適用するネットワークアドミッションコントロールポリシーの名前を選択します。オプションの NAC ポリシーを各グループポリシーに割り当てることができます。デフォルト値は --None-- です。
- [Manage] : [Configure NAC Policy] ダイアログボックスが開きます。1 つ以上の NAC ポリシーを設定すると、[NAC Policy] 属性の横のドロップダウンリストに、設定した NAC ポリシー名がオプションとして表示されます。
- [Access Hours] : このユーザに適用される既存のアクセス時間ポリシーがある場合はその名前を選択するか、または新しいアクセス時間ポリシーを作成します。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [--Unrestricted--] です。[Manage] をクリックして、[Browse Time Range] ダイアログボックスを開きます。このダイアログボックスでは、時間範囲を追加、編集、または削除できます。
- [Simultaneous Logins] : このユーザに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザアクセスを禁止します。



(注) 最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

- [Restrict Access to VLAN] : (オプション) 「VLAN マッピング」とも呼ばれます。このパラメータにより、このグループポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。ASA は、このグループからのすべてのトラフィックを指定された VLAN に転送します。この属性を使用して VLAN をグループポリシーに割り当て、アクセスコントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウンリストには、デフォルト値 ([無制限 (Unrestricted)]) の他に、この ASA で設定されている VLAN だけが表示されます。



(注) この機能は、HTTP 接続の場合には有効ですが、FTP および CIFS 接続では使用できません。

- **[Connection Profile (Tunnel Group) Lock]** : このパラメータを使用すると、選択された接続プロファイル (トンネルグループ) を使用する VPN アクセスのみを許可し、別の接続ファイルを使用するアクセスを回避できます。デフォルトの継承値は [None] です。

- **Maximum Connect Time** : [Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザ接続時間を分単位で設定します。

ここで指定した時間が経過すると、システムは接続を終了します。最小値は1分、最大値は 35791394 分 (4000 年超) です。制限なしの接続時間を許可するには、[Unlimited] をオンにします (デフォルト)。

- **Idle Timeout** : [Inherit] チェックボックスをオフにした場合、このパラメータでアイドル時間を分単位で設定します。

この期間に接続で通信アクティビティがない場合、接続は終了します。最小時間は1分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。

- **[Security Group Tag (SGT)]** : このグループポリシーで接続する VPN ユーザに割り当てられる SGT タグの数値を入力します。

- **[On smart card removal]** : デフォルトのオプション [Disconnect] を選択した場合は、認証に使用されるスマートカードが取り外されると、クライアントは接続を切断します。接続の間、スマートカードをコンピュータに保持することをユーザに要求しない場合は、[Keep the connection] をクリックします。

スマートカードの取り外しに関する設定は、RSA スマートカードを使用する Microsoft Windows でのみ機能します。

- **Maximum Connection Time Alert Interval** : ユーザにメッセージを表示する、最大接続時間に達するまでの時間間隔。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、セッションアラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ~ 30 分のセッションアラート間隔を指定します。

- **Periodic Certificate Authentication Interval** : 証明書認証が定期的に再実行されるまでの時間間隔 (時間単位)。

[Inherit] チェックボックスがオフになっている場合、定期的な証明書検証の実行間隔を設定できます。範囲は 1 ~ 168 時間で、デフォルトは無効になっています。無制限の検証を許可するには、[Unlimited] をオンにします。

内部グループポリシーの設定、サーバ属性

[Group Policy]> [Servers] ウィンドウで、DNS サーバ、WINS サーバおよび DNS スコープを設定します。DNS および WINS サーバはフルトンネルクライアント (IPsec、AnyConnect、SVC、L2TP/IPsec) のみに適用され、名前解決に使用されます。DHCP スコープは、DHCP アドレス割り当てが設定されている場合に使用されます。

手順

ステップ 1 [Configuration]> [Remote Access VPN]> [Network (Client) Access]> [Group Policies]> [Add/Edit]> [Servers] を選択します。

ステップ 2 DefaultGroupPolicy を編集する場合を除き、[DNSサーバーの継承 (DNS Servers Inherit)] チェックボックスをオフにして、このグループで使用する DNS サーバの IPv4 または IPv6 アドレスを追加します。2つの IPv4 アドレスと2つの IPv6 アドレスを指定できます。

複数の DNS サーバを指定する場合、リモートアクセスクライアントは、このフィールドで指定された順序で DNS サーバを使用しようとします。

ここで行った変更は、ASDM のこのグループポリシーを使用しているクライアントの [Configuration]> [Remote Access VPN]> [DNS] ウィンドウで設定された DNS 設定より優先されます。

ステップ 3 [WINSサーバーの継承 (WINS Servers Inherit)] チェックボックスをオフにして、プライマリおよびセカンダリ WINS サーバの IP アドレスを入力します。最初に指定する IP アドレスがプライマリ WINS サーバの 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 サーバの IP アドレスです。

ステップ 4 [More Options] バーの二重矢印をクリックして、[More Options] エリアを展開します。

ステップ 5 [DHCPスコープの継承 (DHCP Scope Inherit)] をオフにして、DHCP スコープを定義します。

接続プロファイルのアドレスプールに DHCP サーバを設定した場合、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。

ステップ 6 デフォルトドメインが [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [DNS] ウィンドウで指定されていない場合は、[デフォルトドメイン (Default Domain)] フィールドで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 というドメイン名とトップレベルドメインを使用します。

ステップ 7 [OK] をクリックします。

ステップ 8 [適用 (Apply)] をクリックします。

内部グループポリシー、ブラウザ プロキシ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [Browser Proxy]

このダイアログボックスでは、Microsoft Internet Explorer の設定を再構成するためにクライアントにプッシュダウンされる属性を設定します。

- [Proxy Server Policy] : クライアント PC の Microsoft Internet Explorer ブラウザのプロキシアクション (「メソッド」) を設定します。
 - [Do not modify client proxy settings] : このクライアント PC の Internet Explorer の HTTP ブラウザ プロキシ サーバ設定を変更しません。
 - [Do not use proxy] : クライアント PC の Internet Explorer の HTTP プロキシ設定をディセーブルにします。
 - [Select proxy server settings from the following] : 選択内容に応じて、[Auto detect proxy]、[Use proxy server settings given below]、および [Use proxy auto configuration (PAC) given below] のチェックボックスをオンにします。
 - [Auto-detect proxy] : クライアント PC で、Internet Explorer の自動プロキシサーバ検出の使用をイネーブルにします。
 - [Use proxy server settings specified below] : [Proxy Server Name or IP Address] フィールドで設定された値を使用するように、Internet Explorer の HTTP プロキシ サーバ設定値を設定します。
 - [Use proxy auto configuration (PAC) given below] : [Proxy Auto Configuration (PAC)] フィールドで指定したファイルを、自動コンフィギュレーション属性のソースとして使用するように指定します。
- [Proxy Server Settings] : Microsoft Internet Explorer を使用して、Microsoft クライアントのプロキシサーバパラメータを設定します。
 - [Server Address and Port] : このクライアント PC で適用される、Microsoft Internet Explorer サーバの IP アドレスまたは名前、およびポートを指定します。

- [Bypass Proxy Server for Local Addresses] : クライアント PC での Microsoft Internet Explorer ブラウザ プロキシ ローカルバイパス設定値を設定します。[Yes] を選択するとローカルバイパスがイネーブルになり、[No] を選択するとローカルバイパスがディセーブルになります。
- [Exception List] : プロキシ サーバ アクセスから除外するサーバの名前と IP アドレスを一覧表示します。プロキシサーバ経由のアクセスを行わないアドレスのリストを入力します。このリストは、[Internet Explorer の Proxy Settings] ダイアログボックスにある [Exceptions] リストに相当します。
- [Proxy Auto Configuration Settings] : PAC URL は自動設定ファイルの URL を指定します。このファイルには、ブラウザがプロキシ情報を探せる場所が記述されています。プロキシ自動コンフィギュレーション (PAC) 機能を使用する場合、リモートユーザは、Cisco AnyConnect VPN クライアントを使用する必要があります。

多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティングする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サードパーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

また、大規模ネットワークを構築している企業では、複数のプロキシサーバを設定し、一時的な状態に基づいてユーザがその中からプロキシサーバを選択できるようにすることが必要になる場合があります。pac ファイルを使用すると、管理者は数多くのプロキシからのプロキシを社内のすべてのクライアントコンピュータに使用するかを決定する単一のスクリプト ファイルを作成できます。

次に、PAC ファイルを使用する例をいくつか示します。

- ロード バランシングのためリストからプロキシをランダムに選択します。
- サーバのメンテナンススケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシサーバを指定します。
- ローカルサブネットを元に、ローミングユーザ用に最も近いプロキシを指定します。

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション (.pac) ファイルを作成できます。pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシサーバを指定するロジックを含む JavaScript ファイルです。[PAC URL] フィールドを使用して、pac ファイルの取得元 URL を指定します。ブラウザは、pac ファイルを使用してプロキシ設定を判断します。

- Proxy Lockdown

- [Allow Proxy Lockdown for Client System] : この機能をイネーブルにすると、AnyConnect VPN セッションの間、Microsoft Internet Explorer の [Connections] タブが非表示になります。また、Windows 10 バージョン 1703 (以降) では、この機能を有効にすると、AnyConnect VPN セッションの間、設定アプリのシステムプロキシタブも非表示になります。この機能を無効にしても、Microsoft Internet Explorer の [Connections] タブと設定アプリのプロキシタブの表示は変わりません。これらのタブのデフォルト設定は、ユーザのレジストリ設定に応じて表示または非表示になります。



(注) AnyConnect VPN セッションの間、設定アプリのシステム プロキシ タブを非表示にするには、AnyConnect バージョン 4.7.03052 以降が必要です。

AnyConnect クライアントの内部グループ ポリシー

内部グループ ポリシー、詳細、AnyConnect クライアント

- [Keep Installer on Client System] : リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的な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 ユーザの接続時間が短縮されます。
- [Compression] : 圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティ アプライアンスとクライアント間の通信パフォーマンスが向上します。
- [Datagram TLS] : Datagram Transport Layer Security により、一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、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を改善します。
- [Ignore Don't Defrag (DF) Bit] : この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバに対する使用などがあります。
- [Client Bypass Protocol] : クライアントプロトコルバイパス機能を使用すると、ASA が IPv6 トラフィックだけを予期しているときの AnyConnect クライアントによる 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。

AnyConnect 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 AnyConnect 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、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、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てください。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。

- [FQDN of This Device] : この情報は、VPN セッションの再確立で使用される ASA IP アドレスを解決するために、ネットワークローミングの後でクライアントに使用されます。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)。



(注) AnyConnect 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、AnyConnect 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。

- [MTU] : SSL 接続の MTU サイズを調整します。256 ~ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Keepalive Messages] : [Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブメッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通じた接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモートユーザが、Microsoft Outlook や Microsoft Internet Explorer な

どのソケットベースのアプリケーションを実際に実行していないときでも、クライアントが切断と再接続を行わないことが保証されます。

- [Optional Client Modules to Download] : ダウンロード時間を短縮するために、AnyConnect クライアントは、サポートしている各機能に必要なモジュールだけを (ASA から) ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。AnyConnect クライアントには、次のモジュールが含まれています (一部の旧バージョンではモジュールの数が少なくなります)。
 - AnyConnect DART : トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システム ログのスナップショットおよびその他の診断情報がキャプチャされ、.zip ファイルがデスクトップに作成されます。
 - AnyConnect ネットワーク アクセス マネージャ : 以前は Cisco Secure Services Client と呼ばれていました。このモジュールは、有線とワイヤレスの両方のネットワークにアクセスするための 802.1X (レイヤ 2) とデバイス認証を備えています。
 - AnyConnect SBL : Start Before Logon (SBL) では、Windows のログイン ダイアログ ボックスが表示される前に AnyConnect を開始することにより、ユーザが Windows にログインする前に VPN 接続を介してユーザを企業インフラに強制的に接続します。
 - AnyConnect Web セキュリティ モジュール : 以前は ScanSafe Hostscan と呼ばれていました。このモジュールは、AnyConnect に統合されています。また、Web ページの要素を分解して、同時に各要素を分析できるようにします。その後、定義されているセキュリティ ポリシーに基づいて、受け入れ可能なコンテンツを許可し、悪意があるコンテンツや許容できないコンテンツをドロップします。
 - AnyConnect テレメトリ モジュール : 悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティ アプライアンス (WSA) に送信します。WSA では、このデータを使用して、URL のフィルタリング ルールを改善します。



(注) テレメトリ モジュールは AnyConnect バージョン 4.0 ではサポートされません。

- ASA ポスチャ モジュール : 以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。このポスチャ モジュールは AnyConnect に統合され、これにより AnyConnect は、ASA へのリモート アクセス接続を確立する前にポスチャ アセスメントのクレデンシャルを収集できるようになります。
- ISE ポスチャ : OPSWAT v3 ライブラリを使用してポスチャ チェックを実行し、エンドポイントの適合性を評価します。その後、エンドポイントが適合するまでネットワーク アクセスを制限したり、ローカル ユーザの権限を強化したりできます。
- AMP イネーブラ : エンドポイント向けの高度なマルウェア防御 (AMP) を導入する手段として使用されます。社内でローカルにホストされているサーバからエンドポイントのサブセットに AMP for Endpoints ソフトウェアをプッシュし、既存のユーザベースに AMP サービスをインストールします。

- ネットワーク可視性モジュール：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。NVM（ネットワーク可視性モジュール）は、エンドポイントのテレメトリを収集して、フローデータとファイルレピュテーションを syslog に記録し、さらに、ファイルの分析と UI インターフェイスの提供を行うコレクタ（サードパーティベンダー）にもフロー レコードをエクスポートします。
- Umbrella Roaming Security モジュール：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。Cisco Umbrella Roaming と OpenDNS Umbrella サービスのいずれかに対するサブスクリプションを提供し、Intelligent Proxy および IP レイヤ適用機能を追加します。Umbrella Security Roaming プロファイルは、対応するサービスと各展開を関連付けて、対応する保護レベルを自動的に有効にします（コンテンツフィルタリング、複数のポリシー、強力なレポート、Active Directory 統合、または基本的な DNS レイヤセキュリティ）。
- [Always-On VPN]：AnyConnect サービス プロファイルの常時接続 VPN フラグ設定をディセーブルにするか、または AnyConnect サービス プロファイル設定を使用する必要があるかを決定します。常時接続 VPN 機能により、ユーザがコンピュータにログオンすると、AnyConnect は VPN セッションを自動的に確立します。VPN セッションは、ユーザがコンピュータからログオフするまで維持されます。物理的な接続が失われてもセッションは維持され、AnyConnect は、適応型セキュリティ アプライアンスとの物理的な接続の再確立を絶えず試行し、VPN セッションを再開します。

常時接続 VPN によって、企業ポリシーを適用して、セキュリティ脅威からデバイスを保護できます。常時接続 VPN を使用して、エンドポイントが信頼ネットワーク内ではない場合にいつでも AnyConnect が VPN セッションを確立したことを確認できます。イネーブルにすると、接続が存在しない場合のネットワーク接続の管理方法を決定するポリシーが設定されます。



(注) 常時接続 VPN には、AnyConnect セキュア モビリティ機能をサポートする AnyConnect リリースが必要です。

- [Client Profiles to Download]：プロファイルはコンフィギュレーションパラメータのグループであり、AnyConnect クライアントで VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク可視性モジュール、および Umbrella Roaming Security モジュールの設定に使用されます。[Add] をクリックして [Select AnyConnect Client Profiles] ウィンドウを起動すると、以前グループ ポリシー用に作成されたプロファイルを指定できます。

AnyConnect トラフィックに対するスプリット トンネリングの設定

スプリット トンネリングは、一部の AnyConnect ネットワーク トラフィックを VPN トンネルに誘導して通過させ（暗号化）、他のネットワーク トラフィックを VPN トンネルの外に誘導します（非暗号化、つまり「クリア テキストの状態」）。

スプリット トンネリングを設定するには、スプリット トンネリング ポリシーを作成し、そのポリシーにアクセス コントロール リストを設定し、グループ ポリシーにスプリット トンネル ポリシーを追加します。グループ ポリシーをクライアントに送信する際に、クライアントはスプリット トンネリング ポリシーの ACL を使用してどこにネットワーク トラフィックを送信するかを決定します。



(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。

Windows クライアントでは、最初に ASA からのファイアウォール ルールが評価され、次にクライアントのファイアウォール ルールが評価されます。Mac OS X では、クライアントのファイアウォール ルールおよびフィルタ ルールは使用されません。Linux システムの AnyConnect バージョン 3.1.05149 以降では、**circumvent-host-filtering** という名前のカスタム属性をグループ プロファイルに追加して **true** に設定することで、クライアントのファイアウォール ルールおよびフィルタ ルールを評価するように AnyConnect を設定できます。

アクセス リストを作成する場合：

- アクセス コントロール リストには IPv4 および IPv6 両方のアドレスを指定できます。
- 標準 ACL を使用すると、1 つのアドレスまたはネットワークのみが使用されます。
- 拡張 ACL を使用すると、ソース ネットワークがスプリット トンネリング ネットワークになります。この場合、宛先ネットワークは無視されます。
- **any** が設定されたアクセス リストや、**split include** または **split exclude** が 0.0.0.0/0.0.0.0 または ::/0 に設定されたアクセス リストは、クライアントに送信されません。すべてのトラフィックをトンネル経由で送信するには、スプリット トンネルの **Policy** に対して **Tunnel All Networks** を選択します。
- アドレス 0.0.0.0/255.255.255.255 または ::/128 は、スプリット トンネル ポリシーが **Exclude Network List Below** の場合にのみクライアントに送信されます。この設定は、トンネル トラフィックがローカル サブネット宛でないことをクライアントに通知します。
- AnyConnect では、スプリット トンネリング ポリシーで指定されたすべてのサイト、および ASA によって割り当てられた IP アドレスと同じサブネット内にあるすべてのサイトにトラフィックが渡されます。たとえば、ASA によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイント デバイスは、スプリット トンネリング ポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。そのため、割り当てられた IP アドレスが、期待されるローカル サブネットを適切に参照するように、ネットマスクを使用します。

始める前に

- 適切な ACE でアクセス リストを作成する必要があります。

- スプリットトンネルポリシーを IPv4 ネットワーク用と IPv6 ネットワーク用に作成した場合は、指定したネットワークリストが両方のプロトコルで使用されます。このため、ネットワークリストには、IPv4 および IPv6 の両方のトラフィックのアクセスコントロールエントリ (ACE) が含まれている必要があります。これらの ACL を作成していない場合は、一般的操作用コンフィギュレーションガイドを参照してください。

次の手順では、フィールドの隣に [Inherit] チェックボックスがあるすべてのケースで、[Inherit] チェックボックスがオンのままの場合、設定しているグループポリシーは、そのフィールドについて、デフォルトグループポリシーと同じ値を使用することを意味します。[Inherit] チェックボックスをオフにすると、グループポリシーに固有の新しい値を指定できます。

手順

-
- ステップ 1** ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] に移動します。
- ステップ 2** [Add] をクリックして新しいグループポリシーを追加するか、既存のグループポリシーを選択して [Edit] をクリックします。
- ステップ 3** [Advanced] > [Split Tunneling] を選択します。
- ステップ 4** [DNS Names] フィールドに、トンネルを介して AnyConnect で解決するドメイン名を入力します。これらの名前は、プライベートネットワーク上のホストに対応します。split-include トンネリングが設定されている場合は、指定された DNS サーバがネットワークリストに含まれている必要があります。フィールドには、完全修飾ドメイン名、IPv4 アドレス、または IPv6 アドレスを入力できます。
- ステップ 5** スプリットトンネリングをディセーブルにするには、[Yes] をクリックして [Send All DNS Lookups Through Tunnel] をイネーブルにします。このオプションを設定すると、DNS トラフィックが物理アダプタに漏れず、クリアテキストで送信されるトラフィックが拒否されます。DNS 解決に失敗すると、アドレスは未解決のまま残ります。AnyConnect クライアントは、VPN 外のアドレスを解決しようとはしません。
- スプリットトンネリングをイネーブルにするには、[No] を選択します (デフォルト)。この設定では、クライアントはスプリットトンネルポリシーに従ってトンネルを介して DNS クエリを送信します
- ステップ 6** スプリットトンネリングを設定するには、[Inherit] チェックボックスをオフにして、スプリットトンネリングポリシーを選択します。[Inherit] チェックボックスをオフにしない場合、グループポリシーでは、デフォルトのグループポリシー **DfltGrpPolicy** で定義されたスプリットトンネリング設定が使用されます。デフォルトグループポリシーのスプリットトンネリングポリシーのデフォルト設定は [Tunnel All Networks] です。

スプリットトンネリングポリシーを定義するには、ドロップダウン [Policy] および [IPv6 Policy] から選択します。[Policy] フィールドでは、IPv4 ネットワークトラフィックのスプリットトンネリングポリシーを定義します。[IPv6 Policy] フィールドでは、IPv6 ネットワークトラフィックのスプリットトンネリングポリシーを選択します。そうした違い以外は、これらのフィールドの目的は同じです。

[Inherit] チェックボックスをオフにした場合は、次のいずれかのポリシー オプションを選択できます。

- [Exclude Network List Below] : クリアテキストで送信されるトラフィックの宛先ネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。
- [Tunnel Network List Below] : [Network List] で指定されたネットワーク間のすべてのトラフィックがトンネリングされます。インクルード ネットワーク リスト内のアドレスへのトラフィックがトンネリングされます。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ードリストも指定できます。これらの除外されたサブネットはトンネリングされず、インクルードリストの残りのネットワークはトンネリングされます。インクルードリストのサブネットではないエクスクルー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。Linux の場合、サブネットの除外をサポートするには、グループ ポリシーにカスタム属性を追加する必要があります。

次に例を示します。

#	Enabled	Source	User	Security Group	Destination	Security Group	Service	Action
TunnelExclude								
1	<input checked="" type="checkbox"/>	10.10.10.0/24			any		IP ip	Deny
2	<input checked="" type="checkbox"/>	10.0.0.0/8			any		IP ip	Permit

- (注) Split-Include ネットワークがローカル サブネットの完全一致 (192.168.1.0/24 など) の場合、対応するトラフィックはトンネリングされています。Split-Include ネットワークがローカル サブネットのスーパーセット (192.168.0.0/16 など) の場合、対応するトラフィックは、ローカルサブネットを除き、トンネリングされています。ローカルサブネットトラフィックもトンネリングするには、一致する Split-Include ネットワーク (192.168.1.0/24 および 192.168.0.0/16 の両方を Split-Include ネットワークとして指定) を追加する必要があります。

Split-Include ネットワークが無効 (0.0.0.0/0.0.0.0 など) の場合、スプリット トンネリングはディセーブルになります (すべてのトラフィックがトンネリングされません)。

- [Tunnel All Networks] : このポリシーは、すべてのトラフィックがトンネリングされるように指定します。この指定では、実質的にスプリット トンネリングは無効になります。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークに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。

ステップ 7 [Network List] フィールドで、スプリット トンネリング ポリシーを適用するアクセス コントロール リストを選択します[Inherit] チェックボックスがオンの場合、グループ ポリシーはデフォルト グループ ポリシーで指定されているネットワーク リストを使用します。

[Manage] コマンドボタンを選択して[ACL Manager] ダイアログボックスを開きます。このボックスでは、ネットワーク リストとして使用するアクセスコントロールリストを設定できます。ネットワーク リストを作成または編集する方法の詳細については、一般的操作用コンフィギュレーション ガイドを参照してください。

拡張 ACL リストには IPv4 アドレスと IPv6 アドレスの両方を含めることができます。

ステップ 8 [Intercept DHCP Configuration Message from Microsoft Clients] は DHCP 代行受信に固有の追加パラメータを示します。DHCP 代行受信によって、Microsoft 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。

- [Intercept] : DHCP 代行受信を許可するかどうかを指定します。[Inherit] を選択しない場合、デフォルト設定は [No] です。
- [Subnet Mask] : 使用するサブネット マスクを選択します。

ステップ 9 [OK] をクリックします。

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 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] 画面を参照します。

ステップ 2 [Add] をクリックし、dynamic-split-exclude-domains を属性タイプとして入力し、説明を入力します。

ステップ 3 この新しい属性をクリックして適用したら、UI 画面上部にある [AnyConnect custom attribute names] リンクをクリックします。

ステップ 4 VPN トンネル外部から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、対応するカスタム属性名を追加します。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。[AnyConnect Custom Attribute Names] 画面の [Value] 部分で、カンマ文字でドメインを区切るカンマ区切り値 (CSV) 形式を使用し

てこれらのドメインを定義します。AnyConnect は、区切り文字を除いて最初の 5000 文字のみを考慮します（約 300 個の通常のサイズのドメイン名）。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。

ステップ 5 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を参照し、ダイナミック スプリット除外トンネリング属性を特定のグループ ポリシーに付加します。

ステップ 6 新しいグループポリシーを作成するか、[Edit] をクリックして既存のグループポリシーを管理することができます。

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、実行されません。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。

ダイナミック スプリット除外トンネリングの設定

ASDM を使用してダイナミック スプリット除外トンネリングを有効にするには、次の設定手順を実行します。ダイナミック スプリット除外ドメインとインクルードドメインの両方が定義されている場合は、ドメイン名の一致による拡張ダイナミック スプリット除外トンネリングが有効になります。たとえば、管理者は example.com へのトラフィックを www.example.com 以外はすべて除外するように設定できます。Example.com はダイナミック スプリット除外ドメインであり、www.example.com はダイナミック スプリット インクルードドメインです。



(注) ダイナミック スプリット除外トンネリングを使用するには、AnyConnect リリース 4.5 (以降) が必要です。また、AnyConnect リリース 4.6 (以降) で、両方のドメインが設定されている場合の拡張ダイナミック スプリット インクルードとスプリット除外のための改善が加えられました。ダイナミック スプリット除外は tunnel-all 設定、split-exclude 設定、および split-include 設定に適用されます。

始める前に

AnyConnect の要件については、「ダイナミック スプリット トンネリング」の項を参照してください。

手順

-
- ステップ 1** [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] 画面を参照します。
- ステップ 2** [Add] をクリックし、dynamic-split-exclude-domains を属性タイプとして入力し、説明を入力します。
- ステップ 3** この新しい属性をクリックして適用したら、UI 画面上部にある [AnyConnect custom attribute names] リンクをクリックします。
- ステップ 4** VPN トンネル外部から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、対応するカスタム属性名を追加します。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。[AnyConnect Custom Attribute Names] 画面の [Value] 部分で、カンマ文字でドメインを区切るカンマ区切り値 (CSV) 形式を使用してこれらのドメインを定義します。AnyConnect は、区切り文字を除いて最初の 5000 文字のみを考慮します (約 300 個の通常のサイズのドメイン名)。その制限を超えるドメイン名は無視されます。
- カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。
- ステップ 5** [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を参照し、ダイナミック スプリット除外トンネリング属性を特定のグループ ポリシーに付加します。
- ステップ 6** 新しいグループポリシーを作成するか、[Edit] をクリックして既存のグループポリシーを管理することができます。
- ステップ 7** 左側のメニューで、[Advanced] > [AnyConnect Client] > [Custom Attributes] をクリックし、ドロップダウンから属性タイプを選択します。
-

ダイナミック スプリット インクルード トンネリングの設定

ASDM を使用してダイナミック スプリット インクルード トンネリングを有効にするには、次の設定手順を実行します。ダイナミック スプリット除外ドメインとインクルードドメインの両方が定義されている場合は、ドメイン名の一致による拡張ダイナミック スプリット インクルード トンネリングが有効になります。たとえば、管理者は domain.com へのトラフィックを www.domain.com 以外はすべて含まれるように設定できます。Domain.com はダイナミック スプリット インクルードドメインであり、www.domain.com はダイナミック スプリット除外ドメインです。



- (注) AnyConnect リリース 4.6 (以降) があり、ダイナミック スプリット インクルード トンネリングを使用する必要があります。また、AnyConnect リリース 4.6 (以降) で、両方のドメインが設定されている場合の拡張ダイナミック スプリット インクルードとスプリット除外のための改善が加えられました。ダイナミック スプリット インクルードは split-include 設定にのみ適用されます。
-

始める前に

AnyConnect の要件については、「ダイナミック スプリット トンネリング」の項を参照してください。

手順

- ステップ 1 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes]** 画面を参照します。
- ステップ 2 **[Add]** をクリックし、属性タイプとして `dynamic-split-include-domains` と入力し、説明を入力します。
- ステップ 3 この新しい属性をクリックして適用したら、UI 画面上部にある **[AnyConnect custom attribute names]** リンクをクリックします。
- ステップ 4 VPN トンネル外部から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、対応するカスタム属性名を追加します。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。 **[AnyConnect Custom Attribute Names]** 画面の **[Value]** 部分で、カンマ文字でドメインを区切るカンマ区切り値 (CSV) 形式を使用してこれらのドメインを定義します。AnyConnect は、区切り文字を除いて最初の 5000 文字のみを考慮します (約 300 個の通常のサイズのドメイン名)。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。
- ステップ 5 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies]** を参照して、ダイナミック スプリット インクルード トンネリング 属性を特定のグループ ポリシーに追加します。
- ステップ 6 新しいグループ ポリシーを作成するか、**[Edit]** をクリックして既存のグループ ポリシーを管理することができます。
- ステップ 7 左側のメニューで、**[Advanced] > [AnyConnect Client] > [Custom Attributes]** をクリックし、ドロップダウンから属性タイプを選択します。

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 AnyConnect Secure Mobility 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 トンネルグループの認証方法は、**[Configuration] > [Remote Access] > [Network (Client) Access] > [AnyConnect Connection Profiles] > [Add/Edit]** に移動し、**[Authentication]** の下の **[Method]** ドロップダウンメニューから選択して **[certificate only]** として設定する必要があります。
 - ステップ 2 次に、同じウィンドウで、**[Advanced] > [Group Alias/Group URL]** を選択し、管理 VPN プロファイルで指定するグループ URL を追加します。
 - ステップ 3 このトンネルグループのグループポリシーには、トンネルグループで設定されたアドレスプールを使用するすべての IP プロトコルに対してスクリプト包含トンネリングが設定されている必要があります。**[Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Edit] > [Advanced] > [Split Tunneling]** から **[Tunnel Network List Below]** を選択します。
 - ステップ 4 （オプション）ユーザが開始したネットワーク通信に影響しないように（管理 VPN トンネルは透過的であるため）スプリット包含トンネリングの設定がデフォルトで必要です。この動作をオーバーライドするには、管理トンネル接続で使用されているグループポリシーにカスタム属性を設定します：[AnyConnect カスタム属性（186 ページ）](#)。
両方の IP プロトコルに対するトンネルグループでアドレスプールが設定されていない場合、グループポリシーで **[Client Bypass Protocol]** をイネーブルにし、アドレスプールのない IP プロトコルと一致するトラフィックが管理 VPN トンネルで中断されないようにする必要があります。
 - ステップ 5 プロファイルを作成し、プロファイルの使用の管理 VPN トンネルを選択します：[AnyConnect クライアントプロファイルの設定（168 ページ）](#)。
-

サブネットの除外をサポートするための Linux の設定

スプリットトンネリング用に **[Tunnel Network List Below]** を設定した場合、Linux ではサブネットの除外をサポートするために追加の設定が必要になります。circumvent-host-filtering という名前のカスタム属性を作成して true に設定し、スプリットトンネリング用に設定されたグループポリシーに関連付ける必要があります。

手順

-
- ステップ 1 ASDM に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] に移動します。
 - ステップ 2 [Add] をクリックし、**circumvent-host-filtering** という名前のカスタム属性を作成して、その値を **true** に設定します。
 - ステップ 3 クライアントファイアウォールに対して使用予定のグループポリシーを編集し、[Advanced] > [AnyConnect Client] > [Custom Attributes] に移動します。
 - ステップ 4 作成したカスタム属性 **circumvent-host-filtering** をスプリット トンネリングに使用するグループポリシーに追加します。
-

内部グループポリシー、AnyConnect クライアント属性

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] には、このグループポリシーで設定可能な AnyConnect クライアントの属性が表示されます。

- [Keep Installer on Client System] : リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的な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 ユーザの接続時間が短縮されます。



(注) [Keep Installer on Client System] は、AnyConnect クライアントのバージョン 2.5 以降でサポートされていません。

- [Datagram Transport Layer Security (DTLS)] : 一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、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を改善します。
- [DTLS Compression] : DTLS における圧縮を設定します。
- [SSL Compression] : SSL/TLS における圧縮を設定します。
- [Ignore Don't Defrag (DF) Bit] : この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバに対する使用などがあります。
- [Client Bypass Protocol] : クライアントプロトコルバイパスでは、ASA が IPv6 トラフィックだけを予期しているときの AnyConnect クライアントによる 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します。

AnyConnect クライアントが ASA に VPN 接続するとき、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。クライアントバイパスプロトコルでは、ASA が IP アドレスを割り当てなかったトラフィックをドロップするか、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決定します。

たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、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てください。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。

- [FQDN of This Device] : この情報は、VPN セッションの再確立で使用される ASA IP アドレスを解決するために、ネットワークローミングの後でクライアントに使用されます。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)。



(注) AnyConnect 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、AnyConnect 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。

- [MTU] : SSL 接続の MTU サイズを調整します。256 ~ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Keepalive Messages] : [Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブメッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通じた接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモートユーザが、Microsoft Outlook や Microsoft Internet Explorer な

どのソケットベースのアプリケーションを実際に実行していないときでも、クライアントが切断と再接続を行わないことが保証されます。

- [Optional Client Modules to Download] : ダウンロード時間を短縮するために、AnyConnect クライアントは、サポートしている各機能に必要なモジュールだけを (ASA から) ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。AnyConnect クライアントのバージョン 4.0 には、次のモジュールが含まれています (旧バージョンではモジュールの数が少なくなります)。
 - AnyConnect DART : トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システム ログのスナップショットおよびその他の診断情報がキャプチャされ、.zip ファイルがデスクトップに作成されます。
 - AnyConnect ネットワーク アクセス マネージャ : 以前は Cisco Secure Services Client と呼ばれていました。このモジュールは、有線とワイヤレスの両方のネットワークにアクセスするための 802.1X (レイヤ 2) とデバイス認証を備えています。
 - AnyConnect SBL : Start Before Logon (SBL) では、Windows のログイン ダイアログ ボックスが表示される前に AnyConnect を開始することにより、ユーザが Windows にログインする前に VPN 接続を介してユーザを企業インフラに強制的に接続します。
 - AnyConnect Web セキュリティ モジュール : 以前は ScanSafe Hostscan と呼ばれていました。このモジュールは、AnyConnect に統合されています。また、Web ページの要素を分解して、同時に各要素を分析できるようにします。その後、定義されているセキュリティ ポリシーに基づいて、受け入れ可能なコンテンツを許可し、悪意があるコンテンツや許容できないコンテンツをドロップします。
 - AnyConnect テレメトリ モジュール : 悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティ アプライアンス (WSA) に送信します。WSA では、このデータを使用して、URL のフィルタリング ルールを改善します。



(注) テレメトリは AnyConnect 4.0 ではサポートされません。

- ASA ポスチャ モジュール : 以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。このポスチャ モジュールは AnyConnect に統合され、これにより AnyConnect は、ASA へのリモート アクセス 接続を確立する前にポスチャ アセスメントのクレデンシャルを収集できるようになります。
- ISE ポスチャ : OPSWAT v3 ライブラリを使用してポスチャ チェックを実行し、エンドポイントの適合性を評価します。その後、エンドポイントが適合するまでネットワーク アクセスを制限したり、ローカル ユーザの権限を強化したりできます。
- AMP イネーブラ : エンドポイント向けの高度なマルウェア防御 (AMP) を導入する手段として使用されます。社内でローカルにホストされているサーバからエンドポイントのサブセットに AMP for Endpoints ソフトウェアをプッシュし、既存のユーザベースに AMP サービスをインストールします。

- ネットワーク可視性モジュール：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。NVM（ネットワーク可視性モジュール）は、エンドポイントのテレメトリを収集して、フローデータとファイルレピュテーションをsyslogに記録し、さらに、ファイルの分析とUIインターフェイスの提供を行うコレクタ（サードパーティベンダー）にもフローレコードをエクスポートします。
- Umbrella Roaming Security モジュール：アクティブなVPNがないときにDNSレイヤセキュリティを提供します。Cisco Umbrella Roaming と OpenDNS Umbrella サービスのいずれかに対するサブスクリプションを提供し、Intelligent Proxy およびIPレイヤ適用機能を追加します。Umbrella Security Roaming プロファイルは、対応するサービスと各展開を関連付けて、対応する保護レベルを自動的に有効にします（コンテンツフィルタリング、複数のポリシー、強力なレポート、Active Directory 統合、または基本的なDNSレイヤセキュリティ）。
- [Always-On VPN]：AnyConnect サービスプロファイルの常時接続VPNフラグ設定をディセーブルにするか、またはAnyConnect サービスプロファイル設定を使用する必要があるかを決定します。常時接続VPN機能により、ユーザがコンピュータにログオンすると、AnyConnectはVPNセッションを自動的に確立します。VPNセッションは、ユーザがコンピュータからログオフするまで維持されます。物理的な接続が失われてもセッションは維持され、AnyConnectは、適応型セキュリティアプライアンスとの物理的な接続の再確立を絶えず試行し、VPNセッションを再開します。

常時接続VPNによって、企業ポリシーを適用して、セキュリティ脅威からデバイスを保護できます。常時接続VPNを使用して、エンドポイントが信頼ネットワーク内ではない場合にいつでもAnyConnectがVPNセッションを確立したことを確認できます。イネーブルにすると、接続が存在しない場合のネットワーク接続の管理方法を決定するポリシーが設定されます。



(注) 常時接続VPNには、AnyConnectセキュアモビリティ機能をサポートするAnyConnectリリースが必要です。

- [Client Profiles to Download]：プロファイルはコンフィギュレーションパラメータのグループであり、AnyConnectクライアントでVPN、ネットワークアクセスマネージャ、Webセキュリティ、ISEポスチャ、AMPイネーブラ、ネットワーク可視性モジュール、およびUmbrella Roaming Securityモジュールの設定に使用されます。[Add]をクリックして[Select AnyConnect Client Profiles]ウィンドウを起動すると、グループポリシー用に以前に作成されたプロファイルを指定できます。

内部グループポリシー、AnyConnect ログイン設定

内部グループポリシーの **Advanced > AnyConnect Client > Login Setting** ペインでは、リモートユーザにAnyConnectクライアントのダウンロードを求めるプロンプトを表示したり、クライアントレスSSLVPNのポータルページにダイレクト接続するようにASAを設定できます。

- [Post Login Setting] : ユーザにプロンプトを表示して、デフォルトのポスト ログイン選択を実行するためのタイムアウトを設定する場合に選択します。
- [Default Post Login Selection] : ログイン後に実行するアクションを選択します。

クライアント ファイアウォールによる VPN でのローカル デバイス サポートの有効化

内部グループ ポリシーの [Advanced] > [AnyConnect Client] > [Client Firewall] ペインでは、クライアントでのパブリック ネットワークとプライベート ネットワークの処理に影響するクライアント システムのファイアウォールに送信するルールを設定できます。

リモートユーザが ASA に接続すると、すべてのトラフィックがその VPN 接続を介してトンネリングされるため、ユーザはローカル ネットワーク上のリソースにアクセスできなくなります。こうしたリソースには、ローカル コンピュータと同期するプリンタ、カメラ、Windows Mobile デバイス (テザラ デバイス) などが含まれます。この問題は、クライアント プロファイルで [Local LAN Access] を有効にすることで解消されます。ただし、ローカル ネットワークへのアクセスが無制限になるため、一部の企業ではセキュリティやポリシーについて懸念が生じる可能性があります。プリンタやテザラ デバイスなど特定タイプのローカル リソースに対するアクセスを制限するエンドポイントの OS のファイアウォールルールを導入するように ASA を設定できます。

そのための操作として、印刷用の特定ポートに対するクライアント ファイアウォールルールを有効にします。クライアントでは、着信ルールと発信ルールが区別されます。印刷機能の場合、クライアントでは発信接続に必要なポートは開放されますが、着信トラフィックはすべてブロックされます。



- (注) 管理者としてログインしたユーザは、ASA によりクライアントへ展開されたファイアウォールルールを修正できることに注意が必要です。限定的な権限を持つユーザは、ルールを修正できません。どちらのユーザの場合も、接続が終了した時点でクライアントによりファイアウォールルールが再適用されます。

クライアント ファイアウォールを設定している場合、ユーザが Active Directory (AD) サーバで認証されると、クライアントでは引き続き ASA のファイアウォール ポリシーが適用されます。ただし、AD グループポリシーで定義されたルールは、クライアントファイアウォールのルールよりも優先されます。

以下の項では、次の処理を行うための手順について説明します。

- [ローカルプリンタをサポートするためのクライアントファイアウォールの展開 \(96 ページ\)](#)
- [VPN のテザラ デバイス サポートの設定 \(99 ページ\)](#)

ファイアウォールの動作に関する注意事項

ここに記載したのは、AnyConnect クライアントではファイアウォールがどのように使用されるかについての注意事項です。

- ファイアウォールルールには送信元 IP は使用されません。クライアントでは、ASA から送信されたファイアウォールルール内の送信元 IP 情報は無視されます。送信元 IP は、ルールがパブリックかプライベートかに応じてクライアントが特定します。パブリックルールは、クライアント上のすべてのインターフェイスに適用されます。プライベートルールは、仮想アダプタに適用されます。
- ASA は、ACL ルールに対して数多くのプロトコルをサポートしています。ただし、AnyConnect のファイアウォール機能でサポートされているのは、TCP、UDP、ICMP、および IP のみです。クライアントでは、異なるプロトコルでルールが受信された場合、そのルールは無効なファイアウォールルールとして処理され、さらにセキュリティ上の理由からスプリット トンネリングが無効となり、フルトンネリングが使用されます。
- ASA 9.0 から、パブリック ネットワーク ルールおよびプライベート ネットワーク ルールは、ユニファイドアクセス コントロール リストをサポートしています。これらのアクセス コントロール リストは、同じルールで IPv4 および IPv6 トラフィックを定義する場合に使用できます。

ただし次のように、オペレーティング システムによって動作が異なるため注意が必要です。

- Windows コンピュータの場合、Windows Firewall では拒否ルールが許可ルールに優先します。ASA により許可ルールが AnyConnect クライアントへプッシュされても、ユーザがカスタムの拒否ルールを作成していれば、AnyConnect ルールは適用されません。
- Windows Vista の場合、ファイアウォールルールが作成されると、Windows Vista ではポート番号の範囲がカンマ区切りの文字列として認識されます。ポート範囲は、最大で 300 ポートです (1 ~ 300、5000 ~ 5300 など)。指定した範囲が 300 ポートを超える場合は、最初の 300 ポートに対してのみファイアウォールルールが適用されます。
- ファイアウォール サービスが AnyConnect クライアントにより開始される必要がある (システムにより自動的に開始されない) Windows ユーザは、VPN 接続の確立にかなりの時間を要する場合があります。
- Mac コンピュータの場合、AnyConnect クライアントでは、ASA で適用されたのと同じ順序でルールが適用されます。グローバルルールは必ず最後になるようにしてください。
- サードパーティ ファイアウォールの場合、AnyConnect クライアント ファイアウォールとサードパーティ ファイアウォールの双方で許可されたタイプのトラフィックのみ通過できます。AnyConnect クライアントで許可されている特定のタイプのトラフィックであっても、サードパーティファイアウォールによってブロックされれば、そのトラフィックはクライアントでもブロックされます。

ローカル プリンタをサポートするためのクライアント ファイアウォールの展開

ASA は、ASA バージョン 8.3(1) 以降および ASDM バージョン 6.3(1) 以降で、AnyConnect クライアント ファイアウォール機能をサポートします。この項では、ローカル プリンタへのアクセスが許可されるようにクライアント ファイアウォールを設定する方法、および VPN 接続の失敗時にファイアウォールを使用するようクライアント プロファイルを設定する方法について説明します。

クライアント ファイアウォールの制限事項

クライアント ファイアウォールを使用してローカル LAN アクセスを制限する場合には次の制限事項が適用されます。

- OS の制限事項により、Windows XP が実行されているコンピュータのクライアント ファイアウォールポリシーは、着信トラフィックに対してのみ適用されます。発信ルールおよび双方向ルールは無視されます。これには、「permit ip any any」などのファイアウォールルールが含まれます。
- ホスト スキャンや一部のサードパーティ ファイアウォールは、ファイアウォールを妨害する可能性があります。

以下の表は、送信元ポートおよび宛先ポートの設定により影響を受けるトラフィックの方向をまとめたものです。

送信元ポート	宛先ポート	影響を受けるトラフィックの方向
特定のポート番号	特定のポート番号	着信および発信
範囲または「すべて」 (値は 0)	範囲または「すべて」 (値は 0)	着信および発信
特定のポート番号	範囲または「すべて」 (値は 0)	着信のみ
範囲または「すべて」 (値は 0)	特定のポート番号	発信のみ

ローカル印刷に関する ACL ルールの例

ACL AnyConnect_Client_Local_Print は、クライアント ファイアウォールを設定しやすくするために、ASDM を備えています。グループポリシーの [Client Firewall] ペインのパブリック ネットワーク ルールのために ACL を選択する際は、一覧に次の ACE を含めます。

表 1: AnyConnect_Client_Local_Print の ACL ルール

説明	Permission	インターフェイス	プロトコル	送信元ポート	Destination Address	宛先ポート
すべて拒否	拒否	パブリック	いずれか (Any)	デフォルト	いずれか (Any)	デフォルト
LPD	許可	パブリック	TCP	デフォルト	いずれか (Any)	515

説明	Permission	インターフェイス	プロトコル	送信元ポート	Destination Address	宛先ポート
IPP	許可	パブリック	TCP	デフォルト	いずれか (Any)	631
プリンタ	許可	パブリック	TCP	デフォルト	いずれか (Any)	9100
mDNS	許可	パブリック	UDP	デフォルト	224.0.0.251	5353
LLMNR	許可	パブリック	UDP	デフォルト	224.0.0.252	5355
NetBios	許可	パブリック	TCP	デフォルト	いずれか (Any)	137
NetBios	許可	パブリック	UDP	デフォルト	いずれか (Any)	137

(注) デフォルトのポート範囲は 1 ~ 65535 です。



(注) ローカル印刷を有効にするには、定義済み ACL ルール「allow Any Any」に対し、クライアントプロファイルの [Local LAN Access] 機能を有効にする必要があります。

VPN のローカル印刷サポートの設定

エンドユーザがローカルプリンタに出力できるようにするには、グループポリシーで標準 ACL を作成します。ASA はその ACL を VPN クライアントに送信し、VPN クライアントはクライアントのファイアウォール設定を変更します。

手順

- ステップ 1** グループポリシーで、AnyConnect クライアントファイアウォールを有効にします。
[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。
- ステップ 2** グループポリシーを選択して、[Edit] をクリックします。
- ステップ 3** [Advanced] > [AnyConnect Client] > [Client Firewall] を選択します。プライベートネットワークルールに対応する [Manage] をクリックします。
- ステップ 4** 前述した ACE を含む ACL を作成します。この ACL をプライベートネットワークルールとして追加します。
- ステップ 5** 常時接続の自動VPNポリシーを有効にし、かつクローズドポリシーを指定している場合、VPN 障害が発生するとユーザはローカルリソースにアクセスできません。このシナリオでは、プロ

ファイルエディタの [Preferences (Part 2)] に移動し、[Apply last local VPN resource rules] をオンにすることによって、ファイアウォールルールを適用できます。

VPN のテザー デバイス サポートの設定

テザー デバイスをサポートして企業ネットワークを保護する場合は、グループポリシーで標準的な ACL を作成し、テザーデバイスで使用する宛先アドレスの範囲を指定します。さらに、トンネリング VPN トラフィックから除外するネットワークリストとしてスプリットトンネリング用の ACL を指定します。また、VPN 障害時には最後の VPN ローカルリソースルールが使用されるようにクライアントプロファイルを設定することも必要です。



- (注) AnyConnect を実行しているコンピュータと同期する必要がある Windows モバイルデバイスについては、ACL で IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。

手順

- ステップ 1 ASDM で、[Group Policy] > [Advanced] > [Split Tunneling] を選択します。
- ステップ 2 [Network List] フィールドの隣にある [Inherit] チェックボックスをオフにし、[Manage] をクリックします。
- ステップ 3 [Extended ACL] タブをクリックします。
- ステップ 4 [Add] > [Add ACL] を選択します。新しい ACL の名前を指定します。
- ステップ 5 テーブルで新しい ACL を選択して、[Add] をクリックし、さらに [Add ACE] をクリックします。
- ステップ 6 [Action] に対して [Permit] オプション ボタンを選択します。
- ステップ 7 宛先条件エリアで、IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。
- ステップ 8 [Service] に対して IP を選択します。
- ステップ 9 [OK] をクリックします。
- ステップ 10 [OK] をクリックして、ACL を保存します。
- ステップ 11 内部グループポリシーの [Split Tunneling] ペインで、ステップ 7 で指定した IP アドレスに応じて [Inherit for the Policy or IPv6 Policy] チェックボックスをオフにして、[Exclude Network List Below] を選択します。[Network List] で、作成した ACL を選択します。
- ステップ 12 [OK] をクリックします。
- ステップ 13 [Apply] をクリックします。

内部グループポリシー、AnyConnect クライアントキーの再生成

ASA とクライアントがキーを再生成し、暗号キーと初期ベクトルについて再ネゴシエーションするときに、キー再生成ネゴシエーションが実行され、接続のセキュリティが強化されます。

内部グループポリシーの [Advanced] > [AnyConnect Client] > [Key Regeneration] ペインでは、キー再生成のパラメータを設定します。

- [Renegotiation Interval] : セッションの開始からキーの再生成が実行されるまでの分数を 1 ~ 10080 (1 週間) の範囲で指定するには、[Unlimited] チェックボックスをオフにします。
- [Renegotiation Method] : [Inherit] チェックボックスをオフにして、デフォルトのグループポリシーとは異なる再ネゴシエーション方式を指定します。キー再生成をディセーブルにするには、[None] オプション ボタンを選択し、キー再生成時に新しいトンネルを確立するには、[SSL] または [New Tunnel] オプション ボタンを選択します。



(注) [Renegotiation Method] 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せん。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。

内部グループポリシー、AnyConnect クライアント、デッドピア検出

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、AnyConnect 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 AnyConnect SSL VPN クライアント間の接続のみに適用されます。DPD はパディングを許可しない標準の実装に基づいているため IPsec を使用できず、クライアントレス SSL VPN がサポートされません。
- 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の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。

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] の順に移動し、目的のグループポリシーを追加 ([Add]) または編集 ([Edit]) し、[Advanced] > [AnyConnect Client] > [Dead Peer Detection] ペインを開きます。
- または特定のユーザポリシーに到達するには、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] に移動し、目的のユーザアカウントを追加 ([Add]) または編集 ([Edit]) し、[VPN Policy] > [AnyConnect Client] > [Dead Peer Detection] ペインを開きます。

ステップ 2 ゲートウェイ側の検出を設定します。

DPD をセキュリティアプライアンス (ゲートウェイ) によって実行することを指定するには、[Disable] チェックボックスをオフにします。セキュリティアプライアンスが DPD を実行する間隔を 30 秒 (デフォルト) から 3600 秒の範囲で入力します。値 300 が推奨されます。

ステップ 3 クライアント側の検出を設定します。

DPD をクライアントが実行することを指定するには、[Disable] チェックボックスをオフにします。クライアントが DPD を実行する間隔を 30 秒 (デフォルト) から 3600 秒の範囲で入力します。値 300 が推奨されます。

内部グループポリシー、クライアントレス ポータルの AnyConnect カスタマイズ

内部グループポリシーの [Advanced] > [AnyConnect Client] > [Customization] ペインでは、グループポリシーのクライアントレスポータルのログインページをカスタマイズできます。

- [Portal Customization] : [AnyConnect Client/SSL VPN] ポータルページに適用するカスタマイゼーションを選択します。事前設定済みのポータルカスタマイゼーションオブジェクトを選択するか、またはデフォルトグループポリシーで定義されているカスタマイゼーションを受け入れることができます。デフォルトは DfltCustomization です。
 - [Manage] : [Configure GUI Customization object]s ダイアログボックスが開きます。このダイアログボックスでは、カスタマイゼーションオブジェクトの追加、編集、削除、インポート、またはエクスポートを指定できます。
- [Homepage URL](オプション) : グループポリシーに関連付けられたユーザのクライアントレスポータルに表示するホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。クライアントレスユーザには、認証の成功後すぐにこのページが表示されます。AnyConnect は、VPN 接続が正常に確立されると、この URL に対してデフォルトの Web ブラウザを起動します。



(注) AnyConnect は、Linux プラットフォーム、Android モバイル デバイス、および Apple iOS モバイル デバイスでこのフィールドを現在サポートしていません。設定されている場合、これらの AnyConnect クライアントによって無視されます。

- [Use Smart Tunnel for Homepage] : ポート転送を使用する代わりにポータルに接続するスマート トンネルを作成します。
- [Access Deny Message] : アクセスを拒否するユーザに表示するメッセージを作成するには、このフィールドに入力します。

内部グループポリシーの AnyConnect クライアント カスタム属性の設定

内部グループポリシーの [Advanced] > [AnyConnect Client] > [Custom Attributes] ペインは、このポリシーに現在割り当てられているカスタム属性を示します。このダイアログボックスでは、すでに定義済みのカスタム属性をこのポリシーに関連付けるか、カスタム属性を定義してこのポリシーに関連付けることができます。

カスタム属性は AnyConnect クライアントに送信され、アップグレードの延期などの機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を1つ以上定義できます。機能に対して設定する固有のカスタム属性の詳細については、使用している AnyConnect リリースの『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

カスタム属性は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] および [AnyConnect Custom Attribute Names] で事前に定義することもできます。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループポリシーの両方で使用されます。

この手順を使用して、カスタム属性を追加または編集します。設定済みのカスタム属性を削除することもできますが、別のグループポリシーに関連付けられている場合は編集または削除できません。

手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] > [Custom Attributes] に移動します。
- ステップ 2** [Add] をクリックして [Create Custom Attribute] ペインを開きます。
- ステップ 3** ドロップダウンリストから事前に定義された属性タイプを選択するか、次の手順を実行して属性タイプを設定します。
 - a) [管理 (Manage)] をクリックし、[カスタム属性タイプの設定 (Configure Custom Attribute Types)] ペインで [追加 (Add)] をクリックします。

- b) [カスタム属性タイプの作成 (Create Custom Attribute Type)] ペインで、新しい属性の [タイプ (Type)] と [説明 (Description)] を入力します。どちらのフィールドも必須項目です。AnyConnect カスタム属性オプションについては、[AnyConnect カスタム属性 \(186 ページ\)](#) を参照してください。
- c) [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、新しく定義したカスタム属性のタイプを選択します。

ステップ 4 [値の選択 (Select Value)] を選択します。

ステップ 5 [値の選択 (Select value)] ドロップダウンリストから事前に定義された名前付きの値を選択するか、次の手順を実行して新しい名前付きの値を設定します。

- a) [管理 (Manage)] をクリックし、[カスタム属性の設定 (Configure Custom Attributes)] ペインで [追加 (Add)] をクリックします。
- b) [カスタム属性名の作成 (Create Custom Attribute Name)] ペインで、前に選択または設定した属性タイプを選択し、新しい属性の [名前 (Name)] と [値 (Value)] を入力します。どちらのフィールドも必須項目です。

値を追加するには、[追加 (Add)] をクリックして値を入力し、[OK] をクリックします。値は 420 文字を超えてはなりません。値がこの長さを超える場合は、追加の値コンテンツ用の複数の値を追加します。設定値は AnyConnect クライアントに送信される前に連結されます。

- c) [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、この属性の新しく定義した名前付きの値を選択します。

ステップ 6 [カスタム属性の作成 (Create Custom Attribute)] ペインで [OK] をクリックします。

IPsec (IKEv1) クライアントの内部グループポリシー

内部グループポリシー、IPsec (IKEv1) クライアントの一般属性

[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] で、[Add or Edit Group Policy] > [IPsec] ダイアログボックスを使用すると、追加または変更するグループポリシーのトンネリングプロトコル、フィルタ、接続設定、サーバを指定できます。

- [Re-Authentication on IKE Re-key] : [Inherit] チェックボックスがオフである場合に、IKE キーの再生成が行われたときの再認証をイネーブルまたはディセーブルにします。ユーザは、30 秒以内にクレデンシャルを入力する必要があります。また、約 2 分間で SA が期限切れになり、トンネルが終了するまでの間に、3 回まで入力を再試行できます。
- [Allow entry of authentication credentials until SA expires] : 設定済み SA の最大ライフタイムまで、ユーザは認証クレデンシャルをこの回数再入力できます。
- [IP Compression] : [Inherit] チェックボックスがオフである場合に、IP Compression をイネーブルまたはディセーブルにします。

- **[Perfect Forward Secrecy]** : **[Inherit]** チェックボックスがオフである場合に、完全転送秘密 (PFS) をイネーブルまたはディセーブルにします。PFS は、特定の IPsec SA のキーが他のシークレット (他のキーなど) から導出されたものでないことを保証します。つまり、PFS では、攻撃者があるキーを突破しても、そこから他のキーを導出することはできないことが保証されます。PFS がイネーブルになっていない場合は、IKE SA の秘密キーが突破されると、その攻撃者は、IPsec のすべての保護データをコピーし、IKE SA のシークレットの知識を使用して、その IKE SA によって設定された IPsec SA のセキュリティを侵すことができると推測されます。PFS を使用すると、攻撃者が IKE を突破しても、直接 IPsec にはアクセスできません。その場合、攻撃者は各 IPsec SA を個別に突破する必要があります。
- **[Store Password on Client System]** : クライアントシステムでのパスワードの保管をイネーブルまたはディセーブルにします。



(注) パスワードをクライアントシステムで保管すると、潜在的なセキュリティリスクが発生します。

- **[IPsec over UDP]** : IPsec over UDP の使用をイネーブルまたはディセーブルにします。
- **[IPsec over UDP Port]** : IPsec over UDP で使用する UDP ポートを指定します。
- **[Tunnel Group Lock]** : **[Inherit]** チェックボックスまたは値 **[None]** が選択されていない場合に、選択したトンネルグループをロックします。
- **[IPsec Backup Servers]** : **[Server Configuration]** フィールドと **[Server IP Addresses]** フィールドをアクティブにします。これによって、これらの値が継承されない場合に使用する UDP バックアップサーバを指定できます。
 - **[Server Configuration]** : IPsec バックアップサーバとして使用するサーバ設定オプションを一覧表示します。使用できるオプションは、**[Keep Client Configuration]** (デフォルト)、**[Use Backup Servers Below]**、および **[Clear Client Configuration]** です。
 - **[Server Addresses (space delimited)]** : IPsec バックアップサーバの IP アドレスを指定します。このフィールドは、**[Server Configuration]** で選択した値が **Use Backup Servers Below** である場合にだけ使用できます。

内部グループポリシーの IPsec (IKEv1) クライアントのアクセスルールについて

このダイアログボックスの **[Client Access Rules]** テーブルには、クライアントアクセスルールを 25 件まで表示できます。クライアントアクセスルールを追加するときには次のフィールドを設定します。

- **[Priority]** : このルールの優先順位を選択します。
- **[Action]** : このルールに基づいてアクセスを許可または拒否します。

- [VPN Client Type] : このルールを適用する VPN クライアントのタイプ (ソフトウェアまたはハードウェア) を指定します。ソフトウェアクライアントの場合は、すべての Windows クライアントまたはサブセットを自由形式のテキストで指定します。
- [VPN Client Version] : このルールを適用する VPN クライアントのバージョンを指定します (複数可)。このコラムには、このクライアントに適用されるソフトウェアまたはファームウェア イメージのカンマ区切りリストが含まれます。エントリーは自由形式のテキストで、* はすべてのバージョンと一致します。

クライアント アクセス ルールの定義

- 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。ただし、ユーザがデフォルト グループ ポリシーに存在するルールを継承する場合があります。
- 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。
- * 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。
- 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。

内部グループポリシー、IPsec (IKEv1) クライアントのクライアント ファイアウォール

[Add or Edit Group Policy] の [Client Firewall] 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行うことができます。これらのファイアウォール機能を使用できるのは、Microsoft Windows 上で動作している 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。

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は、適切なファイアウォール オプションを選択できます。

最初のシナリオでは、リモートユーザの 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。

[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] > [Client Firewall]

フィールド

- [Inherit] : グループポリシーがデフォルトグループポリシーからクライアントのファイアウォール設定を取得するかどうかを決めます。このオプションはデフォルト設定です。設定すると、このダイアログボックスにある残りの属性がその設定によって上書きされ、名前がグレー表示になります。
- [Client Firewall Attributes] : (実装されている場合) 実装されているファイアウォールのタイプやファイアウォールポリシーなど、クライアントのファイアウォール属性を指定します。
- [Firewall Setting] : ファイアウォールが存在するかどうかを一覧表示します。存在する場合には、そのファイアウォールが必須かオプションかも示します。[No Firewall] (デフォルト) を選択すると、このダイアログボックスにある残りのフィールドは、いずれもアクティブになりません。このグループのユーザをファイアウォールで保護する場合は[Firewall Required] または [Firewall Optional] 設定を選択します。

[Firewall Required] を選択した場合は、このグループのユーザ全員が指定されたファイアウォールを使用する必要があります。指定されたサポート対象のファイアウォールがインストールされておらず、実行されていない場合、ASAは接続を試行したセッションをすべてドロップします。この場合、ASAは、ファイアウォール設定が一致しないことをVPNクライアントに通知します。



- (注) グループでファイアウォールを必須にする場合には、そのグループに Windows VPN クライアント以外のクライアントが存在しないことを確認してください。グループ内のその他のクライアント (クライアントモードの ASA 5505 を含む) は接続できません。

このグループに、まだファイアウォールに対応していないリモートユーザがいる場合は、[Firewall Optional] を選択します。Firewall Optional 設定を使用すると、グループ内のすべてのユーザが接続できるようになります。ファイアウォールに対応しているユーザは、ファイアウォールを使用できます。ファイアウォールなしで接続するユーザには、警告

メッセージが表示されます。この設定は、一部のユーザがファイアウォールをサポートしており、他のユーザがサポートしていないグループを作成するときに役立ちます。たとえば、移行途中のグループでは、一部のメンバはファイアウォール機能を設定し、別のユーザはまだ設定していないことがあります。

- **[Firewall Type]** : シスコを含む複数のベンダーのファイアウォールを一覧表示します。**[Custom Firewall]** を選択すると、**[Custom Firewall]** の下のフィールドがアクティブになります。指定したファイアウォールが、使用できるファイアウォールポリシーと関連している必要があります。設定したファイアウォールにより、サポートされるファイアウォールポリシー オプションが決まります。
- **[Custom Firewall]** : カスタムファイアウォールのベンダー ID、製品 ID、および説明を指定します。
 - **[Vendor ID]** : このグループ ポリシーのカスタム ファイアウォールのベンダーを指定します。
 - **[Product ID]** : このグループ ポリシー用に設定するカスタム ファイアウォールの製品名またはモデル名を指定します。
 - **[Description]** : (任意) カスタム ファイアウォールについて説明します。
- **[Firewall Policy]** : カスタム ファイアウォール ポリシーのタイプとソースを指定します。
 - **[Policy defined by remote firewall (AYT)]** : ファイアウォール ポリシーをリモート ファイアウォール (Are You There) によって定義するように指定します。**Policy defined by remote firewall (AYT)** は、このグループのリモート ユーザのファイアウォールが、各自の PC に存在することを意味しています。このローカル ファイアウォールが、VPN クライアントにファイアウォール ポリシーを適用します。ASA は、指定されたファイアウォールがインストールされ、実行している場合のみ、このグループの VPN クライアントが接続できるようにします。指定されたファイアウォールが実行されていない場合、接続は失敗します。接続が確立すると、VPN クライアントがファイアウォールを 30 秒ごとにポーリングして、そのファイアウォールが実行されていることを確認します。ファイアウォールの実行が停止すると、VPN クライアントはセッションを終了します。
 - **[Policy pushed (CPP)]** : ポリシーがピアからプッシュされるように指定します。このオプションを選択する場合は、**[Inbound Traffic Policy]** および **[Outbound Traffic Policy]** リストと **[Manage]** ボタンがアクティブになります。ASA は、**[Policy Pushed (CPP)]** ドロップダウンリストで選択されたフィルタによって定義されるトラフィック管理ルールを、このグループの VPN クライアントに適用します。メニューで選択できるのは、デフォルトフィルタを含めて、この ASA で定義されているフィルタです。ASA がこれらのルールを VPN クライアントにプッシュすることに注意してください。ASA ではなく VPN クライアントに対してこれらのルールを作成して定義する必要があります。たとえば、「in」と「out」はそれぞれ、VPN クライアントに着信するトラフィックと、VPN クライアントから発信されるトラフィックです。VPN クライアントにローカルファイアウォールもある場合、ASA からプッシュされたポリシーはローカルファ

ファイアウォールのポリシーと連携して機能します。いずれかのファイアウォールのルールでブロックされたすべてのパケットがドロップされます。

- [Inbound Traffic Policy] : 着信トラフィックに対して使用できるプッシュポリシーを一覧表示します。
- [Outbound Traffic Policy] : 発信トラフィックに対して使用できるプッシュポリシーを一覧表示します。
- [Manage] : [ACL Manager] ダイアログボックスを表示します。このダイアログボックスで、アクセスコントロールリスト (ACL) を設定できます。

内部グループポリシー、IPsec (IKEv1) のハードウェアクライアント属性

[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] > [Hardware Client] ダイアログボックスで、Easy VPN Remote クライアントに送信されるグループポリシー属性を設定します。ASA における Easy VPN のサポートの詳細については、[Easy VPN \(265 ページ\)](#) の章を参照してください。



(注) VPN 3002 ハードウェアクライアントは耐用年数末期で、サポートが終了しています。

- [Inherit] : (複数インスタンス) 対応する設定が、その後続く明示的な指定ではなく、デフォルトグループポリシーから値を取得することを示します。これは、このダイアログボックスの属性すべてのデフォルト設定になります。
- [Require Interactive Client Authentication] : インタラクティブクライアント認証の要求をイネーブルまたはディセーブルにします。このパラメータはデフォルトではディセーブルになっています。

ディセーブルにすると、ハードウェアクライアントに保存されているクレデンシャルが認証に使用されます。クレデンシャルが保存されていない場合は、ハードウェアクライアントが手動で認証します。保存されているクレデンシャルまたは入力されたクレデンシャルが有効な場合は、トンネルが確立されます。

このオプションをイネーブルにすると、クライアントにユーザ名とパスワードが保存されているかどうかに関係なく、トンネルが開始されるたびにハードウェアクライアントに対して手動でユーザ名とパスワードを認証するように要求することによって、セキュリティが強化されます。入力したクレデンシャルが有効な場合は、トンネルが確立されます。

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、ユーザがユーザ名とパスワードを入力する必要があります。

- **[Require Individual User Authentication]** : 個別のユーザ認証の要求をイネーブルまたはディセーブルにします。個別ユーザ認証は、VPN 3002 のプライベート ネットワークの許可されないユーザが中央サイトにアクセスできないように保護します。このパラメータはデフォルトではディセーブルになっています。

個別ユーザ認証をイネーブルにした場合は、トンネルがすでに存在していても、ハードウェアクライアントを介して接続する各ユーザは、ASA の背後にあるネットワークにアクセスするために、Web ブラウザを開いて手動で有効なユーザ名とパスワードを入力する必要があります。

認証を行うには、ブラウザの **[Location]** フィールドまたは **[Address]** フィールドに、ハードウェアクライアントのプライベート インターフェイスの IP アドレスを入力する必要があります。ブラウザに、ハードウェアクライアントのログイン ダイアログボックスが表示されます。認証するには、**[Connect/Login Status]** をクリックします。ASA の背後のリモート ネットワークにデフォルト ホームページがある場合、または、ASA の背後のリモート ネットワーク上にある Web サイトをブラウザで開く場合、ハードウェアクライアントは、ユーザログイン用の適切なページをブラウザで開きます。正常にログインすると、元々入力していたページがブラウザに表示されます。

ユーザ認証がイネーブルになっている場合は、コマンドラインインターフェイスを使用してログインできません。ブラウザを使用する必要があります。ASA の背後のネットワーク上にある Web ベースではないリソース（電子メールなど）にアクセスを試みる場合は、ブラウザを使用して認証を行うまで、接続に失敗します。

バナーを表示するには、個々のユーザ認証をイネーブルにする必要があります。1 人のユーザは、同時に最大 4 セッションのログインを実行できます。

プライマリ ASA でユーザ認証が必要な場合は、どのバックアップ サーバにもユーザ認証を設定する必要があります。

- **[User Authentication Idle Timeout]** : ユーザのタイムアウト期間を設定します。セキュリティ アプライアンスは、この期間にユーザトラフィックを受信しないと、接続を終了します。タイムアウト期間として、特定の分数または無期限を指定できます。
 - **[Unlimited]** : 接続がタイムアウトにならないように指定します。このオプションは、デフォルト 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。
 - **[Minutes]** : タイムアウト期間を分単位で指定します。1 ~ 35791394 の整数を使用します。デフォルト値は **Unlimited** です。

`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のアイドル タイムアウト値になります。

- [Cisco IP Phone Bypass] : Cisco IP Phone にインタラクティブ個別ユーザ認証プロセスをバイパスさせます (イネーブルな場合)。デフォルトでは、Cisco IP Phone Bypass はディセーブルになっています。

IP Phone 接続にネットワーク拡張モードを使用するように、ハードウェアクライアントを設定する必要があります。

- [LEAP Bypass] : [Require Individual User Authentication] がイネーブルの場合にのみ適用されます。シスコの無線デバイスからの LEAP パケットに、個々のユーザ認証プロセスをバイパスさせます。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、ユーザは、個別のユーザ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。

- [Require Interactive Client Authentication] がディセーブルになっている。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。
- [Require Individual User Authentication] がイネーブルになっている。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。
- [Allow Network Extension Mode] : このグループのハードウェアクライアントによるネットワーク拡張モードの使用を決定します。このパラメータはデフォルトではディセーブルになっています。ネットワーク拡張モードがディセーブルになっている場合、ハードウェアクライアントはポートアドレス変換モードで ASA に接続する必要があります。

Call Manager は実際の IP アドレスでだけ通信できるため、ハードウェアクライアントが IP Phone 接続をサポートするには、ネットワーク拡張モードが必要です。



- (注) このグループのハードウェアクライアントを同様に設定する必要があります。ネットワーク拡張モードを使用するようにハードウェアクライアントが設定されており、接続先の ASA でネットワーク拡張モードがディセーブルになっている場合、ハードウェアクライアントは4秒ごとに接続を試行し、すべての試行が拒否されます。このような場合、ハードウェアクライアントは、接続先の ASA に不要な処理負荷をかけることとなります。多数のハードウェアクライアントがこのように誤設定されていると、セキュリティアプライアンスのサービス提供能力が損なわれます。

クライアントレス SSL VPN の内部グループ ポリシー

内部グループ ポリシー、クライアントレス SSL VPN 一般属性

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit] > [General]

[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 ポリシーのトンネリングプロトコル、フィルタ、接続設定、サーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルトグループポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

[Add Internal Group Policy] > [General] ダイアログボックスには、次の属性が表示されます。

- [Name] : このグループポリシーの名前を最大 64 文字で指定します (スペースの使用可)。Edit 機能の場合、このフィールドは読み取り専用です。
- [Banner] : ログイン時にユーザに対して表示するバナー テキストを指定します。全体的なバナーの長さは最大 4000 文字です。デフォルト値はありません。

クライアントレス ポータルおよび AnyConnect クライアントは部分的な HTML をサポートしています。バナーがリモートユーザに適切に表示されるようにするには、次のガイドラインに従います。

- クライアントレス ユーザの場合は、
 タグを使用します。
- [Tunneling Protocols] : このグループが使用できるトンネリングプロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。
- [Clientless SSL VPN] : SSL/TLS による VPN の使用を指定します。この VPN では、ソフトウェアやハードウェアのクライアントは必要なく、Web ブラウザを使用して ASA へのセキュアリモートアクセス トンネルが確立されます。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル

共有（Web 対応）、電子メール、およびその他の TCP ベースアプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。

- [SSL VPN Client] : Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して MUS がサポートされるようにする必要があります。
- [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2] : AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェアアップデート、クライアントプロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- [L2TP over IPsec] : 一部の一般的 PC やモバイル PC のオペレーティングシステムで提供される VPN クライアントを使用しているリモートユーザは、L2TP over IPsec によって、パブリック IP ネットワーク経由でセキュアな接続を確立できます。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。セキュアな接続は、IPsec 転送モード用に設定する必要があります。
- [Web ACL] : (Clientless SSL VPN 専用) トラフィックをフィルタリングする場合は、ドロップダウンリストからアクセス コントロール リスト (ACL) を選択します。選択する前に ACL を表示、変更、追加、または削除する場合は、リストの横にある [Manage] をクリックします。
- [Access Hours] : このユーザに適用される既存のアクセス時間ポリシーがある場合はその名前を選択するか、または新しいアクセス時間ポリシーを作成します。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [--Unrestricted--] です。時間範囲オブジェクトを表示または追加するには、リストの横にある [Manage] をクリックします。
- [Simultaneous Logins] : このユーザに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザアクセスを禁止します。



(注) 最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

- [Restrict Access to VLAN] : (オプション) 「VLAN マッピング」とも呼ばれます。このパラメータにより、このグループポリシーが適用されるセッションの出力 VLAN インター

フェイスを指定します。ASA は、このグループのすべてのトラフィックを指定された VLAN に転送します。この属性を使用して VLAN をグループポリシーに割り当て、アクセスコントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウンリストには、デフォルト値 (Unrestricted) の他に、この ASA で設定されている VLAN だけが表示されます。



(注) この機能は、HTTP 接続の場合には有効ですが、FTP および CIFS 接続では使用できません。

- **[Connection Profile (Tunnel Group) Lock]** : このパラメータを使用すると、選択された接続プロファイル (トンネルグループ) を使用する VPN アクセスのみを許可し、別の接続ファイルを使用するアクセスを回避できます。デフォルトの継承値は [None] です。
- **Maximum Connect Time** : [Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザ接続時間を分単位で設定します。
ここで指定した時間が経過すると、システムは接続を終了します。最小値は1分、最大値は 35791394 分 (4000 年超) です。制限なしの接続時間を許可するには、[Unlimited] をオンにします (デフォルト)。
- **Idle Timeout** : [Inherit] チェックボックスをオフにした場合、このパラメータでアイドル時間を分単位で設定します。
この期間に接続で通信アクティビティがない場合、接続は終了します。最小時間は1分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。
- **Maximum Connection Time Alert Interval** : ユーザにメッセージを表示する、最大接続時間に達するまでの時間間隔。
[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、セッションアラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ~ 30 分のセッションアラート間隔を指定します。
- **Idle Timeout Alert Interval** : アイドルタイムアウトに達すると、ユーザにメッセージが表示されます。
[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、アイドルアラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ~ 30 分のセッションアラート間隔を指定します。
- **Periodic Certificate Authentication Interval** : 証明書認証が定期的に再実行されるまでの時間間隔 (時間単位)。
[Inherit] チェックボックスがオフになっている場合、定期的な証明書検証の実行間隔を設定できます。範囲は 1 ~ 168 時間で、デフォルトは無効になっています。無制限の検証を許可するには、[Unlimited] をオンにします。

内部グループポリシー、クライアントレス SSL VPN アクセス ポータル

[Portal] 属性により、クライアントレス SSL VPN 接続を確立するこのグループポリシーのメンバのポータル ページに表示されるコンテンツが決まります。このペインでは、ブックマーク リストと URL エントリ、ファイルサーバアクセス、ポート転送とスマートトンネル、ActiveX リレー、および HTTP の設定をイネーブルにできます。

- [Bookmark List] : あらかじめ設定されたブックマーク リストを選択するか、または [Manage] をクリックして新しいリストを作成します。ブックマークはリンクとして表示され、ユーザはこのリンクを使用してポータル ページから移動できます。
- [URL Entry] : リモート ユーザが URL をポータル URL フィールドに直接入力できるようにする場合にイネーブルにします。
- [File Access Control] : 共通インターネットファイルシステム (CIFS) ファイルの「非表示共有」の表示状態を制御します。非表示共有は、共有名の末尾のドル記号 (\$) で識別されます。たとえば、ドライブ C は C\$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザはこれらの非表示リソースを参照またはアクセスすることを禁止されます。
 - [File Server Entry] : リモート ユーザがファイルサーバの名前を入力できるようにする場合にイネーブルにします。
 - [File Server Browsing] : リモート ユーザが使用可能なファイルサーバを参照できるようにする場合にイネーブルにします。
 - [Hidden Share Access] : 共有フォルダを非表示にする場合にイネーブルにします。
- [Port Forwarding Control] : Java Applet によるクライアントレス SSL VPN 接続により、ユーザが TCP ベースのアプリケーションにアクセスできるようにします。
 - [Port Forwarding List] : このグループポリシーに関連付ける事前設定済み TCP アプリケーションのリストを選択します。新しいリストを作成したり、既存のリストを編集したりするには、[Manage] をクリックします。
 - [Auto Applet Download] : ユーザが始めてログインするときに実行される、Java Applet の自動インストールおよび起動をイネーブルにします。
 - [Applet Name] : [Applet] ダイアログボックスのタイトルバーの名前を、指定する名前に変更します。デフォルトの名前は [Application Access] です。
- [Smart Tunnel] : スマートトンネルで使用されるクライアントレス (ブラウザベース) SSL VPN セッションにおいて、ASA がパスウェイ、セキュリティ アプライアンスがプロキシサーバである場合に、スマートトンネルのオプションを指定します。
 - [Smart Tunnel Policy] : ネットワーク リストから選択し、いずれか 1 つのトンネル オプションを指定します ([use smart tunnel for the specified network]、[do not use smart tunnel for the specified network]、または [use tunnel for all network traffic])。スマートトンネルネットワークをグループポリシーまたはユーザ名に割り当てると、そのグループポリシーまたはユーザ名にセッションが関連付けられているすべてのユーザの場合

にスマート トンネル アクセスがイネーブルになりますが、リストで指定されているアプリケーションへのスマート トンネル アクセスは制限されます。スマート トンネル リストを表示、追加、変更、または削除するには、[Manage] をクリックします。

- [Smart Tunnel Application] : ドロップダウン リストから選択し、エンドステーションにインストールされている TCP ベースのアプリケーション Winsock 2 をイントラネット上のサーバに接続します。スマート トンネル アプリケーションを表示、追加、変更、または削除するには、[Manage] をクリックします。
- [Smart Tunnel all Applications] : すべてのアプリケーションをトンネリングするには、このチェックボックスをオンにします。ネットワークリストから選択したり、エンドユーザが外部アプリケーション用に起動する可能性がある実行ファイルを認識したりすることなく、すべてのアプリケーションがトンネリングされます。
- [Auto Start] : ユーザのログイン時に、スマート トンネル アクセスを自動的に開始するには、このチェックボックスをオンにします。ユーザのログイン時にスマート トンネル アクセスを開始するこのオプションは Windows だけに適用されます。ユーザのログイン時にスマート トンネル アクセスをイネーブルにして、ユーザに手動で開始するように要求する場合はこのチェックボックスをオフにします。ユーザは、[Clientless SSL VPN Portal] ページの [Application Access] > [Start Smart Tunnels] ボタンを使用してアクセスを開始できます。
- [Auto Sign-on Server List] : ユーザがサーバへのスマート トンネル 接続を確立するときユーザ クレデンシアルを再発行する場合、ドロップダウン リストからリスト名を選択します。各スマート トンネル 自動サインオン リストのエントリは、ユーザ クレデンシアルのサブミッションを自動化するサーバを示します。スマート トンネル 自動サインオン リストを表示、追加、変更、または削除するには、[Manage] ボタンをクリックします。
- [Windows Domain Name (Optional)] : 共通命名規則 (domain\username) が認証に必要な場合、自動サインオン二次ユーザ名に追加する Windows のドメインを指定します。たとえば、ユーザ名 qu_team の認証を行う場合、CISCO と入力して CISCO\qu_team を指定します。自動サインオンサーバリストに関連するエントリを設定する場合、[Use Windows domain name with user name] オプションもオンにする必要があります。
- [ActiveX Relay] : クライアントレスユーザが Microsoft Office アプリケーションをブラウザから起動できるようにします。アプリケーションは、セッションを使用して Microsoft Office ドキュメントのダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。

その他のオプション :

- [HTTP Proxy] : クライアントへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー (Java、ActiveX、Flash など) に対して有効です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送プロキシは、ブラウザの古いプロキシ設定を自動的に修正し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTTP アプレットプロキシでは、HTML、CSS、

JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。

- [Auto Start (HTTP Proxy)] : ユーザのログイン時に HTTP プロキシを自動的にイネーブルにする場合にオンにします。ユーザ ログイン時にスマート トンネル アクセスをイネーブルにして、ユーザに手動で開始するように要求する場合はオフにします。
- [HTTP Compression] : クライアントレス SSL VPN セッションでの HTTP データの圧縮をイネーブルにします。

内部グループポリシーの設定、クライアントレス SSL VPN のポータルのカスタマイズ

グループポリシーのカスタマイゼーションを設定するには、事前設定済みのポータル カスタマイゼーション オブジェクトを選択するか、またはデフォルト グループポリシーで定義されているカスタマイゼーションを受け入れます。表示する URL を設定することもできます。

クライアントレス SSL VPN アクセス接続にアクセス ポータルをカスタマイズするための手順は、ネットワーク アクセス クライアント接続と同じです。[内部グループポリシー、クライアントレス ポータルの AnyConnect カスタマイズ \(101 ページ\)](#) を参照してください。

内部グループポリシー、クライアントレス SSL VPN のログイン設定

リモートユーザに AnyConnect クライアントのダウンロードを求めるプロンプトを表示したり、クライアントレス SSL VPN のポータルページに移動するように ASA を設定できます。[内部グループポリシー、AnyConnect ログイン設定 \(94 ページ\)](#) を参照してください。

内部グループポリシー、クライアントレス SSL VPN アクセス用のシングルサインオンサーバと自動サインオンサーバ

シングルサインオンサーバと自動サインオンサーバを設定するには、[内部グループポリシー、クライアントレス SSL VPN アクセス ポータル \(114 ページ\)](#) を参照してください。

サイト間内部グループポリシー

サイト間 VPN 接続のグループポリシーでは、トンネリングプロトコル、フィルタ、および接続設定を指定します。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルトグループポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

フィールド

[Add Internal Group Policy] > [General] ダイアログボックスには、次の属性が表示されます。これらの属性は、SSL VPN と IPsec セッション、またはクライアントレス SSL VPN セッションに適用されます。そのため、いくつかの属性は、1つのタイプのセッションに表示され、他のタイプには表示されません。

- **[Name]** : このグループポリシーの名前を指定します。Edit機能の場合、このフィールドは読み取り専用です。
- **[Tunneling Protocols]** : このグループが許可するトンネリングプロトコルを指定します。ユーザは、選択されているプロトコルだけを使用できます。次の選択肢があります。
 - **[Clientless SSL VPN]** : SSL VPN (SSL/TLS を利用する VPN) を使用することを指定します。この VPN では、ソフトウェアやハードウェアのクライアントは必要なく、Web ブラウザを使用して ASA へのセキュアなリモートアクセストンネルが確立されます。クライアントレス SSL VPN を使用すると、HTTPS インターネットサイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有 (Web 対応)、電子メール、およびその他の TCP ベースアプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
 - **[SSL VPN Client]** : Cisco AnyConnect VPN クライアントまたはレガシー SSL VPN クライアントの使用を指定します。AnyConnect クライアントを使用している場合は、このプロトコルを選択して MUS がサポートされるようにする必要があります。
 - **[IPsec IKEv1]** : IP セキュリティプロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site (ピアツーピア) 接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
 - **[IPsec IKEv2]** : AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェアアップデート、クライアントプロファイル、GUI のローカリゼーション (翻訳) とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
 - **[L2TP over IPsec]** : 一部の一般的な PC やモバイル PC のオペレーティングシステムで提供される VPN クライアントを使用しているリモートユーザは、L2TP over IPsec によって、パブリック IP ネットワーク経由でセキュリティアプライアンスやプライベート企業ネットワークへのセキュアな接続を確立できます。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。セキュリティアプライアンスは、IPsec 転送モード用に設定する必要があります。
- **[Filter]** : (Network (Client) Access 専用) 使用するアクセスコントロールリストを指定するか、またはグループポリシーから値を継承するかどうかを指定します。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。フィルタおよびルールを設定する方法については、[Group Policy] ダイアログボックスを参照してください。ACL を表示および設定できる [ACL Manager] を開くには、[Manage] をクリックします。
- **Idle Timeout** : [Inherit] チェックボックスをオフにした場合、このパラメータでアイドル時間を分単位で設定します。

この期間に接続で通信アクティビティがない場合、接続は終了します。最小時間は1分、最大時間は10080分であり、デフォルトは30分です。接続時間を無制限にするには、[Unlimited] をオンにします。

- **Maximum Connect Time** : [Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザ接続時間を分単位で設定します。

ここで指定した時間が経過すると、システムは接続を終了します。最小値は1分、最大値は35791394分（4000年超）です。制限なしの接続時間を許可するには、[Unlimited] をオンにします（デフォルト）。

- **Periodic Certificate Authentication Interval** : 証明書認証が定期的に再実行されるまでの時間間隔（時間単位）。

[Inherit] チェックボックスがオフになっている場合、定期的な証明書検証の実行間隔を設定できます。範囲は1～168時間で、デフォルトは無効になっています。無制限の検証を許可するには、[Unlimited] をオンにします。

ローカルユーザの VPN ポリシー属性の設定

この手順では、既存のユーザを編集する方法について説明します。ユーザを追加するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択し、[Add] をクリックします。詳細については、一般的操作コンフィギュレーションガイドを参照してください。

始める前に

デフォルトで、ユーザアカウントはデフォルトグループポリシー DfltGrpPolicy から設定値を継承します。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。

手順

- ステップ 1** ASDM を開始し、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] の順に選択します。
- ステップ 2** 設定するユーザを選択し、[Edit] をクリックします。
- ステップ 3** 左側のペインで、[VPN Policy] をクリックします。
- ステップ 4** ユーザのグループポリシーを指定します。ユーザポリシーは、このグループポリシーの属性を継承します。この画面にデフォルトグループポリシーの設定を継承するように設定されている他のフィールドがある場合、このグループポリシーで指定された属性がデフォルトグループポリシーで設定された属性より優先されます。
- ステップ 5** ユーザが使用できるトンネリングプロトコルを指定するか、グループポリシーから値を継承するかどうかを指定します。

目的の [Tunneling Protocols] チェックボックスをオンにし、次のトンネリングプロトコルのいずれかを選択します。

- (SSL/TLS を利用する VPN) クライアントレス SSL VPN では、Web ブラウザを使用して VPN コンセントレータへのセキュアなリモート アクセス トンネルを確立し、ソフトウェア クライアントもハードウェア クライアントも必要としません。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有 (Web 対応)、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
- SSL VPN クライアントは、Cisco AnyConnect Client アプリケーションのダウンロード後にユーザが接続できるようにします。ユーザは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザが接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。
- [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site (ピアツーピア) 接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2] : AnyConnect セキュア モビリティ クライアントによってサポートされています。IKEv2 を使用した IPsec を使用する AnyConnect 接続では、ソフトウェア アップデート、クライアント プロファイル、GUI のローカライゼーション (翻訳) とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- 一部の一般的な PC やモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザは、L2TP over IPsec によって、パブリック IP ネットワーク経由で ASA およびプライベート企業ネットワークへのセキュアな接続を確立できます。

(注) プロトコルを選択しなかった場合は、エラー メッセージが表示されます。

ステップ 6 使用するフィルタ (IPv4 または IPv6) を指定するか、またはグループ ポリシーの値を継承するかどうかを指定します。

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。

- a) フィルタとルールを設定するには、**[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter]** の順に選択します。
- b) **[Manage]** をクリックして、ACL と ACE を追加、編集、および削除できる **[ACL Manager]** ペインを表示します。

ステップ 7 接続プロファイル (トンネル グループ ロック) がある場合、それを継承するかどうか、または選択したトンネル グループ ロックを使用するかどうかを指定します。

特定のロックを選択すると、ユーザのリモート アクセスはこのグループだけに制限されます。**[Tunnel Group Lock]** では、VPN クライアントで設定されたグループと、そのユーザが割り当てられているグループが同じかどうかをチェックすることによって、ユーザが制限されます。一

致していない場合、ASA はユーザが接続できないようにします。[Inherit] チェックボックスがオフの場合、デフォルト値は [None] です。

ステップ 8 [Store Password on Client System] 設定をグループから継承するかどうかを指定します。

[Inherit] チェックボックスをオフにすると、[Yes] および [No] のオプション ボタンが有効になります。[Yes] をクリックすると、ログインパスワードがクライアントシステムに保存されず（セキュリティが低下するおそれのあるオプションです）。接続ごとにユーザにパスワードの入力を求めるようにするには、[No] をクリックします（デフォルト）。セキュリティを最大限に確保するためにも、パスワードの保存を許可しないことを推奨します。

ステップ 9 [Connection Settings] を設定します。

a) このユーザに適用するアクセス時間ポリシーを指定する、そのユーザの新しいアクセス時間ポリシーを作成する、または [Inherit] チェックボックスをオンのままにします。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [Unrestricted] です。

[Manage] をクリックして、[Add Time Range] ダイアログボックスを開きます。このダイアログボックスでアクセス時間の新規セットを指定できます。

b) ユーザによる同時ログイン数を指定します。Simultaneous Logins パラメータは、このユーザに指定できる最大同時ログイン数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザアクセスを禁止します。

(注) 最大値を設定で制限しておかない同時に多数の接続が許可されるため、セキュリティとパフォーマンスの低下を招くおそれがあります。

c) VPN 接続の [Maximum Connect Time] を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。

[Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザ接続時間を分単位で指定します。最小値は 1 分、最大値は 35791394 分（4000 年超）です。制限なしの接続時間を許可するには、[Unlimited] をオンにします（デフォルト）。

d) VPN 接続の [Idle Timeout] を分単位で指定します。この期間に接続で通信アクティビティがない場合、接続は終了します。

[Inherit] チェックボックスがオフになっている場合、このパラメータでアイドルタイムアウトを分単位で指定します。最小時間は 1 分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。

ステップ 10 [Timeout Alerts] を設定します。

a) [Maximum Connection Time Alert Interval] を指定します。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、最大接続アラート間隔は 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1～30 分のセッションアラート間隔を指定します。

b) [Idle Alert Interval] を指定します。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、アイドルアラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1～30 分のセッションアラート間隔を指定します。

- ステップ 11** このユーザに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address (Optional)] 領域で、IPv4 アドレスとサブネットマスクを入力します。
- ステップ 12** このユーザに専用の IPv6 アドレスを設定するには、[Dedicated IPv6 Address (Optional)] 領域に IPv6 プレフィックスを含む IPv6 アドレスを入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。
- ステップ 13** 特定の [Clientless SSL VPN] または [AnyConnect Client] 設定を設定します。これは、左側ペインでこれらのオプションをクリックすることにより行います。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。
- ステップ 14** 実行コンフィギュレーションに変更を適用するには、[OK] をクリックします。

接続プロファイル

接続プロファイル（トンネルグループとも呼ばれる）では、VPN 接続の接続属性を設定します。これらの属性は、Cisco AnyConnect VPN クライアント、クライアントレス SSL VPN 接続、および IKEv1 と IKEv2 のサードパーティ VPN クライアントに適用されます。

AnyConnect 接続プロファイル、メインペイン

AnyConnect 接続プロファイルのメインペインでは、インターフェイス上のクライアントアクセスを有効にして、接続プロファイルを追加、編集、および削除できます。ログイン時にユーザが特定の接続を選択できるようにするかどうかも指定できます。

- [Access Interfaces] : アクセスをイネーブルにするインターフェイスをテーブルから選択できます。このテーブルのフィールドには、インターフェイス名やチェックボックスが表示され、アクセスを許可するかどうかを指定します。
- インターフェイス テーブルの AnyConnect 接続に設定するインターフェイスの行で、インターフェイスでイネーブルにするプロトコルをオンにします。SSL アクセス、IPSec アクセス、またはその両方を許可できます。

SSL をオンにすると、DTLS (Datagram Transport Layer Security) がデフォルトでイネーブルになります。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。

IPsec (IKEv2) アクセスをオンにすると、クライアント サービスがデフォルトでイネーブルになります。クライアント サービスには、ソフトウェアアップデート、クライアントプロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張 Anyconnect 機能が含まれていま

す。クライアントサービスをディセーブルにしても、AnyConnect クライアントでは IKEv2 との基本的な IPsec 接続が確立されます。

- [Device Certificate] : RSA キーまたは ECDSA キーの認証の証明書を指定できます。 [デバイス証明書の指定 \(123 ページ\)](#) を参照してください。
 - [Port Setting] : HTTPS および DTLS (RA クライアントのみ) 接続のポート番号を設定します。 [接続プロファイル、ポート設定 \(123 ページ\)](#) を参照してください。
 - [Bypass interface access lists for inbound VPN sessions] : [Enable inbound VPN sessions to bypass interface ACLs] がデフォルトでオンになっています。セキュリティアプライアンスが、すべての VPN トラフィックのインターフェイス ACL の通過を許可します。たとえば、外部インターフェイス ACL が復号化されたトラフィックの通過を許可しない場合でも、セキュリティアプライアンスはリモートプライベートネットワークを信頼し、復号化されたパケットの通過を許可します。このデフォルトの動作を変更できます。インターフェイス ACL に VPN 保護対象トラフィックの検査を行わせるためには、このチェックボックスをオフにします。
- Login Page Setting
 - ユーザはそのエイリアスで識別される接続プロファイルをログインページで選択できます。このチェックボックスをオンにしない場合、デフォルト接続プロファイルは DefaultWebVPNGroup です。
 - [Shutdown portal login page.] : ログインがディセーブルの場合に Web ページを表示します。
 - [Connection Profiles] : 接続 (トンネルグループ) のプロトコル固有属性を設定します。
 - [Add/Edit] : 接続プロファイル (トンネルグループ) を追加または編集します。
 - [Name] : 接続プロファイルの名前。
 - [Aliases] : 接続プロファイルの別名。
 - [SSL VPN Client Protocol] : SSL VPN クライアントにアクセス権を与えるかどうかを指定します。
 - [Group Policy] : この接続プロファイルのデフォルトグループポリシーを表示します。
 - [Allow user to choose connection, identified by alias in the table above, at login page] : [Login] ページでの接続プロファイル (トンネルグループ) エイリアスの表示をイネーブルにする場合はオンにします。
 - [Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.] : このオプションでは、接続プロファイルの選択プロセス時にグループ URL および証明書の値の相対的優先度を指定します。ASA で、推奨される値と一致する値が見つからない場合は、別の値に一致する接続プロファイルが選択されます。VPN エンドポイントで指定したグループ URL を、同じグループ URL を指定する接続プロファイルと照合するために、多数の古

い ASA ソフトウェア リリースで使用されるプリファレンスを利用する場合にのみ、このオプションをオンにします。このオプションは、デフォルトではオフになっています。オフにした場合、ASA は接続プロファイルで指定した証明書フィールド値を、エンドポイントで使用する証明書のフィールド値と照合して、接続プロファイルを割り当てます。

デバイス証明書の指定

[Specify Device Certificate] ペインを使用すると、接続を試みたときに、クライアントに対して ASA を識別する証明書を指定できます。この画面は、AnyConnect 接続プロファイルおよびクライアントレス接続プロファイル用です。Always-on IPsec/IKEv2 などの特定の AnyConnect 機能では、有効で信頼できるデバイスの証明書を ASA で利用できる必要があります。

ASA リリース 9.4.1 以降では、ECDSA 証明書を（AnyConnect クライアントとクライアントレス SSL の両方からの）SSL 接続に使用できます。このリリース以前は、AnyConnect IPsec 接続用の ECDSA 証明書だけがサポートされ、設定されました。

手順

-
- ステップ 1** (VPN 接続のみ) [Certificate with RSA Key] 領域で、次のいずれかのタスクを実行します。
- 1つの証明書を選択して、両方のプロトコルを使用してクライアントを認証する場合、[Use the same device certificate for SSL and IPsec IKEv2] チェックボックスをオンのままにします。リストボックスで使用できる証明書を選択したり、[Manage] をクリックして、使用する ID 証明書を作成したりできます。
 - [Use the same device certificate for SSL and IPsec IKEv2] チェックボックスをオフにして、SSL 接続または IPsec 接続の別個の証明書を指定します。
- ステップ 2** [Device Certificate] リストボックスから証明書を選択します。
- 必要な証明書が表示されない場合は、[Manage] ボタンをクリックして、ASA の ID 証明書を管理します。
- ステップ 3** (VPN 接続のみ) [ECDSA key] フィールドの [Certificate] で、リストボックスから ECDSA の証明書を選択するか、[Manage] をクリックして、ECDSA の ID 証明書を作成します。
- ステップ 4** [OK] をクリックします。
-

接続プロファイル、ポート設定

ASDM の接続プロファイル ペインで SSL および DTLS 接続（リモートアクセスのみ）のポート番号を設定します。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles]

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles]

フィールド

- [HTTPS Port] : HTTPS (ブラウザベース) SSL 接続用にイネーブルにするポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。
- [DTLS Port] : DTLS 接続用にイネーブルにする UDP ポート。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。

AnyConnect 接続プロファイル、基本属性

AnyConnect VPN 接続の基本属性を設定するには、[AnyConnect Connection Profiles] セクションで [Add] または [Edit] を選択します。[Add/Edit AnyConnect Connection Profile] > [Basic] ダイアログボックスが開きます。

- [Name] : [Add] の場合、追加する接続プロファイルの名前を指定します。[Edit] の場合、このフィールドは編集できません。
- [Aliases] : (任意) この接続の代替名を 1 つ以上入力します。名前は、スペースまたは句読点で区切ることができます。
- [Authentication] : 認識の方法を、次の中から 1 つ選択し、認証処理で使用する AAA サーバグループを指定します。
 - [Method] : 複数証明書認証のためのプロトコル交換を定義し、両方のセッションタイプでこれを利用するために認証プロトコルが拡張されています。AnyConnect SSL と IKEv2 クライアントプロトコルでセッションごとに複数の証明書を検証できます。使用する認証タイプを、AAA、AAA と証明書、証明書のみ、SAML、複数証明書および AAA、または複数証明書から選択します。選択に応じて、接続するために証明書を提供する必要がある場合があります。
 - [AAA Server Group] : ドロップダウンリストから AAA サーバグループを選択します。デフォルトの設定は LOCAL です。その場合、ASA が認証を処理するように指定されます。選択する前に、[Manage] をクリックして、このダイアログボックスの上に別のダイアログボックスを開き、AAA サーバグループの ASA コンフィギュレーションを表示したり変更することができます。
 - LOCAL 以外のグループを選択すると、[Use LOCAL if Server Group Fails] チェックボックスが選択できるようになります。
 - [Use LOCAL if Server Group fails] : Authentication Server Group 属性によって指定されたグループに障害が発生したときに、LOCAL データベースをイネーブルにする場合はオンにします。
- [Client Address Assignment] : 使用する DHCP サーバ、クライアントアドレスプール、クライアント IPv6 アドレスプールを選択します。
 - [DHCP Servers] : 使用する DHCP サーバの名前または IP アドレスを入力します。

- **[Client Address Pools]** : クライアントアドレス割り当てで使用する、選択可能な設定済みの IPv4 アドレス プールの名前を入力します。選択する前に、**[Select]** をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレスプールを表示したり、変更を加えたりすることができます。IPv4 アドレス プールを追加または編集する方法の詳細については を参照してください。
- **[Client IPv6 Address Pools]** : クライアント アドレス割り当てで使用する、選択可能な設定済みの IPv6 アドレス プールの名前を入力します。選択する前に、**[Select]** をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレスプールを表示したり、変更を加えたりすることができます。IPv6 アドレス プールを追加または編集する方法の詳細については を参照してください。
- **[Default Group Policy]** : 使用するグループ ポリシーを選択します。
 - **[Group Policy]** : この接続のデフォルト グループ ポリシーとして割り当てる VPN グループ ポリシーを選択します。VPN グループ ポリシーは、ユーザ指向属性値のペアの集合で、デバイスで内部に、またはRADIUSサーバで外部に保存できます。デフォルト値は `DfltGrpPolicy` です。**[Manage]** をクリックして別のダイアログボックスを重ねて開き、グループ ポリシー コンフィギュレーションに変更を加えることができます。
 - **[Enable SSL VPN client protocol]** : VPN 接続の SSL をイネーブルにする場合にオンにします。
 - **[Enable IPsec (IKEv2) client protocol]** : 接続で IKEv2 を使用する IPsec をイネーブルにする場合にオンにします。
 - **[DNS Servers]** : ポリシーの DNS サーバの IP アドレスを入力します (1 つまたは複数)。
 - **[WINS Servers]** : ポリシーの WINS サーバの IP アドレスを入力します (1 つまたは複数)。
 - **[Domain]** : デフォルトのドメイン名を入力します。
- **[Find]** : 検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、**[Next]** または **[Previous]** をクリックして検索を開始します。

接続プロファイル、詳細属性

[Advanced] メニュー項目とそのダイアログボックスでは、この接続に関する次の特性を設定できます。

- 一般属性
- クライアント アドレス指定属性
- 認証属性

- 認可属性
- アカウンティング属性
- ネーム サーバ属性
- クライアントレス SSL VPN 属性



(注) SSL VPN 属性および 2 次認証属性は、SSL VPN 接続プロファイルにだけ適用されます。

AnyConnect 接続プロファイル、一般属性

- [Enable Simple Certificate Enrollment (SCEP) for this Connection Profile]
- [Strip the realm from username before passing it on to the AAA server]
- [Strip the group from username before passing it on to the AAA server]
- [Group Delimiter]
- [Enable Password Management] : ユーザへのパスワード期限切れ通知に関するパラメータを設定できます。
 - [Notify user __ days prior to password expiration] : パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時に ASDM がユーザに通知するよう指定します。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ~ 180 日です。
 - [Notify user on the day password expires] : パスワードが期限切れになる当日にユーザに通知します。

いずれの場合でも、変更されずにパスワードが期限切れになったとき、ASA ではユーザによるパスワードの変更が可能です。現在のパスワードの期限が切れていなければ、ユーザはそのパスワードで引き続きログインできます。

この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。
- [Translate Assigned IP Address to Public IP Address] : 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、内部サーバおよびネットワークセキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。この機能は、トンネルグループごとに 1 つのインターフェイスでイネーブルにすることができます。

- **[Enable the address translation on interface]** : アドレス変換を可能にし、アドレスが表示されるインターフェイスを選択することができます。 *outside* は AnyConnect 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) ルーティングの問題および他の制限事項のため、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。

- **[Find]** : 検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、 **[Next]** または **[Previous]** をクリックして検索を開始します。

接続プロファイル、クライアントアドレス指定

接続プロファイルの **[Client Addressing]** ペインでは、この接続プロファイルで使用するために特定のインターフェイスに IP アドレス プールを割り当てます。 **[Client Addressing]** ペインはすべてのクライアント接続プロファイルに共通で、次の ASDM パスからアクセスできます。

- **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles]**
- **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles]**
- **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles]**

ここで設定するアドレス プールは、接続プロファイルの **[Basic]** ペインでも設定できます。

AnyConnect 接続プロファイルでは、IPv4 アドレス プールだけでなく IPv6 アドレス プールも割り当てることができます。

クライアントアドレス指定を設定するには、リモートアクセスクライアント接続プロファイル (AnyConnect、IKEv1 または IKEv2) を開き、 **[Advanced] > [Client Addressing]** を選択します。

- アドレスプールのコンフィギュレーションを表示または変更するには、ダイアログボックスの **[Add]** または **[Edit]** をクリックします。 **[Assign Address Pools to Interface]** ダイアログボックスが開きます。このダイアログボックスでは、ASA で設定されたインターフェイスに IP アドレス プールを割り当てることができます。 **[Select]** をクリックします。このダイアログボックスを使用して、アドレスプールのコンフィギュレーションを表示します。アドレスプールのコンフィギュレーションを変更するには、次の手順を実行します。
 - ASA にアドレス プールを追加するには、 **[Add]** をクリックします。 **[Add IP Pool]** ダイアログボックスが開きます。

- ASA のアドレスプールのコンフィギュレーションを変更するには、[Edit] をクリックします。プール内のアドレスが使用されていない場合には、[Edit IP Pool] ダイアログボックスが開きます。

使用中の場合はアドレスプールを変更できません。[Edit] をクリックしたときにアドレスプールが使用中であった場合、ASDM は、エラーメッセージとともに、プール内のそのアドレスを使用している接続名およびユーザ名の一覧を表示します。

- ASA 上のアドレスプールを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

使用中の場合はアドレスプールを削除できません。[Delete] をクリックしたときにアドレスプールが使用中であった場合、ASDM は、エラーメッセージとともに、プール内のそのアドレスを使用している接続名の一覧を表示します。

- アドレスプールをインターフェイスに割り当てるには、[Add] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。アドレスプールを割り当てるインターフェイスを選択します。[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ダイアログボックスが開きます。インターフェイスに割り当てる個々の未割り当てプールをダブルクリックするか、または個々の未割り当てプールを選択して [Assign] をクリックします。隣のフィールドにプール割り当ての一覧が表示されます。[OK] をクリックして、これらのアドレスプールの名前を [Address Pools] フィールドに取り込み、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。
- インターフェイスに割り当てられているアドレスプールを変更するには、そのインターフェイスをダブルクリックするか、インターフェイスを選択して [Edit] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。アドレスプールを削除するには、各プール名をダブルクリックし、キーボードの [Delete] キーを押します。インターフェイスにその他のフィールドを割り当てる場合は、[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ダイアログボックスが開きます。[Assign] フィールドには、インターフェイスに割り当てられているアドレスプール名が表示されます。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。[OK] をクリックして、これらのアドレスプールの名前を [Address Pools] フィールドを確認し、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。
- エントリを削除するには、そのエントリを選択して [Delete] をクリックします。

関連トピック

[接続プロファイル、クライアントアドレス指定、追加または編集](#) (128 ページ)

[接続プロファイル、アドレスプール](#) (129 ページ)

[接続プロファイル、詳細、IP プールの追加または編集](#) (129 ページ)

接続プロファイル、クライアントアドレス指定、追加または編集

接続プロファイルにアドレスプールを割り当てるには、[Advanced]>[Client Addressing] を選択し、[Add] または [Edit] を選択します。

- [Interface] : アドレス プールの割り当て先インターフェイスを選択します。デフォルトは DMZ です。
- [Address Pools] : 指定したインターフェイスに割り当てられるアドレス プールを指定します。
- [Select] : [Select Address Pools] ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てられるアドレス プールを1つ以上選択できます。選択内容は、[Assign Address Pools to Interface] ダイアログボックスの [Address Pools] フィールドに表示されます。

接続プロファイル、アドレス プール

[Connection Profile] > [Advanced] の [Select Address Pools] ダイアログボックスに、クライアントアドレス割り当てに使用可能なアドレスプールのプール名、開始アドレスと終了アドレス、およびサブネットマスクが表示されます。そのリストを使って接続プロファイルを追加、編集、または削除できます。

- [Add] : [Add IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、新しい IP アドレス プールを設定できます。
- [Edit] : [Edit IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、選択した IP アドレス プールを変更できます。
- [Delete] : 選択したアドレス プールを削除します。確認されず、やり直しもできません。
- [Assign] : インターフェイスに割り当てられているアドレス プール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。

接続プロファイル、詳細、IP プールの追加または編集

[Connection Profile] > [Advanced] の [Add or Edit IP Pool] ダイアログボックスを使用すれば、クライアントアドレス割り当て用の IP アドレスの範囲を指定または変更できます。

- [Name] : IP アドレス プールに割り当てられている名前を指定します。
- [Starting IP Address] : プールの最初の IP アドレスを指定します。
- [Ending IP Address] : プールの最後の IP アドレスを指定します。
- [Subnet Mask] : プール内のアドレスに適用するサブネット マスクを選択します。

AnyConnect 接続プロファイル、認証属性

[Connection Profile] > [Advanced] > [Authentication] タブで、次のフィールドを設定できます。

- [Interface-specific Authentication Server Groups] : 指定のインターフェイスに対する認証サーバグループの割り当てを管理します。

- [Add or Edit] : [Assign Authentication Server Group to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバグループを指定するとともに、選択したサーバグループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
- [Delete] : 選択したサーバグループをテーブルから削除します。確認されず、やり直しもできません。
- [Username Mapping from Certificate] : ユーザ名を抽出する方法およびデジタル証明書のフィールドを指定できます。



(注) この機能はマルチコンテキストモードではサポートされません。

- [Pre-fill Username from Certificate] : 指定した証明書のフィールドからユーザ名を抽出し、このパネルの後に続くオプションに従って、ユーザ名/パスワード認証および認可に使用します。
- [Hide username from end user] : 抽出したユーザ名はエンドユーザに表示されません。
- [Use script to choose username] : デジタル証明書からユーザ名を選択する場合に使用するスクリプト名を指定します。デフォルトは [None] です。
- [Add or Edit] : [Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザ名のマッピングに使用するスクリプトを定義できます。
- [Delete] : 選択したスクリプトを削除します。確認されず、やり直しもできません。
- [Use the entire DN as the username] : 証明書の [Distinguished Name] フィールド全体をユーザ名として使用する場合に指定します。
- [Specify the certificate fields to be used as the username] : ユーザ名に結合する 1 つ以上のフィールドを指定します。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country (国名) : 2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name (一般名) : 人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。

属性	定義
EA	E-mail Address（電子メールアドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザプリンシパル名）。

- [Primary Field]：ユーザ名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field]は無視されます。
- [Secondary Field]：[Primary Field]が指定されていない場合、使用するフィールドを選択します。
- [Find]：検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next]または [Previous] をクリックして検索を開始します。

接続プロファイル、2次認証属性

[Connection Profile] > [Advanced] の下の [Secondary Authentication] を使用すれば、二重認証としても知られる 2 次認証を設定することができます。2 次認証が有効になっている場合は、エンドユーザがログオンするときに有効な認証クレデンシャルを 2 セット入力する必要があります。

す。証明書のユーザ名の事前入力と2次認証を組み合わせで使用できます。このダイアログボックスのフィールドは、1次認証で設定するフィールドと似ていますが、これらのフィールドは2次認証にだけ関連します。

二重認証がイネーブルになっている場合、これらの属性はユーザ名として使用する1つ以上のフィールドを証明書から選択します。証明書属性からセカンダリユーザ名を設定すると、セキュリティアプライアンスは、指定された証明書フィールドを、2次ユーザ名/パスワード認証処理に2つ目のユーザ名を使用するよう強制されます。



(注) 証明書のセカンダリユーザ名とともに2次認証サーバグループも指定する場合でも、認証処理にはプライマリユーザ名だけが使用されます。

- [Secondary Authorization Server Group] : セカンダリ クレデンシャルを抽出する認証サーバグループを指定します。
 - [Server Group] : セカンダリ サーバ AAA グループとして使用する認証サーバグループを選択します。デフォルトは none です。SDI サーバグループはセカンダリサーバグループにできません。
 - [Manage] : [Configure AAA Server Group] ダイアログボックスが開きます。
 - [Use LOCAL if Server Group fails] : 指定したサーバグループに障害が発生した場合の LOCAL データベースへのフォールバックを指定します。
 - [Use primary username] : ログインダイアログがユーザ名を1つだけ要求するよう指定します。
 - [Attributes Server] : プライマリ属性サーバかセカンダリ属性サーバかを選択します。



(注) この接続プロファイルにも認証サーバを指定すると、その認証サーバの設定が優先されます。ASAはセカンダリ認証サーバを無視します。

- [Session Username Server] : プライマリ セッションユーザ名サーバかセカンダリセッションユーザ名サーバかを指定します。
- [Interface-Specific Authorization Server Groups] : 指定のインターフェイスに対する認可サーバグループの割り当てを管理します。
 - [Add or Edit] : [Assign Authentication Server Group to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバグループを指定するとともに、選択したサーバグループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。

- **[Delete]** : 選択したサーバグループをテーブルから削除します。確認されず、やり直しもできません。
- **[Username Mapping from Certificate]** : ユーザ名を抽出するデジタル証明書のフィールドを指定できます。
- **[Pre-fill Username from Certificate]** : このパネルで指定されている最初のフィールドおよび2番目のフィールドから、2次認証に使用される名前を抽出する場合にオンにします。この属性をオンにする前に、AAA および証明書の認証方式を設定する必要があります。これを行うには、同じウィンドウの **[Basic]** パネルに戻り、**[Method]** の横の **[Both]** をオンにします。
- **[Hide username from end user]** : 2次認証に使用されるユーザ名を VPN ユーザに非表示にする場合にオンにします。
- **[Fallback when a certificate is unavailable]** : この属性は、**[Hide username from end user]** がオンの場合にのみ使用可能です。証明書が使用不可な場合は、Cisco Secure Desktop のホストスキャンデータを使用して、2次認証のユーザ名を事前入力します。
- **[Password]** : 2次認証に使用されるパスワードの取得方式として次のいずれかを選択します。
 - **[Prompt]** : ユーザにパスワードを入力するようプロンプトを表示します。
 - **[Use Primary]** : すべての2次認証に1次認証のパスワードを再利用します。
 - **[Use]** : すべての2次認証の共通セカンダリパスワードを入力します。
- **[Specify the certificate fields to be used as the username]** : ユーザ名として一致する1つ以上のフィールドを指定します。セカンダリユーザ名/パスワード認証または認可に証明書のユーザ名事前入力機能でこのユーザ名を使用するには、ユーザ名事前入力およびセカンダリユーザ名事前入力も設定する必要があります。
 - **[Primary Field]** : ユーザ名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、**[Secondary Field]** は無視されます。
 - **[Secondary Field]** : **[Primary Field]** が指定されていない場合、使用するフィールドを選択します。

最初のフィールドおよび2番目のフィールドの属性には、次のオプションがあります。

属性	定義
C	Country (国名) : 2文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name (一般名) : 人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。

属性	定義
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メールアドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザプリンシパル名）。

- [Use the entire DN as the username]：完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得します。
- [Use script to select username]：デジタル証明書からユーザ名を抽出するスクリプトを指定します。デフォルトは [None] です。
 - [Add or Edit]：[Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザ名のマッピングに使用するスクリプトを定義できます。
 - [Delete]：選択したスクリプトを削除します。確認されず、やり直しもできません。

AnyConnect 接続プロファイル、認可属性

AnyConnect 接続プロファイルの [Authorization] ダイアログボックスを使用すれば、インターフェイス固有の認可サーバグループを表示、追加、編集、または削除することができます。このダイアログボックスのテーブルの各行には、インターフェイス固有サーバグループのステータスが表示されます。表示されるのは、インターフェイス名、それに関連付けられたサーバグループ、および選択したサーバグループで障害が発生したときにローカルデータベースへのフォールバックがイネーブルになっているかどうかです。

このペインのフィールドは、AnyConnect、IKEv1、IKEv2、およびクライアントレス SSL 接続プロファイルで共通です。

- [Authorization Server Group] : 認可パラメータを記述する認可サーバグループを指定します。
 - [Server Group] : 使用する認可サーバグループを選択します。デフォルトは none です。
 - [Manage] : [Configure AAA Server Group] ダイアログボックスが開きます。AAA サーバの設定については、[クライアントレス SSL VPN 接続プロファイル、認証、サーバグループの追加 \(144 ページ\)](#) を参照してください。
 - [Users must exist in the authorization database to connect] : ユーザがこの基準を満たす必要がある場合は、このチェックボックスをオンにします。
- [Interface-specific Authorization Server Groups] : 指定のインターフェイスに対する認可サーバグループの割り当てを管理します。
 - [Add or Edit] : [Assign Authentication Server Group to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバグループを指定するとともに、選択したサーバグループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
 - [Delete] : 選択したサーバグループをテーブルから削除します。確認されず、やり直しもできません。
- [Username Mapping from Certificate] : ユーザ名を抽出するデジタル証明書のフィールドを指定できます。
 - [Use script to select username] : デジタル証明書からユーザ名を選択する場合に使用するスクリプト名を指定します。デフォルトは [None] です。証明書フィールドからユーザ名を選択するスクリプトを作成する方法については、を参照してください。
 - [Add or Edit] : [Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザ名のマッピングに使用するスクリプトを定義できます。
 - [Delete] : 選択したスクリプトを削除します。確認されず、やり直しもできません。

- [Use the entire DN as the username] : 証明書の [Distinguished Name] フィールド全体をユーザ名として使用する場合に指定します。
- [Specify the certificate fields to be used as the username] : ユーザ名に結合する 1 つ以上のフィールドを指定します。
- [Primary Field] : ユーザ名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。
- [Secondary Field] : [Primary Field] が指定されていない場合、使用するフィールドを選択します。
- [Find] : 検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

AnyConnect接続プロファイル、認可、ユーザ名を選択するためのスクリプトの内容の追加

AnyConnect 接続プロファイルの [Authorization] ペインで [use a script to select username] を選択し、[Add] または [Edit] ボタンをクリックすると、次のフィールドが表示されます。

スクリプトでは、他のマッピングオプションでは表示されない認可用の証明書フィールドを使用できます。



(注) スクリプトを使用した証明書からのユーザ名事前入力でクライアント証明書のユーザ名が見つからない場合、AnyConnect クライアントおよびクライアントレス WebVPN に「Unknown」と表示されます。

- [Script Name] : スクリプトの名前を指定します。認証および認可のスクリプト名は同じでなければなりません。ここでスクリプトを定義し、CLI は、この機能を実行するために同じスクリプトを使用します。
- [Select script parameters] : スクリプトの属性および内容を指定します。
- [Value for Username] : ユーザ名として使用する一般的な DN 属性のドロップダウンリスト (Subject DN) から属性を選択します。
- [No Filtering] : 指定した DN 名全体を使用するよう指定します。
- [Filter by substring] : 開始インデックス (一致する最初の文字の文字列内の位置) および終了インデックス (検索する文字列数) を指定します。このオプションを選択する場合、開始インデックスは、空白にはできません。終了インデックスを空白にするとデフォルトは -1 となり、文字列全体が一致するかどうか検索されます。

たとえば、ホスト/ユーザの値を含む DN 属性の Common Name (CN) を選択したとします。次の表に、さまざまな戻り値を実現する部分文字列を使用してこの値をフィルタする方法を示します。戻り値は、ユーザ名として実際に事前入力される値です。

表 2: 部分文字列によるフィルタリング

開始インデックス	終了インデックス	戻り値
1	5	host/
6	10	user
6	-1	user

この表の3行目のようにマイナスのインデックスを使用して、文字列の最後から部分文字列の最後まで（この場合は「user」の「r」）カウントするよう指定します。

部分文字列によるフィルタリングを使用する場合、検索する部分文字列の長さがわかっていることが必要です。次の例では、正規表現照合または Lua 形式のカスタム スクリプトを使用します。

- 例 1 : [Regular Expression Matching] : [Regular Expression] フィールドに検索に適用する正規表現を入力します。一般的な正規表現の演算子が適用されます。「Email Address (EA)」DN 値の @ 記号までのすべての文字列をフィルタリングするために正規表現を使用するとします。`^[^@]*` がこれを実行できる正規表現の 1 つです。この例では、DN 値に `user1234@example.com` が含まれている場合、正規表現の後の戻り値は `user1234` となります。
- 例 2 : [Use custom script in LUA format] : 検索フィールドを解析するために、LUA プログラム言語で記述されたカスタムスクリプトを指定します。このオプションを選択すると、カスタム LUA スクリプトをフィールドに入力できるようになります。スクリプトは次のようになります。

```
return cert.subject.cn..'/'..'cert.subject.1
```

1 つのユーザ名として使用する 2 つの DN フィールド、ユーザ名 (cn) および地域 (l) を結合し、2 つのフィールド間にスラッシュ (/) 文字を挿入します。

次の表に LUA スクリプトで使用可能な属性名と説明を示します。



(注) LUA では、大文字と小文字が区別されます。

表 3: 属性名と説明

属性名	説明
cert.subject.c	Country
cert.subject.cn	Common Name
cert.subject.dnq	DN 修飾子
cert.subject.ea	電子メールアドレス

cert.subject.genq	世代修飾子
cert.subject.gn	名
cert.subject.i	イニシャル
cert.subject.l	地名
cert.subject.n	名前
cert.subject.o	マニュアルの構成
cert.subject.ou	組織単位
cert.subject.ser	サブジェクト シリアル番号
cert.subject.sn	姓
cert.subject.sp	州/県
cert.subject.t	Title
cert.subject.uid	ユーザ ID
cert.issuer.c	Country
cert.issuer.cn	Common Name
cert.issuer.dnq	DN 修飾子
cert.issuer.ea	電子メールアドレス
cert.issuer.genq	世代修飾子
cert.issuer.gn	名
cert.issuer.i	イニシャル
cert.issuer.l	地名
cert.issuer.n	名前
cert.issuer.o	マニュアルの構成
cert.issuer.ou	組織単位
cert.issuer.ser	発行元シリアル番号
cert.issuer.sn	姓
cert.issuer.sp	州/県
cert.issuer.t	Title

cert.issuer.uid	ユーザ ID
cert.serialnumber	証明書シリアル番号
cert.subjectaltname.upn	ユーザ プリンシパル名

トンネルグループ スクリプトをアクティブにしているときにエラーが発生し、スクリプトがアクティブにならなかった場合、管理者のコンソールにエラー メッセージが表示されます。

クライアントレス SSL VPN 接続プロファイル、インターフェイスへの認可サーバグループの割り当て

このダイアログボックスでは、インターフェイスを AAA サーバグループに関連付けられます。結果は、[Authorization] ダイアログボックスのテーブルに表示されます。

- [Interface] : インターフェイスを選択します。デフォルトは DMZ です。
- [Server Group] : 選択したインターフェイスに割り当てるサーバグループを選択します。デフォルトは LOCAL です。
- [Manage] : [Configure AAA Server Group] ダイアログボックスが開きます。

接続プロファイル、アカウントिंग

[Connection Profile] > [Advanced] の [Accounting] ペインでは、ASA 全体のアカウントिंग オプションを設定します。

- [Accounting Server Group] : アカウントिंगに使用するすでに定義済みのサーバグループを選択します。
- [Manage] : AAA サーバグループを作成できる [Configure AAA Server Groups] ダイアログボックスが開きます。

接続プロファイル、グループエイリアスとグループ URL

[Connection Profile] > [Advanced] の [GroupAlias/Group Group URL] ダイアログボックスで、リモート ユーザのログイン時に表示される内容に影響を与える属性を設定します。

このダイアログのフィールドは AnyConnect クライアントおよびクライアントレス SSL VPN で同じですが、クライアントレス SSL VPN には追加のフィールドが1つあります。接続プロファイルのタブの名前は、AnyConnect では [Group URL/Group Alias] で、クライアントレス SSL VPN では [Clientless SSL VPN] です。

- [Login and Logout (Portal) Page Customization (Clientless SSL VPN only)] : 適用する事前設定されたカスタマイズ属性を指定することにより、ユーザ ログイン ページの外観を設定します。デフォルトは DfltCustomization です。新しいカスタマイゼーションオブジェクトを作成するには、[Manage] をクリックします。

- [Enable the display of Radius Reject-Message on the login screen] : 認証が拒否されたときにログイン ダイアログボックスに RADIUS-reject メッセージを表示するには、このチェックボックスをオンにします。
- [Enable the display of SecurID message on the login screen] : ログイン ダイアログボックスに SecurID メッセージを表示するには、このチェックボックスをオンにします。
- [Connection Aliases] : 接続エイリアスとそのステータス。ログイン時にユーザが特定の接続（トンネルグループ）を選択できるように接続が設定されている場合は、ユーザのログイン ページに接続エイリアスが表示されます。エイリアスを追加または削除するには、[Add] または [Delete] ボタンをクリックします。エイリアスを編集するには、テーブルでそのエイリアスをダブルクリックし、エントリを編集します。イネーブルになっているステータスを変更するには、テーブル内のチェックボックスをオンまたはオフにします。
- [Group URLs] : グループ URL とそのステータス。ログイン時にユーザが特定のグループを選択できるように接続が設定されている場合は、ユーザのログイン ページにグループ URL が表示されます。URL を追加または削除するには、[Add] または [Delete] ボタンをクリックします。URL を編集 ([Edit]) するには、テーブル内の URL をダブルクリックしてエントリを編集します。イネーブルになっているステータスを変更するには、テーブル内のチェックボックスをオンまたはオフにします。
- [Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored.)] : グループ URL に接続しているクライアントで Cisco Secure Desktop のアプリケーションを実行するかどうかを選択します。これらのオプションは、グループ URL を追加する場合にのみ表示されます。クライアントを免除すると、セキュリティアプライアンスがこれらのユーザからエンドポイント基準を受信しなくなるので、ユーザが VPN にアクセスにできるように DAP コンフィギュレーションの変更が必要になることがあります。次のオプションから選択します。
 - [Always run CSD] : グループ URL に接続しているすべてのクライアントで Hostscan を実行します。
 - [Disable CSD for both AnyConnect and clientless SSL VPN] : グループ URL に接続しているすべてのクライアントの Hostscan 処理を免除します。
 - [Disable CSD for AnyConnect only] : グループ URL に接続している AnyConnect クライアントの Hostscan 処理を免除します。ただし、クライアントレス接続では Hostscan を使用します。

接続プロファイル、クライアントレス SSL VPN

[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] ダイアログボックスには、現在定義されているクライアントレス SSL VPN 接続プロファイルおよびグローバルのクライアントレス オプションが一覧表示されます。

- **[Access Interfaces]** : アクセスでイネーブルにするインターフェイスを選択できます。このテーブルのフィールドには、インターフェイス名やチェックボックスが表示され、アクセスを許可するかどうかを指定します。
 - **[Device Certificate]** : RSA キーまたは ECDSA キーまたはトラストポイントの認証の証明書を指定できます。2つのトラストポイントを設定するオプションがあります。クライアントは、ベンダー ID ペイロードによる ECDSA のサポートを示します。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。
 - **[Manage]** : **[Manage Identity Certificates]** ダイアログボックスが開きます。このダイアログボックスでは、選択した証明書の詳細を追加、編集、削除、エクスポート、または表示できます。
 - **[Port Setting]** : クライアントレス SSL および IPsec (IKEv2) 接続のポート番号を設定します。範囲は 1 ~ 65535 です。デフォルトはポート 443 です。
- **Login Page Setting**
 - エイリアスで識別される接続プロファイルをログインページで選択できます。選択しない場合は、**DefaultWebVPNGroup** が接続プロファイルになります。ユーザのログインページに、ユーザが接続で使用する特定のトンネルグループを選択するためのドロップダウンリストが表示されるように指定します。
 - **[Allow user to enter internal password on the login page]** : 内部サーバへのアクセス時に異なるパスワードを入力するオプションを追加します。
 - **[Shutdown portal login page]** : ログインがディセーブルの場合に Web ページを表示します。
- **[Connection Profiles]** : この接続 (トンネルグループ) の接続ポリシーを決定するレコードを示した接続テーブルを表示します。各レコードによって、その接続のデフォルトグループポリシーが識別されます。レコードには、プロトコル固有の接続パラメータが含まれています。
 - **[Add]** : 選択した接続の **[Add Clientless SSL VPN]** ダイアログボックスが開きます。
 - **[Edit]** : 選択した接続の **[Edit Clientless SSL VPN]** ダイアログボックスが開きます。
 - **[Delete]** : 選択した接続をテーブルから削除します。確認されず、やり直しもできません。
 - **[Name]** : 接続プロファイルの名前。
 - **[Enabled]** : イネーブルになっている場合にチェックマークが付きます。
 - **[Aliases]** : 接続プロファイルの別名。
 - **[Authentication Method]** : 使用する認証方式を指定します。
 - **[Group Policy]** : この接続プロファイルのデフォルトグループポリシーを表示します。

- [Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.] : このオプションでは、接続プロファイルの選択プロセス時にグループ URL および証明書の値の相対的プリファレンスを指定します。ASA で、エンドポイントによって指定された推奨される値を、接続プロファイルによって指定された推奨される値と照合できない場合は、別の値と一致する接続プロファイルが選択されます。VPN エンドポイントで指定したグループ URL を、同じグループ URL を指定する接続プロファイルと照合するために、多数の古い ASA ソフトウェアリリースで使用されるプリファレンスを利用する場合にのみ、このオプションをオンにします。このオプションは、デフォルトではオフになっています。オフにした場合、ASA は接続プロファイルで指定した証明書フィールド値を、エンドポイントで使用する証明書のフィールド値と照合して、接続プロファイルを割り当てます。

クライアントレス SSL VPN 接続プロファイル、基本属性

[Clientless SSL VPN Connection Profile] > [Advanced] > [Basic] ダイアログボックスでは、基本属性を設定します。

- [Name] : 接続名を指定します。編集機能の場合、このフィールドは読み取り専用です。
- [Aliases] : (任意) この接続の代替名を 1 つ以上指定します。[Clientless SSL VPN Access Connections] ダイアログボックスでそのオプションを設定している場合に、ログイン ページに別名が表示されます。
- [Authentication] : 認証パラメータを指定します。
 - [Method] : この接続で、AAA 認証、証明書認証、またはその両方を使用するかどうかを指定します。デフォルトは AAA 認証です。
 - [AAA server Group] : この接続の認証処理で使用する AAA サーバグループを選択します。デフォルトは LOCAL です。
 - [Manage] : [Configure AAA Server Group] ダイアログボックスが開きます。
- [DNS Server Group] : この接続の DNS サーバグループとして使用するサーバを選択します。デフォルトは DefaultDNS です。
- [Default Group Policy] : この接続で使用するデフォルト グループ ポリシーのパラメータを指定します。
 - [Group Policy] : この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。
 - [Clientless SSL VPN Protocol] : この接続でのクライアントレス SSL VPN プロトコルをイネーブルまたはディセーブルにします。

クライアントレス SSL VPN 接続プロファイル、一般属性

[Clientless SSL VPN Connection Profile] > [Advanced] > [General] ダイアログボックスを使用して、AAA サーバに渡す前にユーザ名からレلمとグループを除去するかどうかを指定し、パスワード管理オプションを指定します。

- [Password Management] : AAA サーバからの account-disabled インジケータの上書きに関するパラメータと、ユーザに対するパスワード期限切れ通知に関するパラメータを設定できます。
- [Enable notification password management] : このチェックボックスをオンにすると、次の2つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを決定します。デフォルトでは、パスワードが期限切れになるより14日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は1～180日です。



(注) この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

いずれの場合でも、変更されずにパスワードが期限切れになったとき、ASA ではユーザによるパスワードの変更が可能です。現行のパスワードが失効していない場合、ユーザ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。

このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。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。

クライアントレス SSL VPN 接続プロファイル、認証

[Clientless SSL VPN Connection Profile] > [Advanced] > [Authentication] ダイアログボックスでは、インターフェイス固有の認可サーバグループを表示、追加、編集、または削除できます。このダイアログボックスのテーブルの各行には、インターフェイス固有サーバグループのステータスが表示されます。表示されるのは、インターフェイス名、それに関連付けられたサーバグループ、および選択したサーバグループで障害が発生したときにローカルデータベースへのフォールバックがイネーブルになっているかどうかです。

[Authentication] ペインのフィールドは、AnyConnect の認証と同じです ([AnyConnect 接続プロファイル、認証属性 \(129 ページ\)](#) を参照)。

クライアントレス SSL VPN 接続プロファイル、認証、サーバグループの追加

[Clientless SSL VPN Connection Profile] > [Advanced] > [Authentication] ダイアログボックスの [Add] ボタンをクリックすると、インターフェイスを AAA サーバグループに関連付けることができます。

この設定を行うフィールドについては、[クライアントレス SSL VPN 接続プロファイル、インターフェイスへの認可サーバグループの割り当て \(139 ページ\)](#) を参照してください。

クライアントレス SSL VPN 接続プロファイル、2 次認証

クライアントレス SSL の 2 次認証設定フィールドは、[接続プロファイル、2 次認証属性 \(131 ページ\)](#) に記載されている AnyConnect クライアント アクセスと同様です。

クライアントレス SSL VPN 接続プロファイル、認可

クライアントレス SSL の認可設定フィールドは、AnyConnect、IKEv1、および IKEv2 の場合と同じです。これらのフィールドの詳細については、[AnyConnect 接続プロファイル、認可属性 \(135 ページ\)](#) を参照してください。

クライアントレス SSL VPN 接続プロファイル、NetBIOS サーバ

クライアントレス SSL VPN 接続プロファイルの [Advanced] > [NetBIOS Servers] ダイアログボックスには、設定済みの NetBIOS サーバの属性が表示されます。[Add or Edit Tunnel Group dialog box for Clientless SSL VPN access] > [NetBIOS] ダイアログボックスを使用すれば、トンネルグループの NetBIOS 属性を設定することができます。クライアントレス SSL VPN では、NetBIOS と Common Internet File System (共通インターネット ファイル システム) プロトコルを使用して、リモートシステム上のファイルにアクセスしたり、ファイルを共有したりします。Windows コンピュータにそのコンピュータ名を使用してファイル共有接続をしようとする、指定されたファイルサーバはネットワーク上のリソースを識別する特定の NetBIOS 名と対応します。

ASA は、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを送信します。クライアントレス SSL VPN では、リモートシステムのファイルにアクセスまたは共有するための NetBIOS が必要です。

NBNS 機能を動作させるには、少なくとも 1 台の NetBIOS サーバ (ホスト) を設定する必要があります。冗長性を実現するために NBNS サーバを 3 つまで設定できます。ASA は、リストの最初のサーバを NetBIOS/CIFS 名前解決に使用します。クエリーが失敗すると、次のサーバが使用されます。

[NetBIOS Servers] ペインのフィールド

- [IP Address] : 設定された NetBIOS サーバの IP アドレスを表示します。
- [Master Browser] : サーバが WINS サーバであるか、あるいは CIFS サーバ (つまりマスター ブラウザ) にもなれるサーバであることを表します。

- [Timeout (seconds)] : サーバが NBNS クエリーに対する応答を待つ最初の時間を秒単位で表示します。この時間を過ぎると、次のサーバにクエリーを送信します。
- [Retries] : 設定されたサーバに対する NBNS クエリーの送信を順番にリトライする回数を表示します。言い換えれば、エラーを返すまでサーバのリストを巡回する回数ということです。最小リトライ数は0です。デフォルトの再試行回数は2回です。最大リトライ数は10です。
- [Add/Edit] : NetBIOS サーバを追加します。[Add or Edit NetBIOS Server] ダイアログボックスが開きます。
- [Delete] : 選択した NetBIOS 行をリストから削除します。
- [Move Up/Move Down] : ASA は、このボックスに表示された順序で、NetBIOS サーバに NBNS クエリーを送信します。このボックスを使用して、クエリーをリスト内で上下に動かすことにより、優先順位を変更します。

クライアントレス SSL VPN 接続プロファイル、クライアントレス SSL VPN

クライアントレス接続プロファイルの [Advanced] > [Clientless SSL VPN] ペインでは、ログイン時にリモート ユーザに表示される内容に影響する属性を設定できます。

このダイアログと AnyConnect 接続プロファイルのフィールドは似ているため、詳細については [接続プロファイル、グループエイリアスとグループ URL \(139 ページ\)](#) を参照してください。

IKEv1 接続プロファイル

IKEv1 接続プロファイルは、L2TP/IPsec などのネイティブ VPN クライアントとサードパーティ VPN クライアントの認証ポリシーを定義します。IKEv1 接続プロファイルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] ペインで設定します。

- [Access Interfaces] : IPsec アクセスでイネーブルにするインターフェイスを選択します。デフォルトでは、アクセス方式は何も選択されていません。
- [Connection Profiles] : 既存の IPsec 接続の設定済みパラメータを表形式で表示します。[Connections] テーブルには、接続ポリシーを決定するレコードが表示されます。1つのレコードによって、その接続のデフォルトグループポリシーが識別されます。レコードにはプロトコル固有の接続パラメータが含まれています。テーブルには、次のカラムがあります。
 - [Name] : IPsec IKEv1 接続の名前または IP アドレスを指定します。

- [IPsec Enabled] : IPsec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPsec Remote Access Connection] の [Basic] ダイアログボックスでイネーブルにします。
- [L2TP/IPsec Enabled] : L2TP/IPsec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPsec Remote Access Connection] の [Basic] ダイアログボックスでイネーブルにします。
- [Authentication Server Group] : 認証を提供できるサーバグループの名前。
- [Group Policy] : この IPsec 接続のグループ ポリシーの名前を示します。



(注) [Delete] : 選択したサーバグループをテーブルから削除します。確認されず、やり直しもできません。

IPsec リモート アクセス接続プロファイル、[Basic] タブ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] > [Add/Edit] > [Basic] の [Add or Edit IPsec Remote Access Connection Profile Basic] ダイアログボックスを使用すると、L2TP-IPsec を含めて、IPsec IKEv1 VPN 接続用の共通属性を設定できます。

- [Name] : 接続プロファイルの名前。
- [IKE Peer Authentication] : IKE ピアを設定します。
 - [Pre-shared key] : 接続用の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Identity Certificate] : ID 証明書が設定され、登録されている場合は、ID 証明書の名前を選択します。[Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、選択した証明書の詳細を追加、編集、削除、エクスポート、表示できます。
- [User Authentication] : ユーザ認証で使用するサーバの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
 - [Server Group] : ユーザ認証で使用するサーバグループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバグループを選択すると、[Fallback] チェックボックスが選択できるようになります。サーバグループを追加するには、[Manage] ボタンをクリックします。
 - [Fallback] : 指定したサーバグループで障害が発生した場合に、ユーザ認証で LOCAL を使用するかどうかを指定します。
- [Client Address Assignment] : クライアント属性の割り当てに関連する属性を指定します。

- [DHCP Servers] : 使用する DHCP サーバの IP アドレスを指定します。最大で 10 台までのサーバをスペースで区切って追加できます。
- [Client Address Pools] : 事前定義済みのアドレス プールを 6 個まで指定します。アドレス プールを定義するには、[Select] ボタンをクリックします。
- [Default Group Policy] : デフォルト グループ ポリシーに関連する属性を指定します。
- [Group Policy] : この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。このグループ ポリシーに関連付ける新しいグループ ポリシーを定義するには、[Manage] をクリックします。
- [Enable IPsec protocol] と [Enable L2TP over IPsec protocol] : この接続で使用するプロトコルを選択します。

[Add/Edit Remote Access Connections] > [Advanced] > [General]

このダイアログボックスを使用して、AAA サーバに渡す前にユーザ名からレルムとグループを除去するかどうかを指定し、パスワード管理パラメータを指定します。

- [Strip the realm from the username before passing it on to the AAA server] : ユーザ名を AAA サーバに渡す前に、レルム（管理ドメイン）をユーザ名から除去する処理をイネーブルまたはディセーブルにします。認証時にユーザ名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウントिंग）のユーザ名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@example.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザ名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。



(注) レルムとグループの両方をユーザ名に追加できます。その場合、ASA は、AAA 機能に対してグループ用とレルム用に設定されたパラメータを使用します。このオプションの形式は、ユーザ名 `[@realm][<# または !>グループ]` となります (例: `JaneDoe@example.com#VPNGroup`)。このオプションを選択した場合は、グループデリミタとして `#` または `!` を使用する必要があります。これは、`@` がレルムデリミタとしても使用されている場合、ASA が `@` をグループデリミタと解釈できないからです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザが `example.com` ドメインに存在する場合には、Kerberos レルムを `EXAMPLE.COM` と表記します。

ASA には、`user@grouppolicy` のサポートは含まれません。L2TP/IPsec クライアントだけが、`user@tunnelgroup` を介したトンネルスイッチングをサポートしています。

- [Strip the group from the username before passing it on to the AAA server] : ユーザ名を AAA サーバに渡す前に、レルム (管理ドメイン) をユーザ名から除去する処理をイネーブルまたはディセーブルにします。認証時にユーザ名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザ名に追加し、Group Lookup をイネーブルにすると、ASA は、デリミタの左側にある文字をすべてユーザ名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループデリミタは `@`、`#`、および `!` で、`@` が Group Lookup のデフォルトです。ユーザ名<デリミタ>グループの形式でグループをユーザ名に追加します (例: `JaneDoe@VPNGroup`、`JaneDoe#VPNGroup` や `JaneDoe!VPNGroup`)。
- [Password Management] : AAA サーバからの account-disabled インジケータの上書きに関するパラメータと、ユーザに対するパスワード期限切れ通知に関するパラメータを設定できます。
 - [Enable notification upon password expiration to allow user to change password] : このチェックボックスをオンにすると、次の2つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザに通知するか、またはパスワードが期限切れになる当日にユーザに通知するかを選択できます。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザへの通知を開始し、以後、ユーザがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ~ 180 日です。



- (注) この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

いずれの場合でも、変更されずにパスワードが期限切れになったとき、ASA ではユーザによるパスワードの変更が可能です。現行のパスワードが失効していない場合、ユーザ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。

このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。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。

この機能では、MS-CHAPv2 を使用する必要があります。

IKEv1 クライアントアドレス指定

クライアントアドレス指定の設定はすべてのクライアント接続プロファイルに共通です。詳細については、[接続プロファイル](#)、[クライアントアドレス指定 \(127 ページ\)](#) を参照してください。

IKEv1 接続プロファイル、認証

このダイアログボックスは、IPsec on Remote Access および Site-to-Site トンネルグループの場合に表示されます。このダイアログボックスでの設定は、ASA 全体に渡ってこの接続プロファイル（トンネルグループ）に適用されます。インターフェイスごとに認証サーバグループを設定するには、[Advanced] をクリックします。このダイアログボックスでは、次の属性を設定できます。

- [Authentication Server Group] : LOCAL グループ（デフォルト）などの利用可能な認証サーバグループを一覧表示します。None も選択可能です。None または Local 以外を選択すると、[Use LOCAL if Server Group Fails] チェックボックスが利用できるようになります。
- [Use LOCAL if Server Group fails] : Authentication Server Group 属性によって指定されたグループで障害が発生した場合に、LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。

[Enable Group Lookup] ボックスをオフにすると、ユーザ名のみに基づく認証を設定できません。[Enable Group Lookup] ボックスと [Strip Group] の両方をオンにすると、AAA サーバでグループ名が付加されたユーザのデータベースを維持しながら、同時にユーザ名のみに基づいてユーザを認証することができます。

IKEv1 接続プロファイル、認可

認可の設定はすべてのクライアント接続プロファイルに共通です。詳細については、[AnyConnect 接続プロファイル、認証属性 \(129 ページ\)](#) を参照してください。

IKEv1 接続プロファイル、アカウントティング

アカウントティングの設定はすべてのクライアント接続プロファイルに共通です。詳細については、[接続プロファイル、アカウントティング \(139 ページ\)](#) を参照してください。

IKEv1 接続プロファイル、IPsec

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edi] > [Advanced] > [IPsec]

- [Send certificate chain] : 証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [IKE Peer ID Validation] : IKE ピア ID 検証を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [IKE Keep Alive] : ISAKMP キープアライブ モニタリングをイネーブルにして設定します。
 - [Disable Keep Alives] : ISAKMP キープアライブをイネーブルまたはディセーブルにします。
 - [Monitor Keep Alives] : ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
 - [Confidence Interval] : ISAKMP キープアライブの信頼間隔を指定します。これは、ASA がキープアライブ モニタリングを開始するまでに、ピアがアイドル状態を継続できる秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
 - [Retry Interval] : ISAKMP キープアライブのリトライ間の待機秒数を指定します。デフォルト値は 2 秒です。
 - [Head end will never initiate keepalive monitoring] : 中央サイトの ASA がキープアライブ モニタリングを開始しないように指定します。

IKEv1 接続プロファイル、IPsec、IKE 認証

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edi] > [Advanced] > [IPsec] > [IKE Authentication]

- [Default Mode] : 上記の none、xauth、または hybrid からデフォルトの認証モードを選択できます。

- [Interface-Specific Mode] : 認証モードをインターフェイスごとに指定します。
- [Add/Edit/Delete] : [Interface/Authentication Modes] テーブルに対して、選択したインターフェイスと認証モードのペアを追加/編集/削除します。
- [Interface] : 名前付きインターフェイスを選択します。デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
- [Authentication Mode] : 上記の none、xauth、または hybrid から認証モードを選択できます。

IKEv1 接続プロファイル、IPsec、クライアントソフトウェアの更新

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edit] > [Advanced] > [IPsec] > [Client Software Update]

[Client VPN Software Update Table] : インストールされている各クライアント VPN ソフトウェアパッケージについて、クライアントタイプ、VPNクライアントのリビジョン、およびイメージ URL を一覧表示します。クライアントタイプごとに、許可されるクライアントソフトウェアリビジョンと、必要に応じて、ソフトウェアアップグレードをダウンロードする URL または IP アドレスを指定できます。クライアントアップデートメカニズム (Client Update ダイアログボックスに詳細説明があります) は、この情報を使用して、各 VPN クライアントが適切なリビジョンレベルで実行されているかどうか、適切であれば、通知メッセージとアップデートメカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。

- [Client Type] : VPN クライアントタイプを識別します。
- [VPN Client Revisions] : 許可される VPN クライアントのリビジョンレベルを指定します。
- [Location URL] : 適切な VPN クライアントソフトウェアイメージをダウンロードできる URL または IP アドレスを指定します。ダイアログボックススペースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアントモードの ASA 5505 では、URL は tftp:// 形式である必要があります。

IKEv1 接続プロファイル、PPP

この IKEv1 接続プロファイルを使用して PPP 接続で許可される認証プロトコルを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] > [Add/Edit] > [Advanced] > [PPP] を開きます。

このダイアログボックスは、IPsec IKEv1 リモートアクセス接続プロファイルにだけ適用されます。

- [CHAP] : PPP 接続で CHAP プロトコルの使用をイネーブルにします。
- [MS-CHAP-V1] : PPP 接続で MS-CHAP-V1 プロトコルの使用をイネーブルにします。

- [MS-CHAP-V2] : PPP 接続で MS-CHAP-V2 プロトコルの使用をイネーブルにします。
- [PAP] : PPP 接続で PAP プロトコルの使用をイネーブルにします。
- [EAP-PROXY] : PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。EAP は、Extensible Authentication protocol (拡張認証プロトコル) を意味します。

IKEv2 接続プロファイル

IKEv2 接続プロファイルでは、AnyConnect VPN クライアントに対する EAP、証明書ベース、および事前共有キーベースの認証を定義します。ASDM の設定パネルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles] です。

- [Access Interfaces] : IPsec アクセスでイネーブルにするインターフェイスを選択します。デフォルトでは、アクセス方式は何も選択されていません。
- [Bypass interface access lists for inbound VPN sessions] : 着信 VPN セッションのインターフェイスアクセスリストをバイパスするには、このチェックボックスをオンにします。グループポリシーおよびユーザポリシーのアクセスリストはすべてのトラフィックに常に適用されます。
- [Connection Profiles] : 既存の IPsec 接続の設定済みパラメータを表形式で表示します。[Connection Profiles] テーブルには、接続ポリシーを決定するレコードが表示されます。1 つのレコードによって、その接続のデフォルトグループポリシーが識別されます。レコードにはプロトコル固有の接続パラメータが含まれています。テーブルには、次のカラムがあります。
 - [Name] : IPsec 接続の名前または IP アドレスを指定します。
 - [IKEv2 Enabled] : オンになっている場合は、IKEv2 プロトコルがイネーブルになっていることを示します。
 - [Authentication Server Group] : 認証に使用するサーバグループの名前を指定します。
 - [Group Policy] : この IPsec 接続のグループポリシーの名前を示します。



(注) [Delete] : 選択したサーバグループをテーブルから削除します。確認されず、やり直しもできません。

IPsec IKEv2 接続プロファイル : [Basic] タブ

[Add or Edit IPsec Remote Access Connection Profile Basic] ダイアログボックスでは、IPsec IKEv2 接続の共通属性を設定します。

- [Name] : 接続名を特定します。

- [IKE Peer Authentication] : IKE ピアを設定します。
 - [Pre-shared key] : 接続用の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Enable Certificate Authentication] : オンにすると、認証に証明書を使用できます。
 - [Enable peer authentication using EAP] : オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
 - [Send an EAP identity request to the client] : リモートアクセス VPN クライアントに EAP 認証要求を送信できます。

- [Mobike RRC] : Mobike RRC を有効/無効にします。
 - [Enable Return Routability Check for mobike] : Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレスの変更をチェックする Return Routability を有効/無効にします。

- [User Authentication] : ユーザ認証で使用するサーバの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
 - [Server Group] : ユーザ認証で使用するサーバグループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバグループを選択すると、[Fallback] チェックボックスが選択できるようになります。
 - [Manage] : [Configure AAA Server Group] ダイアログボックスが開きます。
 - [Fallback] : 指定したサーバグループで障害が発生した場合に、ユーザ認証で LOCAL を使用するかどうかを指定します。

- [Client Address Assignment] : クライアント属性の割り当てに関連する属性を指定します。
 - [DHCP Servers] : 使用する DHCP サーバの IP アドレスを指定します。最大で 10 台までのサーバをスペースで区切って追加できます。
 - [Client Address Pools] : 事前定義済みのアドレスプールを 6 個まで指定します。[Select] をクリックすると、[Address Pools] ダイアログボックスが開きます。

- [Default Group Policy] : デフォルト グループ ポリシーに関連する属性を指定します。
 - [Group Policy] : この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。
 - [Manage] : [Configure Group Policies] ダイアログボックスが開きます。このダイアログボックスでは、グループ ポリシーを追加、編集、または削除できます。
 - [Client Protocols] : この接続で使用するプロトコルを選択します。デフォルトでは、IPsec と L2TP over IPsec の両方が選択されています。

- [Enable IKEv2 Protocol] : リモート アクセス接続プロファイルで使用する IKEv2 プロトコルをイネーブルにします。これは、先ほど選択したグループ ポリシーの属性です。

IPsec リモート アクセス接続プロファイル : [Advanced] > [IPsec] タブ

IPsec (IKEv2) 接続プロファイルの [IPsec] テーブルに次のフィールドがあります。

- [Send certificate chain] : 証明書チェーン全体の送信をイネーブルまたはディセーブルにする場合にオンにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [IKE Peer ID Validation] : IKE ピア ID の有効性をチェックしないか、必須とするか、あるいは証明書によってサポートされている場合にチェックするかをドロップダウンリストから選択します。

IPsec または SSLVPN 接続プロファイルへの証明書のマッピング

ASA は、クライアント証明書認証による IPsec 接続要求を受信すると、設定されているポリシーに従って接続に接続プロファイルを割り当てます。そのポリシーは、設定したルールを使用でき、証明書 OU フィールド、IKE ID (ホスト名、IP アドレス、キー ID など)、ピア IP アドレス、またはデフォルト接続プロファイルを使用できます。SSL 接続の場合、ASA は設定されているルールだけを使用します。

ルールを使用する IPsec 接続または SSL 接続の場合、ASA は一致するものが見つかるまでルールに対して証明書の属性を評価します。一致するルールが見つかり、そのルールに関連付けられた接続プロファイルを接続に割り当てます。一致するルールが見つからない場合、ASA は、デフォルトの接続プロファイル (IPsec の場合は DefaultRAGroup、SSL VPN の場合は DefaultWEBVPNGroup) を接続に割り当てます。ユーザは、接続プロファイルがイネーブルになっていれば、ポータルページに表示されるドロップダウンリストからその接続プロファイルを選択できます。この接続プロファイルの接続を 1 回試みた場合の結果は、証明書が有効かどうか、そして接続プロファイルの認証設定によって異なります。

ポリシーに一致する証明書グループは、証明書ユーザの権限グループを特定するために使用する方法を定義します。

[Policy] ペインで照合するポリシーを設定します。照合するルールを選択する場合は、[Rules] ペインに移動してルールを指定します。

証明書/接続プロファイル マップ、ポリシー

IPsec 接続において、ポリシーに一致する証明書グループは、証明書ユーザの権限グループを特定するために使用する方法を定義します。これらのポリシーの設定項目は、[Configuration]

> [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Policy] で設定します。

- [Use the configured rules to match a certificate to a group] : [Rules] で定義したルールを使用できます。
- [Use the certificate OU field to determine the group] : 組織ユニット フィールドを使用して、証明書に一致するグループを決定できます。この設定は、デフォルトでオンになっています。
- [Use the IKE identity to determine the group] : [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [IKE Parameters] で定義した ID を使用できます。IKE ID は、IP アドレス、キー ID により、または自動で指定されます。
- [Use the peer IP address to determine the group] : ピアの IP アドレスを使用できます。この設定は、デフォルトでオンになっています。
- [Default to Connection Profile] : どの方法にも一致しなかった場合に使用する、証明書ユーザのデフォルト グループを選択できます。この設定は、デフォルトでオンになっています。[Default]にあるデフォルトグループをクリックして、リストをグループ化します。設定にはグループが必要です。リスト内にグループがない場合は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] でグループを定義する必要があります。

証明書/接続プロファイル マップのルール

IPsec 接続において、ポリシーに一致する証明書グループは、証明書ユーザの権限グループを特定するために使用する方法を定義します。プロファイルマップは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Rules] で作成します。

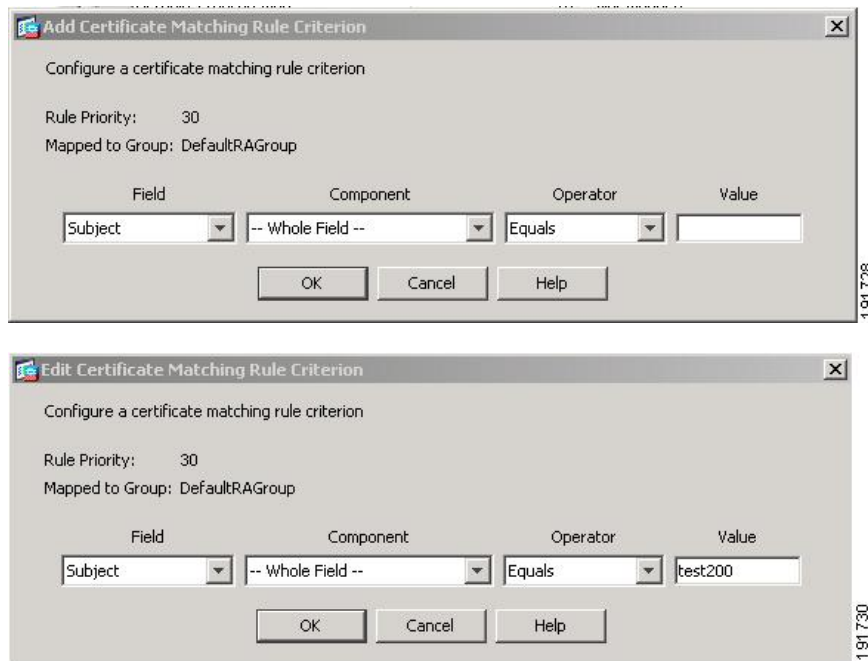
このペインには、証明書/接続プロファイルマップのリストとマッピング基準が表示されます。

証明書/接続プロファイル マップ、証明書照合ルール基準の追加

接続プロファイルをマッピング ルールにマップするマップ プロファイルを作成します。

- [Map] : 次のいずれかを選択します。
 - [Existing] : ルールを含めるマップの名前を選択します。
 - [New] : ルールの新しいマップ名を入力します。
- [Priority] : 10 進数を入力して、接続要求を受け取ったときに ASA がマップを評価する順序を指定します。定義されている最初のルールのデフォルト プライオリティは 10 です。ASA は各接続を評価する際に、優先順位番号が最も小さいマップから評価します。
- [Mapped to Connection Profile] : 以前は「トンネル グループ」と呼んでいた接続プロファイルを選択して、このルールにマッピングします。

次の項で説明するマップへのルール基準の割り当てを行わない場合、ASA はそのマップ エントリを無視します。



証明書照合ルール基準の追加/編集

このダイアログボックスは、接続プロファイルにマッピング可能な証明書照合ルール基準を設定するために使用します。

- [Rule Priority] : (表示専用) 接続要求を受け取ったときに ASA がマップを評価する順序。ASA は各接続を評価する際に、優先順位番号が最も小さいマップから評価します。
- [Mapped to Group] : (表示専用) ルールが割り当てられている接続プロファイル。
- [Field] : ドロップダウン リストから、評価する証明書の部分を選択します。
 - [Subject] : 証明書を使用するユーザまたはシステム。CA のルート証明書の場合は、Subject と Issuer が同じです。
 - [Alternative Subject] : サブジェクト代替名拡張により、追加する ID を証明書のサブジェクトにバインドできます。
 - [Issuer] : 証明書を発行した CA または他のエンティティ (管轄元) 。
 - [Extended Key Usage] : 一致の候補として選択できる、より高度な基準を提供するクライアント証明書の拡張。
- [Component] : ([Subject of Issuer] が選択されている場合にのみ適用されます) 。ルールで使用する識別名コンポーネントを次の中から選択します。

DN フィールド	定義
Whole Field	DN 全体。
Country (C)	2文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name (CN)	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier (DNQ)	特定の DN 属性。
E-mail Address (EA)	証明書を所有するユーザ、システム、またはエンティティの電子メールアドレス。
Generational Qualifier (GENQ)	Jr.、Sr.、または III などの世代修飾子。
Given Name (GN)	証明書所有者の名前（名）。
Initials (I)	証明書所有者の姓と名の最初の文字。
Locality (L)	組織が所在する市町村。
Name (N)	証明書所有者の名前。
Organization (O)	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit (OU)	組織内のサブグループ。
Serial Number (SER)	証明書のシリアル番号。
Surname (SN)	証明書所有者の姓。
State/Province (S/P)	組織が所在する州や県。
Title (T)	証明書所有者の役職（Dr. など）。
User ID (UID)	証明書所有者の ID 番号。
Unstructured Name (UNAME)	unstructuredName 属性タイプは、サブジェクトの名前を非構造化 ASCII 文字列として指定します。
IP Address (IP)	IP アドレス フィールド。

- [Operator] : ルールで使用する演算子を選択します。
 - [Equals] : 認定者名フィールドが値に完全一致する必要があります。

- [Contains] : 認定者名フィールドに値が含まれている必要があります。
- [Does Not Equal] : 認定者名フィールドが値と一致しないようにします。
- [Does Not Contain] : 認定者名フィールドに値が含まれないようにします。
- [Value] : 255 文字までの範囲で演算子のオブジェクトを指定します。Extended Key Usage 機能の場合、ドロップダウンリストで事前定義された値のいずれかを選択するか、他の拡張の OID を入力できます。事前定義された値は次のとおりです。

選択項目	キー使用の目的	OID 文字列
clientauth	クライアント認証	1.3.6.1.5.5.7.3.2
codesigning	コード署名	1.3.6.1.5.5.7.3.3
emailprotection	安全な電子メール保護	1.3.6.1.5.5.7.3.4
ocspsigning	OCSP 署名	1.3.6.1.5.5.7.3.9
serverauth	サーバ認証	1.3.6.1.5.5.7.3.1
timestamping	タイム スタンプ	1.3.6.1.5.5.7.3.8

Site-to-Site 接続プロファイル

[Connection Profiles] ダイアログボックスには、現在設定されている Site-to-Site 接続プロファイル（トンネルグループ）の属性が表示されます。このダイアログボックスを使用すれば、接続プロファイル名を解析するときに使用するデリミタを選択したり、接続プロファイルを追加、変更、または削除したりすることもできます。

ASA では、IPv4 または IPv6 の IPsec LAN-to-LAN VPN 接続は IKEv1 または IKEv2 を使用してサポートされ、内部ネットワークと外部ネットワークは内部および外部 IP ヘッダーを使用してサポートされます。

[Site to Site Connection Profile] ペインのフィールド

- [Access Interfaces] : インターフェイスのリモートピアデバイスによってアクセスできるデバイス インターフェイスのテーブルが表示されます。
 - [Interface] : アクセスをイネーブルまたはディセーブルにするデバイス インターフェイス。
 - [Allow IKEv1 Access] : ピア デバイスによる IPsec IKEv1 アクセスをイネーブルにする場合にオンにします。
 - [Allow IKEv2 Access] : ピア デバイスによる IPsec IKEv2 アクセスをイネーブルにする場合にオンにします。

- [Connection Profiles] : プロファイルを追加、編集、または削除できる接続プロファイルのテーブルを表示します。
 - [Add] : [Add IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
 - [Edit] : [Edit IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
 - [Delete] : 選択した接続プロファイルを削除します。確認されず、やり直しもできません。
 - [Name] : 接続プロファイルの名前。
 - [Interface] : 接続プロファイルがイネーブルになっているインターフェイス。
 - [Local Network] : ローカル ネットワークの IP アドレスを指定します。
 - [Remote Network] : リモート ネットワークの IP アドレスを指定します。
 - [IKEv1 Enabled] : 接続プロファイルに対してイネーブルになっている IKEv1 を表示します。
 - [IKEv2 Enabled] : 接続プロファイルに対してイネーブルになっている IKEv2 を表示します。
 - [Group Policy] : 接続プロファイルのデフォルト グループ ポリシーを表示します。

Site-to-Site 接続プロファイル、追加または編集

[Add or Edit IPsec Site-to-Site Connection] ダイアログボックスでは、IPsec Site-to-Site 接続を作成または変更できます。このダイアログボックスでは、IP アドレス (IPv4 または IPv6) の指定、接続名の指定、インターフェイスの選択、IKEv1 ピアおよび IKEv2 ピアとユーザ認証パラメータの指定、保護されたネットワークの指定、および暗号化アルゴリズムの指定を行うことができます。

2つのピアの内部および外部ネットワークが IPv4 の場合 (内部および外部インターフェイス上のアドレスが IPv4 の場合)、ASA では、シスコまたはサードパーティのピアとの LAN-to-LAN VPN 接続がサポートされます。

IPv4 アドレッシングと IPv6 アドレッシングが混在した、またはすべて IPv6 アドレッシングの LAN-to-LAN 接続については、両方のピアが Cisco ASA 5500 シリーズ セキュリティ アプライアンスの場合、および両方の内部ネットワークのアドレッシング方式が一致している場合 (両方が IPv4 または両方が IPv6 の場合) は、セキュリティ アプライアンスで VPN トンネルがサポートされます。

具体的には、両方のピアが Cisco ASA 5500 シリーズ ASA の場合、次のトポロジがサポートされます。

- ASA の内部ネットワークが IPv4 で、外部ネットワークが IPv6 (内部インターフェイス上のアドレスが IPv4 で、外部インターフェイス上のアドレスが IPv6)

- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv4（内部インターフェイス上のアドレスが IPv6 で、外部インターフェイス上のアドレスが IPv4）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv6（内部および外部インターフェイス上のアドレスが IPv6）

[Basic] パネルのフィールド

- [Peer IP Address] : IP アドレス (IPv4 または IPv6) を指定し、そのアドレスをスタティックにするかどうかを指定できます。
- [Connection Name] : この接続プロファイルに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。接続名が、[Peer IP Address] フィールドで指定される IP アドレスと同じになるように指定できます。
- [Interface] : この接続で使用するインターフェイスを選択します。
- [Protected Networks] : この接続で保護されているローカルおよびリモート ネットワークを選択または指定します。
 - [IP Address Type] : アドレスが IPv4 アドレスまたは IPv6 アドレスのいずれであるかを指定します。
 - [Local Network] : ローカル ネットワークの IP アドレスを指定します。
 - [...] : [Browse Local Network] ダイアログボックスが開きます。このダイアログボックスでは、ローカル ネットワークを選択できます。
 - [Remote Network] : リモート ネットワークの IP アドレスを指定します。
- [IPsec Enabling] : この接続プロファイルのグループ ポリシー、およびそのポリシーで指定したキー交換プロトコルを指定します。
 - [Group Policy Name] : この接続プロファイルに関連付けられているグループ ポリシーを指定します。
 - [Manage] : [Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモート ネットワークを選択できます。
 - [Enable IKEv1] : 指定したグループ ポリシーでキー交換プロトコル IKEv1 をイネーブルにします。
 - [Enable IKEv2] : 指定したグループ ポリシーでキー交換プロトコル IKEv2 をイネーブルにします。
- [IKEv1 Settings] タブ : IKEv1 の次の認証設定および暗号化設定を指定します。
 - [Pre-shared Key] : トンネルグループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。

- [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
- [IKE Policy] : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [Manage] : [Configure IKEv1 Proposals] ダイアログボックスが開きます。
- [IPsec Proposal] : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [IKEv2 Settings] タブ : IKEv2 の次の認証設定および暗号化設定を指定します。
 - [Local Pre-shared Key] : トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Local Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。
 - [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
 - [Remote Peer Pre-shared Key] : トンネル グループのリモートピア事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Remote Peer Certificate Authentication] : この接続プロファイルの IKEv2 接続用の証明書認証を許可するには、[Allowed] をオンにします。
 - [Manage] : 証明書の表示や新規証明書の追加を実行できる [Manage CA Certificates] ダイアログが開きます。
 - [IKE Policy] : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
 - [Manage] : [Configure IKEv1 Proposals] ダイアログボックスが開きます。
 - [IPsec Proposal] : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
 - [Select] : IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開きます。
 - この接続プロファイルには、[Advanced] > [Crypto Map Entry, and Adv] もあります。

Site-to-Site トンネル グループ

ASDM ペインの [Configuration] > [Site-to-Site VPN] > [Advanced] > [Tunnel Groups] では、IPsec Site-to-Site 接続プロファイル（トンネル グループ）の属性を指定します。また、IKE ピアと

ユーザ認証パラメータの選択、IKE キープアライブ モニタリングの設定、およびデフォルトグループポリシーの選択も行うことができます。

- [Name] : このトンネルグループに割り当てられた名前を指定します。Edit機能の場合、このフィールドは表示専用です。
- [IKE Authentication] : IKE ピアの認証で使用する事前共有キーおよび ID 証明書パラメータを指定します。
 - [Pre-shared Key] : トンネルグループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Identity Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。
 - [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
 - [IKE Peer ID Validation] : IKE ピア ID の有効性をチェックするかどうかを指定します。デフォルトは Required です。
- [IPsec Enabling] : この接続プロファイルのグループポリシー、およびそのポリシーで指定したキー交換プロトコルを指定します。
 - [Group Policy Name] : この接続プロファイルに関連付けられているグループポリシーを指定します。
 - [Manage] : [Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモートネットワークを選択できます。
 - [Enable IKEv1] : 指定したグループポリシーでキー交換プロトコル IKEv1 をイネーブルにします。
 - [Enable IKEv2] : 指定したグループポリシーでキー交換プロトコル IKEv2 をイネーブルにします。
- [IKEv1 Settings] タブ : IKEv1 の次の認証設定および暗号化設定を指定します。
 - [Pre-shared Key] : トンネルグループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。



(注) 一部のプロファイルは、エンドポイントがリモートアクセスまたは 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)。

-
- [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
- [IKE Policy] : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [Manage] : [Configure IKEv1 Proposals] ダイアログボックスが開きます。
- [IPsec Proposal] : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [IKEv2 Settings] タブ : IKEv2 の次の認証設定および暗号化設定を指定します。
 - [Local Pre-shared Key] : トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Local Device Certificate] : 認証で使用する ID 証明書がある場合は、その名前を指定します。
 - [Manage] : [Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
 - [Remote Peer Pre-shared Key] : トンネル グループのリモートピア事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
 - [Remote Peer Certificate Authentication] : この接続プロファイルの IKEv2 接続用の証明書認証を許可するには、[Allowed] をオンにします。
 - [Manage] : 証明書の表示や新規証明書の追加を実行できる [Manage CA Certificates] ダイアログが開きます。
 - [IKE Policy] : IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
 - [Manage] : [Configure IKEv1 Proposals] ダイアログボックスが開きます。
 - [IPsec Proposal] : IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
 - [Select] : IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開きます。
- [IKE Keepalive] : IKE キープアライブ モニタリングをイネーブルにし、設定を行います。次の属性の中から 1 つだけ選択できます。
 - [Disable Keep Alives] : IKE キープアライブをイネーブルまたはディセーブルにします。

- [Monitor Keep Alives] : IKE キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
- [Confidence Interval] : IKE キープアライブの信頼間隔を指定します。これは、ASA がキープアライブ モニタリングを開始するまでに、ピアがアイドル状態を継続できる秒数です。最小 10 秒、最大 300 秒です。リモートアクセス グループのデフォルトは 10 秒です。
- [Retry Interval] : IKE キープアライブのリトライ間の待機秒数を指定します。デフォルト値は 2 秒です。
- [Head end will never initiate keepalive monitoring] : 中央サイトの ASA がキープアライブ モニタリングを開始しないように指定します。

Site-to-Site 接続プロファイル、暗号マップ エントリ

このダイアログボックスでは、現在の Site-to-Site 接続プロファイルの暗号パラメータを指定します。

- [Priority] : 一意のプライオリティ (1 ~ 65,543、1 が最高のプライオリティ)。IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモートピアに送信します。リモートピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。
- [Perfect Forward Secrecy] : 特定の IPsec SA のキーが他の秘密情報 (他のキーなど) から導出されたものでないことを保証します。PFS により、攻撃者がキーを突破できたとしても、そのキーから他のキーを導出できないようにします。PFS をイネーブルにすると、Diffie-Hellman Group リストがアクティブになります。
 - [Diffie-Hellman Group] : 2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1 (768 ビット)、Group 2 (1024 ビット)、および Group 5 (1536 ビット) の中から選択します。
- [Enable NAT-T] : このポリシーの NAT Traversal (NAT-T) をイネーブルにします。これにより IPsec ピアは、NAT デバイスを介してリモートアクセスと LAN-to-LAN の両方の接続を確立できます。
- [Enable Reverse Route Injection] : リモート トンネルのエンドポイントによって保護されているネットワークとホストのルーティングプロセスに、スタティックルートが自動的に挿入されるようにすることができます。
- [Security Association Lifetime] : セキュリティ アソシエーション (SA) の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。

- [Time] : 時 (hh) 、分 (mm) 、および秒 (ss) 単位で SA のライフタイムを指定します。
- [Traffic Volume] : キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロードデータのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。
- [Static Crypto Map Entry Parameters] : ピア IP アドレスが Static に指定されている場合に、次の追加パラメータを指定します。
 - [Connection Type] : 許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。
 - [Send ID Cert. Chain] : 証明書チェーン全体の送信をイネーブルにします。
 - [IKE Negotiation Mode] : SA、Main、または Aggressive の中から、セットアップでキー情報を交換するときのモードを設定します。ネゴシエーションの発信側が使用するモードも設定されます。応答側は自動ネゴシエーションします。Aggressive モードは高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。[Aggressive] を選択すると、[Diffie-Hellman Group] リストがアクティブになります。
 - [Diffie-Hellman Group] : 2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1 (768 ビット) 、Group 2 (1024 ビット) 、および Group 5 (1536 ビット) の中から選択します。

CA 証明書の管理

CA 証明書の管理は、リモートアクセス VPN とサイト間 VPN に適用されます。

- Site-to_site の場合 : [IKE Peer Authentication] の [Manage] をクリックすると、[Manage CA Certificates] ダイアログボックスが開きます。
- リモートアクセス VPN では、[Certificate Management] > [CA Certificates] をクリックします。

このダイアログボックスを使用して、IKE ピア認証で使用可能な CA 証明書のリストのエントリを、表示、追加、編集、および削除します。[Manage CA Certificates] ダイアログボックスには、証明書の発行先、証明書の発行元、証明書の有効期限、および利用データなど、現在設定されている証明書の情報が一覧表示されます。

- [Add or Edit] : [Install Certificate] ダイアログボックスまたは [Edit Certificate] ダイアログボックスが開きます。これらのダイアログボックスでは、証明書の情報を指定し、証明書をインストールできます
- [Show Details] : テーブルで選択する証明書の詳細情報を表示します。

- [Delete] : 選択した証明書をテーブルから削除します。確認されず、やり直しもできません。

Site-to-Site 接続プロファイル、証明書のインストール

このダイアログボックスを使用して、新しい CA 証明書をインストールします。次のいずれかの方法で証明書を取得できます。

- 証明書ファイルを参照してファイルからインストールします。
- 事前取得済みの PEM 形式の証明書テキストをこのダイアログボックス内のボックスに貼り付けます。
- [Use SCEP] : Simple Certificate Enrollment Protocol (SCEP) の使用を指定します。証明書サービスのアドオンは、Windows Server 2003 ファミリで実行されます。SCEP プロトコルのサポートを提供し、これによりシスコのルータおよび他の中間ネットワーク デバイスは、証明書を取得できます。
 - [SCEP URL: http://] : SCEP 情報のダウンロード元の URL を指定します。
 - [Retry Period] : SCEP クエリー間の必須経過時間を分数で指定します。
 - [Retry Count] : リトライの最大許容回数を指定します。
- [More Options] : [Configure Options for CA Certificate] ダイアログボックスが開きます。

このダイアログボックスを使用して、この IPsec リモートアクセス接続の CA 証明書の取得に関する詳細を指定します。このダイアログボックスに含まれるダイアログボックスは、[Revocation Check]、[CRL Retrieval Policy]、[CRL Retrieval Method]、[OCSP Rules]、および [Advanced] です。

[Revocation Check] ダイアログボックスは、CA 証明書失効確認に関する情報を指定するために使用します。

- オプション ボタンにより、失効状態について証明書をチェックするかどうかを指定します。[Do not check certificates for revocation] または [Check Certificates for revocation] を選択します。
- [Revocation Methods area] : 失効チェックに使用する方法 (CRL または OCSP) 、およびそれらの方法を使用する順序を指定できます。いずれか一方または両方の方法を選択できます。

AnyConnect VPN クライアント イメージ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Software] ペインに、ASDM で設定された AnyConnect クライアント イメージが一覧表示されます。

[AnyConnect Client Image] テーブル : ASDM で設定されたパッケージファイルが表示されます。ASA がリモート PC にイメージをダウンロードする順序を設定できます。

- [Add] : [Add AnyConnect Client Image] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをクライアントイメージファイルとして指定したり、フラッシュメモリから、クライアントイメージとして指定するファイルを参照したりできます。また、ファイルをローカルコンピュータからフラッシュメモリにアップロードすることもできます。
- [Replace] : [Replace AnyConnect Client Image] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをクライアントイメージとして指定して、[SSL VPN Client Image] テーブルで選択したイメージと置換できます。また、ファイルをローカルコンピュータからフラッシュメモリにアップロードすることもできます。
- [Delete] : テーブルからイメージを削除します。イメージを削除しても、パッケージファイルはフラッシュから削除されません。
- [Move Up] および [Move Down] : 上矢印と下矢印を使用して、ASA がリモート PC にクライアントイメージをダウンロードする順序を変更します。テーブルの一番上にあるイメージを最初にダウンロードします。このため、最もよく使用するオペレーティングシステムで使用されるイメージを一番上に移動する必要があります。

AnyConnect VPN クライアントイメージ、追加/交換

このペインでは、ASA フラッシュメモリ上のファイルの名前を指定して、そのファイルを AnyConnect クライアントイメージとして追加したり、テーブルにすでに記載されているイメージと置換することができます。また、識別するファイルをフラッシュメモリから参照したり、ローカルコンピュータからファイルをアップロードしたりすることもできます。

- [Flash SVC Image] : SSL VPN クライアントイメージとして識別する、フラッシュメモリ内のファイルを指定します。
- [Browse Flash] : フラッシュメモリに格納されているすべてのファイルを参照できる [Browse Flash Dialog] ダイアログボックスを表示します。
- [Upload] : [Upload Image] ダイアログボックスが表示されます。このダイアログボックスでは、クライアントイメージとして指定するファイルをローカル PC からアップロードできます。
- [Regular expression to match user-agent] : ASA が、ブラウザから渡された User-Agent 文字列との照合に使用する文字列を指定します。モバイルユーザの場合、この機能を使用してモバイルデバイスの接続時間を短縮できます。ブラウザは ASA に接続するときに、HTTP ヘッダーに User-Agent 文字列を含めます。ASA が文字列を受信し、その文字列がいずれかのイメージ用に設定された式と一致すると、他のクライアントイメージはテストされず、一致したイメージがただちにダウンロードされます。

AnyConnect VPN クライアントイメージ、イメージのアップロード

このペインでは、ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリに格納されている、AnyConnect クライアント イメージとして識別するファイルのパスを指定できます。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリから、識別するファイルを参照できます。

- [Local File Path] : ローカル コンピュータに格納されている、SSL VPN クライアント イメージとして識別するファイルの名前を指定します。
- [Browse Local Files] : [Select File Path] ダイアログボックスが表示されます。このダイアログボックスでは、ローカル コンピュータ上のすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- [Flash File System Path] : セキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント イメージとして識別するファイルの名前を指定します。
- [Browse Flash] : [Browse Flash] ダイアログボックスが表示されます。このダイアログボックスでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- [Upload File] : ファイルのアップロードを開始します。

AnyConnect VPN クライアント接続の設定

AnyConnect クライアント プロファイルの設定

AnyConnect クライアント プロファイルをすべての AnyConnect ユーザにグローバルに展開するか、またはユーザのグループ ポリシーに基づいてユーザに展開するように ASA を設定できます。通常、ユーザは、インストールされている AnyConnect モジュールごとに 1 つのクライアント プロファイルを持ちます。ユーザに複数のプロファイル割り当てることもできます。たとえば、複数の場所で作業するユーザには、複数のプロファイルが必要になることがあります。一部のプロファイル設定 (SBL など) は、グローバル レベルで接続を制御します。その他の設定は、特定のホストに固有であり、選択されたホストにより異なります。

AnyConnect クライアント プロファイルの作成と展開、およびクライアント機能の制御の詳細については、『AnyConnect VPN Client Administrator Guide』を参照してください。

クライアント プロファイルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] で設定します。

[Add/Import] : [Add AnyConnect Client Profiles] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュ メモリ内のファイルをプロファイルとして指定したり、フラッシュ メモリを参照してプロファイルとして指定するファイルを検索したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。

- [Profile Name] : グループ ポリシーの AnyConnect クライアント プロファイルを指定します。
- [Profile Usage] : 最初に作成されたときにプロファイルに割り当てられた用途 (VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク 可視性モジュール、Umbrella Roaming Security、または管理 VPN トンネル) を表示します。ASDM が、XML ファイルで指定された用途を認識しない場合、ドロップ ダウン リストが選択可能になり、用途タイプを手動で選択できます。
- [Profile Location] : ASA のフラッシュ メモリ内のプロファイル ファイルへのパスを指定します。このファイルが存在しない場合、ASA はプロファイルテンプレートに基づいてファイルを作成します。
- [Group Policy] : プロファイルのグループ ポリシーを指定します。プロファイルは、AnyConnect クライアントとともにこのグループ ポリシーに属しているユーザにダウンロードされます。

[Edit] : [Edit SSL VPN Client Profile] ウィンドウが表示されます。このウィンドウでは、プロファイルに含まれている AnyConnect クライアント機能の設定を変更できます。

[エクスポート (Export)]

- [Device Profile Path] : プロファイル ファイルのパスおよびファイル名を表示します。
- [Local Path] : パスとファイル名を指定してプロファイル ファイルをエクスポートします。
- [Browse Local] : ローカル デバイス ファイル システムを参照するには、これをクリックしてウィンドウを起動します。

[Delete] : テーブルからプロファイルを削除します。プロファイルを削除しても、XML ファイルはフラッシュから削除されません。

[AnyConnect Client Profiles] テーブル : AnyConnect クライアント プロファイルとして指定された XML ファイルを表示します。

AnyConnect トラフィックに対するネットワーク アドレス変換の免除

ネットワーク アドレス変換 (NAT) を実行するように ASA を設定した場合は、AnyConnect クライアント、内部ネットワーク、および DMZ の企業リソースが相互に接続を開始できるように、リモートアクセス AnyConnect クライアント トラフィックを変換の対象外にする必要があります。AnyConnect クライアント トラフィックを変換の対象外にできないと、AnyConnect クライアントおよび他の企業リソースが通信できなくなります。

「アイデンティティ NAT」 (「NAT 免除」とも呼ばれている) によりアドレスを自らに変換できます。これにより効果的に NAT が回避されます。アイデンティティ NAT は2つのアドレス プール、アドレス プールとサブネットワーク、または2つのサブネットワーク間で適用できます。

この手順は、例にあるネットワーク トポロジの次の仮定のネットワーク オブジェクト間でアイデンティティ NAT を設定する方法を示しています。それらは、Engineering VPN アドレス

プール、Sales VPN アドレス プール、ネットワーク内、DMZ ネットワーク、およびインターネットです。アイデンティティ NAT 設定ではそれぞれ、NAT 規則が 1 つ必要です。

表 4: VPN クライアントのアイデンティティ NAT を設定するネットワーク アドレス アドレッシング

ネットワークまたはアドレス プール	ネットワーク名またはアドレス プール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレス プール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレス プール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

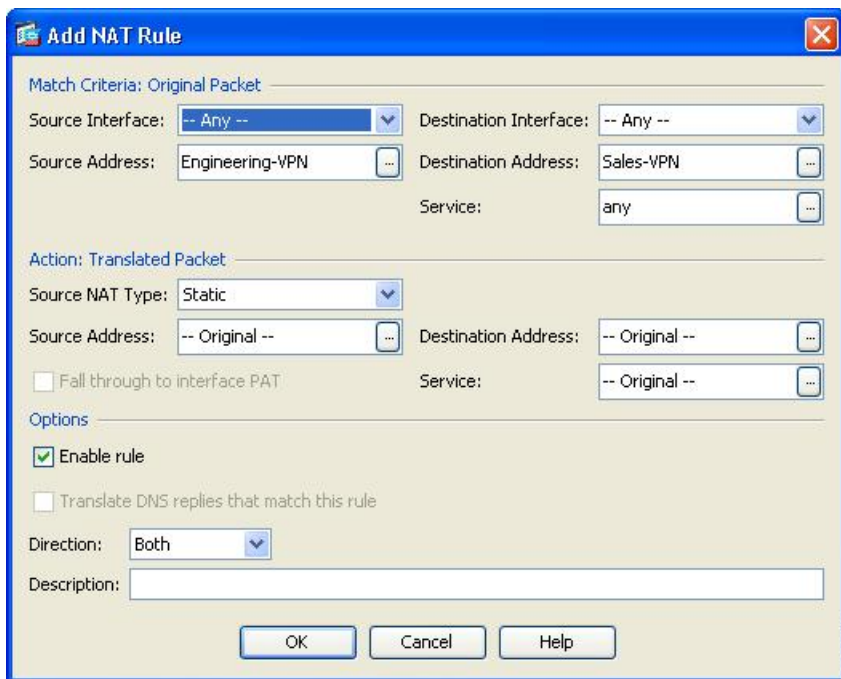
手順

ステップ 1 ASDM にログインし、[Configuration] > [Firewall] > [NAT Rules] に移動します。

ステップ 2 Engineering VPN アドレス プールのホストが Sales VPN アドレス プールのホストに接続できるよう、NAT 規則を作成します。ASA が Unified NAT テーブルの他の規則よりも先にこの規則を評価するように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] に移動します。

(注) NAT ルールはトップダウン方式で最初に一致したルールから順に適用されます。ASA によりいったんパケットが特定の NAT 規則と一致すると、それ以上評価は行われません。ASA が NAT 規則を早まって広範な NAT 規則に一致しないよう、Unified NAT テーブルの先頭に最も固有の NAT 規則を配置することが重要です。

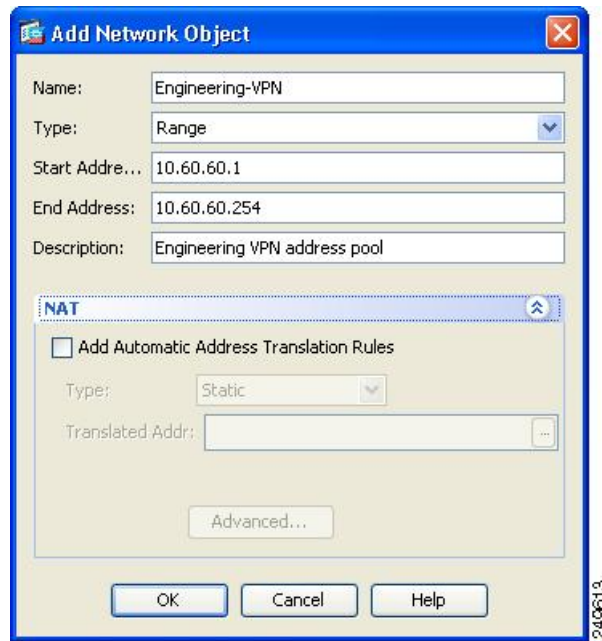
図 1: [Add NAT Rule] ダイアログ ボックス



a) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの [Range] として定義します。自動アドレス トランスレーションルールは追加しないでください。
- [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Sales VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの [Range] として定義します。自動アドレス トランスレーションルールは追加しないでください。

図 2: VPN アドレス プールのネットワーク オブジェクトの作成



- b) [Action Translated Packet] エリアで、次のフィールドを設定します。
- [Source NAT Type:] Static
 - [Source Address:] Original
 - [Destination Address:] Original
 - [Service:] Original
- c) [Options] エリアで、次のフィールドを設定します。
- [Enable rule] をオンにします。
 - [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
 - [Direction:] Both
 - [Description:] 規則の説明を入力します。
- d) [OK] をクリックします。
- e) [適用 (Apply)] をクリックします。

CLI の例 :

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN
Sales-VPN
```

- f) [Send] をクリックします。

ステップ 3 ASA が NAT を実行しているときに、同じ VPN プール内の 2 つのホストが互いに接続できるように、またはそれらのホストが VPN トンネル経由でインターネットに接続できるように、[Enable traffic between two or more hosts connected to the same interface] オプションをイネーブルにする必要があります。これを行うには、ASDM で [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] を選択します。[Interface] パネルの下の [Enable traffic between two or more hosts connected to the same interface] をオンにして、[Apply] をクリックします。

CLI の例 :

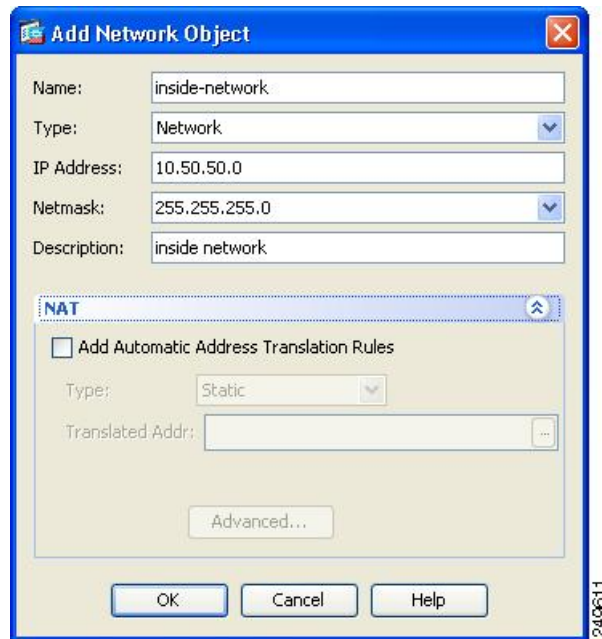
```
same-security-traffic permit inter-interface
```

ステップ 4 Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。上記で規則を作成したときと同様にこの規則を作成します。ただし、[Match criteria: Original Packet] エリアで、Engineering VPN アドレス プールを送信元と宛先の両方のアドレスとして指定します。

ステップ 5 Engineering VPN リモートアクセスクライアントが「内部」ネットワークに到達できるよう NAT 規則を作成します。この規則が他の規則よりも先に処理されるように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。

a) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、内部ネットワークを表すネットワーク オブジェクトを作成します。オブジェクトタイプをアドレスの [Network] として定義します。自動アドレス トランスレーション ルールは追加しないでください。
- [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。

図 3: *inside-network* オブジェクトの追加

- b) [Action Translated Packet] エリアで、次のフィールドを設定します。
- [Source NAT Type:] Static
 - [Source Address:] Original
 - [Destination Address:] Original
 - [Service:] Original
- c) [Options] エリアで、次のフィールドを設定します。
- [Enable rule] をオンにします。
 - [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
 - [Direction:] Both
 - [Description:] 規則の説明を入力します。
- d) [OK] をクリックします。
- e) [適用 (Apply)] をクリックします。

CLI の例

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

ステップ 6 ステップ 5 の方法に従って新しい規則を作成し、Engineering VPN アドレスプールと DMZ ネットワーク間の接続のアイデンティティ NAT を設定します。DMZ ネットワークを送信元アドレス、Engineering VPN アドレスプールを宛先アドレスとして使用します。

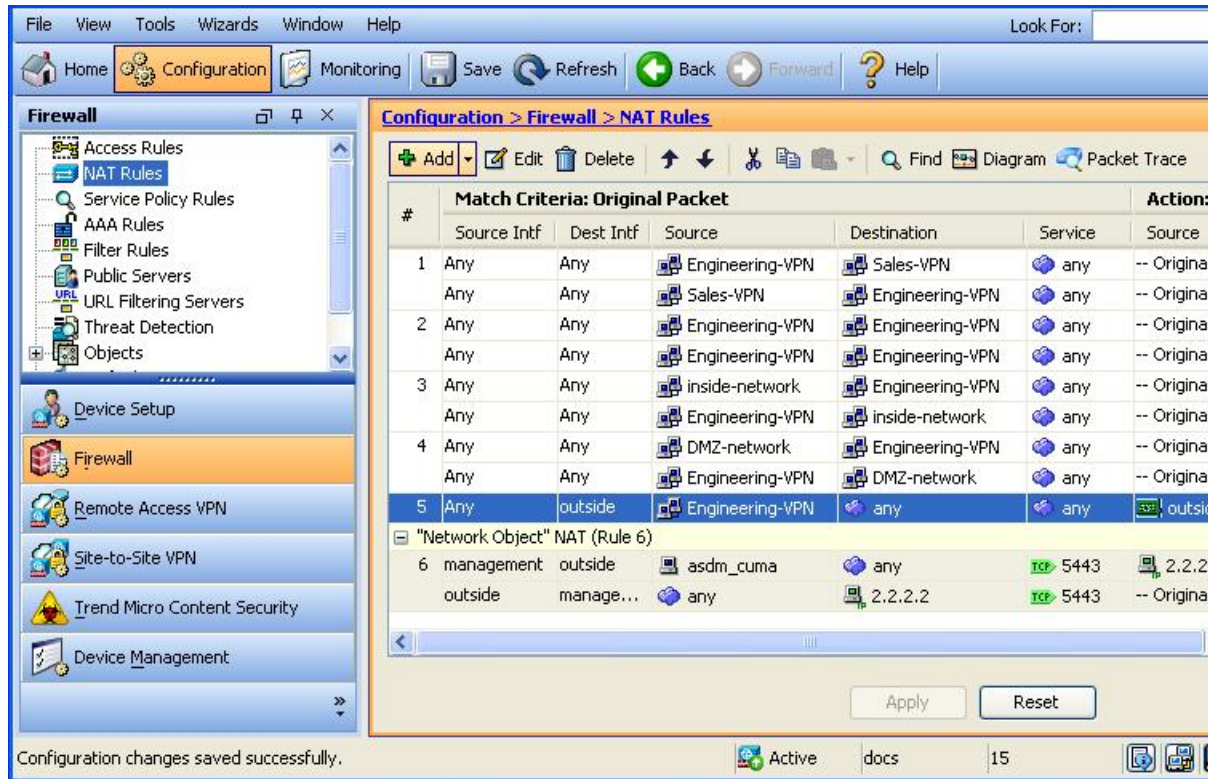
ステップ 7 新しい NAT 規則を作成し、Engineering VPN アドレスプールがトンネル経由でインターネットにアクセスできるようにします。この場合、アイデンティティ NAT は使用しません。送信元アドレスをプライベートアドレスからインターネットルーティング可能なアドレスに変更するためです。この規則を作成するには、次の手順に従います。

- a) この規則が他の規則よりも先に処理されるように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。
- b) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。
 - [Source Interface:] Any
 - [Destination Interface:] Any。 [Action: Translated Packet] エリアの [Source Address] で [outside] を選択すると、このフィールドに自動的に「outside」が入力されます。
 - [Source Address] : [Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレスプールを表すネットワーク オブジェクトを選択します。
 - [Destination Address:] Any
- c) [Action Translated Packet] エリアで、次のフィールドを設定します。
 - [Source NAT Type:] Dynamic PAT (Hide)
 - [Source Address:] [Source Address] ブラウズ ボタンをクリックして、outside インターフェイスを選択します。
 - [Destination Address:] Original
 - [Service:] Original
- d) [Options] エリアで、次のフィールドを設定します。
 - [Enable rule] をオンにします。
 - [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
 - [Direction:] Both
 - [Description:] 規則の説明を入力します。
- e) [OK] をクリックします。
- f) [適用 (Apply)] をクリックします。

CLI の例 :

```
nat (any,outside) source dynamic Engineering-VPN interface
```

図 4: Unified NAT テーブル



- ステップ 8** Engineering VPN アドレス プールがそのプール自体、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネットに到達するように設定した後に、Sales VPN アドレス プールについて同じプロセスを繰り返す必要があります。アイデンティティ NAT を使用して、Sales VPN アドレス プールトラフィックが、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネット間のネットワーク アドレス変換の対象外となるようにします。
- ステップ 9** ASA の [File] メニューで [Save Running Configuration to Flash] を選択し、アイデンティティ NAT 規則を実装します。

AnyConnect HostScan

AnyConnect ポスチャ モジュールにより、AnyConnect Secure Mobility Client 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、および、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 の前提条件

AnyConnect Secure Mobility Client をポスチャ 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

次の AnyConnect 機能は、ポスチャ モジュールをインストールする必要があります。

- SCEP 認証
- AnyConnect テレメトリ モジュール

ポスチャモジュール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。

AnyConnect HostScan のライセンス

ポスチャ モジュールには、次の AnyConnect ライセンシング要件があります。

- 基本 HostScan 用 AnyConnect Apex。
- 修復には、Advanced Endpoint Assessment ライセンスが必要です。

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 のインストールまたはアップグレード

この手順では、ASDM を使用して、HostScan 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нта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、『[AnyConnect 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 ASDMDAP 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。

手順

- ステップ 1** hostscan_version-k9.pkg ファイルをコンピュータにダウンロードします。
- ステップ 2** ASDM を起動し、[Configuration][Remote Access VPN]>[Secure Desktop Manager] [Host Scan Image] > を選択します。
- ステップ 3** [Upload] をクリックして、HostScan パッケージのコピーをコンピュータから ASA のドライブに転送する準備を行います。
- ステップ 4** [Upload Image] ダイアログボックスで [Browse Local Files] をクリックして、ローカルコンピュータ上の HostScan パッケージを検索します。
- ステップ 5** 先ほどダウンロードした hostscan_version-k9.pkg ファイルを選択し、[Select] をクリックします。[Local File Path] フィールドと [Flash File System Path] フィールドで選択したファイルのパスは、HostScan パッケージのアップロード先のパスを反映しています。ASA に複数のフラッシュドライブがある場合は、別のフラッシュドライブを示すように [Flash File System Path] を編集できます。
- ステップ 6** [Upload File] をクリックします。ASDM によって、ファイルのコピーがフラッシュカードに転送されます。情報ダイアログボックスに、ファイルがフラッシュに正常にダウンロードされたことが表示されます。
- ステップ 7** [OK] をクリックします。
- ステップ 8** [Use Uploaded Image] ダイアログで [OK] をクリックして、現在のイメージとしてアップロードした HostScan パッケージファイルを使用します。
- ステップ 9** [Enable HostScan] がオンになっていない場合はオンにします。
- ステップ 10** [Apply] をクリックします。
- ステップ 11** [File] メニューから [Save Running Configuration To Flash] を選択します。

HostScan のアンインストール

HostScan 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 が有効になっている場合でも ASA による HostScan パッケージの展開が回避されます。HostScan をアンインストールしても、HostScan パッケージはフラッシュ ドライブから削除されません。

手順

-
- ステップ 1** ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan Image] > に移動して、HostScan をアンインストールします。
 - ステップ 2** [Uninstall] をクリックし、確認のために [Yes] をクリックします。
 - ステップ 3** [Uninstall] をクリックします。
-

グループ ポリシーへの AnyConnect フィーチャ モジュールの割り当て

次の手順で、AnyConnect フィーチャ モジュールとグループ ポリシーを関連付けます。VPN ユーザが ASA に接続するときに、ASA はこれらの AnyConnect フィーチャ 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に AnyConnect フィーチャ 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 AnyConnect Module Name

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	AnyConnect モジュール/機能名
dart	AnyConnect DART (診断およびレポート ツール)
vpngina	AnyConnect SBL (ログイン前の起動)
websecurity	AnyConnect Web セキュリティ モジュール
telemetry	AnyConnect テレメトリ モジュール
posture	AnyConnect ポスチャ モジュール
nam	AnyConnect 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	AnyConnect 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 の関連マニュアル

HostScan がエンドポイント コンピュータからポストチャクredentials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、AnyConnect クライアントでの HostScan の動作の詳細については、『[Cisco AnyConnect Secure Mobility Client Administrator Guide](#)』を参照してください。

AnyConnect セキュア モビリティ ソリューション

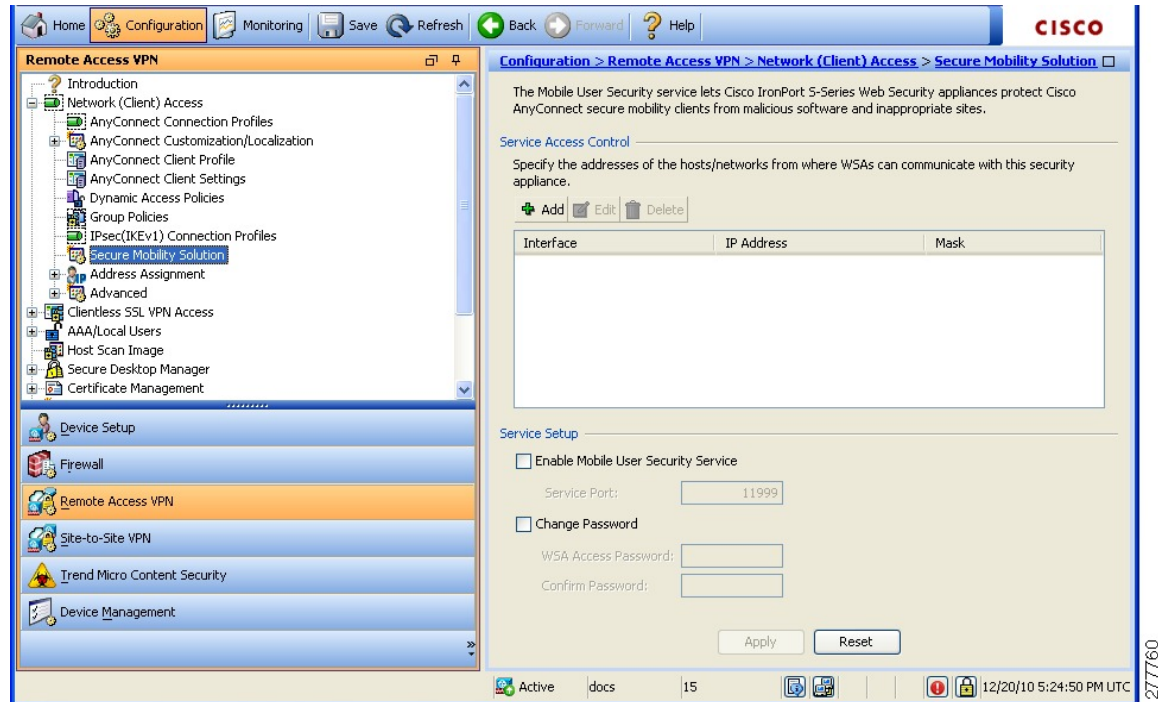
AnyConnect セキュア モビリティは、従業員の移動時に企業の利益と資産をインターネットの脅威から保護します。AnyConnect Secure Mobility により Cisco IronPort S シリーズ Web セキュリティ アプライアンスは Cisco AnyConnect セキュア モビリティ クライアントをスキャンでき、クライアントを悪意あるソフトウェアや不適切なサイトから確実に保護します。クライアントは、Cisco IronPort S シリーズ Web セキュリティ アプライアンス保護がイネーブルになっているか定期的に確認します。



- (注) この機能には、Cisco AnyConnect セキュア モビリティ クライアントの AnyConnect セキュア モビリティ ライセンス サポートを提供する Cisco IronPort Web セキュリティ アプライアンスのリリースが必要です。また、AnyConnect Secure Mobility 機能をサポートする AnyConnect リリースが必要です。AnyConnect 3.1 以降はこの機能をサポートしていません。

セキュア モビリティ ソリューションを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Secure Mobility Solution] の順に選択します。

図 5: [Mobile User Security] ウィンドウ



- [Service Access Control] : WSA の通信元となるホストまたはネットワーク アドレスを指定します。
 - [Add] : 選択した接続の [Add MUS Access Control Configuration] ダイアログボックスが開きます。
 - [Edit] : 選択した接続の [Edit MUS Access Control Configuration] ダイアログボックスが開きます。
 - [Delete] : 選択した接続をテーブルから削除します。確認されず、やり直しもできません。
- [Enable Mobile User Security Service] : VPN を介したクライアントとの接続を開始します。イネーブルにすると、ASA への接続時に WSA によって使用されるパスワードを入力する必要があります。WSA が存在しない場合、ステータスは disabled になります。
- [Service Port] : サービスをイネーブルにする場合、サービスのどのポート番号を使用するかを指定します。ポートの範囲は 1 ~ 65535 で、管理システムにより WSA にプロビジョニングされた対応する値と一致させる必要があります。デフォルトは 11999 です。
- [Change Password] : WSA アクセス パスワードを変更できます。
- [WSA Access Password] : ASA と WSA の間の認証で必要となる共有シークレットパスワードを指定します。このパスワードは、管理システムにより WSA にプロビジョニングされた対応するパスワードと一致させる必要があります。
- [Confirm Password] : 指定したパスワードを再入力します。

- [Show WSA Sessions] : ASA に接続された WSA のセッション情報を表示できます。接続されている (または接続された) WSA のホスト IP アドレスおよび接続時間がダイアログボックスに返されます。

Add or Edit MUS Access Control

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Secure Mobility Solution] の下の [Add or Edit MUS Access Control] ダイアログボックスで、AnyConnect クライアントの Mobile User Security (MUS) アクセスを設定します。

- [Interface Name] : ドロップダウン リストを使用して、追加または編集しているインターフェイス名を選択します。
- [IP Address] : IPv4 アドレスまたは IPv6 アドレスを入力できます。
- [Mask] : ドロップダウン リストを使用して、該当のマスクを選択します。

AnyConnect のカスタマイズとローカリゼーション

AnyConnect VPN クライアントをカスタマイズして、リモート ユーザに、会社のイメージを表示できます。[AnyConnect Customization/Localization] のフィールドを使用すれば、次のタイプのカスタマイズされたファイルをインポートすることができます。

- **Resources** : AnyConnect クライアントの変更された GUI アイコン。
- **Binary** : AnyConnect インストーラに代わる実行可能ファイル。これには、GUI ファイルのほか、VPN クライアント プロファイル、スクリプト、その他のクライアント ファイルが含まれます。
- **Script** : AnyConnect が VPN 接続を確立する前または後に実行するスクリプト。
- **GUI Text and Messages** : AnyConnect クライアントが使用するタイトルとメッセージ。
- **Customized Installer** : クライアントのインストールを変更するトランスフォーム。
- **Localized Installer** : クライアントで使用される言語を変更するトランスフォーム。

各ダイアログでは次のアクションを実行できます。

- [Import] をクリックすると、[Import AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。
- [Export] をクリックすると、[Export AnyConnect Customization Objects] ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。
- [Delete] をクリックすると、選択したオブジェクトが削除されます。



(注) この機能はマルチ コンテキスト モードではサポートされません。

AnyConnect のカスタマイズとローカリゼーション、リソース

インポートするカスタム コンポーネントのファイル名は、AnyConnect GUI で使用されるファイル名と一致している必要があります。これはオペレーティング システムによって異なり、Mac および Linux では大文字と小文字が区別されます。たとえば、Windows クライアント用の企業ロゴを置き換えるには、独自の企業ロゴを `company_logo.png` としてインポートする必要があります。別のファイル名でインポートすると、AnyConnect インストーラはそのコンポーネントを変更しません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合は、その実行ファイルから任意のファイル名のリソースファイル呼び出すことができます。

イメージをソースファイルとして（たとえば、`company_logo.bmp`）インポートする場合、インポートしたイメージは、同じファイル名を使用して別のイメージを再インポートするまで、AnyConnect をカスタマイズします。たとえば、`company_logo.bmp` をカスタム イメージに置き換えて、このイメージを削除する場合、同じファイル名を使用して新しいイメージ（または元のシスコ ロゴ イメージ）をインポートするまで、クライアントはこのイメージの表示を継続します。

AnyConnect のカスタマイズとローカリゼーション、バイナリとスクリプト

[AnyConnect Customization/Localization] : [Binary]

Windows、Linux、または Mac (PowerPC または Intel ベース) コンピュータの場合、AnyConnect クライアント API を使用する独自のクライアントを展開できます。クライアントのバイナリ ファイルを置き換えることによって、AnyConnect GUI および AnyConnect CLI を置き換えます。

[Import] ダイアログのフィールドは次のとおりです。

- **Name** 置き換える AnyConnect ファイルの名前を入力します。
- **Platform** ファイルを実行する OS プラットフォームを選択します。
- **Select a file** ファイル名は、インポートするファイルの名前と同じにする必要はありません。

[AnyConnect Customization/Localization] : [Script]

スクリプトの展開およびスクリプトの制限事項の詳細については、『AnyConnect VPN Client Administrators Guide』を参照してください。

[Import] ダイアログのフィールドは次のとおりです。

- **Name** : スクリプトの名前を入力します。名前には正しい拡張子を指定してください。例 : myscript.bat.
- **Script Type** : スクリプトを実行するタイミングを選択します。

ASA でファイルをスクリプトとして識別できるように、AnyConnect によって、プレフィックス `scripts_` とプレフィックス `OnConnect` または `OnDisconnect` がユーザのファイル名に追加されます。クライアントが接続すると、ASA は、リモートコンピュータ上の適切なターゲット ディレクトリにスクリプトをダウンロードします。その際、`scripts_` プレフィックスは削除され、`OnConnect` または `OnDisconnect` プレフィックスはそのまま残ります。たとえば、myscript.bat スクリプトをインポートした場合、ASA 上では、スクリプトは `scripts_OnConnect_myscript.bat` となります。リモート コンピュータ上では、スクリプトは `OnConnect_myscript.bat` となります。

スクリプトの実行の信頼性を確保するために、すべての ASA で同じスクリプトを展開するように設定します。スクリプトを修正または置換する場合は、旧バージョンと同じ名前を使用し、ユーザが接続する可能性のあるすべての ASA に置換スクリプトを割り当てます。ユーザが接続すると、新しいスクリプトにより同じ名前のスクリプトが上書きされます。

- **Platform** : ファイルを実行する OS プラットフォームを選択します。
- **Select a file** : ファイル名は、スクリプトに対して指定した名前と同じである必要はありません。

ASDM によってファイルがソース ファイルからインポートされ、[Name] に対して指定した新しい名前が作成されます。

AnyConnect のカスタマイズとローカリゼーション、GUI テキストとメッセージ

デフォルトの変換テーブルを編集するか、または新しいテーブルを作成して、AnyConnect クライアント GUI に表示されるテキストとメッセージを変更できます。このペインは、[Language Localization] ペインと同じ機能を持ちます。より高度な言語変換については、[Configuration] > [Remote Access VPN] > [Language Localization] に移動します。

上部ツールバーにある通常のボタンに加えて、このペインには [Add] ボタンと、追加のボタンを備えた [Template] エリアがあります。

Add : [Add] ボタンをクリックするとデフォルトの変換テーブルのコピーが開き、直接編集したり保存することができます。保存ファイルの言語を選択し、ファイル内のテキストの言語を後で編集することができます。

変換テーブルのメッセージをカスタマイズする場合、msgid は変更しないでください。msgstr 内のテキストを変更します。

テンプレートの言語を指定します。テンプレートはキャッシュメモリ内の変換テーブルになり、指定した名前が付きます。ブラウザの言語オプションと互換性のある短縮形を使用してく

ださい。たとえば、中国語のテーブルを作成するときに IE を使用している場合は、IE によって認識される zh という略語を使用します。

[Template] セクション

- テンプレート領域を展開してデフォルトの英語変換テーブルにアクセスするには、[Template] をクリックします。
- デフォルトの英語変換テーブルを表示し、必要に応じて保存するには、[View] をクリックします。
- デフォルトの英語変換テーブルのコピーを表示せずに保存するには、[Export] をクリックします。

AnyConnect のカスタマイズとローカリゼーション、カスタマイズされたインストーラ トランスフォーム

作成した独自のトランスフォームを、クライアント インストーラ プログラムを使用して展開することによって、AnyConnect クライアント GUI を大幅にカスタマイズすることができます (Windows のみ)。トランスフォームを ASA にインポートすると、インストーラ プログラムを使用して展開されます。

トランスフォームの適用先として選択できるのは Windows だけです。トランスフォームの詳細については、『Cisco AnyConnect Secure Mobility Client Administration Guide』を参照してください。

AnyConnect のカスタマイズとローカリゼーション、ローカライズされたインストーラ トランスフォーム

トランスフォームを使用して、クライアント インストーラ プログラムに表示されるメッセージを翻訳できます。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

AnyConnect カスタム属性

カスタム属性は AnyConnect クライアントに送信され、以下に示すような機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。多数のさまざまな用途のカスタム属性を作成および設定します。

- **DSCP Preservation Allowed** : (DSCP の保存を有効化) このカスタム属性を設定すると、Windows または Mac のオペレーティング システム プラットフォームで DTLS 接続の Differentiated Services Code Point (DSCP) が制御されます。この属性を使用すると、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順位付けし、優先順位付けされたトラフィックにマークを付けてアウトバウンド接続の質を改善することができます。詳細については、『[Cisco AnyConnect Secure Mobility Client Administration Guide](#)』の「Enable DSCP Preservation」セクションを参照してください。

値は True または False です。デフォルトでは、AnyConnect 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値を false に設定し、接続を再初期化します。

- **DeferredUpdateAllowed** または **DeferredUpdateAllowed_ComplianceModule** : (ASA で更新の延期を有効化) これらのカスタム属性が設定されている場合に、クライアントのアップデートが利用可能になると、AnyConnect は更新を実行するか延期するかをユーザに尋ねるダイアログを開きます。詳細については、「[Enable AnyConnect Client Deferred Upgrade](#)」または『[Cisco AnyConnect Secure Mobility Client Administration Guide](#)』の「[Configure Deferred Update on an ASA](#)」を参照してください。

値は True または False です。True の場合、更新の延期が有効になります。更新の延期が無効 (False) の場合、下記の設定は無視されます。

- **DeferredUpdateMinimumVersion_ComplianceModule** または

DeferredUpdateMinimumVersion : 更新を延期できるようにするためにインストールする必要がある最小バージョンの AnyConnect。

値は x.x.x で、デフォルトは 0.0.0 です。

- **DeferredUpdateDismissTimeout** : 更新の延期を確認するダイアログが表示されてから、自動的に閉じるまでの秒数。更新の延期を確認するダイアログが表示される場合にのみ適用されます。

値は 0 ~ 300 秒です。デフォルトは 150 秒です。

- **DeferredUpdateDismissResponse** : DeferredUpdateDismissTimeout の発生時に実行するアクション。

値は defer (延期) または update (更新) です。デフォルトは update です。

- **dynamic-split-exclude-domains** <属性名><ドメインのリスト> または **dynamic-split-include-domains** <属性名><ドメインのリスト> : (ダイナミック スプリット トンネリングを有効化) このカスタム属性を作成することにより、トンネルの確立後に、ホストの 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。dynamic-split-exclude-domains を追加することにより、VPN トンネルの外部のクライアントによるアクセスが必要なクラウドまたは Web サービスを入力できます。詳細については、『[Cisco AnyConnect Secure Mobility Client Administration Guide](#)』の「[About Dynamic Split Tunneling](#)」を参照してください。

値の属性名には、任意の名前を指定できます。たとえば、anyconnect-custom-data dynamic-split-exclude-domains excludeddomains webex.com, ciscospark.com のようにします。

- **managementTunnelAllAllowed** : (管理 VPN トンネルを有効化) ユーザが開始したネットワーク通信に影響しないように (管理 VPN トンネルは透過的であるため) スプリット包含トンネリングの設定がデフォルトで必要です。

値は true または false です。この動作をオーバーライドするには、属性名と値の両方を true に設定します。両方の IP プロトコルの設定が tunnel-all、split-exclude、split-include、または bypass のいずれかの場合、AnyConnect は次に管理トンネル接続に進みます。

- **no-dhcp-server-route** : (パブリック DHCP サーバルートを設定) このカスタム属性を使用すると、[Tunnel All Network] が設定されている場合にローカル DHCP トラフィックがクリアテキストでフローできます。AnyConnect は、AnyConnect クライアントが接続するとローカル DHCP サーバに特定のルートを追加してホスト マシンの LAN アダプタに暗黙的フィルタを適用し、そのルートについて DHCP トラフィック以外のすべてのトラフィックをブロックします。詳細については、『Cisco AnyConnect Secure Mobility Client Administration Guide』の「Set Public DHCP Server Route」のセクションを参照してください。

値は true または false です。トンネル確立時のパブリック DHCP サーバルート作成を避けるために、no-dhcp-server-route カスタム属性が存在し、true に設定されている必要があります。

- **circumvent-host-filtering** : (サブネットの除外をサポートするように Linux を設定) [Tunnel Network List Below] がスプリットトンネリング用に設定されている場合はサブネットの除外をサポートするように、Linux を設定します。詳細については、サブネットの除外をサポートするための Linux の設定 (90 ページ) を参照してください。

値は true または false です。true に設定します。

- **tunnel-from-any-source** : (Linux のみ) AnyConnect は、Split-Include または Split-Exclude トンネルモードの任意の送信元アドレスを持つパケットを許可します。VM インスタンスまたは Docker コンテナ内のネットワークアクセスを許可できます。



(注) VM/Docker で使用されるネットワークは、最初にトンネルから除外する必要があります。

- **perapp** : モバイルデバイス (Android または Apple iOS のみ) 上の特定のアプリケーションセットで VPN 接続が使用されます。詳細については、『Cisco AnyConnect Secure Mobility Client Administration Guide』の「Create Per App Custom Attributes」セクションを参照してください。

値を指定する際は、ポリシーツールから BASE64 形式をコピーしてここに貼り付けて、1 つ以上の値を追加します。

これらの機能の使用をさらに完全にするには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > メニューで、定義済みカスタム属性のほとんどを特定のグループ ポリシーに関連付ける必要があります。

IPsec VPN クライアント ソフトウェア



- (注) VPN クライアントは耐用年数末期で、サポートが終了しています。VPN クライアントの設定については、ASA バージョン 9.2 に関する ASDM のマニュアルを参照してください。AnyConnect セキュア モビリティ クライアントにアップグレードすることを推奨します。

Zone Labs Integrity Server

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Zone Labs Integrity Server] パネルでは、Zone Labs Integrity Server をサポートするように ASA を設定できます。このサーバは、プライベート ネットワークにアクセスするリモートクライアントでセキュリティ ポリシーを適用する目的で設計された Integrity System というシステムの一部です。実質的には、ASA がファイアウォールサーバに対するクライアント PC のプロキシとして機能し、Integrity クライアントと Integrity サーバ間で必要なすべての Integrity 情報をリレーします。



- (注) 現在のリリースのセキュリティアプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザインターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、ASA 上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

- [Server IP address] : Integrity サーバの IP アドレスを入力します。ドット付き 10 進数を使用します。
- [Add] : 新しいサーバ IP アドレスを Integrity サーバのリストに追加します。このボタンは、Server IP アドレス フィールドにアドレスが入力されるとアクティブになります。
- [Delete] : 選択したサーバを Integrity サーバのリストから削除します。
- [Move Up] : 選択したサーバを Integrity サーバのリスト内で上に移動します。このボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。
- [Move Down] : 選択したサーバを Integrity サーバのリスト内で下に移動します。このボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。
- [Server Port] : アクティブな Integrity サーバをリッスンする ASA のポート番号を入力します。このフィールドは、Integrity Server のリストにサーバが少なくとも 1 台以上存在する場合にだけ使用できます。デフォルトポート番号は 5054、範囲は 10 ~ 10000 です。このフィールドは、Integrity Server リスト内にサーバが存在する場合にだけ使用できます。

- [Interface] : アクティブな Integrity サーバと通信する ASA インターフェイスを選択します。このインターフェイス名メニューは、Integrity Server リスト内にサーバが存在する場合にだけ使用できます。
- [Fail Timeout] : ASA がアクティブな Integrity サーバに到達できないことを宣言するまでの待機秒数を入力します。デフォルトは 10 で、範囲は、5 ~ 20 です。
- [SSL Certificate Port] : SSL 認証で使用する ASA のポートを指定します。デフォルトのポートは 80 です。
- [Enable SSL Authentication] : ASA によるリモートクライアントの SSL 証明書の認証をイネーブルにする場合にオンにします。デフォルトでは、クライアント SSL 認証はディセーブルになっています。
- [Close connection on timeout] : タイムアウト時に ASA と Integrity サーバ間の接続を終了する場合にオンにします。デフォルトでは、接続が維持されます。
- [Apply] : 設定を実行している ASA に Integrity サーバの設定を適用します。
- [Reset] : まだ適用されていない Integrity サーバの設定の変更を削除します。

ISE ポリシーの適用

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、およびアカウントिंग (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 のユーザまたはユーザ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
- AnyConnect
- L2TP/IPsec

システムフローは次のとおりです。

1. エンドユーザが VPN 接続を要求します。
2. ASA は、ISE に対してユーザを認証し、ネットワークへの限定アクセスを提供するユーザ 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 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。

ISE 許可変更の設定

ISE 認可変更を設定するには、ISE RADIUS サーバを含むサーバグループを作成し、リモートアクセス VPN 設定プロファイル（トンネル）でそのサーバグループを使用します。

手順

ステップ 1 ISE サーバの RADIUS AAA サーバグループを設定します。

次の手順は、最小限の設定を示しています。必要に応じて、グループの他の設定を調整できます。大部分の設定には、ほとんどのネットワークに適したデフォルト設定があります。RADIUS AAA サーバグループの設定の詳細については、一般的なコンフィギュレーションガイドを参照してください。

- a) **[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups]** を選択します。
- b) **[AAA Server Group]** 領域で、**[Add]** をクリックします。
- c) **[Server Group]** フィールドにグループの名前を入力します。
- d) **[Protocol]** ドロップダウンリストから RADIUS サーバタイプを選択します。
- e) **[Enable interim accounting update]** と **[Update Interval]** を選択し、RADIUS 中間アカウンティング更新メッセージが定期的に生成されるようにします。

ISE は、ASA などの NAS デバイスから受信するアカウンティ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（アカウンティ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ティ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。

これらの更新を送信する間隔を時間単位で変更できます。デフォルトは 24 時間で、指定できる範囲は 1 ~ 120 です。

- f) **[Enable dynamic authorization]** を選択します。

このオプションは、AAA サーバグループの RADIUS の動的認可（ISE 許可変更、CoA）サービスをイネーブルにします。VPN トンネルでサーバグループを使用すると、対応する RADIUS サーバグループが 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ッスンします。別のポートを使用するように ISE サーバが設定されていない限り、ポート（1700）を変更しないでください。有効な範囲は 1024 ～ 65535 です。

- g) 認証に ISE を使用しない場合は、[Use authorization only mode] を選択します。

このオプションは、サーバ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 サーバ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にこのサーバグループを使用する可能性があるからです。

- h) [OK] をクリックして、サーバグループを保存します。
i) サーバグループを選択したら、[Servers in the Selected Group] リストで [Add] をクリックし、ISE RADIUS サーバをグループに追加します。

キー属性を以下に示します。必要に応じて、他の設定用にデフォルトを調整できます。

- [Interface Name] : ISE サーバに到達するためのインターフェイス。
- [Server Name or IP Address] : ISE サーバのホスト名または IP アドレス。
- (任意) [Server Secret Key] : 接続を暗号化するキー。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 サーバ上のキーと同じ値になります。

- j) [OK] をクリックして、サーバをグループに追加します。

サーバグループに別の ISE サーバを追加します。

ステップ 2 リモートアクセス VPN で ISE サーバグループを使用するために、設定プロファイルを更新します。

以下の手順は、ISE 関連の設定オプションにのみ該当します。機能的なリモートアクセス VPN を作成するには、その他のオプションも設定する必要があります。リモートアクセス VPN の実装については、このマニュアルの他の箇所の説明に従ってください。

- a) **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles]** を選択します。
b) [Connection Profiles] テーブルで、プロファイルを追加または編集します。
c) [Basic] ページで、認証方式を設定します。
- 認証に ISE サーバを使用する場合は、**[Authentication] > [Method]** に対して [AAA] を選択し、次に ISE AAA サーバグループを選択します。

- 許可用にのみ ISE サーバグループを設定する場合は、別の認証方式 ([Certificate] など) を選択します。
- d) **[Advanced]** > **[Authorization]** ページで、[Authorization Server Group] に対して ISE サーバグループを選択します。
 - e) **[Advanced]** > **[Accounting]** ページで、ISE サーバグループを選択します。
 - f) [OK] をクリックして変更を保存します。
-



第 5 章

VPN の IP アドレス

- [IP アドレス割り当てポリシーの設定 \(195 ページ\)](#)
- [ローカル IP アドレス プールの設定 \(197 ページ\)](#)
- [DHCP アドレス指定の設定 \(200 ページ\)](#)
- [ローカル ユーザへの IP アドレスの割り当て \(201 ページ\)](#)

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。

- **[Use authentication server]** : ユーザ単位で外部認証、認可、アカウンティングサーバ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。AAA サーバは、`[Configuration] > [AAA Setup]` ペインで設定できます。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。
- **[Use DHCP]** : DHCP サーバから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバを設定する必要があります。また、DHCP サーバで使用可能な IP アドレスの範囲も定義する必要があります。DHCP を使用する場合は、`[Configuration] > [Remote Access VPN] > [DHCP Server]` ペインでサーバを設定します。この方法は IPv4 の割り当てポリシーに使用できます。
- **[Use an internal address pool]** : 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。この方法を使用する場合は、`[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools]` ペインで IP アドレスプールを設定します。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。
- **[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、これはチェック

くされません。つまり、ASA は遅延時間を課しません。遅延時間を設定する場合は、チェックボックスをオンにし、IP アドレスを再割り当てするまでの時間を 1 ～ 480 の範囲で指定します。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。

IP アドレス割り当てオプションの設定

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

ステップ 2 [IPv4 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server]: IP アドレスを提供するために設定した認証、許可、アカウントिंग (AAA) サーバを使用できるようにします。
- [Use DHCP]: IP アドレスを提供するために設定したダイナミック ホスト コンフィギュレーション プロトコル (DHCP) サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカル アドレス プール設定を使用できるようにします。

[Use internal address pools] を有効にする場合、IPv4 アドレスが解放された後、そのアドレスの再利用を有効にできます。You can specify a range of minutes from 0-480 after which the IP v4 address can be reused.

ステップ 3 [IPv6 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server]: IP アドレスを提供するために設定した認証、許可、アカウントिंग (AAA) サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカル アドレス プール設定を使用できるようにします。

ステップ 4 [Apply] をクリックします。

ステップ 5 [OK] をクリックします。

アドレス割り当て方式の表示

手順

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] の順に選択します。

ローカル IP アドレス プールの設定

VPN リモート アクセス トンネルに対して IPv4 または IPv6 アドレス プールを設定するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] > [Add/Edit IP Pool] を選択します。アドレス プールを削除するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] を選択します。削除するアドレス プールを選択し、[Delete] をクリックします。

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。

ローカル IPv4 アドレス プールの設定

[IP Pool] エリアには、設定されたアドレス プールが、名前ごとに、それぞれの IP アドレス範囲（たとえば、10.10.147.100～10.10.147.177）とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプール内のアドレスがすべて割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

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。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。

ステップ 2 IPv4 アドレスを追加するには、**[Add] > [IPv4 Address pool]** をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、**[Edit]** をクリックします。

ステップ 3 **[Add/Edit IP Pool]** ダイアログボックスで、次の情報を入力します。

- **[Pool Name]** : アドレス プールの名前を入力します。最大 64 文字を指定できます。
- **[Starting Address]** : 設定されたそれぞれのプールで使用可能な最初の IP アドレスを示します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- **[Ending Address]** : 設定されたそれぞれのプールで使用可能な最後の IP アドレスを示します。たとえば 10.10.147.177 のように、ドット付き 10 進数表記を使用します。
- **[Subnet Mask]** : この IP アドレスが常駐するサブネットを指定します。

ステップ 4 **[Apply]** をクリックします。

ステップ 5 **[OK]** をクリックします。

ローカル IPv6 アドレス プールの設定

[IP Pool] エリアには、設定されたアドレス プールが、名前ごとに、開始 IP アドレス範囲、アドレスプレフィックス、プールに設定できるアドレス数とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプール内のアドレスがすべて割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

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。

手順

ステップ 1 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools]** を選択します。

ステップ 2 IPv6 アドレスを追加するには、**[Add] > [IPv6 Address pool]** をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、**[Edit]** をクリックします。

ステップ 3 **[Add/Edit IP Pool]** ダイアログボックスで、次の情報を入力します。

- **[Name]** : 設定された各アドレス プールの名前を表示します。
- **[Starting IP Address]** : 設定されたプールで使用可能な最初の IP アドレスを入力します。たとえば、2001:DB8::1 となります。
- **[Prefix Length]** : IP アドレスプレフィックス長をビット単位で入力します。たとえば、32 は CIDR 表記で /32 を表します。プレフィックス長は、IP アドレスが常駐するプールのサブネットを定義します。

- [Number of Addresses] : 開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [OK] をクリックします。

グループポリシーへの内部アドレス プールの割り当て

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集している内部ネットワーク（クライアント）アクセスグループポリシーのアドレスプール、トンネリングプロトコル、フィルタ、接続設定、およびサーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルトグループポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

同じグループポリシーで IPv4 と IPv6 両方のアドレスポリシーを設定できます。同じグループポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

手順

-
- ステップ 1 ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。
 - ステップ 2 新しいグループポリシーを作成するか、内部アドレス プールを設定するグループポリシーを作成し、[Edit] をクリックします。
[General attributes] ペインは [group policy] ダイアログで、デフォルトで選択されています。
 - ステップ 3 [Address Pools] フィールドを使用して、このグループポリシーの IPv4 アドレス プールを指定します。[Select] をクリックし、IPv4 アドレス プールを追加または編集します。
 - ステップ 4 [IPv6 Address Pools] フィールドを使用して、このグループポリシーに使用する IPv6 アドレス プールを指定します。[Select] をクリックし、IPv6 アドレス プールを追加または編集します。
 - ステップ 5 [OK] をクリックします。
 - ステップ 6 [Apply] をクリックします。
-

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、およびその DHCP サーバで使用可能な 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 サーバを識別できます。また、DHCP オプションはユーザに転送されず、ユーザはアドレス割り当てのみを受信します。

手順

ステップ 1 DHCP サーバを設定します。

DHCP サーバを使用して IPv6 アドレスを AnyConnect クライアントに割り当てることはできません。

- a) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [アドレス割り当て (Address Assignment)] > [割り当てポリシー (Assignment Policy)] で DHCP が有効になっていることを確認します。
- b) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [DHCP サーバ (DHCP Server)] を選択して、DHCP サーバを設定します。

ステップ 2 接続プロファイルで DHCP サーバを定義します。

- a) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [AnyConnect 接続プロファイル (AnyConnect Connection Profiles)] を選択します。
- b) [Connection Profiles] エリアで [Add] または [Edit] をクリックします。
- c) 接続プロファイルの設定ツリーで、[Basic] をクリックします。
- d) [Client Address Assignment] エリアで、クライアントに IP アドレスを割り当てるために使用する DHCP サーバの IPv4 アドレスを入力します。たとえば、**172.33.44.19** と指定します。

ステップ 3 DHCP スコープを定義するために、接続プロファイルに関連付けられたグループポリシーを編集します。

- a) [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [グループポリシー (Group Policies)] を選択します。
- b) 編集するグループ ポリシーをダブルクリックします。
- c) 設定ツリーで、[Server] をクリックします。
- d) 下矢印をクリックして、[More Options] エリアを拡大表示します。
- e) [DHCPスコープの継承 (DHCP Scope Inherit)] をオフにして、DHCP スコープを定義します。

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。

- f) [OK] をクリックします。
- g) [適用 (Apply)] をクリックします。

ローカル ユーザへの IP アドレスの割り当て

グループ ポリシーを使用するようにローカル ユーザ アカウントを設定し、また AnyConnect 属性を設定することもできます。IP アドレスの他のソースに障害が発生した場合に、これらのユーザ アカウントがフォールバックを提供するので、管理者は引き続きアクセスできます。

始める前に

ユーザを追加または編集するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] の順に選択し、[Add] または [Edit] をクリックします。

デフォルトでは、[Edit User Account] 画面の設定ごとに [Inherit] チェックボックスがオンになっています。つまり、ユーザアカウントは、デフォルトグループポリシー DfltGrpPolicy のその設定の値を継承するということです。

各設定内容をオーバーライドする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。次の詳細な手順では IP アドレスの設定について説明します。設定の完全な詳細については [ローカル ユーザの VPN ポリシー属性の設定 \(118 ページ\)](#) を参照してください。

手順

-
- ステップ 1 ASDM を開始し、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] の順に選択します。
 - ステップ 2 設定するユーザを選択し、[Edit] をクリックします。
 - ステップ 3 左側のペインで、[VPN Policy] をクリックします。
 - ステップ 4 このユーザに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address (Optional)] 領域で、IPv4 アドレスとサブネットマスクを入力します。
 - ステップ 5 このユーザに専用の IPv6 アドレスを設定するには、[Dedicated IPv6 Address (Optional)] 領域に IPv6 プレフィックスを含む IPv6 アドレスを入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。
 - ステップ 6 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。
-



第 6 章

ダイナミック アクセス ポリシー

この章では、ダイナミック アクセス ポリシーを設定する方法を説明します。

- [ダイナミック アクセス ポリシーについて \(203 ページ\)](#)
- [ダイナミック アクセス ポリシーのライセンス \(206 ページ\)](#)
- [ダイナミック アクセス ポリシーの設定 \(206 ページ\)](#)
- [DAP の AAA 属性選択基準の設定 \(209 ページ\)](#)
- [DAP のエンドポイント属性選択基準の設定 \(213 ページ\)](#)
- [LUA を使用した DAP における追加の DAP 選択基準の作成 \(228 ページ\)](#)
- [DAP アクセスと許可ポリシー属性の設定 \(234 ページ\)](#)
- [DAP トレースの実行 \(239 ページ\)](#)
- [DAP の例 \(240 ページ\)](#)

ダイナミック アクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティレベルが異なるリモート アクセス サイトからのログインなど、複数の変数が影響する可能性があります。VPN 環境でのユーザ認可のタスクは、スタティックな設定のネットワークでの認可タスクよりもかなり複雑です。

ASA ではダイナミック アクセス ポリシー (DAP) によって、これらのさまざまな変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザ トンネルまたはユーザセッションに関連付ける一連のアクセスコントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイントセキュリティの問題に対処します。つまり、ASA では、定義したポリシーに基づき、特定のセッションへのアクセス権が特定のユーザに付与されます。ASA は、ユーザが接続した時点で、DAP レコードからの属性を選択または集約することによって DAP を生成します。DAP レコードは、リモートデバイスのエンドポイントセキュリティ情報および認証されたユーザの AAA 認可情報に基づいて選択されます。選択された DAP レコードは、ユーザ トンネルまたはセッションに適用されます。

DAP システムには、注意を必要とする次のコンポーネントがあります。

- **DAP 選択コンフィギュレーションファイル**：セッション確立中に DAP レコードを選択して適用するために ASA が使用する、基準が記述されたテキストファイル。ASA 上に保存されます。ASDM を使用して、このファイルを変更したり、XML データ形式で ASA にアップロードしたりできます。DAP 選択設定ファイルには、ユーザが設定するすべての属性が記載されています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタ、ポート転送、URL のリストとして設定されたアクセス ポリシーなどがあります。
- **DfltAccess ポリシー**：常に DAP サマリー テーブルの最後のエントリで、プライオリティは必ず 0。デフォルトアクセスポリシーのアクセスポリシー属性を設定できますが、AAA 属性またはエンドポイント属性は含まれておらず、これらの属性は設定できません。DfltAccessPolicy は削除できません。また、サマリー テーブルの最後のエントリになっている必要があります。

詳細については、『*Dynamic Access Deployment Guide*』
<https://supportforums.cisco.com/docs/DOC-1369> を参照してください。

DAP によるリモート アクセス プロトコルおよびポストチャ評価ツールのサポート

ASA は、管理者が設定したポストチャ評価ツールを使用してエンドポイントセキュリティ属性を取得します。このポストチャ評価ツールには、AnyConnect ポストチャ モジュール、独立したホストスキャンパッケージ、および NAC が含まれます。

次の表に、DAP がサポートしている各リモート アクセス プロトコル、その方式で使用可能なポストチャ評価ツール、およびそのツールによって提供される情報を示します。

サポートされるリモート アクセス プロトコル	AnyConnect ポストチャ モジュール ホストスキャンパッケージ Cisco Secure Desktop (Endpoint Assessment ホストスキャン拡張機能がイネーブルでない)	AnyConnect ポストチャ モジュール ホストスキャンパッケージ Cisco Secure Desktop (Endpoint Assessment ホストスキャン拡張機能がイネーブルである)	NAC	Cisco NAC アプライアンス
	ファイル情報、レジストリ キーの値、実行プロセス、オペレーティング システムを返す	マルウェア対策およびパーソナルファイアウォールソフトウェアの情報を返す	NAC ステータスを返す	VLAN タイプと VLAN ID を返す

サポートされるリモート アクセス プロトコル	AnyConnect ポスチャ モジュール ホスト スキャン パッケージ Cisco Secure Desktop (Endpoint Assessment ホスト スキャン 拡張機能がイネーブルでない)	AnyConnect ポスチャ モジュール ホスト スキャン パッケージ Cisco Secure Desktop (Endpoint Assessment ホスト スキャン 拡張機能がイネーブルである)	NAC	Cisco NAC アプリアンス
IPsec VPN	非対応	×	対応	対応
Cisco AnyConnect VPN	対応	対応	対応	対応
クライアントレス (ブラウザベース) SSL VPN	対応	対応	×	×
PIX カットスルー プロキシ (ポスチャ 評価は使用不可)	非対応	非対応	非対応	×

DAP によるリモート アクセス接続のシーケンス

次のシーケンスに、標準的なリモート アクセス接続を確立する場合の概要を示します。

1. リモート クライアントが VPN 接続を試みます。
2. ASA は、設定された NAC 値と Cisco Secure Desktop の Host Scan 値を使用してポスチャ 評価を実行します。
3. ASA は、AAA を介してユーザを認証します。AAA サーバは、ユーザの認可属性も返します。
4. ASA は AAA 認可属性をそのセッションに適用し、VPN トンネルを確立します。
5. ASA は、AAA 認可情報とセッションのポスチャ 評価情報に基づいて DAP レコードを選択します。
6. ASA は選択した DAP レコードから DAP 属性を集約し、その集約された属性が DAP ポリシーになります。
7. ASA はその DAP ポリシーをセッションに適用します。

ダイナミック アクセス ポリシーのライセンス



(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。

ダイナミックアクセスポリシー (DAP) には、次のいずれかのライセンスが必要です。

- AnyConnect Apex : すべての DAP 機能を使用する場合。
- AnyConnect Plus : オペレーティングシステムおよびオペレーティングシステムまたは AnyConnect のバージョンチェック専用。

関連トピック

[DAP への AnyConnect エンドポイント属性の追加 \(216 ページ\)](#)

ダイナミック アクセス ポリシーの設定

始める前に

- 特に記載のない限り、DAP エンドポイント属性を設定する前に、ホスト スキャンをインストールする必要があります。
- HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『[AnyConnect HostScan 4.3.x to 4.6.x Migration Guide](#)』を参照してください。
- Java Web Start セキュリティの問題のため、デバイスで webvpn ベースの設定を使用する場合は、設定した値を高度なエンドポイント属性に入力できないことがあります。この問題を解決するには、ASDM デスクトップアプリケーションを使用するか、または Java セキュリティの例外として AEA 関連の URL を追加します。
- ファイル、プロセス、レジストリのエンドポイント属性を設定する前に、ファイル、プロセス、レジストリの基本ホスト スキャン属性を設定する必要があります。手順については、ASDM を起動して [Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] の順に選択し、[Help] をクリックしてください。
- DAP は、ASCII 文字のみサポートされます。

手順

- ステップ 1 ASDM を起動し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] または [Clientless SSL VPN Access] > [Dynamic Access Policies] を選択します。

(注) [Add]、[Edit]、および [Delete] アクションの下に [Incompatible] アクションボタンが表示される場合は、内部ライブラリの更新により既存 DAP ポリシー（HostScan 4.3.x 以前を使用して作成）と互換性がなくなったバージョン（4.6.x以降）に HostScan をアップグレードしようとしています。ワンタイム移行手順を実行して、設定を適応させる必要があります。

[Incompatible] アクションが表示される場合は、HostScan のアップグレードが開始され、設定の移行が必要になったことを示しています。詳細な手順については、『[AnyConnect Hostscan 4.3.x to 4.6.x Migration Guide](#)』を参照してください。

ステップ 2 特定のマルウェア対策またはパーソナル ファイアウォールのエンドポイント属性を含めるには、ページの最上部近くの [CSD configuration] リンクをクリックします。次に、Cisco Secure Desktop および HostScan の拡張機能をイネーブルにします。このリンクは、これら両方の機能をすでにイネーブルにしている場合には表示されません。

ステップ 3 設定済みの DAP のリストを表示します。

テーブルには次のフィールドが表示されます。

- [ACL Priority] : DAP レコードのプライオリティを表示します。

ASA は、複数の DAP レコードからネットワーク ACL と Web タイプ ACL を集約するとき、この値を使用して ACL を論理的に順序付けします。ASA は、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。番号が大きいほどプライオリティが高いことを意味します。たとえば、値が 4 の DAP レコードは値が 2 のレコードよりも高いプライオリティを持つこととなります。プライオリティは、手動での並べ替えはできません。

- [Name] : DAP レコードの名前を表示します。
- [Network ACL List] : セッションに適用されるファイアウォール ACL の名前を表示します。
- [Web-Type ACL List] : セッションに適用される SSL VPN ACL の名前を表示します。
- [Description] : DAP レコードの目的を説明します。

ステップ 4 [Add] または [Edit] をクリックして、[ダイナミック アクセス ポリシーの追加または編集（208 ページ）](#) を実行します。

ステップ 5 [Apply] をクリックして DAP 設定を保存します。

ステップ 6 [Find] フィールドを使用して、ダイナミック アクセス ポリシー（DAP）を検索します。

このフィールドへの入力を開始すると、DAP テーブルの各フィールドの先頭部分の文字が検索され、一致するものが検出されます。ワイルドカードを使用すると、検索範囲が広がります。

たとえば、[Find] フィールドに「sal」と入力した場合は、Sales という名前の DAP とは一致しますが、Wholesalers という名前の DAP とは一致しません。[Find] フィールドに *sal と入力すると、テーブル内の **Sales** または **Wholesalers** のうち、最初に出現したものが検出されます。

ステップ 7 [ダイナミック アクセス ポリシーのテスト \(209 ページ\)](#) を実行して設定を確認します。

ダイナミック アクセス ポリシーの追加または編集

手順

ステップ 1 ASDM を起動し、**[Configuration] > [Remote Access VPN] > [Network (Client) Access]** または **[Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add]** または **[Edit]** を選択します。

ステップ 2 このダイナミック アクセス ポリシーの名前（必須）と説明（オプション）を入力します。

- [Policy Name] は、4 ～ 32 文字の文字列で、スペースは使用できません。
- DAP の [Description] フィールドには 80 文字まで入力できます。

ステップ 3 [ACL Priority] フィールドで、そのダイナミック アクセス ポリシーのプライオリティを設定します。

セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数値が大きいほどプライオリティは高くなります。有効値の範囲は 0 ～ 2147483647 です。デフォルト値は 0 です

ステップ 4 この DAP の選択基準を指定します。

- a) [Selection Criteria] ペインのドロップダウンリスト（ラベルなし）で、ユーザがこのダイナミック アクセス ポリシーを使用するには、すべてのエンドポイント属性を満たすことに加えて、ここで設定される AAA 属性値のいずれか ([ANY]) またはすべて ([ALL]) が必要となるのか、それとも一切不要 ([NONE]) であるのかを選択します。

重複するエントリは許可されません。AAA 属性やエンドポイント属性を指定せずに DAP レコードを設定すると、レコードがすべての選択基準を満たしていることになるので、ASA は常にそのレコードを選択します。

- b) [AAA Attributes] フィールドの [Add] または [Edit] をクリックして、[DAP の AAA 属性選択基準の設定 \(209 ページ\)](#) を実行します。
- c) [Endpoint Attributes] 領域で [Add] または [Edit] をクリックして、[DAP のエンドポイント属性選択基準の設定 \(213 ページ\)](#) を実行します。
- d) [Advanced] フィールドをクリックして、[LUA を使用した DAP における追加の DAP 選択基準の作成 \(228 ページ\)](#) を実行します。この機能を使用するには、[Lua プログラミング言語](#)の知識が必要です。

- [AND/OR]：基本的な選択ルールと、ここで入力する論理式との関係を定義します。つまり、すでに設定されている AAA 属性およびエンドポイント属性に新しい属性を追加するのか、またはそれら設定済みの属性に置き換えるのかを指定します。デフォルトは AND です。

- [Logical Expressions] : それぞれのタイプのエンドポイント属性のインスタンスを複数設定できます。新しい AAA 選択属性またはエンドポイント選択属性（あるいはその両方）を定義するフリー形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、テキストを DAP XML ファイルにコピーするだけです。処理は ASA によって行われ、解析不能な式は破棄されます。

(注) DAPXML (DAP.xml) ファイルは構成ファイルです。ASDM は、ファイルのエクスポートまたはインポートをサポートしていません。手動または CLI を介してファイルを変更またはアップロードしないでください。構成の問題が生じる可能性があります。

ステップ 5 この DAP のアクセス/許可ポリシー属性を指定します。

ここで設定する属性値は、既存のユーザ、グループ、トンネルグループ、およびデフォルトのグループレコードを含め、AAA システムの認可値を上書きします。[DAP アクセスと許可ポリシー属性の設定 \(234 ページ\)](#) を参照してください。

ステップ 6 [OK] をクリックします。

ダイナミック アクセス ポリシーのテスト

このペインでは、認可属性値のペアを指定することによって、デバイスで設定される DAP レコードセットが取得されるかどうかをテストできます。

手順

ステップ 1 属性値のペアを指定するには、[AAA Attribute] テーブルと [Endpoint Attribute] テーブルに関連付けられた [Add/Edit] ボタンを使用します。

[Add/Edit] ボタンをクリックすると表示されるダイアログは、[Add/Edit AAA Attributes] ウィンドウと [Add/Edit Endpoint Attributes] ダイアログボックスに表示されるダイアログに似ています。

ステップ 2 [Test] ボタンをクリックします。

デバイス上の DAP サブシステムは、各レコードの AAA およびエンドポイント選択属性を評価するときに、これらの値を参照します。結果は、[Test Results] 領域に表示されます。

DAP の AAA 属性選択基準の設定

DAP は AAA サービスを補完します。用意されている認可属性のセットは限られていますが、それらの属性によって AAA で提供される認可属性を無効にできます。AAA 属性は、Cisco AAA

属性階層から指定するか、ASA が RADIUS または LDAP サーバから受信する応答属性一式から指定できます。ASA は、ユーザの AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。ASA は、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

手順

DAP レコードの選択基準として AAA 属性を設定するには、[Add/Edit AAA Attributes] ダイアログボックスで、使用する Cisco、LDAP、または RADIUS 属性を設定します。これらの属性は、入力する値に対して「=」または「!=」のいずれかに設定できます。各 DAP レコードに設定可能な AAA 属性の数に制限はありません。AAA 属性の詳細については、[AAA 属性の定義 \(212 ページ\)](#) を参照してください。

[AAA Attributes Type] : ドロップダウンリストを使用して、Cisco、LDAP、または RADIUS 属性を選択します。

- [Cisco] : AAA 階層モデルに保存されているユーザ認可属性を参照します。DAP レコードの AAA 選択属性に、これらのユーザ認可属性の小規模なサブセットを指定できます。次の属性が含まれます。
 - [Group Policy] : VPN ユーザセッションに関連付けられているグループポリシー名を示します。セキュリティアプライアンスでローカルに設定するか、IETF クラス (25) 属性として RADIUS/LDAP から送信します。最大 64 文字です。
 - [Assigned IP Address] : ポリシーに指定する IPv4 アドレスを入力します。フルトンネル VPN クライアント (IPsec、L2TP/IPsec、SSL VPN AnyConnect) に割り当てられた IP アドレスは、クライアントレス SSL VPN には割り当てられません。クライアントレスセッションにはアドレスの割り当てがないからです。
 - [Assigned IPv6 Address] : ポリシーに指定する IPv6 アドレスを入力します。
 - [Connection Profile] : コネクションまたはトンネリングのグループ名。最大 64 文字です。
 - [Username] : 認証されたユーザのユーザ名。最大 64 文字です。ローカル認証、RADIUS 認証、LDAP 認証のいずれかを、またはその他の認証タイプ (RSA/SDI、NT Domain などのいずれかを使用している場合に適用されます)。
 - [=!] : と等しい/と等しくない
- [LDAP] : LDAP クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答属性値のペアを保存します。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザレコードとグループレコードの両方が LDAP サーバから読み込まれると、このシナリオが発生する場合があります。ユーザレコード属性が最初に読み込まれ、グループレコード属性よりも常に優先されます。

Active Directory グループメンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf 応答属性に対する特別な処理が行われます。AD memberOf 属性は、AD 内のグループレコードの DN 文字列を指定します。グループの名前は、DN 文字

列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP 応答メッセージ内に追加の memberOf 属性が存在する場合、それらの属性からグループ名が抽出され、前の AAA memberOf 属性と結合されて、グループ名がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

LDAP 認証/認可サーバへの VPN リモートアクセスセッションが次の 3 つの Active Directory グループ (memberOf 列挙) のいずれかを返す場合は、次の通りとなります。

```
cn=Engineering,ou=People,dc=company,dc=com
```

```
cn=Employees,ou=People,dc=company,dc=com
```

```
cn=EastCoastast,ou=People,dc=company,dc=com
```

ASA は、Engineering、Employees、EastCoast の 3 つの Active Directory グループを処理します。これらのグループは、aaa ldap の選択基準としてどのような組み合わせでも使用できます。

LDAP 属性は、DAP レコード内の属性名と属性値のペアで構成されています。LDAP 属性名は、構文に従う必要があり、大文字、小文字を区別します。たとえば、AD サーバが部門として返す値の代わりに、LDAP 属性の Department を指定した場合、DAP レコードはこの属性設定に基づき一致しません。

(注) [Value] フィールドに複数の値を入力するには、セミコロン (;) をデリミタとして使用します。次に例を示します。

```
eng;sale; cn=Audgen VPN,ou=USERS,o=OAG
```

- [RADIUS] : RADIUS クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ RADIUS 応答属性値のペアを保存します。RADIUS クライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザレコードおよびグループレコードの両方が RADIUS サーバから読み込まれた場合、このシナリオが発生する可能性があります。ユーザレコード属性が最初に読み込まれ、グループレコード属性よりも常に優先されます。

RADIUS 属性は、DAP レコード内の属性番号と属性値のペアで構成されています。

(注) RADIUS 属性について、DAP は Attribute ID = 4096 + RADIUS ID と定義します。次に例を示します。

RADIUS 属性「Access Hours」の Radius ID は 1 であり、したがって DAP 属性値は $4096 + 1 = 4097$ となります。

RADIUS 属性「Member Of」の Radius ID は 146 であり、したがって DAP 属性値は $4096 + 146 = 4242$ となります。

- LDAP および RADIUS 属性には、次の値があります。
 - [Attribute ID] : 属性の名前/番号。最大 64 文字です。
 - [Value] : 属性名 (LDAP) または数値 (RADIUS) 。

[Value] フィールドに複数の値を入力するには、セミコロン (;) をデリミタとして使用します。例 : eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- [=!]= : と等しい/と等しくない

- LDAP には、[Get AD Groups] ボタンが含まれます。 [Active Directory グループの取得 \(212 ページ\)](#) を参照してください。

Active Directory グループの取得

Active Directory サーバにクエリーを実行し、このペインで利用可能な AD グループを問い合わせることができます。この機能は、LDAP を使用している Active Directory サーバだけに適用されます。このボタンは、Active Directory LDAP サーバに対して、ユーザが属するグループのリスト (memberOf 列挙) の問い合わせを実行します。このグループ情報を使用し、ダイナミック アクセス ポリシーの AAA 選択基準を指定します。

AD グループは、バックグラウンドで CLI の **how-ad-groups** コマンドを使用することで LDAP サーバから取得されます。ASA がサーバの応答を待つデフォルト時間は 10 秒です。aaa-server ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用し、時間を調整できます。

[Edit AAA Server] ペインで Group Base DN を変更し、Active Directory 階層の中で検索を開始するレベルを変更できます。このウィンドウでは、ASA がサーバの応答を待つ時間も変更できます。これらの機能を設定するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] > [Edit AAA Server] を選択します。



(注) Active Directory サーバに多数のグループが存在する場合は、サーバが応答パケットに含めることのできるデータ量の制限に従って、取得した AD グループのリスト (または **show ad-groups** コマンドの出力) が切り詰められることがあります。この問題を回避するには、フィルタ機能を使用し、サーバが返すグループ数を減らしてください。

[AD Server Group] : AD グループを取得する AAA サーバグループの名前。

[Filter By] : 表示されるグループ数を減らすために、グループ名またはグループ名の一部を指定します。

[Group Name] : サーバから取得された AD グループのリスト。

AAA 属性の定義

次の表に、DAP で使用できる AAA 選択属性名の定義を示します。属性名フィールドは、LUA 論理式での各属性名を入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] セクションで使用します。

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
シスコ	aaa.cisco.grouppolicy	AAA	string	64	ASA 上のグループ ポリシー名、または RADIUS/LDAP サーバから IETF-Class (25) 属性として送信されたグループポリシー名
	aaa.cisco.ipaddress	AAA	number	-	フルトンネル VPN クライアントに割り当てられた IP アドレス (IPsec、L2TP/IPsec、SSL VPN AnyConnect)
	aaa.cisco.tunnelgroup	AAA	string	64	接続プロファイル (トンネルグループ) の名前
	aaa.cisco.username	AAA	string	64	認証されたユーザの名前 (ローカル認証や認可を使用している場合に適用)
LDAP	aaa.ldap.<label>	LDAP	string	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	string	128	RADIUS 属性値ペア

DAF のエンドポイント属性選択基準の設定

エンドポイント属性には、エンドポイントシステム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。ASA は、セッション確立時にエンドポイント属性の集合を動的に生成し、セッションに関連付けられているデータベースにそれらの属性を保存します。各 DAF レコードには、ASA がセッションの DAF レコードを選択するために満たす必要があるエンドポイント選択属性が指定されています。ASA は、設定されている条件をすべて満たす DAF レコードだけを選択します。

始める前に

- DAF レコードの選択基準としてエンドポイント属性を設定することは、[ダイナミックアクセスポリシーの設定 \(206 ページ\)](#) のための大きなプロセスの一部です。DAF の選択基準としてエンドポイント属性を設定する前に、この手順を確認します。
- エンドポイント属性の詳細については、「[エンドポイント属性の定義 \(223 ページ\)](#)」を参照してください。
-

- メモリ常駐型のマルウェア対策およびパーソナル ファイアウォール プログラムをホスト スキャンがチェックする方法の詳細については、[DAP とマルウェア対策およびパーソナル ファイアウォール プログラム \(223 ページ\)](#) を参照してください。

手順

ステップ 1 [Add] または [Edit] をクリックして、次のいずれかのエンドポイント属性を選択基準として追加します。

各タイプのエンドポイント属性のインスタンスを複数作成できます。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

- [DAP へのマルウェア対策エンドポイント属性の追加 \(215 ページ\)](#)
- [DAP へのアプリケーション属性の追加 \(215 ページ\)](#)
- [DAP への AnyConnect エンドポイント属性の追加 \(216 ページ\)](#)
- [DAP へのファイル エンドポイント属性の追加 \(217 ページ\)](#)
- [DAP へのデバイス エンドポイント属性の追加 \(218 ページ\)](#)
- [DAP への NAC エンドポイント属性の追加 \(219 ページ\)](#)
- [DAP へのオペレーティング システム エンドポイント属性の追加 \(219 ページ\)](#)
- [DAP へのパーソナル ファイアウォール エンドポイント属性の追加 \(220 ページ\)](#)
- [DAP へのポリシー エンドポイント属性の追加 \(220 ページ\)](#)
- [DAP へのプロセス エンドポイント属性の追加 \(221 ページ\)](#)
- [DAP へのレジストリ エンドポイント属性の追加 \(221 ページ\)](#)
- [DAP への複数証明書認証属性の追加 \(222 ページ\)](#)

ステップ 2 条件に一致する DAP ポリシーを指定します。

これらのエンドポイント属性のタイプごとに、ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する (Match all = AND、デフォルト) のか、またはそれらのインスタンスを 1 つだけ持つように要求する (Match Any = OR) のかを決定します。

- [Logical Op] をクリックします。
- エンドポイント属性のタイプごとに、[Match Any] (デフォルト) または [Match All] を選択します。
- [OK] をクリックします。

ステップ 3 [ダイナミック アクセス ポリシーの追加または編集 \(208 ページ\)](#) に戻ってください。

DAP へのマルウェア対策エンドポイント属性の追加

始める前に

HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『[AnyConnect HostScan 4.3.x to 4.6.x Migration Guide](#)』を参照してください。

手順

- ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Anti-Malware] を選択します。
- ステップ 2 適切なボタン [Installed] または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子 ([Name]/[Operation]/[Value] 列の下のフィールド) をインストールするか、またはインストールしないかを指定します。
- ステップ 3 リアルタイム スキャンを有効または無効のどちらにするかを決定します。
- ステップ 4 [Vendor] リストボックスで、テスト対象のマルウェア対策ベンダーの名前をクリックします。
- ステップ 5 [Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリストボックスから選択します。
- ステップ 6 [Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい (=)、等しくない (!=)、より小さい (<)、より大きい (>)、以下 (<=)、または以上 (>=) に設定します。

リスト ボックスで選択したバージョンに x が付いている場合 (たとえば 3.x) は、この x を具体的なリリース番号で置き換えます (たとえば 3.5)。
- ステップ 7 [Last Update] チェックボックスをオンにします。最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く ([<]) 実行するか、遅く ([>]) 実行するかを指定できます。
- ステップ 8 [OK] をクリックします。

DAP へのアプリケーション属性の追加

手順

- ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Application] を選択します。
- ステップ 2 [Client Type] の操作フィールドで、[=] (等しい) または [!=] (等しくない) を選択します。
- ステップ 3 [Client type] リスト ボックスで、テスト対象のリモートアクセス接続のタイプを指定します。
- ステップ 4 [OK] をクリックします。

DAP への AnyConnect エンドポイント属性の追加

AnyConnect エンドポイント属性（モバイルポスチャまたは AnyConnect アイデンティティ拡張機能（ACIDex）とも呼ばれる）は、AnyConnect VPN クライアントが ASA にポスチャ情報を伝えるために使用されます。ダイナミック アクセス ポリシーでは、このエンドポイント属性を使用してユーザを認可します。

モバイルポスチャ属性をダイナミック アクセス ポリシーに組み込むと、エンドポイントにホスト スキャンや Cisco Secure Desktop がエンドポイントにインストールされていなくても適用できます。

一部のモバイルポスチャ属性は、モバイルデバイス上で実行している AnyConnect クライアントにのみ関連します。その他のモバイルポスチャ属性は、モバイルデバイス上で実行している AnyConnect クライアントと AnyConnect デスクトップクライアント上で実行している AnyConnect クライアントの両方に関連します。

始める前に

モバイルポスチャを活用するには、AnyConnect Mobile ライセンスと、AnyConnect Essentials ライセンスが ASA にインストールされている必要があります。これらのライセンスをインストールする企業は、DAP 属性および他の既存のエンドポイント属性に基づいてサポートされているモバイルデバイスの DAP ポリシーを適用できます。これには、モバイルデバイスからのリモートアクセスの許可または拒否が含まれます。

手順

ステップ 1 [Endpoint Attribute Type] リストボックスで [AnyConnect] を選択します。

ステップ 2 [Client Version] チェックボックスをオンにして、等しい (=)、等しくない (!=)、より小さい (<)、より大きい (>)、以下 (<=)、または以上 (>=) を操作フィールドで選択してから、[Client Version] フィールドで AnyConnect クライアントバージョン番号を指定します。

このフィールドを使用すると、モバイルデバイス（携帯電話やタブレットなど）のクライアントバージョンを評価できるほか、デスクトップやラップトップデバイスのクライアントバージョンも評価できます。

ステップ 3 [Platform] チェックボックスをオンにして、等しい (=) または等しくない (!=) を操作フィールドで選択してから、[Platform] リストボックスでオペレーティングシステムを選択します。

このフィールドを使用すると、モバイルデバイス（携帯電話やタブレットなど）のオペレーティングシステムを評価できるほか、デスクトップやラップトップデバイスのオペレーティングシステムも評価できます。プラットフォームを選択すると、追加の属性フィールドである [Device Type] と [Device Unique ID] が使用可能になります。

ステップ 4 [Platform Version] チェックボックスをオンにして、等しい (=)、等しくない (!=)、より小さい (<)、より大きい (>)、以下 (<=)、または以上 (>=) を操作フィールドで選択してから、[Platform Version] フィールドでオペレーティングシステムバージョン番号を指定します。

作成する DAP レコードにこの属性も含まれるようにするには、前の手順でプラットフォームも必ず指定してください。

- ステップ 5** [Platform] チェックボックスをオンにした場合は、[Device Type] チェックボックスをオンにすることができます。等しい (=) または等しくない (!=) を操作フィールドで選択してから、デバイスを [Device Type] フィールドで選択するか入力します。

サポートされるデバイスであるにもかかわらず、[Device Type] フィールドのリストに表示されていない場合は、[Device Type] フィールドに入力できます。デバイス タイプ情報を入手する最も確実な方法は、AnyConnect クライアントをエンドポイントにインストールして ASA に接続し、DAP トレースを実行することです。DAP トレースの結果の中で、**endpoint.anyconnect.devicetype** の値を見つけます。この値を [Device Type] フィールドに入力する必要があります。

- ステップ 6** [Platform] チェックボックスをオンにした場合は、[Device Unique ID] チェックボックスをオンにすることができます。等しい (=) または等しくない (!=) を操作フィールドで選択してから、デバイスの一意の ID を [Device Unique ID] フィールドに入力します。

[Device Unique ID] によって個々のデバイスが区別されるので、特定のモバイルデバイスに対するポリシーを設定できます。デバイスの一意の ID を取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.deviceuniqueid** の値を見つける必要があります。この値を [Device Unique ID] フィールドに入力する必要があります。

- ステップ 7** [Platform] をオンにした場合は、[MAC Addresses Pool] フィールドに MAC アドレスを追加できます。等しい (=) または等しくない (!=) を操作フィールドで選択してから、MAC アドレスを指定します。各 MAC アドレスのフォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字 (0 ~ 9、A ~ F、または a ~ f) です。MAC アドレスは、1 つ以上の空白スペースで区切る必要があります。

MAC アドレスによって個々のシステムが区別されるので、特定のデバイスに対するポリシーを設定できます。システムの MAC アドレスを取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.macaddress** の値を見つける必要があります。この値を [MAC Address Pool] フィールドに入力する必要があります。

- ステップ 8** [OK] をクリックします。

DAP へのファイル エンドポイント属性の追加

始める前に

ファイル エンドポイント属性を設定する前に、どのファイルをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] を選択します。詳細については、そのページの [Help] をクリックします。

手順

-
- ステップ 1** [Endpoint Attribute Type] リスト ボックスで [File] を選択します。
- ステップ 2** [Exists] と [Does not exist] のオプション ボタンでは、選択したエンドポイント属性とそれに付随する修飾子 ([Exists]/[Does not exist] ボタンの下にあるフィールド) が存在する必要があるかどうかに応じて、該当するものを選択します。
- ステップ 3** [Endpoint ID] リスト ボックスで、スキャン対象のファイル エントリに等しいエンドポイント ID をドロップダウン リストから選択します。
- ファイルの情報が [Endpoint ID] リスト ボックスの下に表示されます。
- ステップ 4** [Last Update] チェックボックスをオンにしてから、更新日からの日数が指定の値よりも小さい (<) と大きい (>) のどちらを条件とするかを操作フィールドで選択します。更新日からの日数を [days] フィールドに入力します。
- ステップ 5** [Checksum] チェックボックスをオンにしてから、テスト対象ファイルのチェックサム値と等しい (=) または等しくない (!=) のどちらを条件とするかを操作フィールドで選択します。
- ステップ 6** [Compute CRC32 Checksum] をクリックすると、テスト対象のファイルのチェックサム値が計算されます。
- ステップ 7** [OK] をクリックします。
-

DAP へのデバイス エンドポイント属性の追加

手順

-
- ステップ 1** [Endpoint Attribute Type] リスト ボックスで [Device] を選択します。
- ステップ 2** [Host Name] チェックボックスをオンにしてから、テスト対象デバイスのホスト名と等しい (=) または等しくない (!=) のどちらを条件とするかを操作フィールドで選択します。完全修飾ドメイン名 (FQDN) ではなく、コンピュータのホスト名のみを使用します。
- ステップ 3** [MAC address] チェックボックスをオンにしてから、テスト対象のネットワーク インターフェイス カードの MAC アドレスと等しい (=) または等しくない (!=) のどちらを条件とするかを操作フィールドで選択します。1 つのエントリにつき MAC アドレスは 1 つだけです。アドレスのフォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。
- ステップ 4** [BIOS Serial Number] チェックボックスをオンにしてから、テスト対象のデバイスの BIOS シリアル番号と等しい (=) または等しくない (!=) のどちらを条件とするかを操作フィールドで選択します。数値フォーマットは、製造業者固有です。フォーマット要件はありません。
- ステップ 5** [TCP/UDP Port Number] チェックボックスをオンにしてから、テスト対象のリスニング状態の TCP ポートと等しい (=) または等しくない (!=) のどちらを条件とするかを操作フィールドで選択します。

TCP/UDP コンボボックスでは、テスト対象 (TCP (IPv4) 、UDP (IPv4) 、TCP (IPv6) 、または UDP (IPv6)) のポートの種類を選択します。複数のポートをテストする場合は、DAP

の個々のエンドポイント属性のルールをいくつか作成し、それぞれに1個のポートを指定します。

- ステップ 6 [Version of Secure Desktop (CSD)] チェックボックスをオンにしてから、エンドポイント上で実行されるホストスキャンイメージのバージョンと等しい (=) または等しくない (!=) のどちらかを条件とするかを操作フィールドで選択します。
- ステップ 7 [Version of Endpoint Assessment] チェックボックスをオンにしてから、テスト対象のエンドポイントアセスメント (OPSWAT) のバージョンと等しい (=) または等しくない (!=) のどちらかを条件とするかを操作フィールドで選択します。
- ステップ 8 [OK] をクリックします。

DAP への NAC エンドポイント属性の追加

手順

- ステップ 1 [Endpoint Attribute Type] リスト ボックスで [NAC] を選択します。
- ステップ 2 [Posture Status] チェックボックスをオンにしてから、ACSによって受信されるポストチャートクン文字列と等しい (=) または等しくない (!=) のどちらかを条件とするかを操作フィールドで選択します。ポストチャートクン文字列を [Posture Status] テキスト ボックスに入力します。
- ステップ 3 [OK] をクリックします。

DAP へのオペレーティング システム エンドポイント属性の追加

手順

- ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。
 - ステップ 2 [OS Version] チェックボックスをオンにしてから、[OS Version] リスト ボックスで設定するオペレーティング システム (Windows、Mac、または Linux) と等しい (=) または等しくない (!=) のどちらかを条件とするかを操作フィールドで選択します。
 - ステップ 3 [OS Update] チェックボックスをオンにしてから、[OS Update] テキスト ボックスに入力する Windows、Mac、または Linux オペレーティング システムのサービス パックと等しい (=) または等しくない (!=) のどちらかを条件とするかを操作フィールドで選択します。
 - ステップ 4 [OK] をクリックします。
-

DAP へのパーソナル ファイアウォール エンドポイント属性の追加

始める前に

HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『[AnyConnect HostScan 4.3.x to 4.6.x Migration Guide](#)』を参照してください。

手順

-
- ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。
 - ステップ 2 適切なボタン [Installed] または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子 ([Name]/[Operation]/[Valud] 列の下のフィールド) をインストールするか、またはインストールしないかを指定します。
 - ステップ 3 [Vendor] リスト ボックスで、テスト対象のパーソナル ファイアウォール ベンダーの名前をクリックします。
 - ステップ 4 [Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリスト ボックスから選択します。
 - ステップ 5 [Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい (=)、等しくない (!=)、より小さい (<)、より大きい (>)、以下 (<=)、または以上 (>=) に設定します。
 [Version] リスト ボックスで選択したバージョンに x が付いている場合 (たとえば 3.x) は、この x を具体的なリリース番号で置き換えます (たとえば 3.5)。
 - ステップ 6 [Last Update] チェックボックスをオンにします。最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く ([<]) 実行するか、遅く ([>]) 実行するかを指定できます。
 - ステップ 7 [OK] をクリックします。
-

DAP へのポリシー エンドポイント属性の追加

手順

-
- ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Policy] を選択します。
 - ステップ 2 [Location] チェックボックスをオンにしてから、Cisco Secure Desktop Microsoft Windows ロケーション プロファイルと等しい (=) または等しくない (!=) のどちらを条件とするかを操作 フィールドで選択します。Cisco Secure Desktop Microsoft Windows ロケーション プロファイル 文字列を [Location] テキスト ボックスに入力します。

ステップ3 [OK] をクリックします。

DAP へのプロセス エンドポイント属性の追加

始める前に

プロセス エンドポイント属性を設定する前に、どのプロセスをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] を選択します。詳細については、そのページの [Help] をクリックします。

手順

ステップ1 [Endpoint Attribute Type] リスト ボックスで [Process] を選択します。

ステップ2 [Exists] または [Does not exist] のボタンでは、選択したエンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものをクリックします。

ステップ3 [Endpoint ID] リスト ボックスで、スキャン対象のエンドポイント ID をドロップダウン リストから選択します。

エンドポイント ID プロセス情報がリスト ボックスの下に表示されます。

ステップ4 [OK] をクリックします。

DAP へのレジストリ エンドポイント属性の追加

レジストリ エンドポイント属性のスキャンは Windows オペレーティング システムにのみ適用されます。

始める前に

レジストリ エンドポイント属性を設定する前に、どのレジストリ キーをスキャンするかを Cisco Secure Desktop の [Host Scan] ウィンドウで定義します。ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] を選択します。詳細については、そのページの [Help] をクリックします。

手順

ステップ1 [Endpoint Attribute Type] リスト ボックスで [Registry] を選択します。

- ステップ 2** [Exists] または [Does not exist] のボタンでは、レジストリ エンドポイント属性とそれに付随する修飾子 ([Exists]/[Does not exist] ボタンの下にあるフィールド) が存在する必要があるかどうかに応じて、該当するものをクリックします。
- ステップ 3** [Endpoint ID] リスト ボックスで、スキャン対象のレジストリ エントリに等しいエンドポイント ID をドロップダウン リストから選択します。
- レジストリの情報が [Endpoint ID] リスト ボックスの下に表示されます。
- ステップ 4** [Value] チェックボックスをオンにしてから、操作フィールドで等しい (=) または等しくない (!=) を選択します。
- ステップ 5** 最初の [Value] リスト ボックスで、レジストリ キーが dword か文字列かを指定します。
- ステップ 6** 2 つ目の [Value] 操作リスト ボックスに、スキャン対象のレジストリ キーの値を入力します。
- ステップ 7** スキャン時にレジストリエントリの大文字と小文字の違いを無視するには、チェックボックスをオンにします。検索時に大文字と小文字を区別するには、チェックボックスをオフにしてください。
- ステップ 8** [OK] をクリックします。

DAP への複数証明書認証属性の追加

受信した証明書のいずれかを設定されたルールで参照できるように各証明書をインデックス化できます。これらの証明書フィールドに基づいて、接続試行を許可または拒否する DAP ルールを設定できます。

手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] > [Add Endpoint Attribute] の順に移動します。
- ステップ 2** [Endpoint Attribute Type] としてドロップダウンメニューの [Multiple Certificate Authentication] を選択します。
- ステップ 3** 必要に応じて次のいずれかまたはすべてを設定します。
- Subject Name
 - 発行元名
 - Subject Alternate Name
 - Serial Number
- ステップ 4** 証明書ストアをデフォルトの [None] のままにしていずれのストアからの証明書も許可するか、ユーザのみまたはマシンのみを許可するように選択します。[User] または [Machine] を選択する場合、証明書の元のストアを入力する必要があります。この情報は、プロトコルでクライアントによって送信されます。

DAP とマルウェア対策およびパーソナル ファイアウォール プログラム

セキュリティアプライアンスは、ユーザ属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。プリログイン評価モジュールおよび HostScan モジュールは、設定済みエンドポイント属性の情報をセキュリティアプライアンスに返し、DAP サブシステムでは、その情報に基づいてそれらの属性値に一致する DAP レコードを選択します。

マルウェア対策およびパーソナルファイアウォールプログラムのほとんど（すべてではなく）は、アクティブスキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。HostScan は、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブスキャンをサポートしない場合、HostScan はそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブスキャンをサポートしており、そのプログラムでアクティブスキャンがイネーブルになっている場合、HostScan はそのソフトウェアの存在をレポートします。この場合も、セキュリティアプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブスキャンをサポートしており、そのプログラムでアクティブスキャンがディセーブルになっている場合、HostScan はそのソフトウェアの存在を無視します。セキュリティアプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、プログラムがインストールされている場合でも、DAP に関する多数の情報が含まれる **debug trace** コマンドの出力にはプログラムの存在が示されません。



- (注) HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『[AnyConnect HostScan 4.3.x to 4.6.x Migration Guide](#)』を参照してください。

エンドポイント属性の定義

次に、DAP で使用できるエンドポイント選択属性を示します。[Attribute Name] フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Dynamic Access Policy Selection Criteria] ペインの [Advanced] 領域で使用します。label 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
マルウェア対策 (Cisco Secure Desktop が必要)	endpoint.am["label"].exists	ホスト スキャン	true	—	マルウェア対策プログラムが存在する
	endpoint.am["label"].version		string	32	Version
	endpoint.am["label"].description		string	128	マルウェア対策の説明
	endpoint.am["label"].lastupdate		整数	—	マルウェア対策定義を更新してからの経過時間 (秒)
Personal Firewall (Secure Desktop が必要)	endpoint.pfw["label"].exists	ホスト スキャン	true	—	パーソナルファイアウォールが存在する
	endpoint.pfw["label"].version		string	string	Version
	endpoint.pfw["label"].description		string	128	パーソナルファイアウォールの説明

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
AnyConnect (Cisco Secure Desktop やホストスキャンは必要ありません)	endpoint.anyconnect.clientversion	エンドポイント	version	—	AnyConnect クライアントのバージョン
	endpoint.anyconnect.platform		string	—	AnyConnect クライアントがインストールされているオペレーティングシステム
	endpoint.anyconnect.platformversion		version	64	AnyConnect クライアントがインストールされているオペレーティングシステムのバージョン
	endpoint.anyconnect.devicetype		string	64	AnyConnect クライアントがインストールされているモバイルデバイスのタイプ
	endpoint.anyconnect.deviceuniqueid			64	AnyConnect クライアントがインストールされているモバイルデバイスの一意的 ID
	endpoint.anyconnect.macaddress		string	—	AnyConnect クライアントがインストールされているデバイスの MAC アドレス。 フォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字です。
アプリケーション	endpoint.application.clienttype	アプリケーション	string	—	クライアントタイプ： CLIENTLESS ANYCONNECT IPSEC L2TP

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
デバイス	endpoint.device.hostname	エンドポイント	string	64	ホスト名のみ。FQDNではありません
	endpoint.device.MAC		string	—	ネットワークインターフェイスカードの MAC アドレス。1つのエントリにつき MAC アドレスは1つだけです フォーマットは xxxx.xxxx.xxxx である必要があります。x は 16 進数文字です。
	endpoint.device.id		string	64	BIOS シリアル番号。数値フォーマットは、製造業者固有です。フォーマット要件はありません
	endpoint.device.port		string	—	リスニング状態の TCP ポート 1 回線ごとに 1 つのポートを定義できます 1 ~ 65535 の範囲の整数
	endpoint.device.protection_version		string	64	実行されるホストスキャンイメージのバージョン
	endpoint.device.protection_extension		string	64	Endpoint Assessment (OPSWAT) のバージョン

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
ファイル	endpoint.file["label"].exists	Secure Desktop	true	—	ファイルが存在する
	endpoint.file["label"].endpointid				
	endpoint.file["label"].lastmodified		整数	—	ファイルが最後に変更されてからの経過時間 (秒)
	endpoint.file["label"].crc.32		整数	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	string	—	ユーザ定義ステータス ストリング
オペレーティングシステム	endpoint.os.version	Secure Desktop	string	32	オペレーティングシステム
	endpoint.os.servicepack		整数	—	Windows のサービスパック
ポリシー (Policy)	endpoint.policy.location	Secure Desktop	string	64	Cisco Secure Desktop からのロケーション値
プロセス	endpoint.process["label"].exists	Secure Desktop	true	—	プロセスが存在する
	endpoint.process["label"].path		string	255	プロセスのフルパス
Registry	endpoint.registry["label"].type	Secure Desktop	dword string	—	dword
	endpoint.registry["label"].value		string	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	string	—	VLAN タイプ : ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

LUA を使用した DAP における追加の DAP 選択基準の作成

このセクションでは、AAA またはエンドポイント属性の論理式の作成方法について説明します。これを行うには、LUA に関する高度な知識が必要です。LUA のプログラミングの詳細情報については、<http://www.lua.org/manual/5.1/manual.html> を参照してください。

[Advanced] フィールドに、AAA またはエンドポイント選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、テキストを DAP ポリシーファイルにコピーするだけです。処理は ASA によって行われ、解析不能な式は破棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された条件のいずれかを満たす、すべてを満たす、またはいずれも満たさない AAA 属性を使用するように ASA を設定できます。エンドポイント属性は累積され、そのすべてを満たす必要があります。セキュリティアライアンスが任意のエンドポイント属性を使用できるようにするには、LUA で適切な論理式を作成し、ここでその式を入力する必要があります。

次のセクションでは、LUA EVAL 式作成の詳細と例を示します。

- [LUA EVAL 式を作成する構文 \(228 ページ\)](#)
- [DAP EVAL 式の例 \(232 ページ\)](#)
- [追加の LUA 関数 \(230 ページ\)](#)

LUA EVAL 式を作成する構文



(注) [Advanced] モードを使用する必要がある場合は、プログラムを直接的に検証することが可能になり、明確になるため、できるだけ EVAL 式を使用することをお勧めします。

EVAL(<attribute>, <comparison>, {<value> | <attribute>}, [<type>])

<attribute>	AAA 属性または Cisco Secure Desktop から返された属性。属性の定義については、 エンドポイント属性の定義 (223 ページ) を参照してください。
-------------	---

<comparison>	次の文字列のいずれか (引用符が必要)	
	“EQ”	等しい
	“NE”	等しくない
	“LT”	より小さい
	“GT”	より大きい
	“LE”	以下
	“GE”	以上
<value>	引用符で囲まれ、属性と比較する値を含む文字列	
<type>	次の文字列のいずれか (引用符が必要)	
	“string”	大文字、小文字を区別する文字列の比較
	“”	大文字、小文字を区別しない文字列の比較
	“integer”	数値比較で、文字列値を数値に変換
	“hex”	16進数を用いた数値比較で、16進数の文字列を16進数に変換
	“version”	X.Y.Z. 形式 (X、Y、Zは数字) のバージョンを比較

HostScan 4.6 以降の LUA 手順

'ANY' のウイルス対策 (endpoint.am) 用 LUA スクリプト (最終更新済み)

次の LUA スクリプトを使用して、'ANY' のウイルス対策製品/ベンダー (endpoint.am) を確認します。異なる最終更新の間隔に対応するため、修正が適用される場合があります。次の例は、30日 (2592000秒と記載) 以内に実行されたものとする最終更新の方法を示しています。

```
assert(function()
    for k,v in pairs(endpoint.am) do
        if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
"integer"))
            then
```

```

        return true
    end
end
return false
end) ()

```

'ANY' のパーソナル ファイアウォール用 LUA スクリプト

次の LUA スクリプトを使用して、'ANY' のファイアウォール製品/ベンダー (endpoint.pfw) を確認します。

```

assert(function()
    for k,v in pairs(endpoint.pfw) do
        if (EVAL(v.enabled, "EQ", "ok", "string")) then
            return true
        end
    end
    return false
end) ()

```

追加の LUA 関数

ダイナミック アクセス ポリシーで作業している場合、一致基準に高度な柔軟性が必要とされることが考えられます。たとえば、以下に従い別の DAP を適用しなければならない場合があります。

- CheckAndMsg は、DAP がコールするように設定可能な LUA 関数です。条件に基づきユーザ メッセージを生成します。
- 組織ユニット (OU) またはユーザ オブジェクトの他の階層のレベル。
- 命名規則に従ったグループ名に多くの一致候補がある場合、ワイルドカードの使用が必要になることがあります。

ASDM の [DAP] ペイン内の [Advanced] セクションで LUA 論理式を作成し、この柔軟性を実現できます。

DAP CheckAndMsg 関数

ASA は、LUA CheckAndMsg 関数を含む DAP レコードが選択され、それによって接続が終了する結果になる場合にのみ、ユーザにメッセージを表示します。

CheckAndMsg 関数の構文は以下の通りです。

```

CheckAndMsg(value, "<message string if value is true>", "<message string if value if false>")

```

CheckAndMsg 関数の作成時には、以下の点に注意してください。

- CheckAndMsg は、最初の引数として渡された値を返します。
- 文字列比較を使用したくない場合、EVAL 関数を最初の引数として使用してください。次に例を示します。

```
(CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
```

CheckandMsg は EVAL 関数の結果を返し、セキュリティ アプライアンスはその結果を使用して、DAP レコードを選択すべきかどうかを判断します。レコードが選択された結果、ターミネーションとなった場合、セキュリティアプライアンスは適切なメッセージを表示します。

OU ベースの照合の例

DAP は、論理式で LDAP サーバから返される多数の属性を使用できます。DAP トレースの項で出力例を参照するか、debug dap トレースを実行してください。

LDAP サーバはユーザの認定者名 (DN) を返します。これは、ディレクトリ内のどの部分にユーザ オブジェクトがあるかを暗黙的に示します。たとえば、ユーザの DN が CN=Example User、OU=Admins、dc=cisco、dc=com である場合、このユーザは OU=Admins、dc=cisco、dc=com に存在します。すべての管理者がこの OU (または、このレベル以下のコンテナ) に存在する場合、以下のように、この基準に一致する論理式を使用できます。

```
assert(function()
    if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil)
    ) then
        return true
    end
    return false
end) ()
```

この例では、string.find 関数で正規表現を使用できます。この文字列を distinguishedName フィールドの最後にアンカーするには、文字列の最後に \$ を使用します。

グループ メンバーシップの例

AD グループ メンバーシップのパターン照合のために、基本論理式を作成できます。ユーザが複数のグループのメンバーであることが考えられるため、DAP は LDAP サーバからの応答を表内の別々のエントリへと解析します。以下を実行するには、高度な機能が必要です。

- memberOf フィールドを文字列として比較する (ユーザが 1 つのグループだけに所属している場合)。
- 返されたデータが「table」タイプである場合、返されたそれぞれの memberOf フィールドを繰り返し処理する。

そのために記述し、テストした関数を以下に示します。この例では、ユーザが「-stu」で終わるいずれかのグループのメンバーである場合、この DAP に一致します。

```
assert(function()
    local pattern = "-stu$"
    local attribute = aaa.ldap.memberOf
    if ((type(attribute) == "string") and
        (string.find(attribute, pattern) ~= nil)) then
```

```

return true
elseif (type(attribute) == "table") then
    local k, v
    for k, v in pairs(attribute) do
        if (string.find(v, pattern) ~= nil) then
            return true
        end
    end
end
return false
end()

```

アクセス拒否の例

マルウェア対策プログラムが存在しない場合のアクセスを拒否するために、次の関数を使用できます。ターミネーションを実行するためのアクションが設定されている DAP で使用します。

```

assert(
    function()
        for k,v in pairs(endpoint.am) do
            if (EVAL(v.exists, "EQ", "true", "string")) then
                return false
            end
        end
        return CheckAndMsg(true, "Please install antimalware software before connecting.",
            nil)
    end()
)

```

マルウェア対策プログラムがないユーザがログインしようとする、DAP は次のメッセージを表示します。

```
Please install antimalware software before connecting.
```

DAP EVAL 式の例

LUA で論理式を作成する場合は、次の例を参考にしてください。

説明	例
Windows 10 用エンドポイント LUA チェック	<code>(EVAL(endpoint.os.version, "EQ", "Windows 10", "string"))</code>
CLIENTLESS または CVC クライアントタイプに一致するかどうかのエンドポイント LUA チェック。	<code>(EVAL(endpoint.application.clienttype, "EQ", "CLIENTLESS") or EVAL(endpoint.application.clienttype, "EQ", "CVC"))</code>

説明	例
単一マルウェア対策プログラム Symantec Enterprise Protection がユーザの PC にインストールされているかどうかのエンドポイント LUA チェック。インストールされていない場合はメッセージを表示します。	<pre>(CheckAndMsg (EVAL (endpoint.am["538"].description, "NE", "Symantec Endpoint Protection", "string"), "Symantec Endpoint Protection was not found on your computer", nil))</pre>
McAfee Endpoint Protection バージョン 10 から 10.5.3 およびバージョン 10.6以降用のエンドポイント LUA チェック。	<pre>(EVAL (endpoint.am["1637"].version, "GE", "10", "version") and EVAL (endpoint.am["1637"].version, "LT", "10.5.4", "version") or EVAL (endpoint.am["1637"].version, "GE", "10.6", "version"))</pre>
McAfee マルウェア対策定義が過去 10 日 (864000 秒) 以内に更新されたかどうかのエンドポイント LUA チェック。更新が必要な場合はメッセージを表示します。	<pre>(CheckAndMsg (EVAL (endpoint.am["1637"].lastupdate, "GT", "864000", "integer"), "Update needed! Please wait for McAfee to load the latest dat file.", nil))</pre>
debug dap trace で endpoint.os.windows.hotfix["KB923414"] = "true"; が返された後に特定のホットフィックスがあるかどうかのチェック。	<pre>(CheckAndMsg (EVAL (endpoint.os.windows.hotfix["KB923414"], "NE", "true"), "The required hotfix is not installed on your PC.", nil))</pre>

マルウェア対策プログラムのチェックとメッセージの表示

マルウェア対策ソフトウェアにより、エンドユーザが問題に気づいて修正できるようにメッセージを設定できます。アクセスが許可された場合、ASA はポータルページの DAP 評価プロセスで生成されたすべてのメッセージを表示します。アクセスが拒否された場合、ASA は「ターミネーション」状態の原因となったすべてのメッセージを DAP から収集して、ブラウザのログインページに表示します。

次の例は、この機能を使用して Symantec Endpoint Protection のステータスをチェックする方法を示します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます (右端にある二重矢印をクリックして、フィールドを展開します)。

```
(CheckAndMsg (EVAL (endpoint.am["538"].description, "EQ", "Symantec Endpoint Protection", "string") and EVAL (endpoint.am["538"].activescan, "NE", "ok", "string") "Symantec Endpoint Protection is disabled. You must enable before being granted access", nil))
```

2. 同じ [Advanced] フィールドで、[OR] ボタンをクリックします。

3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec Endpoint Protection がインストールされているものの無効になっている PC から接続します。想定される結果は、接続は許可されず、ユーザに次のメッセージが表示されるというものです。「Symantec Endpoint Protection is disabled. You must enable before being granted access」。

マルウェア対策プログラムと 2 日以上経過した定義のチェック

この例では、Symantec または McAfee のマルウェア対策プログラムが存在するかどうか、また、ウイルス定義が 2 日 (172,800 秒) 以内のものであるかどうかを確認します。定義が 2 日以上経過している場合、ASA はセッションを終了し、メッセージと修正用リンクを表示します。このタスクを完了するには、次の手順を実行します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"), "Symantec Endpoint Protection Virus Definitions are Out of Date. You must run LiveUpdate before being granted access", nil)) or (CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"), "McAfee Endpoint Security Virus Definitions are Out of Date. You must update your McAfee Virus Definitions before being granted access", nil))
```

2. 同じ [Advanced] フィールドで、[AND] をクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec または McAfee のマルウェア対策プログラムがインストールされており、バージョンが 2 日以上前のものである PC から接続します。
結果として、接続は許可されず、ユーザに「virus definitions are out of date」というメッセージが表示されることが予測されます。

DAP アクセスと許可ポリシー属性の設定

各タブをクリックして、タブ内のフィールドを設定します。

手順

ステップ 1 特定の接続またはセッションに適用される特別な処理を指定するには、[Action] タブを選択します。

- [Continue] : (デフォルト) セッションにアクセス ポリシー属性を適用します。

- **[Quarantine]** : 検疫を使用すると、VPN 経由ですでにトンネルを確立している特定のクライアントを制限できます。ASA は、制限付き ACL をセッションに適用して制限付きグループを形成します。この基になるのは、選択された DAP レコードです。エンドポイントが管理面で定義されているポリシーに準拠していない場合でも、ユーザはサービスにアクセスして修復できますが、ユーザに制限がかけられます。修復後、ユーザは再接続できません。この再接続により、新しいポストチャセスマメントが起動されます。このアセスマメントに合格すると、接続されます。このパラメータを使用するには、AnyConnect セキュア モビリティ機能をサポートしている AnyConnect リリースが必要です。

- **[Terminate]** : セッションを終了します。

- **[User Message]** : この DAP レコードが選択されるたびに、ポータルページに表示するテキストメッセージを入力します。最大 490 文字を入力できます。ユーザメッセージは、黄色のオーブとして表示されます。ユーザがログインすると、メッセージは 3 回点滅してから静止します。数件の DAP レコードが選択され、それぞれにユーザメッセージがある場合は、ユーザメッセージがすべて表示されます。

URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。例：すべてのコントラクタは、ご使用のマルウェア対策ソフトウェアのアップグレード手順について、[href='http://wwwin.example.com/procedure.html'](http://wwwin.example.com/procedure.html)>Instructions を参照してください。

ステップ 2 [Network ACL Filters] タブを選択し、この DAP レコードに適用されるネットワーク ACL を設定します。

DAP の ACL には、許可ルールまたは拒否ルールを含めることができますが、両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれている場合、ASA はその ACL を拒否します。

- **[Network ACL]** ドロップダウンリスト：この DAP レコードに追加する、すでに設定済みのネットワーク ACL を選択します。ACL には、許可ルールと拒否ルールの任意の組み合わせを指定できます。このフィールドは、IPv4 および IPv6 ネットワーク トラフィックのアクセスルールを定義できる統合 ACL をサポートしています。
- **[Manage]** : ネットワーク ACL を追加、編集、および削除するときにクリックします。
- **[Network ACL]** リスト：この DAP レコードのネットワーク ACL が表示されます。
- **[Add]** : ドロップダウン リストで選択したネットワーク ACL が右側の [Network ACLs] リストに追加されます。
- **[Delete]** : クリックすると、強調表示されているネットワーク ACL が [Network ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

ステップ 3 [Web-Type ACL Filters (clientless)] タブを選択し、この DAP レコードに適用される Web タイプ ACL を設定します。DAP の ACL には、許可または拒否ルールだけを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれている場合、ASA はその ACL を拒否します。

- [Web-Type ACL] ドロップダウン リスト：この DAP レコードに追加する、設定済みの Web-type ACL を選択します。ACL には、許可ルールと拒否ルールの任意の組み合わせを指定できます。
- [Manage]：Web タイプ ACL を追加、編集、削除するときにクリックします。
- [Web-Type ACL] リスト：この DAP レコードの Web-type ACL が表示されます。
- [Add]：ドロップダウン リストで選択した Web タイプ ACL が右側の [Web-Type ACLs] リストに追加されます。
- [Delete]：クリックすると、Web-type ACL の 1 つが [Web-Type ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

ステップ 4 [Functions] タブを選択し、ファイルサーバエントリとブラウジング、HTTP プロキシ、および DAP レコードの URL エントリを設定します。

- [File Server Browsing]：ファイルサーバまたは共有機能の CIFS ブラウジングをイネーブまたはディセーブにします。

ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。CIFS ブラウズ機能では、国際化がサポートされていません。

- [File Server Entry]：ポータルページでユーザがファイルサーバのパスおよび名前を入力できるようにするかどうかを設定します。イネーブになっている場合、ポータルページにファイルサーバエントリのドロワが配置されます。ユーザは、Windows ファイルへのパス名を直接入力できます。ユーザは、ファイルをダウンロード、編集、削除、名前変更、および移動できます。また、ファイルおよびフォルダを追加することもできます。適用可能な Windows サーバでユーザアクセスに対して共有を設定する必要もあります。ネットワークの要件によっては、ユーザがファイルへのアクセス前に認証を受ける必要があることもあります。
- [HTTP Proxy]：クライアントへの HTTP アプレットプロキシの転送に関与します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有効です。このプロキシによって、セキュリティアプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシコンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシコンフィギュレーションにリダイレクトします。HTTP アプレットプロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
- [URL Entry]：ポータルページでユーザが HTTP/HTTPS URL を入力できるようにするかどうかを設定します。この機能がイネーブになっている場合、ユーザは URL エントリボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を使用して、これらの Web サイトにアクセスできます。

SSL VPN を使用しても、すべてのサイトとの通信が必ずしもセキュアになるとはかぎりません。SSL VPN は、企業ネットワーク上のリモート ユーザの PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるリソース）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信はセキュアではありません。

クライアントレス VPN 接続では、ASA はエンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。ユーザが SSL 対応 Web サーバに接続すると、ASA はセキュアな接続を確立し、サーバの SSL 証明書を検証します。エンド ユーザ ブラウザでは提示された証明書を受信しないため、証明書を調査して検証することはできません。SSL VPN の現在の実装では、期限切れになった証明書を提示するサイトとの通信は許可されません。また、ASA は信頼できる CA 証明書の検証も実行しません。このため、ユーザは、SSL 対応の Web サーバと通信する前に、そのサーバにより提示された証明書を分析することはできません。

ユーザのインターネット アクセスを制限するには、[Disable for the URL Entry] フィールドを選択します。これにより、SSL VPN ユーザがクライアントレス VPN 接続中に Web サーフィンできないようにします。

- [Unchanged] : (デフォルト) クリックすると、このセッションに適用されるグループポリシーからの値が使用されます。
- [Enable/Disable] : 機能をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start] : クリックすると HTTP プロキシがイネーブルになり、これらの機能に関連付けられたアプレットが DAP レコードによって自動的に起動するようになります。

ステップ 5 [Port Forwarding Lists] タブを選択し、ユーザセッションのポート転送リストを設定します。

ポート転送によりグループ内のリモート ユーザは、既知の固定 TCP/IP ポートで通信するクライアント/サーバアプリケーションにアクセスできます。リモート ユーザは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモートサーバに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP (FTP over SSH)、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

(注) ポート転送は、一部の SSL/TLS バージョンでは使用できません。

注意 ポート転送 (アプリケーションアクセス) およびデジタル証明書をサポートするために、リモートコンピュータに Sun Microsystems Java ランタイム環境 (JRE) がインストールされていることを確認します。

- [Port Forwarding] : この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged] : クリックすると、属性が実行コンフィギュレーションから削除されます。
- [Enable/Disable] : ポート転送をイネーブルにするかディセーブルにするかを指定します。

- **[Auto-start]** : クリックするとポート転送がイネーブルになり、DAP レコードのポート転送リストに関連付けられたポート転送アプレットが自動的に起動するようになります。
- **[Port Forwarding List]** ドロップダウン リスト : DAP レコードに追加する、設定済みのポート転送リストを選択します。
- **[New...]** : 新規のポート転送リストを設定するときにクリックします。
- **[Port Forwarding Lists]** (ラベルなし) : DAP レコードのポート転送リストが表示されます。
- **[Add]** : クリックすると、ドロップダウンリストで選択したポート転送リストが右側のポート転送リストに追加されます。
- **[Delete]** : クリックすると、選択されているポート転送リストがポート転送リストから削除されます。ASA からポート転送リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。

ステップ 6 **[Bookmarks]** タブを選択し、特定のユーザセッション URL のブックマークを設定します。

- **[Enable bookmarks]** : クリックするとイネーブルになります。このチェックボックスがオフのときは、接続のポータル ページにブックマークは表示されません。
- **[Bookmark]** ドロップダウン リスト : DAP レコードに追加する、設定済みのブックマークを選択します。
- **[Manage...]** : ブックマークを追加、インポート、エクスポート、削除するときにクリックします。
- **[Bookmarks]** (ラベルなし) : この DAP レコードの URL リストが表示されます。
- **[Add>>]** : クリックすると、ドロップダウンリストで選択したブックマークが右側の URL 領域に追加されます。
- **[Delete]** : クリックすると、選択されているブックマークが URL リスト領域から削除されます。ASA からブックマークを削除するには、まず DAP レコードからそのブックマークを削除する必要があります。

ステップ 7 **[Access Method]** タブを選択し、許可するリモート アクセスのタイプを設定します。

- **[Unchanged]** : 現在のリモート アクセス方式を引き続き使用します。
- **[AnyConnect Client]** : Cisco AnyConnect VPN クライアントを使用して接続します。
- **[Web-Portal]** : クライアントレス VPN で接続します。
- **[Both-default-Web-Portal]** : クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトはクライアントレスです。
- **[Both default AnyConnect Client]** : クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトは AnyConnect です。

ステップ 8 **[AnyConnect]** タブを選択し、Always-on VPN フラグのステータスを選択します。

- [Always-On VPN for AnyConnect client] : AnyConnect サービス プロファイル内の Always-on VPN フラグ設定を未変更にするか、ディセーブルにするか、AnyConnect プロファイル設定を使用するかを指定します。

このパラメータを使用するには、Cisco Web セキュリティ アプライアンスのリリースが、Cisco AnyConnect VPN クライアントに対してセキュア モビリティ ソリューション ライセンシングをサポートしている必要があります。また、AnyConnect のリリースが、「セキュア モビリティ ソリューション」の機能をサポートしている必要もあります。詳細については、『Cisco AnyConnect VPN Client Administrator Guide』を参照してください。

ステップ 9 [AnyConnect Custom Attributes] タブを選択し、定義済みのカスタム属性を表示して、このポリシーに関連付けます。また、カスタム属性を定義してから、それらをこのポリシーに関連付けることもできます。

カスタム属性は AnyConnect クライアントに送信され、アップグレードの延期などの機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を1つ以上定義できます。機能に対して設定する固有のカスタム属性の詳細については、使用している AnyConnect リリースの『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

カスタム属性は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] および [AnyConnect Custom Attribute Names] で事前に定義できます。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。

DAP トレースの実行

DAP トレースを実行すると、すべての接続済みデバイスの DAP エンドポイント属性が表示されます。

手順

ステップ 1 SSH ターミナルから ASA にログオンして特権 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。

ステップ 2 DAP デバッグをイネーブルにします。セッションのすべての DAP 属性がターミナルウィンドウに表示されます。

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

ステップ 3 (任意) DAP トレースの出力を検索するには、コマンドの出力をシステム ログに送ります。ASA でのロギングの詳細については、『Cisco ASA Series General Operations ASDM Configuration Guide』の「Configure Logging」を参照してください。

DAP の例

- [DAP を使用したネットワーク リソースの定義 \(240 ページ\)](#)
- [DAP を使用した WebVPN ACL の適用 \(241 ページ\)](#)
- [DAP による CSD チェックの強制とポリシーの適用 \(241 ページ\)](#)

DAP を使用したネットワーク リソースの定義

この例は、ユーザまたはグループのネットワーク リソースを定義する方法として、ダイナミック アクセス ポリシーを設定する方法を示しています。Trusted_VPN_Access という名前の DAP ポリシーは、クライアントレス VPN アクセスと AnyConnect VPN アクセスを許可します。Untrusted_VPN_Access という名前のポリシーは、クライアントレス VPN アクセスだけを許可します。

手順

ステップ 1 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [Endpoint] に移動します。

ステップ 2 各ポリシーの次の属性を設定します。

属性	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	信頼できる	信頼できない
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	信頼できる	信頼できない
LDAP memberOf	Engineering、Managers	ベンダー
ACL		Web-Type ACL
アクセス	AnyConnect および Web Portal	Web Portal

DAP を使用した WebVPN ACL の適用

DAP では、Network ACLs (IPsec および AnyConnect の場合)、Clientless SSL VPN Web-Type ACLs、URL リスト、および Functions を含め、アクセス ポリシー属性のサブセットを直接適用できます。グループ ポリシーが適用されるバナーまたはスプリット トンネル リストなどには、直接適用できません。[Add/Edit Dynamic Access Policy] ペインの [Access Policy Attributes] タブには、DAP が直接適用される属性の完全なメニューが表示されます。

Active Directory/LDAP は、ユーザ グループ ポリシー メンバーシップをユーザ エントリの「memberOf」属性として保存します。AD グループ内のユーザ (memberOf) = ASA が設定済み Web タイプ ACL を適用する Engineering となるように、DAP を定義します。

手順

- ステップ 1 ASDM で、[Add AAA Attributes] ペインに移動します ([Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes section] > [Add AAA Attribute])。
- ステップ 2 AAA 属性タイプとしては、ドロップダウン リストを使用して [LDAP] を選択します。
- ステップ 3 [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。
- ステップ 4 [Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。
- ステップ 5 ペインの [Access Policy Attributes] 領域で、[Web-Type ACL Filters] タブをクリックします。
- ステップ 6 [Web-Type ACL] ドロップダウン リストを使用して、AD グループ (memberOf) = Engineering のユーザに適用する ACL を選択します。

DAP による CSD チェックの強制とポリシーの適用

この例では、ユーザが2つの特定 AD/LDAP グループ (Engineering および Employees) と1つの特定 ASA トンネルグループに属することをチェックする DAP を作成します。その後、ACL をユーザに適用します。

DAP が適用される ACL により、リソースへのアクセスを制御します。それらの ACL は、ASA のグループ ポリシーで定義されるどの ACL よりも優先されます。また ASA は、スプリット トンネリングリスト、バナー、DNS など、DAP で定義または制御されない要素に通常の AAA グループ ポリシー継承ルールと属性を適用します。

手順

- ステップ 1 ASDM で、[Add AAA Attributes] ペインに移動します ([Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes section] > [Add AAA Attribute])。

- ステップ 2** AAA 属性タイプとしては、ドロップダウンリストを使用して [LDAP] を選択します。
- ステップ 3** [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。
- ステップ 4** [Value] フィールドで、ドロップダウンリストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。
- ステップ 5** [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。
- ステップ 6** [Value] フィールドで、ドロップダウンリストを使用して [=] を選択し、隣のフィールドに「Employees」と入力します。
- ステップ 7** AAA 属性タイプとしては、ドロップダウンリストを使用して [Cisco] を選択します。
- ステップ 8** [Tunnel] グループボックスをオンにし、ドロップダウンリストを使用して [=] を選択し、隣のドロップダウンリストで適切なトンネルグループ（接続ポリシー）を選択します。
- ステップ 9** [Access Policy Attributes] 領域の [Network ACL Filters] タブで、前のステップで定義した DAP 基準を満たすユーザーに適用する ACL を選択します。
-



第 7 章

電子メール プロキシ

電子メール プロキシを設定すると、リモート電子メール機能をクライアントレス SSL VPN のユーザに拡張できます。ユーザが電子メール プロキシ経由で電子メール セッションを試行すると、電子メール クライアントが SSL プロトコルを使用してトンネルを確立します。

電子メール プロキシ プロトコルは次のとおりです。

POP3S

POP3S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 995 をリッスンし、ポート 995 または設定されたポートとの接続が自動的に許可されます。POP3 プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に POP3 プロトコルが開始され、認証が行われます。POP3S は、電子メール 受信用のプロトコルです。

IMAP4S

IMAP4S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 993 をリッスンし、ポート 993 または設定されたポートとの接続が自動的に許可されます。IMAP4S プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に IMAP4S プロトコルが開始され、認証が行われます。IMAP4S は、電子メール 受信用のプロトコルです。

SMTPTS

SMTPTS は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 988 をリッスンし、ポート 988 または設定されたポートとの接続が自動的に許可されます。SMTPTS プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に SMTPTS プロトコルが開始され、認証が行われます。SMTPTS は、電子メール 送信用のプロトコルです。

- [電子メール プロキシの設定 \(244 ページ\)](#)
- [AAA サーバ グループの設定 \(244 ページ\)](#)
- [電子メール プロキシを使用するインターフェイスの識別 \(246 ページ\)](#)
- [電子メール プロキシの認証の設定 \(247 ページ\)](#)
- [プロキシ サーバの識別 \(248 ページ\)](#)

- [デリミタの設定 \(249 ページ\)](#)

電子メール プロキシの設定

電子メール プロキシの要件

- 電子メールプロキシを経由してローカルとリモートの両方から電子メールにアクセスするユーザは、電子メールプログラムで、ローカルアクセス用とリモートアクセス用に別々の電子メールアカウントが必要です。
- 電子メールプロキシセッションでユーザが認証される必要があります。

AAA サーバグループの設定

手順

ステップ 1 **[Configuration] > [Features] > [VPN] > [E-mail Proxy] > [AAA]** を参照します。

ステップ 2 適切なタブ ([POP3S]、[IMAP4S]、または [SMTPS]) を選択して AAA サーバグループを関連付け、これらのセッションに適用するデフォルトのグループポリシーを設定します。

- **[AAA server groups]** : **[AAA Server Groups]** パネル ([Configuration] > [Features] > [Properties] > [AAA Setup] > [AAA Server Groups]) に移動する場合にクリックします。ここでは、AAA サーバグループを追加または編集できます。
- **[group policies]** : **[Group Policy]** パネル ([Configuration] > [Features] > [VPN] > [General] > [Group Policy]) に移動する場合にクリックします。ここでは、グループポリシーを追加または編集できます。
- **[Authentication Server Group]** : ユーザ認証用の認証サーバグループを選択します。デフォルトでは、認証サーバが設定されていません。AAA を認証方式として設定した場合には ([Configuration] > [Features AAA] > [VPN] > [E-Mail Proxy] > [Authentication] パネル)、AAA サーバを設定してここで選択しないと、常に認証に失敗します。
- **[Authorization Server Group]** : ユーザ認可用の認可サーバグループを選択します。デフォルトでは、認可サーバが設定されていません。
- **[Accounting Server Group]** : ユーザアカウント用アカウントングサーバグループを選択します。デフォルトでは、アカウントングサーバが設定されていません。
- **[Default Group Policy]** : AAA が CLASSID 属性を返さない場合にユーザに適用するグループポリシーを選択します。長さは、4 ~ 15 文字の英数字です。デフォルトのグループポリシーが指定されていない場合や、CLASSID が存在しない場合、ASA はセッションを確立できません。

- [Authorization Settings] : ASA が認可のために識別するユーザ名の値を設定します。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 認可を必要とするユーザに適用されます。

- [Use the entire DN as the username] : 認可用の認定者名を使用する場合に選択します。
- [Specify individual DN fields as the username] : ユーザ認可用に特定の DN フィールドを指定する場合に選択します。

[DN] フィールドは、プライマリとセカンダリの 2 つを選択できます。たとえば、EA を選択した場合には、ユーザは電子メールアドレスによって認証されます。JohnDoe という一般名 (CN) と johndoe@cisco.com という電子メールアドレスを持つユーザは、John Doe または johndoe として認証されません。彼は johndoe@cisco.com として認証される必要があります。EA および O を選択した場合、John Doe は johndoe@cisco.com および Cisco Systems, Inc. として認証される必要があります。

- [Primary DN Field] : 認可用に設定するプライマリ DN フィールドを選択します。デフォルトは [CN] です。オプションには、次のものが含まれます。

DN フィールド	定義
Country (C)	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name (CN)	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位 (最も固有性の高い) レベルです。
DN Qualifier (DNQ)	特定の DN 属性。
E-mail Address (EA)	証明書を所有するユーザ、システム、またはエンティティの電子メールアドレス。
Generational Qualifier (GENQ)	Jr.、Sr.、または III などの世代修飾子。
Given Name (GN)	証明書所有者の名前 (名)。
Initials (I)	証明書所有者の姓と名の最初の文字。
Locality (L)	組織が存在する市町村。
Name (N)	証明書所有者の名前。
Organization (O)	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit (OU)	組織内のサブグループ。
Serial Number (SER)	証明書のシリアル番号。

DN フィールド	定義
Surname (SN)	証明書所有者の姓。
State/Province (S/P)	組織が所在する州や県。
Title (T)	証明書所有者の役職 (Dr. など)。
User ID (UID)	証明書所有者の ID 番号。

- [Secondary DN Field] : (オプション) 認可能に設定するセカンダリ DN フィールドを選択します。デフォルトは [OU] です。オプションには、上記の表に記載されているものすべてに加えて、[None] があります。これは、セカンダリ フィールドを指定しない場合に選択します。

電子メールプロキシを使用するインターフェイスの識別

[Email Proxy Access] 画面では、電子メールプロキシを設定するインターフェイスを識別できます。電子メールプロキシは、個々のインターフェイスで設定および編集できます。また、1つのインターフェイスで電子メールプロキシを設定および編集すれば、その設定をすべてのインターフェイスに適用できます。管理専用のインターフェイスやサブインターフェイスに対して電子メールプロキシは設定できません。

手順

ステップ 1 [Configuration] > [VPN] > [E-Mail Proxy] > [Access] を参照して、インターフェイスでイネーブルになっている電子メールプロキシを表示します。

- [Interface] : 設定されているすべてのインターフェイスの名前を表示します。
- [POP3S Enabled] : そのインターフェイスで POP3S がイネーブルかどうかを示します。
- [IMAP4s Enabled] : そのインターフェイスで IMAP4S がイネーブルかどうかを示します。
- [SMTPS Enabled] : そのインターフェイスで SMTPS がイネーブルかどうかを示します。

ステップ 2 [Edit] をクリックし、強調表示されているインターフェイスの電子メールプロキシ設定を変更します。

電子メール プロキシの認証の設定

電子メール プロキシのタイプごとに認証方式を設定します。

手順

ステップ 1 [Configuration] > [Features] > [VPN] > [E-mail Proxy] > [Authentication] を参照します。

ステップ 2 複数の認証方式から選択できます。

- [AAA] : AAA 認証を必須にする場合に選択します。このオプションを使用するには、AAA サーバを設定する必要があります。ユーザは、ユーザ名、サーバ、およびパスワードを入力します。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN 名デリミタによって区切りません。
- [Certificate] : 証明書認証を必須にする場合に選択します。

(注) 現在の ASA ソフトウェア リリースでは、証明書認証は電子メール プロキシに対して機能しません。

証明書認証を使用する場合、ユーザは、ASA が SSL ネゴシエーション時に検証できる証明書を持っている必要があります。SMTPS プロキシでは、証明書認証を唯一の認証方式として使用できます。その他の電子メール プロキシでは 2 種類の認証方式が必要です。

証明書認証には、すべて同じ CA から発行された 3 種類の証明書が必要です。

- ASA の CA 証明書。

- クライアント PC の CA 証明書。

- クライアント PC の Web ブラウザ証明書。個人証明書または Web ブラウザ証明書とも呼ばれます。

- [Piggyback HTTPS] : ピギーバック認証を必須にする場合に選択します。

この認証スキームは、ユーザがすでにクライアントレス SSL VPN セッションを確立していることを必須とします。ユーザは電子メールユーザ名だけを入力します。パスワードは不要です。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN 名デリミタによって区切りません。

IMAP は、同時ユーザ数によって制限されない多数のセッションを生成しますが、ユーザ名に対して許可されている同時ログインの数を数えません。IMAP セッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザが新しい接続を確立できません。以下の解決策があります。

SMTPS 電子メールは、最も頻繁にピギーバックを使用します。ほとんどの SMTP サーバが、ユーザがログインすることを許可していないためです。

(注) IMAPは、同時ユーザ数によって制限されない多数のセッションを生成しますが、ユーザ名に対して許可されている同時ログインの数を数えません。IMAPセッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザが新しい接続を確立できません。以下の解決策があります。

- ユーザは IMAP アプリケーションを終了して ASA とのセッションをクリアしてから、新しいクライアントレス SSL VPN 接続を確立できる。

- 管理者が IMAP ユーザの同時ログイン数を増やす ([Configuration] > [Features] > [VPN] > [General] > [Group Policy] > [Edit Group Policy] > [General])。

- 電子メール プロキシの HTTPS/ピギーバック認証をディセーブルにする。

- [Mailhost] : (SMTPS のみ) メールホスト認証を必須にする場合に選択します。POP3S と IMAP4S は必ずメールホスト認証を実行するため、このオプションは、SMTPS の場合に表示されます。この認証方式では、ユーザの電子メールユーザ名、サーバ、およびパスワードが必要です。

プロキシサーバの識別

この [Default Server] パネルでは、ASA のプロキシサーバを識別し、電子メール プロキシに対してデフォルトサーバ、ポート、および非認証セッション制限を設定することができます。

手順

ステップ 1 [Configuration] > [Features] > [VPN] > [E-mail Proxy] > [Default Servers] を参照します。

ステップ 2 次のフィールドを設定します。

- [Name or IP Address] : デフォルトの電子メールプロキシサーバの DNS 名または IP アドレスを入力します。
- [Port] : ASA が電子メールプロキシトラフィックをリッスンするポート番号を入力します。設定されたポートに対する接続が自動的に許可されます。電子メールプロキシは、SSL 接続だけをこのポートで許可します。SSL トンネルが確立された後に電子メールプロキシが開始され、認証が行われます。

デフォルトの設定は次のとおりです。

- 995 (POP3S の場合)
- 993 (IMAP4S の場合)
- 988 (SMTPS の場合)

- [Enable non-authenticated session limit] : 非認証電子メールプロキシセッションの数を制限する場合に選択します。認証プロセスでのセッションの制限を設定でき、それによって DOS 攻撃を防ぎます。新しいセッションが、設定された制限を超えると、ASA が最も古い非認証接続を終了します。非認証接続が存在しない場合には、最も古い認証接続が終了します。それによって認証済みのセッションが終了することはありません。

電子メールプロキシ接続には、3つの状態があります。

- 新規に電子メール接続が確立されると、「認証されていない」状態になります。
- この接続でユーザ名が提示されると、「認証中」状態になります。
- ASA が接続を認証すると、「認証済み」状態になります。

デリミタの設定

このパネルでは、電子メールプロキシ認証で使用するユーザ名/パスワードデリミタとサーバデリミタを設定します。

手順

ステップ 1 [Configuration] > [Features] > [VPN] > [E-mail Proxy] > [Delimiters] を参照します。

ステップ 2 次のフィールドを設定します。

- [Username/Password Delimiter] : VPN ユーザ名と電子メールユーザ名を区切るためのデリミタを選択します。電子メールプロキシで AAA 認証を使用する場合、および VPN ユーザ名と電子メールユーザ名が異なる場合に両方のユーザ名を使用します。電子メールプロキシセッションにログインするときに、ユーザは両方のユーザ名を入力し、ここで設定したデリミタで区切ります。また、電子メールサーバ名も入力します。

(注) クライアントレス SSL VPN 電子メールプロキシユーザのパスワードに、デリミタとして使用されている文字を含めることはできません。

- [Server Delimiter] : ユーザ名と電子メールサーバ名を区切るためのデリミタを選択します。このデリミタは、VPN 名デリミタとは別にする必要があります。電子メールプロキシセッションにログインする場合には、ユーザ名フィールドにユーザ名とサーバの両方を入力します。

たとえば、VPN 名デリミタとして : を使用し、サーバデリミタとして @ を使用する場合には、電子メールプロキシ経由で電子メールプログラムにログインするときに、`vpn_username:e-mail_username@server` という形式でユーザ名を入力します。



第 8 章

VPN の監視

- [VPN 接続グラフの監視 \(251 ページ\)](#)
- [VPN 統計の監視 \(251 ページ\)](#)

VPN 接続グラフの監視

ASA の VPN 接続データをグラフ形式または表形式で表示するには、次の画面を参照してください。

[Monitor IPsec Tunnels]

[Monitoring] > [VPN] > [VPN Connection Graphs] > [IPSec Tunnels]

表示や、エクスポートまたは印刷の準備を行う IPsec トンネル タイプのグラフとテーブルを指定します。

[Monitor Sessions]

[Monitoring] > [VPN] > [VPN Connection Graphs] > [Sessions]

表示や、エクスポートまたは印刷の準備を行う VPN セッション タイプのグラフとテーブルを指定します。

VPN 統計の監視

特定のリモートアクセス、LAN 間、クライアントレス SSL VPN、または電子メールプロキシセッションの詳細なパラメータおよび統計情報を表示するには、次の画面を参照してください。パラメータと統計情報は、セッションプロトコルによって異なります。また、統計情報テーブルの内容は、選択した接続のタイプによって異なります。各詳細テーブルには、それぞれのセッションの関連パラメータがすべて表示されます。

[Monitor Session] ウィンドウ

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ASA の VPN セッション統計情報を表示します。このペインの 2 番目のテーブルの内容は、[Filter By] リストの選択によって異なります。



- (注) 管理者は、非アクティブ状態のユーザ数をトレースし、統計情報を確認できるようになりました。ライセンス数の上限に達することなく、新規ユーザがログインできるように、最も長時間非アクティブなセッションはアイドル状態であると見なされます（自動的にログオフされます）。これらの統計情報には、**show vpn-sessiondb** CLI コマンドを使用してアクセスすることもできます（『[Cisco ASA Command Reference Guide](#)』の適切なリリースを参照してください）。

- [All Remote Access]

このテーブルの値がリモートアクセス（IPsec ソフトウェアおよびハードウェア クライアント）トラフィックに関連することを示します。

- [Username/Connection Profile] : セッションのユーザ名またはログイン名、および接続プロファイル（トンネルグループ）を示します。クライアントが認証にデジタル証明書を使用している場合、フィールドに証明書の Subject CN または Subject OU が表示されます。
- [Group Policy Connection Profile] : セッションのトンネルグループ ポリシー接続プロファイルが表示されます。
- [Assigned IP Address/Public IP Address] : このセッションのリモート クライアントに割り当てられているプライベート（「割り当てられた」）IP アドレスを示します。これは「内部」または「仮想」IP アドレスとも呼ばれ、クライアントはプライベート ネットワーク上のホストとして表示されます。また、このリモートアクセスセッションのクライアントのパブリック IP アドレスも表示します。パブリック IP アドレスは、「外部」IP アドレスとも呼ばれます。通常、これは ISP によってクライアントに割り当てられます。このアドレスにより、クライアントは、パブリック ネットワーク上のホストとして機能することが可能となります。



- (注) [Assigned IP Address] フィールドは、クライアントレス SSL VPN セッションには適用されません。ASA（プロキシ）がすべてのトラフィックの送信元になります。ネットワーク拡張モードにおけるハードウェア クライアントセッションの場合、割り当てられた IP アドレスは、ハードウェア クライアントのプライベート/内部ネットワーク インターフェイスのサブネットです。

- [Ping] : ICMP ping（Packet Internet Groper）パケットを送信して、ネットワークの接続をテストします。具体的には、ASA は選択されたホストに ICMP Echo Request メッセージを送信します。ホストが到達可能な場合は、Echo Reply メッセージが返され、ASA はテストしたホストの名前と共に Success メッセージを表示し、さらに要求を送信してから応答を受信するまでの経過時間も表示します。何らかの理由でシステムに到達できない場合（ホストがダウンしている、ホストで ICMP が実行されていない、ルートが設定されていない、

中間ルータがダウンしている、ネットワークがダウンまたは輻輳しているなど)、ASA では、テストしたホストの名前が記された [Error] 画面が表示されます。

- [LogoutBy] : ログアウトするセッションのフィルタリングに使う基準を選択します。--All Sessions-- 以外を選択した場合、[Logout By] リストの右側のボックスがアクティブになります。値に Protocol for Logout By を選択した場合、ボックスがリストに変わり、ログアウトフィルタとして使用するプロトコルタイプを選択できます。このリストのデフォルト値は IPsec です。Protocol 以外の値を選択した場合は、このボックスに適切な値を入力する必要があります。

[Monitor Active AnyConnect Sessions]

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ユーザ名、IP アドレス、アドレスタイプ、またはパブリックアドレスでソートされた AnyConnect クライアントセッションを表示します。

[Monitor VPN Session Details]

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] > [Details]

選択したセッションのコンフィギュレーション設定、統計情報、およびステータス情報を表示します。

- [NAC Result and Posture Token]

ASDM では、ASA にネットワーク アドミッション コントロールが設定されている場合にのみ、このカラムに値が表示されます。

- [Accepted] : ACS は正常にリモートホストのポスチャを検証しました。
- [Rejected] : ACS はリモートホストのポスチャの検証に失敗しました。
- [Exempted] : ASA に設定されたポスチャ検証免除リストに従って、リモートホストはポスチャ検証を免除されています。
- [Non-Responsive] : リモートホストは EAPoUDP Hello メッセージに応答しませんでした。
- [Hold-off] : ポスチャ検証に成功した後、ASA とリモートホストの EAPoUDP 通信が途絶えました。
- [N/A] : VPN NAC グループポリシーに従い、リモートホストの NAC はディセーブルにされています。
- [Unknown] : ポスチャ検証が進行中です。

ポスチャトークンは、Access Control Server で設定可能な情報文字列です。ACS は情報提供のために ASA にポスチャトークンをダウンロードし、システムモニタリング、レポート、デバッグ、およびロギングを支援します。NAC Result に続く一般的なポスチャトークンは、Healthy、Checkup、Quarantine、Infected または Unknown です。

[Session Details] ペインの [Details] タブには、次のカラムが表示されます。

- **[ID]** : セッションに動的に割り当てられた一意の ID。ID は、セッションへの ASA のインデックスとして機能します。このインデックスを使用して、セッションに関する情報を維持および表示します。
- **[Type]** : セッションのタイプ。IKE、IPsec または NAC。
- **[Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port]** : 実際の (ローカル) ピアの両方に割り当てられているアドレスとポートと外部ルーティングのためにそのピアに割り当てられているアドレスとポート。
- **[Encryption]** : このセッションで使用しているデータ暗号化アルゴリズム (使用している場合)。
- **[Assigned IP Address and Public IP Address]** : このセッションのリモートピアに割り当てられているプライベート IP アドレスを示します。内部または仮想 IP アドレスとも呼ばれ、割り当てられている IP アドレスによって、リモートピアはプライベートネットワーク上にあるように見えます。2 番目のフィールドには、このセッションのリモートコンピュータのパブリック IP アドレスが表示されます。外部 IP アドレスとも呼ばれ、通常、パブリック IP アドレスは ISP によってリモートコンピュータに割り当てられます。これによって、リモートコンピュータはパブリックネットワークのホストとして機能できます。
- **[Other]** : セッションに関連付けられているその他の属性。

次の属性は、IKE セッション、IPsec セッション、および NAC セッションに適用されます。

- **[Revalidation Time Interval]** : 成功した各ポスチャ検証間に必要とされる間隔 (秒数)。
- **[Time Until Next Revalidation]** : 最後のポスチャ検証試行が成功しなかった場合は 0 です。それ以外の場合は、**Revalidation Time Interval** と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
- **[Status Query Time Interval]** : 成功したポスチャ検証またはステータスクエリーの応答と次のステータスクエリーの応答との間に許容される時間 (秒数)。ステータスクエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、ASA がリモートホストに発行する要求です。
- **[EAPoUDP Session Age]** : 最後に成功したポスチャ検証から経過した秒数。
- **[Hold-Off Time Remaining]** : 最後のポスチャ検証が成功した場合は 0 秒です。それ以外の場合は、次のポスチャ確認試行までの秒数です。
- **[Posture Token]** : Access Control Server で設定可能な情報文字列。ACS は情報提供のために ASA にポスチャトークンをダウンロードし、システムモニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャトークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
- **[Redirect URL]** : ポスチャ検証またはクライアントレス認証が終わると、ACS はセッション用のアクセスポリシーを ASA にダウンロードします。Redirect URL は、アクセスポリシーペイロードのオプションの一部です。ASA は、リモートホストのすべての HTTP (ポート 80) 要求と HTTPS (ポート 443) 要求を Redirect URL (存在する場合) にリダイ

レクトします。アクセス ポリシーに Redirect URL が含まれていない場合、ASA はリモート ホストからの HTTP 要求や HTTPS 要求をリダイレクトしません。

Redirect URL は、IPsec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。

[More] : このボタンを押して、セッションやトンネルグループを再検証または初期化します。

ACL タブには、セッションに一致した ACE が含まれる ACL が表示されます。

[Monitor Cluster Loads]

[Monitoring] > [VPN] > [VPN Statistics] > [Cluster Loads]

VPN ロードバランシング クラスタ内のサーバ間における現在のトラフィックの負荷分散を表示します。サーバがクラスタの一部でない場合、このサーバが VPN ロードバランシング クラスタに参加していない旨を伝える情報メッセージが表示されます。

[Monitor Crypto Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Crypto Statistics]

ASA で現在アクティブなユーザと管理者セッションの暗号統計情報を表示します。テーブルの各行は、1 つの暗号統計情報を表示します。

[Monitor Compression Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Compression Statistics]

ASA で現在アクティブなユーザと管理者セッションの圧縮統計情報を表示します。テーブルの各行は、1 つの圧縮統計情報を表示します。

[Monitor Encryption Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Encryption Statistics]

ASA で現在アクティブなユーザと管理者セッションが使用しているデータ暗号化アルゴリズムを表示します。テーブルの各行は、1 つの暗号化アルゴリズム タイプを表示します。

[Monitor Global IKE/IPsec Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Global IKE/IPSec Statistics]

ASA で現在アクティブなユーザと管理者セッションのグローバル IKE/IPsec 統計情報を表示します。テーブルの各行は、1 つのグローバル統計情報を表示します。

[Monitor NAC Session Summary]

アクティブな累積ネットワーク アドミッション コントロール セッションを表示します。

- [Active NAC Sessions] : ポスチャ検証の対象のリモート ピアに関する一般的な統計情報。

- **[Cumulative NAC Sessions]** : 現在ポスチャ検証の対象か、または以前から対象だったリモートピアに関する一般的な統計情報。
- **[Accepted]** : ポスチャ検証に成功し、Access Control Server によってアクセスポリシーが与えられたピアの数。
- **[Rejected]** : ポスチャ検証に失敗し、Access Control Server によってアクセスポリシーが与えられなかったピアの数。
- **[Exempted]** : ASA で設定された **[Posture Validation Exception]** リストのエントリと一致しているため、ポスチャ検証の対象になっていないピアの数。
- **[Non-responsive]** : Extensible Authentication Protocol (EAP) over UDP のポスチャ検証要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。ASA のコンフィギュレーションがクライアントレスホストをサポートしている場合、Access Control Server は、クライアントレスホストに関連付けられているアクセスポリシーをこれらのピアの ASA にダウンロードします。クライアントレスホストをサポートしていない場合、ASA は NAC デフォルトポリシーを割り当てます。
- **[Hold-off]** : ポスチャ検証が成功した後、ASA が EAPoUDP 通信を失ったピアの数。NAC Hold Timer 属性 (**[Configuration]** > **[VPN]** > **[NAC]**) は、このタイプのイベントと次のポスチャ検証試行との間の遅延時間を判定します。
- **[N/A]** : VPN NAC グループポリシーに従って NAC が無効になっているピアの数。
- **[Revalidate All]** : ピアのポスチャまたは割り当てられているアクセスポリシー (ダウンロードされた ACL) が変更された場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションの新しい無条件ポスチャ検証が開始されます。このボタンをクリックするまで各セッションに対して有効だったポスチャ検証と割り当てられているアクセスポリシーは、新しいポスチャ検証が成功または失敗するまで有効のままとなります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。
- **[Initialize All]** : ピアのポスチャまたは割り当てられているアクセスポリシー (ダウンロードされた ACL) が変更され、セッションに割り当てられているリソースをクリアする場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションのポスチャ検証で使用される、EAPoUDP アソシエーションと割り当てられたアクセスポリシーがパージされ、新しい無条件のポスチャ検証が開始されます。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザトラフィックに影響する場合があります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。

[Monitor Protocol Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Protocol Statistics]

ASA で現在アクティブなユーザと管理者セッションが使用しているプロトコルを表示します。テーブルの各行は、1つのプロトコルタイプを表します。

[Monitor VLAN Mapping Sessions]

使用中の各グループ ポリシーの Restrict Access to VLAN パラメータの値で判別された、出力 VLAN に割り当てられているセッション数を表示します。ASA はすべてのトラフィックを指定された VLAN に転送します。

[Monitor SSO Statistics for Clientless SSL VPN Session]

[Monitoring] > [VPN] > [WebVPN] > [SSO Statistics]

ASA に設定されている現在アクティブなシングル サインオン (SSO) サーバの SSO 統計情報を表示します。



第 9 章

SSL 設定

- [SSL 設定 \(259 ページ\)](#)

SSL 設定

次の場所のいずれかで SSL 設定を構成します。

- **[Configuration] > [Device Management] > [Advanced] > [SSL Settings]**
- **[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]**

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。また、DTLS は AnyConnect VPN クライアントの接続に使用されます。[SSL Settings] ペインでは、クライアントとサーバの SSL バージョンおよび暗号化アルゴリズムを設定できます。また、以前に設定したトラストポイントを特定のインターフェイスに適用したり、関連付けられたトラストポイントのないインターフェイスのフォールバックトラストポイントを設定したりすることもできます。



(注) リリース 9.3 (2) では、SSLv3 は廃止されています。現在のデフォルトは [any] ではなく [tlsv1] です。[any] キーワードは廃止されました。[any]、[sslv3] または [sslv3-only] を選択した場合、設定は受け入れられますが警告が表示されます。[OK] をクリックして作業を続行します。ASA の次のメジャー リリースでは、これらのキーワードは ASA から削除されます。

バージョン 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。

フィールド

- [Server SSL Version] : ASA がサーバとして動作するとき使用する、最小の SSL/TLS プロトコルバージョンをドロップダウンリストから指定します。

いずれか (Any)	SSLv2 クライアントの hello を受け入れ、共通の最新バージョンをネゴシエートします。
SSL V3	SSLv2 クライアントの hello を受け入れ、SSLv3 (以降) をネゴシエートします。
TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1 (以降) をネゴシエートします。
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) をネゴシエートします。
DTLSv1	DTLSv1 クライアントの hello を受け入れ、DTLSv1 (以降) をネゴシエートします。
DTLS1.2	DTLSv1.2 クライアントの hello を受け入れ、DTLSv1.2 (以降) をネゴシエートします。



(注) DTLS の設定および使用は、Cisco AnyConnect 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、DTLSV1.2 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 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。

- [Client SSL Version] : ASA がクライアントとして動作するとき使用する、最小の SSL/TLS プロトコルバージョンをドロップダウンリストから指定します。(SSLクライアントロールに対して DTLS は使用不可)

いずれか (Any)	SSLv3 クライアントの hello を送信し、SSLv3 (以降) をネゴシエートします。
SSL V3	SSLv3 クライアントの hello を送信し、SSLv3 (以降) をネゴシエートします。

TLS V1	TLSv1 クライアントの hello を送信し、 TLSv1 (以降) をネゴシエートします。
TLSV1.1	TLSv1.1 クライアントの hello を送信し、 TLSv1.1 (以降) をネゴシエートします。
TLSV1.2	TLSv1.2 クライアントの hello を送信し、 TLSv1.2 (以降) をネゴシエートします。

- [Diffie-Hellmann group to be used with SSL] : ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group1] (768 ビット絶対値)、[Group2] (1024 ビット絶対値)、[Group5] (1536 ビット絶対値)、[Group14] (2048 ビット絶対値、224 ビット素数位数)、および [Group24] (2048 ビット絶対値、256 ビット素数位数) です。デフォルト値は [Group2] です。
- [ECDH group to be used with SSL] : ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group19] (256 ビット EC)、[Group20] (384 ビット EC)、および [Group21] (521 ビット EC) です。デフォルト値は [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。

- [Encryption] : サポートするバージョン、セキュリティ レベル、および SSL 暗号化アルゴリズムを指定します。[Configure Cipher Algorithms/Custom String] ダイアログボックスを使用してテーブル エントリを定義または変更するには、[Edit] をクリックします。SSL 暗号のセキュリティ レベルを選択し、[OK] をクリックします。
 - [Cipher Version] : ASA でサポートされ、SSL 接続に使用される暗号バージョンを一覧表示します。
 - [Cipher Security Level] : ASA でサポートされ、SSL 接続に使用される暗号セキュリティ レベルを一覧表示します。次のいずれかのオプションを選択します。
 - [すべて (All)] : NULL-SHA を含めたすべての暗号方式。
 - [低 (Low)] : NULL-SHA を除くすべての暗号方式。
 - [Medium] : NULL-SHA、DES-CBC-SHA、RC4-MD5 (これがデフォルトです)、RC4-SHA、および DES-CBC3-SHA を除くすべての暗号。
 - [高 (High)] : SHA-2 を使用する AES-256 暗号方式のみが含まれ、TLS バージョン 1.2 にのみ適用されます。
 - [カスタム (Custom)] : [暗号アルゴリズム/カスタム文字列 (Cipher Algorithms/Custom String)] ボックスで指定する 1 つ以上の暗号方式を含む。このオプションでは、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。

- [Cipher Algorithms/Custom String] : ASA でサポートされ、SSL 接続に使用される暗号アルゴリズムを一覧表示します。OpenSSL を使用する暗号の詳細については、<https://www.openssl.org/docs/manmaster/man1/ciphers.html>を参照してください。

ASA は、サポートされている暗号方式の優先順位を、TLSv1.2 のみでサポートされている暗号方式、TLSv1.1 または TLSv1.2 でサポートされていない暗号方式の順に指定します。

説明したように、次の暗号方式がサポートされています。

- [Server Name Indication (SNI)] : ドメイン名とそのドメインに関連付けることを指定します。
[Add/Edit Server Name Indication (SNI)] ダイアログボックスを使用して各インターフェイスのドメインやトラストポイントを定義または変更するには、[Add] または [Edit] をクリックします。

暗号化方式	TLSv1.1 / DTLS V1	TLSV1.2 / DTLSV 1.2
AES128-GCM-SHA256	×	○
AES128-SHA	○	○
AES128-SHA256	×	○
AES256-GCM-SHA384	×	○
AES256-SHA	○	○
AES256-SHA256	×	○
DERS-CBC-SHA	×	×
DES-CBC-SHA	○	○
DHE-RSA-AES128-GCM-SHA256	×	○
DHE-RSA-AES128-SHA	○	○
DHE-RSA-AES128-SHA256	×	○
DHE-RSA-AES256-GCM-SHA384	no	l
DHE-RSA-AES256-SHA	○	○
ECDHE-ECDSA-AES128-GCM-SHA256	×	○
ECDHE-ECDSA-AES128-SHA256	×	○
ECDHE-ECDSA-AES256-GCM-SHA384	×	○
ECDHE-ECDSA-AES256-SHA384	×	○
ECDHE-RSA-AES128-GCM-SHA256	○	○
ECDHE-RSA-AES128-SHA256	×	○
ECDHE-RSA-AES256-GCM-SHA384	×	○

暗号化方式	TLSv1.1 / DTLS V1	TLSv1.2 / DTLSV 1.2
ECDHE-RSA-AES256-SHA384	×	○
NULL-SHA	×	×
RC4-MD5	×	×
RC4-SHA	×	×

- [Specify domain] : ドメイン名を入力します。
- [Select trustpoint to associate with domain] : ドロップダウン リストからトラストポイントを選択します。
- [Certificates] : 各インターフェイスの SSL 認証に使用する証明書を割り当てます。 [Select SSL Certificate] ダイアログボックスを使用して各インターフェイスのトラストポイントを定義または変更するには、[Edit] をクリックします。
 - [Primary Enrolled Certificate] : このインターフェイスの証明書に使用するトラストポイントを選択します。
 - [Load Balancing Enrolled Certificate] : VPN ロードバランシングが設定されている場合、証明書で使用するトラストポイントを選択します。
- [Fallback Certificate] : 証明書が関連付けられていないインターフェイスで使用する証明書を選択します。 [None] を選択すると、ASA はデフォルトの RSA キーペアと証明書を使用します。
- [Forced Certification Authentication Timeout] : 証明書認証がタイムアウトするまでの分数を設定します。
- [Apply] : 変更内容を保存します。
- [Reset] : 変更内容を取り消し、SSL パラメータを以前に定義した値にリセットします。



第 10 章

Easy VPN

この章では、Easy VPN サーバとして任意の ASA を設定する方法、および Easy VPN リモートハードウェアクライアントとして Cisco ASA with FirePOWER- 5506-X、5506W-X、5506H-X、5508-X モデルを設定する方法について説明します。

- [Easy VPN について \(265 ページ\)](#)
- [Easy VPN リモートの設定 \(269 ページ\)](#)
- [Easy VPN サーバの設定 \(272 ページ\)](#)
- [Easy VPN の機能の履歴 \(273 ページ\)](#)

Easy VPN について

Cisco Ezvpn は、リモートオフィスおよびモバイルワーカー向けの VPN の設定と導入を大幅に簡素化します。Cisco Easy VPN は、サイト間 VPN とリモートアクセス VPN の両方に対応した柔軟性、拡張性、使いやすさを備えています。Cisco Unity クライアントプロトコルの実装により、管理者は Easy VPN サーバで大部分の VPN パラメータを定義できるので、Easy VPN リモートの設定がシンプルになります。

Cisco ASA with FirePOWER の 5506-X、5506W-X、5506H-X、および 5508-X モデルは、Easy VPN サーバへの VPN トンネルを開始するハードウェアクライアントとして Easy VPN リモートをサポートします。Easy VPN サーバとして、別の ASA (任意のモデル) または Cisco IOS ベースのルータを使用できます。ASA は、同時に Easy VPN リモートと Easy VPN サーバの両方として動作することはできません。



- (注) Cisco ASA 5506-X、5506W-X、5506H-X、および 5508-X モデルは、L2 スイッチングではなく、L3 スイッチングをサポートしています。内部ネットワーク上で複数のホストやデバイスとともに Easy VPN リモートを使用する場合は、外部スイッチを使用します。ASA の内部ネットワーク上に単一のホストしかない場合、スイッチは必要はありません。

次のセクションでは、Easy VPN のオプションと設定について説明します。ASDM で ASA を Easy VPN リモートハードウェアクライアントとして設定するには、**[Configuration] > [VPN] > [Easy VPN Remote]** に移動します。Easy VPN サーバでグループポリシー属性を設定するに

は、**[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] > [Hardware Client]** に移動します。

Easy VPN インターフェイス

システムの起動時に、セキュリティ レベルによって Easy VPN の外部および内部インターフェイスが決定されます。最もセキュリティ レベルが低い物理インターフェイスは、Easy VPN サーバへの外部接続に使用されます。最もセキュリティ レベルが高い物理または仮想インターフェイスは、セキュアなリソースへの内部接続に使用されます。Easy VPN で、同じ最高セキュリティ レベルの複数のインターフェイスがあることが特定されると、Easy VPN が無効になります。

必要に応じて、**vpnclient secure interface** コマンドを使用して、内部セキュア インターフェイスを物理インターフェイスから仮想インターフェイスに、あるいは仮想インターフェイスから物理インターフェイスに変更することができます。外部インターフェイスを自動的に選択されたデフォルトの物理インターフェイスから変更することはできません。

たとえば、ASA5506 プラットフォームでは、工場出荷時の設定により、BVI が、最高セキュリティ レベルインターフェイスを示す 100 に設定され（メンバーインターフェイスもレベル 100 に設定）、外部インターフェイスのセキュリティ レベルが 0 になっています。Easy VPN はデフォルトでこれらのインターフェイスを選択します。

仮想インターフェイス（ブリッジ型仮想インターフェイスまたは BVI）が起動時に選択されると、または管理者によって内部のセキュアなインターフェイスとして割り当てられると、次の内容が適用されます。

- すべての BVI メンバー インターフェイスは、自身のセキュリティ レベルに関係なく、内部のセキュアなインターフェイスであるとみなされます。
- ACL および NAT ルールをすべてのメンバー インターフェイスに追加する必要があります。AAA ルールは BVI インターフェイスのみに追加されます。

Easy VPN の接続

Easy VPN は IPsec IKEv1 トンネルを使用します。Easy VPN リモート ハードウェア クライアントの設定は、Easy VPN サーバヘッドエンドの VPN の設定と互換性を保つようする必要があります。セカンダリ サーバを使用する場合は、それらの設定をプライマリ サーバと同じにする必要があります。

ASA Easy VPN リモートはプライマリ Easy VPN サーバの IP アドレスを設定し、必要に応じて、最大 10 台のセカンダリ（バックアップ）サーバを設定します。プライマリ サーバへのトンネルをセットアップできない場合、クライアントは最初のセカンダリ VPN サーバへの接続を試み、次に VPN サーバのリストの上から順に 8 秒間隔で接続を試行します。最初のセカンダリ VPN サーバへのトンネルをセットアップできず、その間にプライマリ サーバがオンライン状態になった場合、クライアントは、引き続き 2 番目のセカンダリ VPN サーバへのトンネルのセットアップを試みます。

デフォルトでは、Easy VPN ハードウェア クライアントとサーバは IPSec をユーザ データグラム プロトコル (UDP) パケット内でカプセル化します。一部の環境（特定のファイアウォール

ルールが設定されている環境など) または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準のカプセル化セキュリティプロトコル (ESP、プロトコル 50) またはインターネット キー エクスチェンジ (IKE、UDP 500) を使用するには、TCP パケット内に IPsec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバを設定します。ただし、UDP が許可されている環境では、IPsec over TCP を設定すると不要なオーバーヘッドが発生します。

Easy VPN トンネル グループ

トンネルの確立後、Easy VPN リモートは Easy VPN サーバで設定されたトンネル グループを指定し、これを接続に使用します。Easy VPN サーバは、トンネルの動作を決定する Easy VPN リモートハードウェアクライアントにグループポリシーまたはユーザ属性をプッシュします。特定の属性を変更するには、プライマリまたはセカンダリ Easy VPN サーバとして設定されている ASA でその属性を変更する必要があります。

Easy VPN モードの動作

企業ネットワークからトンネル経由で Easy VPN リモートの背後にあるホストにアクセスできるかどうかは、モードによって決まります。

- クライアント モードはポートアドレス変換 (PAT) モードとも呼ばれ、Easy VPN リモートプライベートネットワーク上のすべてのデバイスを、企業ネットワークのデバイスから分離します。Easy VPN リモートは、内部ホストのすべての VPN トラフィックに対してポートアドレス変換 (PAT) を実行します。Easy VPN リモートのプライベート側のネットワークとアドレスは非表示になっており、直接アクセスすることはできません。Easy VPN クライアントの内部インターフェイスまたは内部ホストに対して、IP アドレスの管理は必要ありません。
- ネットワーク拡張モード (NEM) は、内部インターフェイスとすべての内部ホストが、トンネルを介して企業ネットワーク全体にルーティングできるようにします。内部ネットワークのホストは、スタティック IP アドレスで事前設定されたアクセス可能なサブネットワーク (スタティックまたは DHCP を介して) から IP アドレスを取得します。NEM では、PAT は VPN トラフィックに適用されません。このモードでは、内部ネットワークのホストごとの VPN 設定やトンネルは必要ありません。Easy VPN リモートによってすべてのホストにトンネリングが提供されます。

Easy VPN サーバはデフォルトでクライアント モードになります。Easy VPN リモートにはデフォルト モードがないため、トンネルを確立する前に、必ず、Easy VPN リモートにいずれかの動作モードを指定する必要があります。



(注) NEM モード用に設定された Easy VPN リモート ASA は、自動トンネル起動をサポートしています。自動起動には、トンネルのセットアップに使用するクレデンシャルの設定とストレージが必要です。セキュアユニット認証がイネーブルの場合は、トンネルの自動開始がディセーブルになります。

複数のインターフェイスが設定されているネットワーク拡張モードの Easy VPN リモートは、最もセキュリティレベルが高いインターフェイスからのローカルに暗号化されたトラフィックに対してのみトンネルを構築します。

Easy VPN ユーザ認証

ASA Easy VPN リモートは、自動ログイン用にユーザ名とパスワードを保存できます。

セキュリティを強化するために、Easy VPN サーバは以下を要求できます。

- セキュアユニット認証 (SUA) : 設定されているユーザ名およびパスワードを無視して、ユーザに手動による認証を要求します。デフォルトでは、SUA はディセーブルになっており、Easy VPN サーバで SUA をイネーブルにします。
- 個別ユーザ認証 (IUA) : Easy VPN リモートの背後にいるユーザは、企業 VPN ネットワークへのアクセス権限を得るために、ユーザ認証を受ける必要があります。デフォルトでは、IUA はディセーブルになっており、Easy VPN サーバで IUA をイネーブルにします。

IUA を使用する場合は、ハードウェア クライアントの背後にある特定のデバイス (Cisco IP Phone やプリンタなど) が個々のユーザ認証をバイパスできるようにする必要があります。これを設定するには、Easy VPN サーバで IP Phone Bypass を指定し、Easy VPN リモートで MAC アドレス免除を指定します。

さらに、Easy VPN サーバは、クライアントのアクセスを終了させるまでのアイドルタイムアウト時間を設定または削除できます。

ユーザ名とパスワードが設定されていない場合、SUA がディセーブルになっている場合、または IUA がイネーブルになっている場合、Cisco Easy VPN サーバは HTTP トラフィックを代行受信し、ユーザをログインページにリダイレクトします。HTTP リダイレクションが自動で、Easy VPN サーバ上のコンフィギュレーションが必要ない。

リモート管理

Easy VPN リモートハードウェアクライアントとして動作する ASA は、さらに IPsec 暗号化されるかどうかにかかわらず、SSH または HTTPS を使用して管理アクセスをサポートします。

デフォルトでは、管理トンネルは、SSH または HTTPS 暗号化で IPsec 暗号化を使用します。IPsec 暗号化レイヤをクリアすると、VPN トンネルの外部に管理アクセスできます。トンネル管理をクリアしても、IPsec の暗号化レベルが削除されるだけで、SSH や HTTPS など、その接続に存在する他の暗号化には影響しません。

セキュリティを強化するために、Easy VPN リモートは、IPsec 暗号化および企業側の特定のホストまたはネットワークへの管理アクセスの制限を要求できます。



- (注) NAT デバイスが ASA Easy VPN リモートとインターネットの間で動作している場合は、ASA Easy VPN リモート上に管理トンネルを設定しないでください。そのような設定では、リモート管理をクリアしてください。

コンフィギュレーションにかかわらず、DHCP 要求（更新メッセージを含む）は IPsec トンネル上を流れません。vpnclient management tunnel を使用しても、DHCP トラフィックは許可されません。

Easy VPN リモートの設定

Easy VPN リモート ハードウェア クライアントとして ASA を設定します。



- (注) Cisco ASA with FirePOWER- 5506-X、5506W-X、5506H-X、および 5508-X モデルのみを、Easy VPN リモート ハードウェア クライアントとして設定できます。

はじめる前に

Easy VPN リモートの設定に必要な次の情報を取得します。

- プライマリ Easy VPN サーバのアドレスと、セカンダリ サーバのアドレスのアドレス（セカンダリ サーバを使用できる場合）。
- Easy VPN リモートを動作させるアドレッシング モード（クライアントまたは NEM）。
- Easy VPN サーバグループ ポリシーの名前とパスワード（事前共有鍵）、または目的のグループ ポリシーを選択して認証する事前設定されたトラストポイント。
- Easy VPN サーバに設定されている、VPN トンネルの使用を許可されたユーザ。

[Configuration] > [VPN] > [Easy VPN Remote]

[Enable Easy VPN Remote] : Easy VPN Remote 機能をイネーブルにして、このダイアログボックスの残りのフィールドを設定できるようにします。

[Mode] : [Client mode] または [Network extension mode] を選択します。

- [Client mode] : ポート アドレス変換（PAT）モードを使用して、クライアントに関連する内部ホストのアドレスを企業ネットワークから分離します。
- [Network extension mode] : 内部ホストのアドレスに企業ネットワークからアクセスできるようにします。



(注) Easy VPN リモートが NEM を使用しており、セカンダリ サーバに接続している場合は、各ヘッドエンドへの ASDM 接続を確立し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps] で作成した暗号マップの [Enable Reverse Route Injection] をオンにして、RRI を使用したリモート ネットワークのダイナミック アナウンスメントを設定します。

- [Auto connect] : ネットワーク拡張モードがローカルに設定され、かつ Easy VPN リモートにプッシュされたグループポリシーにスプリットトンネリングが設定されている場合を除き、Easy VPN リモートは自動 IPsec データ トンネルを確立します。両方の条件を満たしている場合は、この属性をオンにすると、IPsec データ トンネルの確立が自動化されます。両方の条件を満たして、この属性をオフにした場合、この属性は無視されます。

[Group Settings] : 事前共有キーまたは X.509 証明書をユーザ認証に使用するかどうかを指定します。

- [Pre-shared key] : 認証での事前共有キーの使用をイネーブルにして、以降の [Group Name]、[Group Password]、[Confirm Password] の各フィールドで、そのキーを含むグループ ポリシー名とパスワードを指定できるようにします。
 - [Group Name] : 認証に使用するグループ ポリシーの名前を指定します。
 - [Group Password] : 特定のグループ ポリシーで使用するパスワードを指定します。
 - [Confirm Password] : 入力したグループ パスワードの確認を必須にします。
- [X.509 Certificate] : 認証に対して、認証局から提供された X.509 デジタル証明書の使用を指定します。
 - [Select Trustpoint] : ドロップダウン リストからトラストポイントを選択できます。トラストポイントは IP アドレスまたはホスト名です。トラストポイントを定義するには、この領域の下部にある [Trustpoint(s) configuration] リンクをクリックします。
 - [Send certificate chain] : 証明書だけでなく、証明書チェーンの送信もイネーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。

[User Settings] : ユーザ ログイン情報を設定します。

- [User Name] : Easy VPN リモートの接続用 VPN ユーザ名を設定します。Xauth には、TACACS+ または RADIUS を使用して IKE 内のユーザを認証する機能があります。Xauth は、RADIUS または別のサポートされているユーザ認証プロトコルを使用して、ユーザを認証します (この場合、Easy VPN ハードウェア クライアント)。セキュア ユニット認証がディセーブルになっており、サーバが Xauth クレデンシャルを要求する場合には、Xauth ユーザ名とパスワード パラメータが使用されます。セキュア ユニット認証がイネーブル

の場合、これらのパラメータは無視され、ASAによって、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。

- [User Password] および [Confirm Password] : Easy VPN リモートの接続用 VPN ユーザパスワードを設定して確認します。

[Easy VPN Server To Be Added] : Easy VPN サーバを追加または削除します。どの ASA も Easy VPN サーバとして動作できます。接続を確立する前にサーバを設定する必要があります。ASA は、IPv4 アドレス、名前データベース、または DNS 名をサポートしており、この順序でアドレスを解決します。Easy VPN Server(s) リストの最初のサーバはプライマリサーバです。プライマリサーバに加え、最大 10 台のバックアップサーバを指定できます。

- [Easy VPN Server(s)] : 設定されている Easy VPN サーバを優先順に一覧表示します。
- [Name or IP Address] : リストに追加する Easy VPN サーバの名前または IP アドレス。
- [Add] および [Remove] : 指定したサーバを [Easy VPN Server(s)] リストに移動、またはリストから削除します。
- [Move Up] および [Move Down] : [Easy VPN Server(s)] リスト内でのサーバの位置を変更します。これらのボタンは、リストにサーバが 1 台以上存在する場合にだけ使用できます。

[Secure Client Interface] : 起動時に最もセキュリティレベルが高い物理インターフェイスまたは BVI がセキュアなリソースへの内部接続に使用されます。別のインターフェイスを使用する場合は、ドロップダウンの選択肢からインターフェイスを選択します。物理または仮想インターフェイスを割り当てることができます。

[Configuration] > [VPN] > [Easy VPN Remote] > [Advanced]

[MAC Exemption] : Easy VPN リモートの接続用デバイスパススルーで使用する MAC アドレスとマスクを設定します。Cisco IP Phone やプリンタなどのデバイスは、認証を実行できないため、個別ユニット認証に追加できません。これらのデバイスに対応するために、Individual User Authentication がイネーブルになっている場合には、MAC Exemption 属性によってイネーブルにされるデバイスパススルー機能が、指定した MAC アドレスを持つデバイスの認証を免除します。

- [MAC Address] : 指定した MAC アドレスを持つデバイスの認証を免除します。

このフィールドで MAC アドレスを指定するための形式は 3 桁の 16 進数値で、45ab.ff36.9999 のようにピリオドで区切られます。MAC アドレスの最初の 24 ビットは、その機器の製造元を示します。最後の 24 ビットは、ユニットの 16 進形式のシリアル番号です。

- [MAC Mask] : このフィールドで MAC マスクを指定するときは、ピリオドで区切った 3 桁の 16 進数値の形式を使用します。たとえば、ffff.ffff.ffff という MAC マスクは特定の MAC アドレスとだけ一致します。すべてがゼロの MAC マスクは、いずれの MAC アドレスとも一致しません。MAC マスク ffff.ff00.0000 は、製造業者が同じであるすべてのデバイスと一致します。
- [Add] および [Remove] : 指定した MAC アドレスとマスクのペアを [MAC Address/Mask] リストに追加、またはリストから削除します。

[Tunneled Management] : デバイス管理のための IPsec 暗号化を設定し、トンネル経由での Easy VPN ハードウェア クライアント接続の管理を許可するネットワークを指定します。

- [Enable Tunneled Management] : すでに管理トンネルに存在する SSH または HTTPS 暗号化に IPsec 暗号化レイヤを追加します。
- [Clear Tunneled Management] : 暗号化を追加せず、すでに管理トンネルに存在する暗号化を使用します。[Clear Tunneled Management] を選択しても、IPsec の暗号化レベルが削除されるだけで、SSH や HTTP など、その接続に存在する他の暗号化には影響しません。
- [IP Address/Mask] : この領域の Enable または Clear 機能によって処理される、設定済みの IP アドレスとマスクのペアを一覧表示します。
 - [IP Address] : VPN トンネルを介した Easy VPN ハードウェアクライアントへの管理アクセスを許可するホストまたはネットワークの IP アドレスを指定します。
 - [Mask] : 対応する IP アドレスのネットワーク マスクを指定します。
 - [Add/Remove] : 指定した IP アドレスとマスクを [IP Address/Mask] リストに移動、またはリストから削除します。

[IPsec Over TCP] : Easy VPN リモートの接続に PCT カプセル化 IPsec を使用するように設定します。



- (注) PCT カプセル化 IPsec を使用するように Easy VPN リモートの接続を設定する場合は、大きなパケットを送信するように ASA を設定する必要があります。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Fragmentation Policies] に移動し、外部インターフェイスをダブルクリックして、[DF Bit Setting Policy] を [Clear] に設定します。

- [Enable] : IPsec over TCP をイネーブルにします。
- [Enter Port Number] : IPsec over TCP 接続で使用するポート番号を指定します。

[Server Certificate] : 証明書マップで指定された特定の証明書を持つ Easy VPN サーバとの接続だけを許可するように、Easy VPN リモートの接続を設定します。このパラメータを使用して、Easy VPN サーバ証明書のフィルタリングをイネーブルにします。

Easy VPN サーバの設定

始める前に

すべてのセカンダリ Easy VPN サーバに、プライマリ Easy VPN サーバと同じオプションと設定が指定されていることを確認します。

手順

- ステップ 1 IPsec IKEv1 のサポート用に Easy VPN サーバを設定します。[一般的な VPN 設定 \(61 ページ\)](#) を参照してください。
- ステップ 2 特定の Easy VPN サーバ属性を設定します。[内部グループ ポリシー、IPsec \(IKEv1\) のハードウェア クライアント属性 \(108 ページ\)](#) を参照してください。

Easy VPN の機能の履歴

機能名	リリース	機能情報
ASA 5506-X、5506W-X、5506H-X および 5508-X の Cisco Easy VPN クライアント	9.5(1)	このリリースは、ASA 5506-X シリーズでの Cisco Easy VPN の使用をサポートし、かつ ASA 5508-X 用の Cisco Easy VPN をサポートします。ASA は、VPN ヘッドエンドに接続すると VPN ハードウェア クライアントとして機能します。ASA の背後にある Easy VPN ポート上のデバイス (コンピュータ、プリンタなど) は、VPN 経由で通信できます。個別に VPN クライアントを実行する必要はありません。ASA インターフェイス 1 つのみで Easy VPN ポートとして機能できます。このポートに複数のデバイスを接続するには、レイヤ 2 スイッチをこのポート上に配置してから、このスイッチにデバイスを接続します。 次の画面が導入されました。 [Configuration] > [VPN] > [Easy VPN Remote]

機能名	リリース	機能情報
<p>BVI サポートのための Easy VPN 拡張</p>	<p>9.9(2)</p>	<p>Easy VPN は、ブリッジ型仮想インターフェイスを内部セキュア インターフェイスとしてサポートするように拡張され、管理者は新しい vpnclient secure interface [interface-name] コマンドを使用して内部セキュア インターフェイスを直接設定できるようになりました。</p> <p>物理インターフェイスまたはブリッジ型仮想インターフェイスを内部セキュア インターフェイスとして割り当てることができます。これが管理者によって設定されていない場合、Easy VPN はそれが独立した物理インターフェイスまたは BVI に関わらず、以前と同じセキュリティ レベルを使用してその内部セキュア インターフェイスを選択します。</p> <p>また、管理アクセスがその BVI で有効になっている場合、telnet、http、ssh などの管理サービスを BVI で設定できるようになりました。</p>



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 \(275 ページ\)](#)
- [仮想トンネル インターフェイスの注意事項 \(275 ページ\)](#)
- [VTI トンネルの作成 \(277 ページ\)](#)

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 VPN の代替策として、仮想トンネル インターフェイスが設定されたピア間に VPN トンネルを作成することができます。これは、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。これは、動的または静的なルートの使用が可能です。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 をサポートする静的 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。

仮想トンネル インターフェイスの注意事項

一般的な設定時の注意事項

- 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、動的または静的なルートを使用することができます。

- 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。
- ネットワークアドレス変換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。
- LAN-to-LAN 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。
- 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。
- 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リストを適用することができます。
- VTI では BGP のみサポートされます。
- ASA が IOS IKEv2 VTI クライアントを終端している場合は、IOS VTI クライアントによって開始されたこの L2L セッションのモード CFG 属性を ASA が取得できないため、IOS の設定交換要求を無効にします。

IPv6 のサポート

IPv6 はサポートされていません。

コンテキストモード

シングルモードでだけサポートされています。

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。

DHCP リレー

DHCP リレーは、仮想トンネルインターフェイス (VTI) ではサポートされていません。

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ル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。

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。レスポンドについては、`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ンドの両方について、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

ステップ 1 [Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] を選択します。

ステップ 2 セキュリティ アソシエーションを確立するための IKEv1 または IKEv2 を設定します。

- IKEv1 を設定します。

- a) [IKEv1 IPsec Proposals (Transform Sets)] パネルで [Add] をクリックします。
- b) [Set Name] を入力します。
- c) [Tunnel] チェックボックスは、デフォルトの選択のままにします。
- d) [ESP Encryption] および [ESP Authentication] を選択します。
- e) [OK] をクリックします。

- IKEv2 を設定します。

- a) [IKEv2 IPsec Proposals] パネルで [Add] をクリックします。
 - b) [Name] と [Encryption] を入力します。
 - c) [Integrity Hash] を選択します。
 - d) [OK] をクリックします。
-

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 [Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] を選択します。
- ステップ 2 [IPsec Profile] パネルで [Add] をクリックします。
- ステップ 3 [Name] に IPsec プロファイル名を入力します。
- ステップ 4 [IKE v1 IPsec Proposal] または [IKE v2 IPsec Proposal] に、IPsec プロファイルのために作成する IKE v1 IPsec プロポーザルまたは IKE v2 IPsec プロポーザルを入力します。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。
- ステップ 5 VTI トンネルの一端をレスポンドアとしてのみ動作させる必要がある場合は、[Responder only] チェックボックスをオンにします。
 - VTI トンネルの一端をレスポンドアとしてのみ動作するように設定できます。レスポンドアのみは、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。
 - イニシエータ側のキー再生成の設定が不明の場合、レスポンドアのみモードを解除して SA の確立を双方向にするか、レスポンドアのみ側の 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 6 (任意) [Enable security association lifetime] チェックボックスをオンにして、セキュリティ アソシエーションの期間の値をキロバイトおよび秒で入力します。
- ステップ 7 (任意) [PFS Settings] チェックボックスをオンにして、必要な Diffie-Hellman グループを選択します。

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。

これにより、暗号キー決定アルゴリズムの強度が確立されます。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。

- ステップ 8** (任意) [Enable sending certificate] チェックボックスをオンにして、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選択します。必要に応じて、[Chain] チェックボックスをオンにします。
- ステップ 9** [OK] をクリックします。
- ステップ 10** [IPsec Proposals (Transform Sets)] メイン パネルで [Apply] をクリックします。
- ステップ 11** [Preview CLI Commands] ダイアログボックスで、[Send] をクリックします。

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** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。
- ステップ 2** [Add] > [VTI Interface] の順に選択します。[Add VTI Interface] ウィンドウが表示されます。
- ステップ 3** [General] タブで、**VTI ID** と入力します。0 ～ 10413 の任意の値を指定できます。最大 100 の VTI インターフェイスがサポートされます。
- (注) 他のデバイスから ASA 5506 に設定を移行する場合は、トンネル ID 範囲に 1 ～ 100 を指定します。これは、ASA 5506 デバイスで使用可能なトンネル範囲 1 ～ 100 に対応させるためです。
- ステップ 4** [Interface Name] を入力します。
[Enable Interface] チェックボックスがオンになっていることを確認します。
- ステップ 5** トンネルの送信元 **IP アドレス** と **サブネット マスク** を入力します。
- ステップ 6** [Advanced] タブをクリックします。
すべてのフィールドに有効な値が入力または選択されていないと、トンネルは、VPN ウィザードに表示されません。
- ステップ 7** 宛先 **IP アドレス** を入力します。
- ステップ 8** 送信元 **インターフェイス** を選択します。
- ステップ 9** [Tunnel Protection with IPsec Profile] フィールドで、IPsec プロファイルを選択します。
- ステップ 10** [Ensure the Enable Tunnel Mode IPv4 IPsec] チェックボックスをオンにします。

ステップ 11 [OK] をクリックします。

ステップ 12 [Interfaces] パネルで [Apply] をクリックします。

ステップ 13 [Preview CLI Commands] ダイアログボックスで、[Send] をクリックします。

更新された設定が読み込まれると、新しい VTI がインターフェイスのリストに表示されます。この新しい VTI は、IPsec サイト間 VPN の作成に使用できます。



第 12 章

VPN の外部 AAA サーバの設定

- [外部 AAA サーバについて \(283 ページ\)](#)
- [外部 AAA サーバを使用する際のガイドライン \(284 ページ\)](#)
- [複数証明書認証の設定 \(284 ページ\)](#)
- [Active Directory/LDAP VPN リモート アクセス許可の例 \(285 ページ\)](#)

外部 AAA サーバについて

この ASA は、外部の LDAP、RADIUS、TACACS+ サーバを使用して、ASA の認証、認可、アカウントリング (AAA) をサポートするように設定できます。外部 AAA サーバは、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、ユーザ認可属性 (ユーザ権利またはユーザ権限とも呼ばれる) 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 (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 サーバ上のユーザ属性：ユーザ認証や認可が成功すると、サーバ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に設定されている属性（ASDM のユーザ 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 サーバからユーザに対して 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、サーバから返されないものを適用します。

LDAP サーバでは、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せん。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、サーバから返されるユーザ属性、ユーザ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

AnyConnect 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証明書（または2つのユーザ証明書）が必要であるため、この機能では AnyConnect Start Before Logon (SBL) を使用できません。

ユーザ名の事前入力フィールドでは、2つ目の（ユーザ）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名は、常にクライアントから受信した2つ目の（ユーザ）証明書から取得されます。

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）証明書は、事前入力および証明書由来のユーザ名のプライマリおよびセカンダリユーザ名による解析対象です。

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。

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。

- [ユーザベースの属性のポリシー適用 \(285 ページ\)](#)
- [特定のグループポリシーへの LDAP ユーザの配置 \(287 ページ\)](#)
- [AnyConnect トンネルのスタティック IP アドレス割り当ての適用 \(289 ページ\)](#)
- [ダイヤルイン許可または拒否アクセスの適用 \(291 ページ\)](#)
- [ログオン時間と Time-of-Day ルールの適用 \(293 ページ\)](#)

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』](#)

ユーザベースの属性のポリシー適用

この例では、ユーザ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

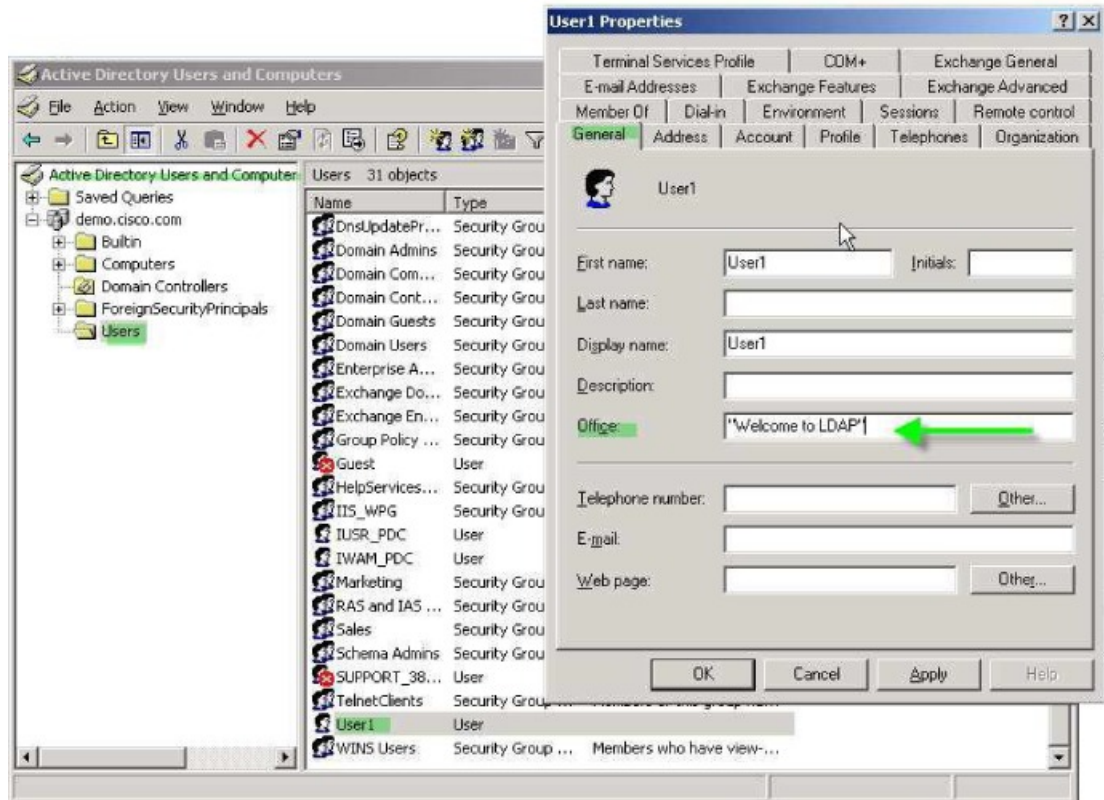
ピングする方法を示します。この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。

AD LDAP サーバ上で設定されたユーザ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にバナーを表示します。

手順

ステップ 1 ユーザ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 サーバに関連付けます。

AAA サーバグループ MS_LDAP のホスト 10.1.1.2 の AAA サーバホスト 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。

特定のグループポリシーへの LDAP ユーザの配置

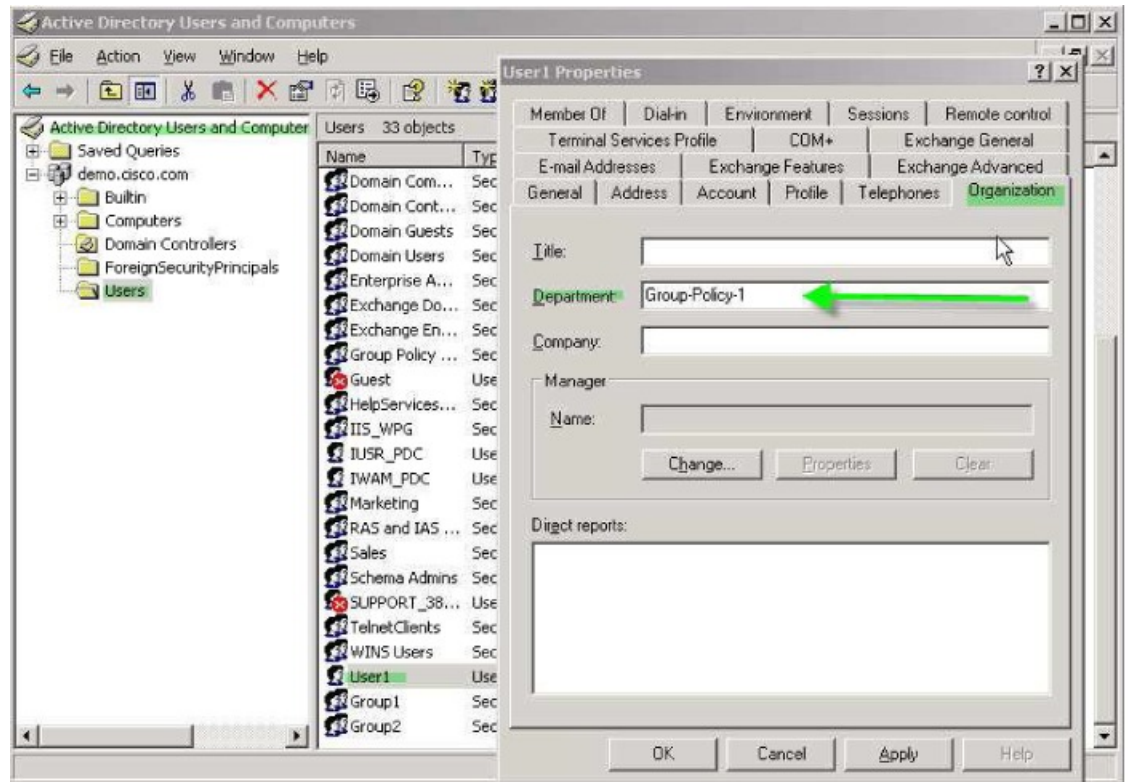
この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続経由で接続します。

LDAP ユーザを特定のグループポリシーに配置するには、[Organization] タブの [Department] フィールドを使用してグループポリシーの名前を入力します。次に、属性マップを作成し、[Department] を Cisco 属性である IETF-Radius-Class にマッピングします。

認証時、ASA はサーバから [Department] の値を取得し、その値を IETF-Radius-Class にマッピングして、User1 をグループポリシーに配置します。

手順

ステップ1 ユーザ名を右クリックして、[Properties] ダイアログボックスの [Organization] タブを開き、[Department] フィールドに「**Group-Policy-1**」と入力します。



ステップ 2 LDAP コンフィギュレーションの属性マップを定義します。

AD 属性 Department を Cisco 属性 IETF-Radius-Class にマッピングします。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

ステップ 3 LDAP 属性マップを AAA サーバに関連付けます。

AAA サーバグループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバ 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 group_policy 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 group_policy
```

ステップ 4 サーバの [Department] フィールドに入力されているグループポリシー Group-policy-1 を ASA に追加し、ユーザに割り当てる必須ポリシー属性を設定します。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

ステップ 5 このユーザとして VPN 接続を確立し、Group-Policy1 からの属性（およびその他に適用可能な、デフォルトのグループポリシーからの属性）がセッションに継承されていることを確認します。

ステップ 6 特権 EXEC モードで **debug ldap 255** コマンドをイネーブルにして、ASA とサーバの間の通信をモニタします。このコマンドからの出力の例を次に示します。これは、主要なメッセージがわかるように編集済みです。

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

AnyConnect トンネルのスタティック IP アドレス割り当ての適用

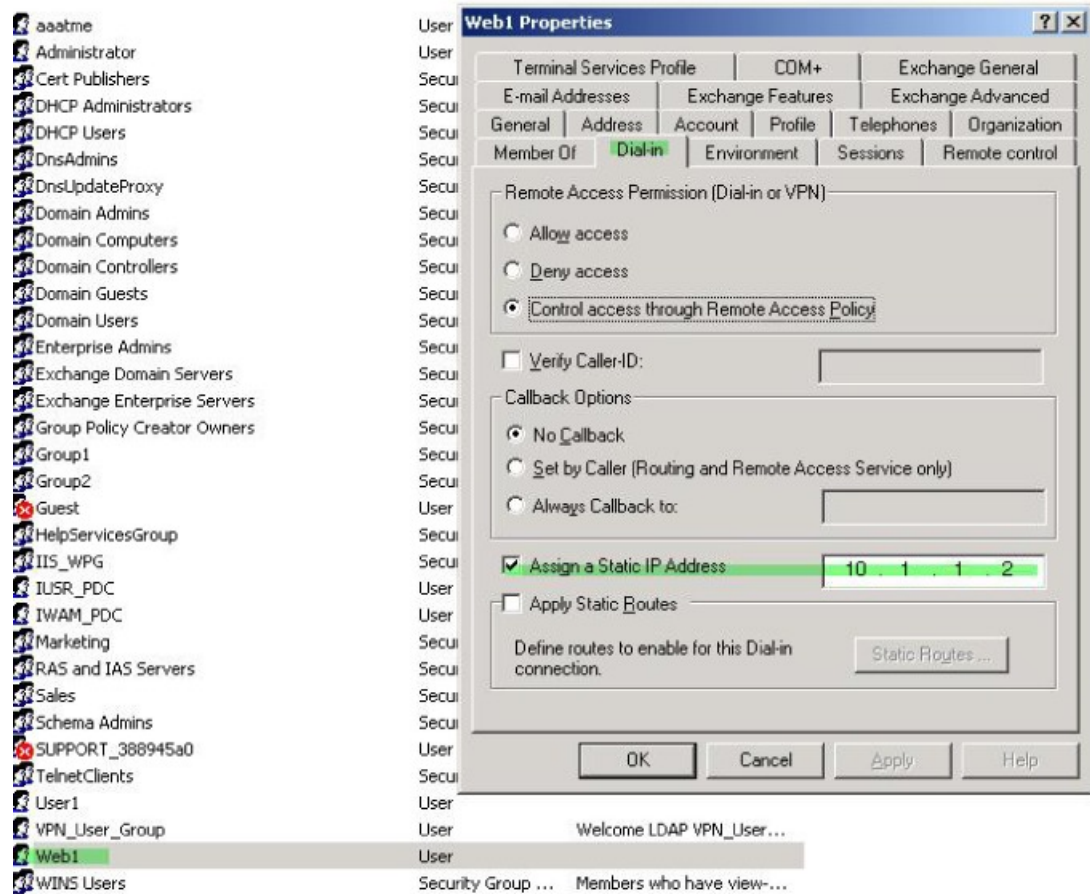
この例は、IPsec クライアントや SSL VPN クライアントなどのフルトンネルクライアントに適用されます。

スタティック AnyConnect スタティック IP 割り当てを適用するには、AnyConnect クライアントユーザ 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 サーバの [Dialin] タブの [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 サーバに関連付けます。

AAA サーバグループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバ 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 AnyConnect クライアントとの接続を確立します。サーバで設定され、ASA にマッピングされた IP アドレスをユーザ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 : AnyConnect 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。

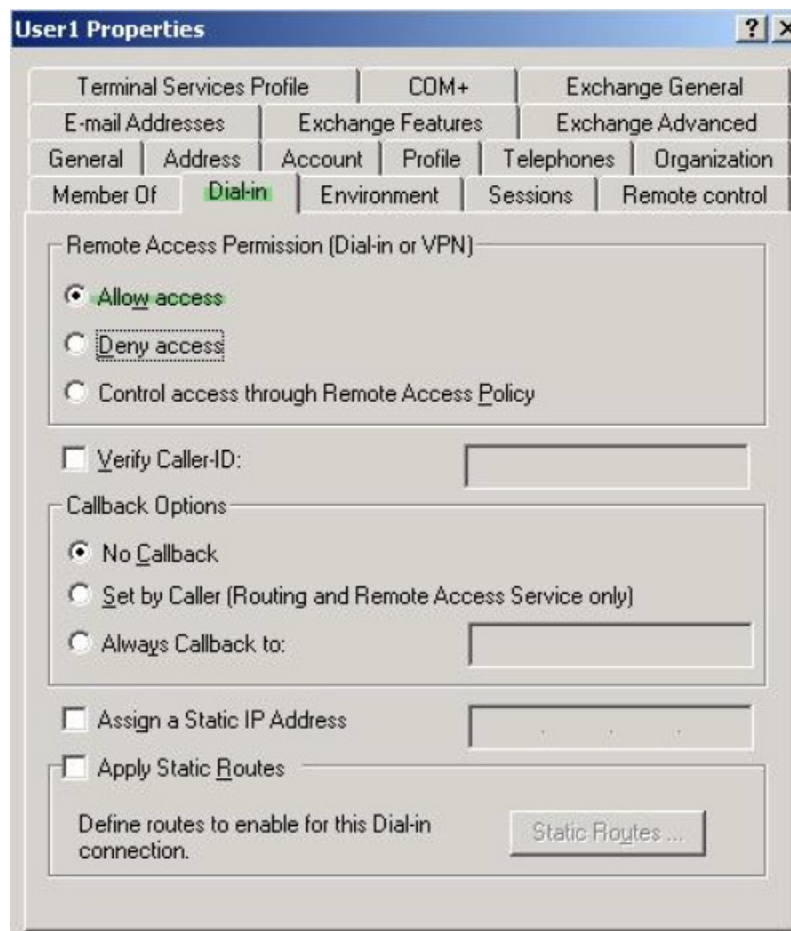
² (2) 注 1 を参照。

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 AnyConnect の両方の接続を許可するがクライアントレス 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] 設定で使用される 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 サーバに関連付けます。

- a) AAA サーバグループ MS_LDAP でホスト 10.1.1.2 の AAA サーバホスト 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。

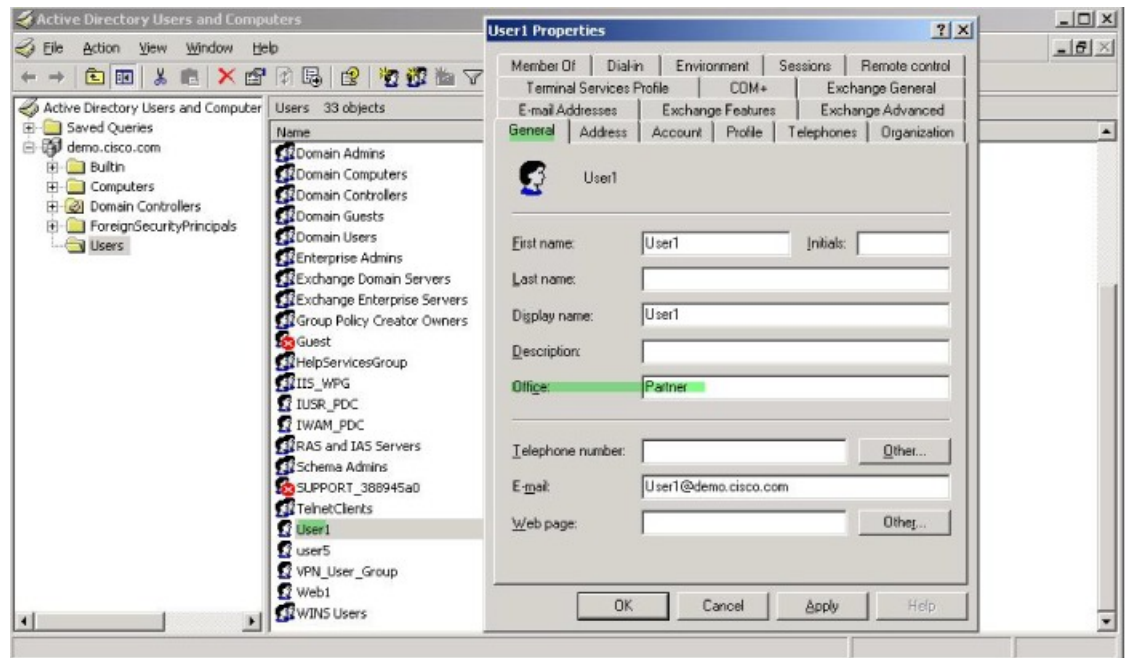
ログオン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザ（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] フィールドで使用される 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 サーバに関連付けます。

AAA サーバグループ `MS_LDAP` のホスト `10.1.1.2` に対して AAA サーバ 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
```



第 II 部

クライアントレス SSL VPN

- [クライアントレス SSL VPN の概要 \(297 ページ\)](#)
- [基本的なクライアントレス SSL VPN のコンフィギュレーション \(301 ページ\)](#)
- [高度なクライアントレス SSL VPN のコンフィギュレーション \(331 ページ\)](#)
- [ポリシー グループ \(371 ページ\)](#)
- [クライアントレス SSL VPN リモートユーザ \(389 ページ\)](#)
- [クライアントレス SSL VPN ユーザ \(403 ページ\)](#)
- [モバイルデバイスでのクライアントレス SSL VPN \(423 ページ\)](#)
- [クライアントレス SSL VPN のカスタマイズ \(425 ページ\)](#)
- [クライアントレス SSL VPN のトラブルシューティング \(473 ページ\)](#)



第 13 章

クライアントレス SSL VPN の概要

- クライアントレス SSL VPN の概要 (297 ページ)
- クライアントレス SSL VPN の前提条件 (298 ページ)
- クライアントレス SSL VPN に関する注意事項と制約事項 (298 ページ)
- クライアントレス SSL VPN のライセンス (300 ページ)

クライアントレス SSL VPN の概要

クライアントレス SSL VPN を使用すると、エンドユーザは SSL 対応 Web ブラウザを使用して、任意の場所から社内ネットワークのリソースに安全にアクセスできます。ユーザは、まず、クライアントレス SSL VPN ゲートウェイで認証し、事前設定されたネットワークリソースにアクセスできるようにします。



- (注) クライアントレス SSL VPN がイネーブルになっている場合、セキュリティコンテキスト (ファイアウォールマルチモードとも呼ばれる) とアクティブ/アクティブ ステートフル フェールオーバーはサポートされません。

クライアントレス SSL VPN は、ソフトウェアまたはハードウェア クライアントを必要とせず、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを作成します。HTTP 経由でインターネットに接続できるほとんどのデバイスから、幅広い Web リソースと、Web 対応およびレガシー アプリケーションに安全かつ簡単にアクセスできます。次の内容で構成されています。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory ファイル共有
- Microsoft Outlook Web Access Exchange Server 2010 および 2013。
- Microsoft Web App to Exchange Server 2010 (8.4(2) 以降において)

- Application Access (他の TCP ベースのアプリケーションにアクセスするためのスマートトンネルまたはポート転送)

クライアントレス SSL VPN は Secure Sockets Layer (SSL) プロトコルとその後継の Transport Layer Security (SSL/TLS1) を使用し、内部サーバとして設定されている特定のサポート対象内部リソースと、リモートユーザとの間にセキュアな接続を実現します。ASA はプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、クライアントレス SSL VPN セッションのユーザに対してグループ単位でリソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

クライアントレス SSL VPN の前提条件

ASA 上のクライアントレス SSL VPN でサポートされるプラットフォームとブラウザについては、『[サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ](#)』を参照してください。

クライアントレス SSL VPN に関する注意事項と制約事項

- ActiveX ページでは、ActiveX リレーをイネーブルにするか、関連するグループポリシーに **activex-relay** を入力しておく必要があります。あるいは、スマートトンネルリストをポリシーに割り当て、エンドポイント上のブラウザプロキシ例外リストにプロキシが指定されている場合、ユーザはそのリストに「shutdown.webvpn.relay.」エントリを追加する必要があります。
- ASA では、Mozilla Firefox、MS Edge、Google Chrome、macOS、または Linux から Windows 共有 (CIFS) Web フォルダへのクライアントレスアクセスはサポートされていません。
- DoD Common Access Card および SmartCard を含む証明書認証は、Safari キーチェーンだけで動作します。
- クライアントレス接続用に信頼できる証明書をインストールしても、クライアントには信頼できない証明書の警告が表示されることがあります。
- ASA は、クライアントレス SSL VPN 接続用の DSA 証明書をサポートしません。RSA 証明書はサポートされます。
- 一部のドメインベースのセキュリティ製品には、ASA から送信された要求を超える要件があります。
- コンフィギュレーション制御の検査機能およびモジュラポリシーフレームワークにおけるその他の検査機能はサポートされません。
- NAT および PAT はクライアントに適用可能ではありません。

- AnyConnect は Web コンテンツに依存せずに下位のネットワーク層で動作するため、クライアントレス WebVPN でサポートされていないと思われる Web アプリケーションにアクセスするように ASA で AnyConnect を設定することを推奨します。
- クライアントレス SSL VPN の一部のコンポーネントには、Java Runtime Environment (JRE) が必要です。macOS v10.12 以降では、Java はデフォルトでインストールされません。macOS での Java のインストール方法については、http://java.com/en/download/faq/java_mac.xml を参照してください。
- クライアントレス VPN セッションを開始すると、RADIUS アカウンティング開始メッセージが生成されます。クライアントレス VPN セッションにはアドレスが割り当てられないため、開始メッセージには Framed-IP-Address が含まれません。レイヤ 3 VPN 接続がクライアントレスポータルページから順番に開始されるとアドレスが割り当てられ、暫定アップデート アカウンティング メッセージで RADIUS サーバに報告されます。weblaunch 機能を使用してレイヤ 3 VPN トンネルが確立される場合、同様の RADIUS の動作が期待できます。この状況では、ユーザが認証された後、レイヤ 3 トンネルが確立される前にアカウンティング開始メッセージがフレーム化 IP アドレスなしで送信されます。レイヤ 3 トンネルが確立されると、この開始メッセージに暫定アップデートメッセージが続きます。
- HTML ページは RFC 2616 に準じている必要があります。ヘッダーの後の空の行は、本文の開始と解釈されます。したがって、ヘッダー間に空の行を挿入すると、一部のヘッダーが本文に表示され、ユーザがページの問題を修正するためにウィンドウを更新する必要がありますが生じる場合があります。
- Java コード処理に使用されるクライアントレス WebVPN Java リライタは、Oracle Forms をサポートしていません。
- クライアントレス WebVPN リライタは、実行時に動的に設定されるため、JavaScript オブジェクトのブラケット表記の割り当てを検出できません。
- クライアントレス WebVPN は、サーバの応答に含まれるチャンクサイズと CRLF 間のスペースをサポートしていません。これは、ASA がチャンクサイズのスペースを予期しておらず、チャンクをまとめることができないためです。
- コンテンツ セキュリティ ポリシー (CSP) はサポートされていません。
- クライアントレス WebVPN リライタを使用すると、Angular のカスタムイベントリスナーおよびロケーション変更が正しく機能しない場合があります。
- クライアントレス WebVPN は、サーバ側の Cross-Origin Resource Sharing (CORS) フィルタをサポートしていません。
- クライアントレス WebVPN リライタは、現在、HTML5 および Javascript Blog API をサポートしていません。
- WebVPN アーキテクチャに従い、Fetch API はサポートされていません。
- クライアントレス WebVPN は、認証時に MDM 属性を RADIUS サーバと共有しません。
- クライアントレスポータル用に設定された複数のグループポリシーがある場合は、ログインページのドロップダウンに表示されます。リストにある最初のグループポリシーで

証明書が必要な場合は、ユーザはマッチング証明書が必要です。グループポリシーの一部が証明書を使用しない場合、非証明書ポリシーを最初に表示するには、リストを設定します。また、「0-Select-a-group」の名前でダミーグループポリシーを作成することもできます。



ヒント グループポリシーの名前をアルファベット順に付けることで、最初に表示されるポリシーを制御できます。また、ポリシーの先頭に数字を付けることもできます。たとえば、1-AAA、2-Certificate とします。

- 別のサーバ上のページへのリンクは ASA からルーティング可能である必要があります。それ以外の場合、ユーザに次のエラーが表示されることがあります。リンクが使用可能で、アクセス制御ルール、SSL 構成、またはその他のファイアウォール機能によってブロックされていないこと、およびサーバへのルートがあることを確認します。

```
Connection failed, Server "<DNS name>" unavailable.
```

クライアントレス SSL VPN のライセンス

AnyConnect セキュア モビリティ クライアントを使用するには、AnyConnect Plus および Apex ライセンスを購入する必要があります。必要なライセンスは、使用する予定の AnyConnect VPN Client および Secure Mobility の機能と、サポートするセッションの数によって異なります。これらのユーザベースのライセンスには、一般的な BYOD のトレンドに合わせたサポートとソフトウェア更新へのアクセスが含まれます。

AnyConnect 4.4 ライセンスは、ASA（および ISR、CSR、ASR）で使用され、また、Identity Services Engine（ISE）、クラウド Web セキュリティ（CWS）、Web セキュリティ アプライアンス（WSA）などの非 VPN ヘッドエンドでも使用されます。ヘッドエンドに関係なく一貫したモデルが使用されるため、ヘッドエンドの移行が発生した場合も影響はありません。

AnyConnect のライセンス モデルについての詳細は、<http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf> を参照してください。



第 14 章

基本的なクライアントレス SSLVPN のコンフィギュレーション

- 各 URL の書き換え (301 ページ)
- クライアントレス SSL VPN アクセスの設定 (302 ページ)
- 信頼できる証明書のプール (303 ページ)
- Java Code Signer (307 ページ)
- プラグインへのブラウザアクセスの設定 (308 ページ)
- ポート転送の設定 (315 ページ)
- ファイルアクセスの設定 (321 ページ)
- SharePoint アクセスのためのクロックの正確性の確保 (323 ページ)
- Virtual Desktop Infrastructure (VDI) (323 ページ)
- クライアント/サーバプラグインへのブラウザアクセスの設定 (327 ページ)

各 URL の書き換え

デフォルトでは、ASA はすべての Web リソース (HTTPS、CIFS、RDP、プラグインなど) に対するすべてのポータルトラフィックを許可します。クライアントレス SSL VPN は、ASA だけに意味のあるものに各 URL をリライトします。ユーザは、要求した Web サイトに接続されていることを確認するために、この URL を使用できません。フィッシング Web サイトからの危険にユーザがさらされるのを防ぐには、クライアントレスアクセスに設定しているポリシー (グループポリシー、ダイナミックアクセスポリシー、またはその両方) に Web ACL を割り当ててポータルからのトラフィックフローを制御します。これらのポリシーの URL エントリをオフに切り替えて、何にアクセスできるかについてユーザが混乱しないようにすることをお勧めします。

図 6: ユーザが入力した URL の例



図 7: セキュリティ アプライアンスによって書き換えられ、ブラウザウィンドウに表示された同じ URL



手順

- ステップ 1** クライアントレス SSL VPN アクセスを必要とするすべてのユーザのグループ ポリシーを設定し、そのグループ ポリシーに対してだけクライアントレス SSL VPN をイネーブルにします。
- ステップ 2** グループ ポリシーを開き、[General] > [More Options] > [Web ACL] を選択して [Manage] をクリックします。
- ステップ 3** 次のいずれかを行う場合、Web ACL を作成します。
- プライベート ネットワーク内の特定のターゲットだけにアクセスを許可する。
 - プライベート ネットワークへのアクセスだけを許可する、インターネット アクセスを拒否する、または信頼できるサイトへのアクセスだけを許可する。
- ステップ 4** クライアントレス SSL VPN アクセス用に設定しているすべてのポリシー（グループポリシー、ダイナミック アクセス ポリシー、またはその両方）に Web ACL を割り当てます。Web ACL を DAP に割り当てるには、DAP レコードを編集し、[Network ACL Filters] タブで Web ACL を選択します。
- ステップ 5** ブラウザベースの接続の確立時に表示されるポータル ページ上の URL エントリをオフに切り替えます。グループ ポリシーのポータル フレームと DAP の [Functions] タブの両方の [URL Entry] の横にある [Disable] をクリックします。DAP 上の URL エントリをオフに切り替えるには、ASDM を使用して DAP レコードを編集し、[Functions] タブをクリックして、URL エントリの横にある [Disable] をオンにします。
- ステップ 6** ユーザに、ポータル ページの上のネイティブ ブラウザの Address フィールドに外部 URL を入力するか、別のブラウザ ウィンドウを開いて、外部サイトにアクセスするかを指示します。

クライアントレス SSL VPN アクセスの設定

クライアントレス SSL VPN アクセスを設定する場合、次の操作が可能です。

- クライアントレス SSL VPN セッション向けに ASA インターフェイスをイネーブルにする、またはオフに切り替える。
- クライアントレス SSL VPN 接続で使用するポートを選択する。
- 同時クライアントレス SSL VPN セッションの最大数を設定する。

手順

- ステップ 1 クライアントレスアクセス用のグループポリシーを設定または作成するには、**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Group Policies]** ペインを選択します。
- ステップ 2 **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Connection Profiles]** に移動します。
- 各 ASA インターフェイスの **[Allow Access]** をイネーブルにするか、オフに切り替えます。
インターフェイスのカラムには、設定されているインターフェイスのリストが表示されず、**[WebVPN Enabled]** フィールドに、インターフェイスのクライアントレス SSL VPN のステータスが表示されます。**[Yes]** の隣に緑のチェックマークが入っていると、クライアントレス SSL VPN はイネーブルになっています。**[No]** の横の赤色の丸は、クライアントレス SSL VPN がオフに切り替えられていることを示します。
 - [Port Setting]** をクリックし、クライアントレス SSL セッションに使用するポート番号 (1 ~ 65535) を入力します。デフォルトは 443 です。ポート番号を変更すると、現在のすべてのクライアントレス SSL VPN 接続が切断されるため、現在のユーザは再接続する必要があります。また、ASDM セッションへの再接続を求めるメッセージが表示されます。
- ステップ 3 **[Configuration]** > **[Remote Access VPN]** > **[Advanced]** > **[Maximum VPN Sessions]** に移動し、**[Maximum Other VPN Sessions]** フィールドで、許可するクライアントレス SSL VPN セッションの最大数を入力します。

信頼できる証明書のプール

ASA は trustpool に信頼できる証明書をグループ化します。trustpool は、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には、Web ブラウザに備わっているものと同様の一連のデフォルト証明書が含まれています。これらの証明書は、管理者がアクティブ化するまで機能しません。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバは自身を証明するために認証局 (CA) が署名したデジタル証明書を提供します。Web ブラウザには、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が含まれています。

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、そのリモートサーバが信頼できるか、および適切なリモートサーバに接続しているかを確認することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局 (CA) 証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

[Configuration] > **[Remote Access VPN]** > **[Certificate Management]** > **[Trusted Certificate Pool]** で、https サイトへの SSL 接続に対して証明書検証を有効にすることができます。また、信頼できる証明書プール内の証明書も管理できます。



(注) ASA trustpool は Cisco IOS trustpool に類似していますが、同一のものではありません。

HTTP サーバ検証の有効化

手順

- ステップ 1 ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択します。
- ステップ 2 [Enable SSL Certificate Check] チェックボックスをオンにします。
- ステップ 3 サーバを検証できなかった場合は、[Disconnect User From HTTPS Site] をクリックして切断します。または、[Allow User to Proceed to HTTPS Site] をクリックして、チェックが失敗した場合でも、ユーザが接続を継続できるようにします。
- ステップ 4 [Apply] をクリックして変更内容を保存します。

証明書のバンドルのインポート

次の形式のいずれかで、さまざまな場所から個々の証明書または証明書のバンドルをインポートできます。

- pkcs7 構造でラップされた DER 形式の x509 証明書。
- PEM 形式 (PEM ヘッダーに囲まれた) の連結した x509 証明書のファイル。

手順

- ステップ 1 ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択します。
- ステップ 2 [Import Bundle] をクリックします。
- ステップ 3 バンドルの場所を選択します。
 - バンドルがコンピュータに保存されている場合は、[Import From a File] をクリックし、[Browse Local Files] をクリックして、バンドルを選択します。
 - バンドルが ASA フラッシュ ファイル システムに保存されている場合は、[Import From Flash] をクリックし、[Browse Flash] をクリックしてファイルを選択します。
 - バンドルがサーバでホストされている場合は、[Import From a URL] をクリックしてリストからプロトコルを選択し、フィールドに URL を入力します。

- 署名検証が失敗したり、バンドルをインポートできない場合に、バンドルをインポートするように設定して、後で個別の証明書エラーを修正します。証明書のいずれかに失敗した場合はバンドル全体が失敗するように、チェックボックスをオフにします。

ステップ 4 [Import Bundle] をクリックします。または、[Cancel] をクリックして変更を破棄します。

(注) [Remove All Downloaded Trusted CA Certificates Prior to Import] チェックボックスをオンにして、新しいバンドルをインポートする前に trustpool をクリアします。

trustpool のエクスポート

trustpool を正しく設定したら、プールをエクスポートする必要があります。これにより、このポイントまで（たとえばエクスポート後に trustpool に追加された証明書を削除する場合など）trustpool を復元できます。ASA フラッシュファイルシステムまたはローカルファイルシステムにプールをエクスポートできます。

ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Export Pool] をクリックします。

手順

ステップ 1 [Export to a File] をクリックします。

ステップ 2 [Browse Local Files] をクリックします。

ステップ 3 trustpool を保存するフォルダを選択します。

ステップ 4 [File Name] ボックスに、trustpool の一意の覚えやすい名前を入力します。

ステップ 5 [Select] をクリックします。

ステップ 6 [Export Pool] をクリックして、ファイルを保存します。または、[Cancel] をクリックして保存を停止します。

証明書の削除

すべての証明書を削除するには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Clear Pool] をクリックします。



(注) trustpool をクリアする前に、現在の設定を復元できるように、現在の trustpool をエクスポートする必要があります。

信頼できる証明書プールのポリシーの編集

手順

-
- ステップ 1** [Revocation Check] : プール内の証明書が失効しているかどうかをチェックするように設定し、さらに、失効のチェックに失敗した場合に、CLR または OCSP のいずれを使用するか、および証明書を無効にするかどうかを選択するように設定します。
- ステップ 2** [Certificate Matching Rules] : 失効または期限切れのチェックから除外する証明書マップを選択します。証明書マップは、AnyConnect またはクライアントレス SSL 接続プロファイル（別名「トンネルグループ」）に証明書をリンクします。
- これらの証明書マップの詳細については、[証明書/接続プロファイルマップのルール（155 ページ）](#) を参照してください。
- ステップ 3** [CRL Options] : CRL キャッシュの更新頻度を 1 ～ 1440 分（24 時間）の間隔で指定します。
- ステップ 4** [Automatic Import] : シスコでは、信頼済み CA の「デフォルト」のリストを定期的に更新しています。[Enable Automatic Import] をオンにして、デフォルト設定を保持するように指定した場合、ASA は 24 時間ごとにシスコのサイトで信頼済み CA の最新リストをチェックします。リストが変更されると、ASA は新しいデフォルトの信頼済み CA リストをダウンロードしてインポートします。
-

trustpool の更新

次のいずれかの条件が満たされる場合は、trustpool を更新する必要があります。

- trustpool の証明書が期限切れまたは再発行されている。
- 公開された CA 証明書のバンドルに、特定のアプリケーションに必要な追加の証明書が含まれている。

完全な更新によって、trustpool のすべての証明書が置き換えられます。

実用的な更新では、新しい証明書を追加したり、既存の証明書を置き換えることができます。

証明書のバンドルの削除

trustpool をクリアすると、デフォルトのバンドルではないすべての証明書が削除されます。

デフォルトのバンドルは削除できません。trustpool をクリアするには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Clear Pool] をクリックします。

信頼できる証明書プールのポリシーの編集

手順

-
- ステップ 1** [Revocation Check] : プール内の証明書が失効しているかどうかをチェックするように設定し、さらに、失効のチェックに失敗した場合に、CLR または OCSP のいずれを使用するか、および証明書を無効にするかどうかを選択するように設定します。
- ステップ 2** [Certificate Matching Rules] : 失効または期限切れのチェックから除外する証明書マップを選択します。証明書マップは、AnyConnect またはクライアントレス SSL 接続プロファイル (別名「トンネルグループ」) に証明書をリンクします。
- これらの証明書マップの詳細については、[証明書/接続プロファイルマップのルール \(155 ページ\)](#) を参照してください。
- ステップ 3** [CRL Options] : CRL キャッシュの更新頻度を 1 ~ 1440 分 (24 時間) の間隔で指定します。
- ステップ 4** [Automatic Import] : シスコでは、信頼済み CA の「デフォルト」のリストを定期的に更新しています。[Enable Automatic Import] をオンにして、デフォルト設定を保持するように指定した場合、ASA は 24 時間ごとにシスコのサイトで信頼済み CA の最新リストをチェックします。リストが変更されると、ASA は新しいデフォルトの信頼済み CA リストをダウンロードしてインポートします。
-

Java Code Signer

コード署名により、デジタル署名が、実行可能なコードそのものに追加されます。このデジタル署名には、さまざまな情報が保持されています。署名以降にそのコードが変更されていないことを保証するだけでなく、署名者を認証する場合に使用することもできます。

コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

Java オブジェクト署名で使用する、設定された証明書をドロップダウン リストから選択します。

Java Code Signer を設定するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Java Code Signer] を選択します。

クライアントレス SSL VPN が変換した Java オブジェクトは、その後、トラストポイントに関連付けられた PKCS12 デジタル証明書により署名されます。[Java Trustpoint] ペインでは、指定されたトラストポイントの場所から PKCS12 証明書とキー関連情報を使用するようにクライアントレス SSL VPN Java オブジェクト署名機能を設定できます。

トラストポイントをインポートするには、[Configuration] > [Properties] > [Certificate] > [Trustpoint] > [Import] を選択します。

プラグインへのブラウザアクセスの設定

ブラウザプラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA では、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合があります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- (Cisco 配布のプラグイン限定) URL で指定された jar ファイルのアンパック
- ASA ファイル システムにファイルを書き込みます。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、メインメニュー オプションと、ポータル ページの [Address] フィールドの横にあるドロップダウン リストについてのオプションを追加します。

次に、以降の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューとアドレス フィールドの変更点を示します。

表 5: クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加される メイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix MetaFrame Services	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	セキュア シェル	ssh://
	Telnet services (v1 および v2 をサポート)	telnet://
vnc	Virtual Network Computing services	vnc://

* 推奨されないプラグイン。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

プラグインは、シングルサインオン（SSO）をサポートします。

プラグインに伴う前提条件

- プラグインへのリモートアクセスを実現するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマークエントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属していません。
- プラグインを使用するには、ActiveX または Oracle Java ランタイム環境（JRE）が必要です。バージョン要件については、『[サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ](#)』の互換性マトリクスを参照してください。

プラグインの使用上の制限



(注) Remote Desktop Protocol プラグインでは、セッションブローカを使用したロードバランシングはサポートされていません。プロトコルによるセッションブローカからのリダイレクションの処理方法のため、接続に失敗します。セッションブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングルサインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと同じクレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメインパスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。
- ステートフルフェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- ステートフルフェールオーバーではなくステートレスフェールオーバーを使用する場合、ブックマーク、カスタマイゼーション、ダイナミック アクセス ポリシーなどのクライアントレス機能は、フェールオーバー ASA ペア間で同期されません。フェールオーバーの発生時に、これらの機能は動作しません。

プラグインのためのセキュリティ アプライアンスの準備

始める前に

ASA インターフェイスでクライアントレス SSL VPN がイネーブルになっていることを確認します。

SSL 証明書的一般名 (CN) として IP アドレスを指定しないでください。リモートユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

手順

ステップ 1 クライアントレス SSL VPN が ASA で有効になっているかどうかを示します。

show running-config

ステップ 2 ASA インターフェイスに SSL 証明書をインストールして、リモート ユーザ接続の完全修飾ドメイン名 (FQDN) を指定します。

シスコによって再配布されたプラグインのインストール

シスコでは、Java ベースのオープン ソース コンポーネントを再配布しています。これは、クライアントレス SSL VPN セッションで Web ブラウザのプラグインとしてアクセスされるコンポーネントで、次のものがあります。

始める前に

ASA のインターフェイスでクライアントレス SSL VPN がイネーブルになっていることを確認します。そのためには、**show running-config** コマンドを入力します。

表 6: シスコが再配布しているプラグイン

プロトコル	説明	再配布しているプラグインのソース *
RDP	<p>Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。</p> <p>リモートデスクトップ ActiveX コントロールをサポートします。</p> <p>RDP および RDP2 の両方をサポートするこのプラグインを使用することをお勧めします。RDP および RDP2 のバージョン 5.1 へのバージョンアップだけがサポートされています。バージョン 5.2 以降はサポートされていません。</p>	http://properjavardp.sourceforge.net/
RDP2	<p>Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。</p> <p>リモートデスクトップ ActiveX コントロールをサポートします。</p> <p>この古いプラグインは、RDP2 だけをサポートします。このプラグインを使用することは推奨しません。代わりに、上記の RDP プラグインを使用してください。</p>	

プロトコル	説明	再配布しているプラグインのソース *
SSH	Secure Shell-Telnet プラグインにより、リモートユーザはリモートコンピュータへの Secure Shell (v1 または v2) または Telnet 接続を確立できます。 キーボードインタラクティブ認証は JavaSSH ではサポートされていないため、(異なる認証メカニズムの実装に使用される) SSH プラグインではサポートされません。	http://javassh.org/
VNC	Virtual Network Computing プラグインを使用すると、リモートユーザはリモートデスクトップ共有 (VNC サーバまたはサービスとも呼ばれる) をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。このバージョンでは、テキストのデフォルトの色が変更されています。また、フランス語と日本語のヘルプファイルもアップデートされています。	http://www.tightvnc.com/

*展開の設定と制限については、プラグインのマニュアルを参照してください。

これらのプラグインは、[Cisco Adaptive Security Appliance Software Download](#) サイトで入手できます。

手順

-
- ステップ 1** ASA との ASDM セッションを確立するために使用するコンピュータに、plugins という名前の一時ディレクトリを作成し、シスコの Web サイトから、必要なプラグインを plugins ディレクトリにダウンロードします。
- ステップ 2** **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Client-Server Plug-ins]** を選択します。

このペインには、クライアントレス SSL セッションで使用可能な現在ロードされているプラグインが表示されます。これらのプラグインのハッシュおよび日付も表示されます。

ステップ 3 [Import] をクリックします。

ステップ 4 [Import Client-Server Plug-in] ダイアログボックスのフィールド値を入力するには、次の説明を参考にしてください。

- [Plug-in Name] : 次のいずれかの値を入力します。
 - **ica**。Citrix MetaFrame または Web Interface サービスへのプラグインアクセスを提供する場合に指定します。
 - Remote Desktop Protocol サービスへのプラグインアクセスを提供するには、**rdp** を入力します。
 - セキュア シェル サービスと Telnet サービスの両方にプラグインアクセスを提供するには、**ssh,telnet** を入力します。
 - Virtual Network Computing サービスにプラグインアクセスを提供するには、**vnc** を入力します。

(注) このメニューの、記載のないオプションは実験的なものであるため、サポートされていません。

- [Select the location of the plugin file] : 次のいずれかのオプションをクリックし、テキストフィールドにパスを挿入します。
 - [Local computer] : 関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Local Files] をクリックしてプラグインを選択し、プラグインを選択して [Select] をクリックします。
 - [Flash file system] : 関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Flash] をクリックしてプラグインを選択し、プラグインを選択して [OK] をクリックします。
 - [Remote Server] : リモートサーバで実行されているサービスに応じて、関連付けられた [Path] 属性の横にあるドロップダウンメニューで [ftp]、[tftp]、または [HTTP] を選択します。隣にあるテキストフィールドに、サーバのホスト名またはアドレスおよびプラグインへのパスを入力します。

ステップ 5 [Import Now] をクリックします。

ステップ 6 [Apply] をクリックします。

これで、以降のクライアントレス SSL VPN セッションでプラグインが使用できるようになりました。

Citrix XenApp Server へのアクセスの提供

サードパーティのプラグインに、クライアントレス SSL VPN ブラウザ アクセスを提供する方法の例として、この項では、Citrix XenApp Server Client にクライアントレス SSL VPN のサポートを追加する方法について説明します。

ASA に Citrix プラグインがインストールされている場合、クライアントレス SSL VPN ユーザは、ASA への接続を使用して Citrix XenApp サービスにアクセスできます。

ステートフル フェールオーバーでは、Citrix プラグインを使用して確立されたセッションが保持されません。フェールオーバー後に Citrix ユーザを再認証する必要があります。

Citrix プラグインの作成とインストール

始める前に

セキュリティ アプリケーションをプラグイン用に準備する必要があります。

(Citrix) 「セキュア ゲートウェイ」を使用しないモードで動作するように Citrix Web Interface ソフトウェアを設定する必要があります。この設定をしないと、Citrix クライアントは Citrix XenApp Server に接続できません。

手順

-
- ステップ 1** シスコのソフトウェア ダウンロード Web サイトから [ica-plugin.zip](#) ファイルをダウンロードします。
- このファイルには、Citrix プラグインを使用するためにシスコがカスタマイズしたファイルが含まれています。
- ステップ 2** Citrix のサイトから [Citrix Java クライアント](#) をダウンロードします。
- Citrix Web サイトのダウンロード領域で [Citrix Receiver]、[Receiver for Other Platforms] の順に選択し、[Find] をクリックします。[Receiver for Java] ハイパーリンクをクリックしてアーカイブをダウンロードします。
- ステップ 3** アーカイブから次のファイルを抽出し、それらを ica-plugin.zip ファイルに追加します。
- JICA-configN.jar
 - JICAEngN.jar
- ステップ 4** Citrix Java クライアントに含まれている EULA によって、Web サーバ上にクライアントを配置するための権限が与えられていることを確認します。
- ステップ 5** ASDM を使用するか、または特権 EXEC モードで次の CLI コマンドを入力して、プラグインをインストールします。

```
import webvpn plug-in protocol ica URL
```

URL は、ホスト名（または IP アドレス）と ica-plugin.zip ファイルへのパスです。

(注) Citrix セッションに SSO サポートを提供する場合は、ブックマークの追加は必須です。次のように、ブックマークで便利な表示を提供する URL パラメータを使用することを推奨します。

`ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768`

ステップ 6 SSL VPN クライアントレスセッションを確立し、ブックマークをクリックするか、Citrix サーバの URL を入力します。

必要に応じて、『[Client for Java Administrator's Guide](#)』を参照してください。

ポート転送の設定

ポート転送により、ユーザはクライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションにアクセスできます。TCP ベースのアプリケーションには次のようなものがあります。

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP (FTP over SSH)
- SSH
- Telnet
- Windows Terminal Service
- XDDTS

その他の TCP ベースのアプリケーションも動作する可能性はありますが、シスコではテストを行っていません。UDP を使用するプロトコルは動作しません。

ポート転送は、クライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションをサポートするためのレガシーテクノロジーです。ポート転送テクノロジーをサポートする設定を事前に構築している場合は、ポート転送の使用を選択することもできます。

ポート転送の代替方法として次のことを検討してください。

- スマート トンネル アクセスを使用すると、ユーザには次のような利点があります。
 - スマート トンネルは、プラグインよりもパフォーマンスが向上します。

- ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザエクスペリエンスが簡略化されます。
- ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。
- ポート転送およびスマート トンネル アクセスとは異なり、プラグインでは、クライアント アプリケーションをリモート コンピュータにインストールする必要がありません。

ASA でポート転送を設定する場合は、アプリケーションが使用するポートを指定します。スマート トンネル アクセスを設定する場合は、実行ファイルまたはそのパスの名前を指定します。

ポート転送の前提条件

- ポート転送（アプリケーションアクセス）およびデジタル証明書をサポートするために、リモート コンピュータに Oracle Java ランタイム環境（JRE）8u131 b11、7u141 b11、6u151 b10 以降がインストールされていることを確認します。
- macOS 10.12 上で Safari を使用しているブラウザベースのユーザは、ASA の URL と共に使用するためにクライアント証明書を特定する必要があります。Safari の URL 解釈方法により、1 回目は末尾にスラッシュを含め、もう 1 回はスラッシュを含めずに指定します。次に例を示します。
 - `https://example.com/`
 - `https://example.com`
- ポート転送またはスマート トンネルを使用する Microsoft Windows 7 SP1 以降のユーザは、ASA の URL を信頼済みサイトゾーンに追加します。信頼済みサイトゾーンにアクセスするには、Internet Explorer を起動し、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Windows 7 SP1（以降の）ユーザは保護モードをオフに切り替えるとスマート トンネル アクセスを使用することもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法の使用はお勧めしません。

ポート転送に関する制限事項

- ポート転送は、スタティック TCP ポートを使用する TCP アプリケーションのみをサポートしています。ダイナミック ポートまたは複数の TCP ポートを使用するアプリケーションはサポートしていません。たとえば、ポート 22 を使用する SecureFTP は、クライアントレス SSL VPN のポート転送を介して動作しますが、ポート 20 と 21 を使用する標準 FTP は動作しません。
- ポート転送は、UDP を使用するプロトコルをサポートしていません。

- ポート転送は Microsoft Outlook Exchange (MAPI) プロキシをサポートしていません。しかし、Microsoft Outlook Exchange Server と連携することにより、Microsoft Office Outlook のスマート トンネルサポートを設定することができます。
- ステートフル フェールオーバーでは、Application Access (ポート転送またはスマート トンネル アクセス) を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- ポート転送は、携帯情報端末 (PDA) への接続はサポートしていません。
- ポート転送を使用するには、Java アプレットをダウンロードしてローカルクライアントを設定する必要があります。これには、ローカルシステムに対する管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

Java アプレットは、エンドユーザの HTML インターフェイスにあるアプレット独自のウィンドウに表示されます。このウィンドウには、ユーザが使用できる転送ポートのリストの内容、アクティブなポート、および送受信されたトラフィック量 (バイト単位) が表示されます。

- ローカル IP アドレス 127.0.0.1 が使用されており、ASA からのクライアントレス SSL VPN 接続によってそれを更新できない場合、ポート転送アプレットでは、ローカルポートとリモートポートが同一のものとして表示されます。その結果、ASA は、127.0.0.2、127.0.0.3 など、ローカルプロキシ ID の新しい IP アドレスを作成します。hosts ファイルを変更して異なるループバックを使用できるため、リモートポートはアプレットでローカルポートとして使用されます。接続するには、ポートを指定せずにホスト名を指定して Telnet を使用します。正しいローカル IP アドレスをローカル ホスト ファイルで使用できます。

ポート転送用の DNS の設定

ポート転送機能は、解決および接続のために、リモートサーバのドメイン名またはその IP アドレスを ASA に転送します。つまり、ポート転送アプレットは、アプリケーションからの要求を受け入れて、その要求を ASA に転送します。ASA は適切な DNS クエリーを作成し、ポート転送アプレットの代わりに接続を確立します。ポート転送アプレットは、ASA に対する DNS クエリーだけを作成します。ポート転送アプレットはホスト ファイルをアップデートして、ポート転送アプリケーションが DNS クエリーを実行したときに、クエリーがループバック アドレスにリダイレクトされるようにします。

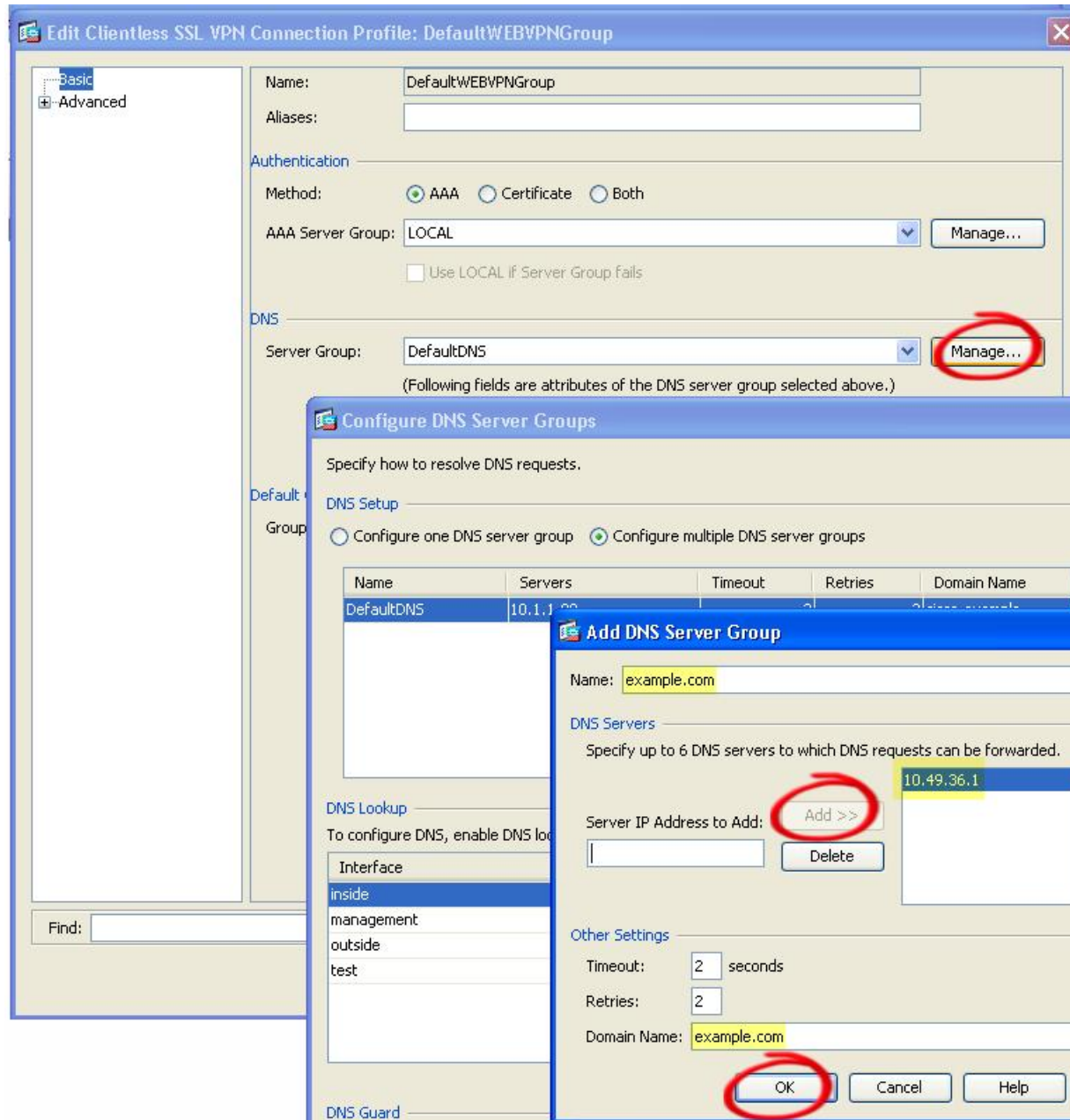
手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] の順にクリックします。

デフォルトのクライアントレス SSL VPN グループ エントリは、クライアントレス接続に使用されるデフォルトの接続プロファイルです。

- ステップ 2** 設定でクライアントレス接続に対してデフォルトのクライアントレス SSL VPN グループ エントリを使用する場合は、そのエントリを強調表示し、[Edit] をクリックします。エントリを使用しない場合は、設定でクライアント接続に対して使用する接続プロファイルを強調表示し、[Edit] をクリックします。
- ステップ 3** [DNS] 領域にスキャンし、ドロップダウン リストから DNS サーバを選択します。ドメイン名をメモしておきます。使用する DNS サーバが ASDM に表示されている場合は、残りのステップを飛ばし、次のセクションに移動します。ポート転送リストのエントリを設定する際、リモートサーバの指定時には、同じドメイン名を入力する必要があります。コンフィギュレーションに DNS サーバがない場合は、残りのステップを続けます。
- ステップ 4** [DNS] 領域で [Manage] をクリックします。
- ステップ 5** [Configure Multiple DNS Server Groups] をクリックします。
- ステップ 6** [Add] をクリックします。
- ステップ 7** [Name] フィールドに新しいサーバ グループ名を入力し、IP アドレスとドメイン名を入力します。

図 8: ポート転送の DNS サーバ値の例



入力したドメイン名を書き留めます。後ほど、ポート転送エントリを設定する際、リモートサーバを指定するために必要になります。

- ステップ 8** [Connection Profiles] ウィンドウが再度アクティブになるまで、**OK** をクリックします。
- ステップ 9** 設定でクライアントレス接続に使用する残りの接続プロファイルすべてに対して、手順を繰り返します。

ステップ 10 [適用 (Apply)] をクリックします。

ポート転送エントリの追加と編集

[Add/Edit Port Forwarding Entry] ダイアログボックスでは、クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションを指定できます。これらのウィンドウで属性に値を割り当てるには、次の手順を実行します。

始める前に

トンネルを確立して IP アドレスを解決するには、[Remote Server] パラメータに割り当てた DNS 名が [Domain Name] および [Server Group] パラメータと一致する必要があります。[Domain] および [Server Group] パラメータのデフォルト設定は、いずれも DefaultDNS です。

手順

- ステップ 1 [Add] をクリックします。
- ステップ 2 アプリケーションが使用する TCP ポート番号を入力します。ローカル ポート番号は、リスト名ごとに 1 度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024～65535 の範囲にあるポート番号を使用します。
- ステップ 3 リモートサーバのドメイン名または IP アドレスを入力します。特定の IP アドレスに対してクライアントアプリケーションを設定しなくて済むよう、ドメイン名を使用することをお勧めします。
- ステップ 4 そのアプリケーション用の well-known ポート番号を入力します。
- ステップ 5 アプリケーションの説明を入力します。最大で 64 文字まで指定可能です。
- ステップ 6 (任意) ポート転送リストを強調表示し、[Assign] をクリックして、選択したリストを 1 つ以上のグループポリシー、ダイナミック アクセス ポリシー、またはユーザポリシーに割り当てます。

ポート フォワーディング リストの割り当て

クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションの名前付きリストを追加または編集できます。グループポリシーとユーザ名ごとに、次のいずれかを行うようにクライアントレス SSL VPN を設定できます。



(注) これらのオプションは、各グループポリシーとユーザ名に対して互いに排他的です。1 つだけ使用してください。

- ユーザのログイン時に自動的にポートフォワーディングアクセスを開始する。
- ユーザのログイン時にポートフォワーディングアクセスをイネーブル化する。ただし、ユーザはクライアントレス SSL VPN ポータルページの [Application Access] > [Start Applications] を使用して、ポートフォワーディングを手動で開始する必要がある。

手順

ステップ 1 リストの英数字の名前を指定します。最大で 64 文字まで指定可能です。

ステップ 2 アプリケーションのトラフィックを受信するローカルポートを入力します。ローカルポート番号は、リスト名ごとに 1 度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024 ~ 65535 の範囲にあるポート番号を使用します。

(注) リモートサーバの IP アドレスまたは DNS 名を入力します。特定の IP アドレスに対してクライアントアプリケーションを設定しなくて済むよう、ドメイン名を使用することをお勧めします。

ステップ 3 アプリケーションのトラフィックを受信するリモートポートを入力します。

ステップ 4 TCP アプリケーションの説明を入力します。最大で 64 文字まで指定可能です。

ポートフォワーディングのイネーブル化と切り替え

デフォルトでは、ポートフォワーディングはオフになっています。

ポートフォワーディングをイネーブルにした場合、ユーザはクライアントレス SSL VPN ポータルページの [Application Access] > [Start Applications] を使用して、手動でポートフォワーディングを開始する必要があります。

ファイルアクセスの設定

クライアントレス SSL VPN は、リモートユーザに HTTPS ポータルページを提供しています。このページは、ASA で実行するプロキシ CIFS クライアントまたは FTP クライアント（あるいはその両方）と連動しています。クライアントレス SSL VPN は、CIFS または FTP を使用して、ユーザが認証の要件を満たしているファイルのプロパティがアクセスを制限しない限り、ネットワーク上のファイルへのネットワークアクセスをユーザに提供します。CIFS クライアントおよび FTP クライアントは透過的です。クライアントレス SSL VPN から送信されるポータルページでは、ファイルシステムに直接アクセスしているかのように見えます。

ユーザがファイルのリストを要求すると、クライアントレス SSL VPN は、そのリストが含まれるサーバの IP アドレスをマスターブラウザに指定されているサーバに照会します。ASA はリストを取得して、ポータルページ上のリモートユーザに送信します。

クライアントレス SSL VPN は、ユーザの認証要件とファイルのプロパティに応じて、ユーザが次の CIFS および FTP の機能呼び出すことができるようにします。

- ドメインとワークグループ、ドメインまたはワークグループ内のサーバ、サーバ内部の共有、および共有部分またはディレクトリ内のファイルのナビゲートとリスト。
- ディレクトリの作成。
- ファイルのダウンロード、アップロード、リネーム、移動、および削除。

ポータルページのメニュー内またはクライアントレス SSL VPN セッション中に表示されるツールバー上にある、[Browse Networks] をリモートユーザがクリックすると、ASA は、通常、ASA と同じネットワーク上またはこのネットワークからアクセス可能な場所にある、マスターブラウザ、WINS サーバ、または DNS サーバを使用して、サーバリストをネットワークに照会します。

マスターブラウザまたは DNS サーバは、クライアントレス SSL VPN がリモートユーザに提供するネットワーク上のリソースのリストを、ASA 上の CIFS/FTP クライアントに表示します。



- (注) ファイルアクセスを設定する前に、ユーザアクセス用のサーバに共有を設定する必要があります。

CIFS ファイル アクセスの要件と制限事項

ユーザが \\server\share\subfolder\personal フォルダにアクセスするには、少なくとも、共有自体を含めたすべての親フォルダに対する読み取り権限を持っている必要があります。

CIFS ディレクトリとローカルデスクトップとの間でファイルをコピーアンドペーストするには、[Download] または [Upload] を使用します。[Copy] ボタンおよび [Paste] ボタンはリモート間のアクションのみで使用でき、ローカルからリモートまたはリモートからローカルへのアクションには使用できません。

Web フォルダからワークステーションのフォルダにファイルをドラッグアンドドロップすると、一時ファイルのように見ることがあります。ビューを更新し、転送されたファイルを表示するには、ワークステーションのフォルダを更新します。

CIFS ブラウズサーバ機能は、2 バイト文字の共有名（13 文字を超える共有名）をサポートしていません。これは、表示されるフォルダのリストに影響を与えるだけで、フォルダへのユーザアクセスには影響しません。回避策として、2 バイトの共有名を使用する CIFS フォルダのブックマークを事前に設定するか、ユーザが `cifs://server/<long-folder-name>` 形式でフォルダの URL またはブックマークを入力します。次に例を示します。

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

ファイルアクセスのサポートの追加



(注) この手順では、マスターブラウザおよび WINS サーバを指定する方法について説明します。代わりに、ASDM を使用して、ファイル共有へのアクセスを提供する URL リストとエントリーを設定することもできます。

ASDM での共有の追加には、マスターブラウザまたは WINS サーバは必要ありません。ただし、Browse Networks リンクへのサポートは提供されません。nbns-server コマンドを入力するときは、ホスト名または IP アドレスを使用して ServerA を参照できます。ホスト名を使用する場合、ASA はホスト名を IP アドレスに解決することを DNS サーバに要求します。

SharePoint アクセスのためのクロックの正確性の確保

ASA 上のクライアントレス SSL VPN サーバは、クッキーを使用して、エンドポイントの Microsoft Word などのアプリケーションと対話します。ASA の時間が正しくないと、SharePoint サーバ上の文書にアクセスしたときに、ASA で設定されたクッキーの有効期間によって Word が正常に機能しなくなる可能性があります。このような誤作動を回避するには、ASA クロックを正しく設定します。NTP サーバと時間をダイナミックに同期させるように、ASA を設定することをお勧めします。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で「日付と時刻の設定」に関する項を参照してください。

Virtual Desktop Infrastructure (VDI)

ASA は、Citrix サーバおよび VMware VDI サーバへの接続をサポートします。

- Citrix の場合、ASA ではクライアントレス ポータルを介してユーザの実行中の Citrix Receiver へアクセスできます。
- VMware は、(スマート トンネル) のアプリケーションとして設定されます。

VDI サーバには、他のサーバアプリケーションのように、クライアントレス ポータルのブックマークを介してアクセスできます。

VDI の制限事項

- 自動サインオンの場合、証明書またはスマートカードを使用する認証はサポートされません。これは、これらの認証形式では間にある ASA を許可しないためです。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。

- スタンドアロン モバイル クライアントを使用している場合は、クライアント証明書の確認、二重認証、内部パスワードと CSD（Vault だけでなく、すべての CSD）はサポートされません。

Citrix モバイルのサポート

Citrix Receiver を実行しているモバイルユーザは、次を実行して Citrix サーバに接続できます。

- AnyConnect で ASA に接続してから Citrix サーバに接続する。
- AnyConnect クライアントを使用せずに ASA を介して Citrix サーバに接続する。ログオンクレデンシャルには次を含めることができます。
 - Citrix ログオン画面の接続プロファイルのエイリアス（トンネルグループエイリアスとも呼ばれる）。VDI サーバは、それぞれ別の権限と接続設定を備えた複数のグループポリシーを持つことができます。
 - RSA サーバが設定されている場合は RSA SecureID トークンの値。RSA サポートには、無効なエントリ用の次のトークンと、最初の PIN または期限切れ PIN 用の新しい PIN を入力するための次のトークンが含まれています。

Citrix の制限

証明書の制限

- 証明書/スマートカード認証は自動サインオンの手段としてはサポートされていません。
- クライアント証明書の確認および CSD はサポートされていません。
- 証明書の Md5 署名は、iOS の既知の問題であるセキュリティ上の問題（<http://support.citrix.com/article/CTX132798>）から動作していません。
- SHA2 シグニチャは Citrix Web サイト（<http://www.citrix.com/>）の説明に従って Windows を除き、サポートされていません。
- 1024 以上のキー サイズはサポートされていません。

その他の制限

- HTTP リダイレクトはサポートされません。Citrix Receiver アプリケーションはリダイレクトでは機能しません。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。

Citrix Mobile Receiver のユーザ ログオンについて

Citrix サーバに接続しているモバイルユーザのログオンは、ASA が Citrix サーバを VDI サーバとして設定したか、または VDI プロキシサーバとして設定したかによって異なります。

Citrix サーバが VDI サーバとして設定されている場合：

1. AnyConnect Secure Mobility Client を使用し、VPN クレデンシャルで ASA に接続します。
2. Citrix Mobile Receiver を使用し、Citrix サーバクレデンシャルで Citrix サーバに接続します（シングルサインオンを設定している場合は、Citrix クレデンシャルは不要です）。

ASA が VDI プロキシサーバとして設定されている場合：

1. Citrix Mobile Receiver を使用し、VPN と Citrix サーバの両方のクレデンシャルを入力して ASA に接続します。最初の接続後、正しく設定されている場合は、以降の接続に必要なのは VPN クレデンシャルだけです。

Citrix サーバをプロキシするための ASA の設定

ASA を Citrix サーバのプロキシとして動作するように設定し、ASA への接続が Citrix サーバへの接続であるかのようにユーザに見せることができます。ASDM の VDI プロキシがイネーブルになっている場合は AnyConnect クライアントは不要です。次の手順は、エンドユーザから Citrix に接続する方法の概要を示します。

手順

-
- ステップ 1** モバイルユーザが Citrix Receiver を起動し、ASA の URL に接続します。
 - ステップ 2** Citrix のログイン画面で、XenApp サーバのクレデンシャルと VPN クレデンシャルを指定します。
 - ステップ 3** 以降、Citrix サーバに接続する場合に必要なのは、VPN クレデンシャルだけです。

XenDesktop および XenApp のプロキシとして ASA を使用すると Citrix Access Gateway は必要なくなります。XenApp サーバ情報が ASA に記録され、ASDM に表示されます。

Citrix サーバのアドレスおよびログイン クレデンシャルを設定し、グループ ポリシーまたはユーザ名にその VDI サーバを割り当てます。ユーザ名とグループ ポリシーの両方を設定した場合は、ユーザ名の設定によってグループ ポリシー設定がオーバーライドされます。

次のタスク

<http://www.youtube.com/watch?v=JMM2RzppaG8>：このビデオでは、ASA を Citrix プロキシとして使用する利点について説明します。

VDI サーバまたは VDI プロキシ サーバの設定

手順

-
- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] の順に選択します。
- ステップ 2** 1 つのサーバで、[Enable VDI Server Proxy] チェックボックスをオンにし、VDI サーバを設定します。
- ステップ 3** VDI サーバに複数のグループ ポリシーを割り当てるには、[Configure All VDI Servers] をオンにします。
- ステップ 4** [Add a VDI Server] を選択し、1 つ以上のグループ ポリシーを割り当てます。
-

グループ ポリシーへの VDI サーバの割り当て

VDI サーバを設定し、グループ ポリシーに割り当てる方法は次のとおりです。

- [VDI Access] ペインで VDI サーバを追加し、サーバにグループ ポリシーを割り当てる。
- グループ ポリシーに VDI サーバを追加する。

手順

-
- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] を参照します。
- ステップ 2** DfltGrpPolicy を編集し、左側のメニューから [More Options] メニューを展開します。
- ステップ 3** [VDI Access] を選択します。
- ステップ 4** [Add] または [Edit] をクリックして、VDI サーバの詳細を表示します。
- [Server (Host Name or IP Address)] : XenApp または XenDesktop サーバのアドレス。この値は、クライアントレス マクロにすることができます。
 - [Port Number (Optional)] : Citrix サーバに接続するためのポート番号。この値は、クライアントレス マクロにすることができます。
 - [Active Directory Domain Name] : 仮想化インフラストラクチャ サーバにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。
 - [Use SSL Connection] : サーバに SSL を使用して接続する場合は、チェックボックスをオンにします。
 - [Username] : 仮想化インフラストラクチャ サーバにログインするためのユーザ名。この値は、クライアントレス マクロにすることができます。

- [Password] : 仮想化インフラストラクチャ サーバにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。

クライアント/サーバ プラグインへのブラウザ アクセスの設定

[Client-Server Plug-in] テーブルには、ASA によってクライアントレス SSL VPN セッションのブラウザで使用可能になるプラグインが表示されます。

プラグインを追加、変更、または削除するには、次のいずれかを実行します。

- プラグインを追加するには、[Import] をクリックします。[Import Plug-ins] ダイアログボックスが開きます。
- プラグインを削除するには、そのプラグインを選択して [Delete] をクリックします。

ブラウザ プラグインのインストールについて

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA では、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合があります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- (Cisco 配布のプラグイン限定) URL で指定された jar ファイルのアンパック
- ASA ファイル システムの `cisco-config/97/plugin` ディレクトリにファイルを書き込みます。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、メインメニュー オプションと、ポータル ページの [Address] フィールドの横にあるドロップダウン リストについてのオプションを追加します。

次の表に、以降の項で説明するプラグインを追加したときの、ポータル ページのメインメニューとアドレス フィールドの変更点を示します。

表 7: クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加される メイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプシ ョン
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://



(注) セカンダリ ASA は、プライマリ ASA からプラグインを取得します。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。



(注) Java プラグインによっては、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインというステータスがレポートされることがあります。open-source プラグインは、ASA ではなくステータスをレポートします。

ブラウザ プラグインのインストールの前提条件

- セキュリティ アプライアンスでクライアントレス セッションがプロキシ サーバを使用するように設定している場合、プラグインは機能しません。



(注) Remote Desktop Protocol プラグインでは、セッションブローカを使用したロードバランシングはサポートされていません。プロトコルによるセッションブローカからのリダイレクションの処理方法のため、接続に失敗します。セッションブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングルサインオン (SSO) をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと同じクレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメインパスワード

ドなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。

- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマークエントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属していません。

ブラウザ プラグインのインストールに関する要件

- シスコでは、GNU 一般公的使用許諾 (GPL) に従い、変更を加えることなくプラグインを再配布しています。GPL により、これらのプラグインを直接改良できません。
- プラグインへのリモートアクセスを実現するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- ステートフルフェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- プラグインを使用するには、ブラウザで ActiveX または Oracle Java ランタイム環境 (JRE) がイネーブルになっている必要があります。64 ビットブラウザには、RDP プラグインの ActiveX バージョンはありません。

RDP プラグインのセットアップ

RDP プラグインをセットアップして使用するには、新しい環境変数を追加する必要があります。

手順

- ステップ 1** [My Computer] を右クリックし、[System Properties] を開いて [Advanced] タブを選択します。
- ステップ 2** [Advanced] タブで、[Environment Variables] ボタンを選択します。
- ステップ 3** [New User Variable] ダイアログボックスで、RF_DEBUG 変数を入力します。
- ステップ 4** [User variables] セクションの新しい環境変数を確認します。
- ステップ 5** バージョン 8.3 以前のクライアントレス SSL VPN のバージョンでクライアント コンピュータを使用していた場合、古い Cisco Portforwarder Control を削除してください。
C:/WINDOWS/Downloaded Program Files ディレクトリを開いて、Portforwarder Control を右クリックして、[Remove] を選択します。
- ステップ 6** Internet Explorer ブラウザのすべてのキャッシュをクリアします。
- ステップ 7** クライアントレス SSL VPN セッションを起動して、RDP ActiveX プラグインを使用して RDP セッションを確立します。

これで Windows アプリケーションのイベント ビューアでイベントを確認できるようになります。

プラグインのためのセキュリティ アプライアンスの準備

手順

ステップ 1 ASA インターフェイスでクライアントレス SSL VPN がイネーブルになっていることを確認します。

ステップ 2 リモート ユーザが完全修飾ドメイン名 (FQDN) を使用して接続する ASA インターフェイスに SSL 証明書をインストールします。

(注) SSL 証明書の一般名 (CN) として IP アドレスを指定しないでください。リモート ユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。



第 15 章

高度なクライアントレス SSL VPN のコンフィギュレーション

- [Microsoft Kerberos Constrained Delegation ソリューション \(331 ページ\)](#)
- [外部プロキシ サーバの使用法の設定 \(337 ページ\)](#)
- [クライアントレス SSL VPN セッションでの HTTPS の使用 \(339 ページ\)](#)
- [アプリケーションプロファイル カスタマイゼーション フレームワークの設定 \(340 ページ\)](#)
- [セッションの設定 \(347 ページ\)](#)
- [エンコーディング \(348 ページ\)](#)
- [コンテンツ キャッシングの設定 \(350 ページ\)](#)
- [Content Rewrite \(352 ページ\)](#)
- [クライアントレス SSL VPN を介した電子メールの使用 \(355 ページ\)](#)
- [ブックマークの設定 \(355 ページ\)](#)

Microsoft Kerberos Constrained Delegation ソリューション

Microsoft の Kerberos Constrained Delegation (KCD) は、プライベートネットワーク内の Kerberos で保護された Web アプリケーションへのアクセスを提供します。

Kerberos Constrained Delegation を機能させるために、ASA はソースドメイン (ASA が常駐するドメイン) とターゲットまたはリソースドメイン (Web サービスが常駐するドメイン) 間の信頼関係を確立する必要があります。ASA は、サービスにアクセスするリモートアクセスユーザの代わりに、ソースから宛先ドメインへの認証パスを横断し、必要なチケットを取得します。

このように認証パスを越えることは、クロスレルム認証と呼ばれます。クロスレルム認証の各フェーズにおいて、ASA は特定のドメインのクレデンシャルおよび後続ドメインとの信頼関係に依存しています。

KCD の機能

Kerberos は、ネットワーク内のエンティティのデジタル識別情報を検証するために、信頼できる第三者に依存しています。これらのエンティティ（ユーザ、ホストマシン、ホスト上で実行されるサービスなど）は、プリンシパルと呼ばれ、同じドメイン内に存在している必要があります。秘密キーの代わりに、Kerberos では、サーバに対するクライアントの認証にチケットが使用されます。チケットは秘密キーから導出され、クライアントのアイデンティティ、暗号化されたセッションキー、およびフラグで構成されます。各チケットはキー発行局によって発行され、ライフタイムが設定されます。

Kerberos セキュリティシステムは、エンティティ（ユーザ、コンピュータ、またはアプリケーション）を認証するために使用されるネットワーク認証プロトコルであり、情報の受け手として意図されたデバイスのみが復号化できるようにデータを暗号化することによって、ネットワーク伝送を保護します。クライアントレス SSL VPN ユーザに Kerberos で保護された Web サービスへの SSO アクセスを提供するように KCD を設定できます。このような Web サービスやアプリケーションの例として、Outlook Web Access (OWA)、SharePoint、および Internet Information Server (IIS) があります。

Kerberos プロトコルに対する 2 つの拡張機能として、プロトコル移行および制約付き委任が実装されました。これらの拡張機能によって、クライアントレス SSL VPN リモートアクセスユーザは、プライベートネットワーク内の Kerberos で認証されるアプリケーションにアクセスできます。

プロトコル移行機能は、ユーザ認証レベルでさまざまな認証メカニズムをサポートし、後続のアプリケーションレイヤでセキュリティ機能（相互認証や制約付き委任など）用に Kerberos プロトコルに切り替えることによって、柔軟性とセキュリティを向上させます。制約付き委任では、ドメイン管理者は、アプリケーションがユーザの代わりにを務めることができる範囲を制限することによって、アプリケーション信頼境界を指定して強制適用できます。この柔軟性は、信頼できないサービスによる危険の可能性を減らすことで、アプリケーションのセキュリティ設計を向上させます。

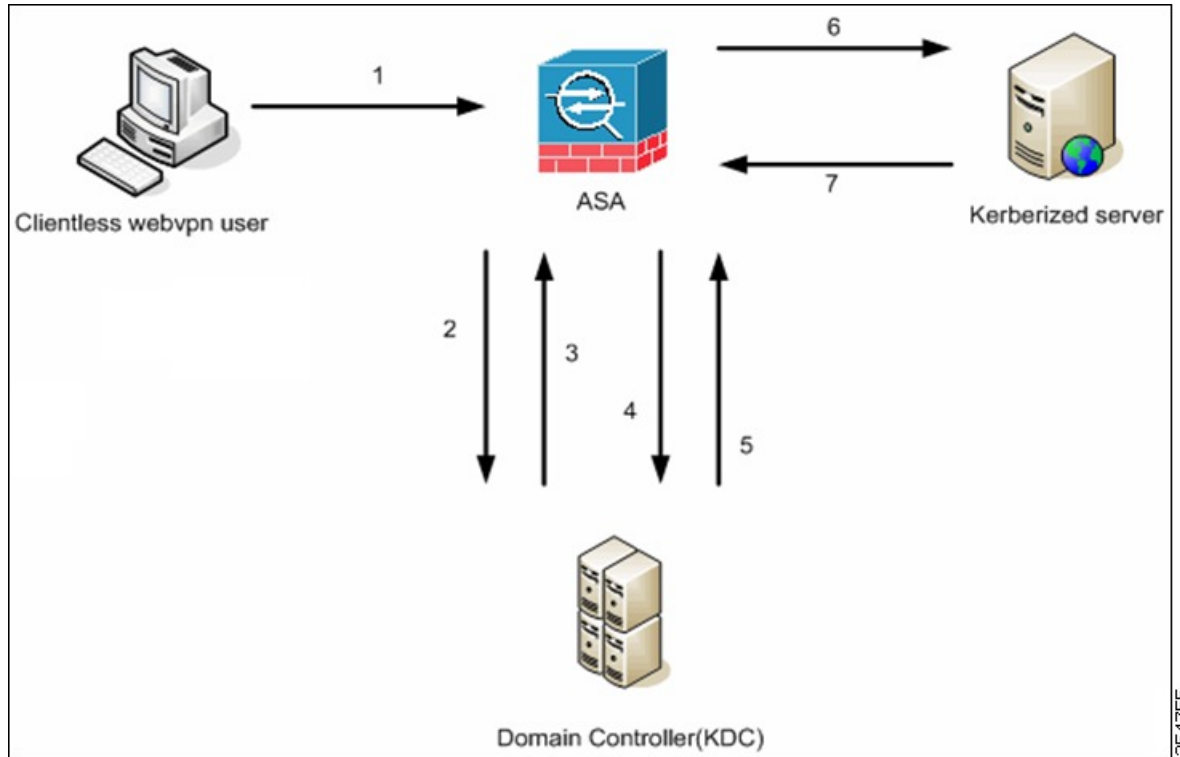
制約付き委任の詳細については、IETF の Web サイト (<http://www.ietf.org>) にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

次の図に、委任に対して信頼されたリソースにユーザがクライアントレスポータルによってアクセスするときに、直接的および間接的に体験するパケットおよびプロセスフローを示します。このプロセスは、次のタスクが完了していることを前提としています。

- ASA 上に設定された KCD
- Windows Active Directory への参加、およびサービスが委任に対して信頼されたことの確認
- Windows Active Directory ドメインのメンバーとして委任された ASA

図 9: KCD プロセス



(注) クライアントレス ユーザセッションは、ユーザに設定されている認証メカニズムを使用して ASA により認証されます (スマートカードクレデンシャルの場合、ASA はデジタル証明書の userPrincipalName を使用して、Windows Active Directory に対して LDAP 許可を実行します)。

1. 認証が成功すると、ユーザは ASA クライアントレス ポータル ページにログインします。ユーザは、URL をポータルページに入力するか、ブックマークをクリックして、Web サービスにアクセスします。この Web サービスで認証が必要な場合、サーバは ASA クレデンシャルの認証確認を行い、サーバがサポートしている認証方式のリストを送信します。



(注) クライアントレス SSL VPN の KCD は、すべての認証方式 (RADIUS、RSA/SDI、LDAP、デジタル証明書など) に対してサポートされています。次の AAA のサポートに関する表を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492

2. 認証確認時の HTTP ヘッダーに基づいて、ASA はサーバで Kerberos 認証が必要かどうかを判断します (これは SPNEGO メカニズムの一部です)。バックエンドサーバとの接続で Kerberos 認証が必要な場合、ASA は、ユーザに代わって、自身のサービスチケットをキー発行局に要求します。

- キー発行局は、要求されたチケットを ASA に返します。これらのチケットは ASA に渡されますが、ユーザの許可データが含まれています。ASA は、ユーザがアクセスする特定のサービス用の KCD からのサービスチケットを要求します。



(注) ステップ 1～3 では、プロトコル移行が行われます。これらのステップの後、Kerberos 以外の認証プロトコルを使用して ASA に対して認証を行うユーザは、透過的に、Kerberos を使用してキー発行局に対して認証されます。

- ASA は、ユーザがアクセスする特定のサービスのサービスチケットをキー発行局に要求します。
- キー発行局は、特定のサービスのサービス チケットを ASA に返します。
- ASA は、サービスチケットを使用して、Web サービスへのアクセスを要求します。
- Web サーバは、Kerberos サービス チケットを認証して、サービスへのアクセスを付与します。認証が失敗した場合は、適切なエラーメッセージが表示され、確認を求められます。Kerberos 認証が失敗した場合、予期された動作は基本認証にフォールバックします。

制約付き委任用の Kerberos サーバグループの作成

Kerberos Constrained Delegation を使用するには、まず、Kerberos AAA サーバグループを設定する必要があります。サーバグループには、Active Directory (AD) ドメインコントローラが含まれている必要があります。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Microsoft KCD Server] の順に選択します。

ステップ 2 [Constrained Delegation] ドロップダウンリストの [Kerberos Server Group] の横にある [New] をクリックします。

必要な Kerberos AAA サーバグループが設定済みの場合は、サーバグループを選択するだけで、この手順をスキップできます。

ステップ 3 [Server Group Name] フィールドにグループの名前を入力するか、デフォルトの名前のままにします。

ステップ 4 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバが非アクティブになった場合、そのサーバは、グループの他のすべてのサーバが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のす

すべてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。

Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 5 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 6 次のサーバを試す前にグループ内の AAA サーバでの AAA トランザクションの失敗の最大数を指定します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

ステップ 7 [Interface Name] で、AD ドメインコントローラへのアクセスに使用できるインターフェイスの名前を選択します。

ステップ 8 グループに追加するドメインコントローラの名前または IP アドレスを入力します。

ステップ 9 サーバへの接続試行のタイムアウト値を指定します。

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the retry interval) until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバは非アクティブ化され、ASA は別の AAA サーバ（設定されている場合）への要求の送信を開始します。

ステップ 10 サーバポートを指定します。サーバポートは、ポート番号 88、または ASA によって Kerberos サーバとの通信に使用される TCP ポートの番号です。

ステップ 11 再試行間隔を選択します。システムはこの時間待機してから接続要求を再試行します。1〜10 秒の範囲で選択できます。デフォルトは 10 秒です。

ステップ 12 Kerberos レルムを設定します。

Kerberos レルム名では数字と大文字だけを使用し、64 文字以内にする必要があります。Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レルムの Active Directory サーバ上で実行する場合は、**name** の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

ASA では、**name** に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

ステップ 13 [OK] をクリックします。

Kerberos Constrained Delegation (KCD) の設定

次の手順では、Kerberos Constrained Delegation (KCD) を実装する方法について説明します。

始める前に

- ドメインコントローラへのアクセス時に経由するインターフェイスで DNS ルックアップをイネーブルにします。認証委任方式として KCD を使用する場合は、ASA、ドメインコントローラ (DC)、委任しているサービスの間でホスト名解決と通信をイネーブルにするために、DNS が必要です。クライアントレス VPN の配置には、社内ネットワーク (通常は内部インターフェイス) を介した DNS ルックアップが必要です。

たとえば、**[Configuration] > [Device Management] > [DNS] > [DNS Client]** に移動し、**[DNS Lookup]** テーブルで内部インターフェイス行の **[DNS Enabled]** セルをクリックして、**[True]** を選択します。

- ドメインレルムを DNS ドメインとして使用して、Active Directory (AD) ドメインコントローラを DNS サーバとして使用するよう DNS を設定します。

たとえば、**[Configuration] > [Device Management] > [DNS] > [DNS Client]** に移動し、内部インターフェイスから 10.1.1.10 を **[Primary DNS Server]** として追加し、EXAMPLE.COM をドメイン名として追加します (サーバグループが複数ある場合は、DefaultDNS サーバグループを選択し、ドメインコントローラを追加します)。

手順

ステップ 1 **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Microsoft KCD Server]** の順に選択します。

ステップ 2 既存の Kerberos AAA サーバグループを選択するか、**[New]** をクリックして新しいグループを作成します。

新しいグループを作成する場合は、[制約付き委任用の Kerberos サーバグループの作成 \(334 ページ\)](#) を参照してください。

ステップ 3 **[Server Access Credentials]** で、AD ドメインに参加するために必要なオプションを設定します。

KCD 用に設定されている場合、ASA は Kerberos キーを取得するために、設定されたサーバとの AD ドメイン参加を開始します。これらのキーは、ASA がクライアントレス SSL VPN ユーザに代わってサービスチケットを要求するために必要です。

- [Username]**、**[Password]** : ドメインコントローラで定義された、ドメインに参加するために使用できるユーザ名、およびユーザアカウントのパスワード。ユーザアカウントには、ドメインにデバイスを追加するための管理者権限またはサービスレベル権限が必要です。

ステップ 4 (オプション) 必要に応じて、サーバグループ構成の設定を調整します。オプションの説明については、[制約付き委任用の Kerberos サーバグループの作成 \(334 ページ\)](#) を参照してください。

ステップ5 (オプション) Kerberos サーバグループテーブルでサーバを追加、編集、削除、またはテストします。Kerberos サーバのパラメータについては、[制約付き委任用の Kerberos サーバグループの作成 \(334 ページ\)](#) を参照してください。

Kerberos Constrained Delegation の監視

KCD を監視するには、次のコマンドを使用します。コマンドを入力するには、[Tools] > [Command Line Interface] または SSH セッションを使用します。

- **show webvpn kcd**

KCD の構成および参加ステータスを表示します。

```
ciscoasa# show webvpn kcd

KCD state:      Domain Join Complete
Kerberos Realm: EXAMPLE.COM
ADI version:    6.8.0_1252
Machine name:   ciscoasa
ADI instance:   root      1181  1178  0 15:35 ?          00:00:01 /asa/bin/start-adi
Keytab file:    -rw----- 1 root root 79 Jun 16 16:06 /etc/krb5.keytab
```

- **show aaa kerberos [username user_id]**

システム上のキャッシュされた Kerberos チケットを表示します。すべてのチケットを表示することも、特定のユーザのチケットだけを表示することもできます。

```
ASA# show aaa kerberos

Default Principal      Valid Starting      Expires              Service Principal
asa@example.COM        06/29/10 18:33:00    06/30/10 18:33:00
krbtgt/example.COM@example.COM
kcduser@example.COM    06/29/10 17:33:00    06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM    06/29/10 17:33:00    06/30/10 17:33:00
http/owa.example.com@example.COM
```

- **clear aaa kerberos tickets [username user_id]**

システム上のキャッシュされた Kerberos チケットをクリアします。すべてのチケットをクリアすることも、特定のユーザのチケットだけをクリアすることもできます。

外部プロキシ サーバの使用法の設定

[Proxies] ペインを使用して、外部プロキシサーバによって HTTP 要求と HTTPS 要求を処理するように ASA を設定します。これらのサーバは、ユーザとインターネットの仲介役として機能します。すべてのインターネットアクセスがユーザ制御のサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネットアクセスと管理制御が保証されます。



(注) HTTP および HTTPS プロキシサービスでは、PDA への接続をサポートしていません。

手順

- ステップ 1** [Use an HTTP Proxy Server] をクリックします。
- ステップ 2** IP アドレスまたはホスト名で HTTP プロキシサーバを識別します。
- ステップ 3** 外部 HTTP プロキシサーバのホスト名または IP アドレスを入力します。
- ステップ 4** HTTP 要求を受信するポートを入力します。デフォルトのポートは 80 です。
- ステップ 5** (任意) HTTP プロキシサーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
- * は、スラッシュ (/) とピリオド (.) を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。
 - ? は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
 - [x-y] は、x から y までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
 - ![x-y] は、範囲外の任意の 1 文字と一致します。
- ステップ 6** (任意) 各 HTTP プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
- ステップ 7** 各 HTTP 要求とともにプロキシサーバに送信されるパスワードを入力します。
- ステップ 8** HTTP プロキシサーバの IP アドレスを指定する方法の代替として、[Specify PAC file URL] を選択して、ブラウザにダウンロードするプロキシ自動コンフィギュレーションファイルを指定できます。ダウンロードが完了すると、PAC ファイルは JavaScript 機能を使用して各 URL のプロキシを識別します。隣接するフィールドに、**http://** を入力し、プロキシ自動設定ファイルの URL を入力します。**http://** の部分を省略すると、ASA はその URL を無視します。
- ステップ 9** HTTPS プロキシサーバを使用するかどうかを選択します。
- ステップ 10** クリックして、IP アドレスまたはホスト名で HTTPS プロキシサーバを識別します。
- ステップ 11** 外部 HTTPS プロキシサーバのホスト名または IP アドレスを入力します。
- ステップ 12** HTTPS 要求を受信するポートを入力します。デフォルトのポートは 443 です。
- ステップ 13** (任意) HTTPS プロキシサーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
- * は、スラッシュ (/) とピリオド (.) を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。

- ? は、スラッシュおよびピリオドを含む、任意の 1 文字と一致します。
- [x-y] は、x から y までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
- [!x-y] は、範囲外の任意の 1 文字と一致します。

ステップ 14 (オプション) 各 HTTPS プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、キーワードを入力します。

ステップ 15 各 HTTPS 要求とともにプロキシサーバに送信されるパスワードを入力します。

クライアントレス SSL VPN セッションでの HTTPS の使用

HTTPS の設定に加えて、Web サイトをプロトコルダウングレード攻撃や cookie ハイジャックから保護するのに役立つ Web セキュリティ ポリシー メカニズムである HTTP Strict-Transport-Security (HSTS) を有効にします。HSTS は、UA およびブラウザを HTTPS Web サイトにリダイレクトし、次のディレクティブを送信することにより指定したタイムアウト期限が切れるまで Web サーバに安全に接続します。

```
Strict-Transport-Security: max-age="31536000; includesubdomains; preload
```

それぞれの説明は次のとおりです。

http-headers : ASA からブラウザに送信されるさまざまな HTTP ヘッダーを設定します。サブモードを設定するか、すべての **http-headers** 設定をリセットします。

- **hsts-client** : HSTS クライアントとして機能する HTTP サーバからの HSTS ヘッダーの処理を開始します。
 - **enable** : HSTS ポリシーを有効または無効にすることができます。有効にすると、既知の HSTS ホストと HSTS ヘッダーに対して HSTS ポリシーが適用されます。
- **hsts-server** : ASA からブラウザに送信する HSTS ヘッダーを設定します。ASA はヘッダーを基に、HTTP ではなく HTTPS を使用したアクセスのみを許可するようブラウザに指示します。
 - **include-sub-domains** : ドメイン所有者は、Web ブラウザの HSTS プリロードリストに含める必要があるドメインを送信できます。



(注) HTTPS サイトからの追加リダイレクトを設定するには、(リダイレクト先のページではなく) リダイレクトに HSTS ヘッダーを保持しておく必要があります。

- **max-age** : ([Enable HSTS] チェックボックスをクリックした後に設定可能) Web サーバが HSTS ホストとして見なされ、HTTPS のみを使用してセキュアにアクセスされる

必要のある時間を秒単位で指定します。デフォルトは 3153600 秒（1 年）です。範囲は 0 ～ 2147483647 秒です。

- **preload** : ブラウザに対し、すでに UA およびブラウザに登録され、HSTS ホストとして取り扱う必要のあるドメインのリストの読み込みを指示します。プリロードされたリストの実装は UA およびブラウザに依存し、各 UA およびブラウザは他のディレクトティブの振る舞いに対して追加の制限を指定することができます。たとえば、Chrome のプリロードリストは、HSTS の最大寿命が少なくとも 18 週（10,886,400 秒）であることを指定します。
- **x-content-type-options** : 「X-Content-Type-Options: nosniff」 応答ヘッダーの送信を有効にします。
- **x-xss-protection** : 「X-XSS-Protection: 1[; mode=block]」 応答ヘッダーの送信を有効にします。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Proxies] の順に選択します。

ステップ 2 ブラウザの HSTS プリロードリストに含める必要があるドメインを送信するには、[Enable HSTS Server] をクリックします。
[Enable HSTS Subdomains] および [Enable HSTS Preload] が有効になり、HSTS サーバを有効にするとデフォルトで有効になります。

ステップ 3 HSTS の有効時間（秒数）である [HSTS Max Age] を指定します。

値の範囲は <0 ～ 2147483647> 秒です。デフォルトは 31536000 秒（1 年）です。この制限に達すると、HSTS は有効ではなくなります。

HSTS の有効時間（秒数）。値の範囲は <0 ～ 2147483647> 秒です。デフォルトは 31536000 秒（1 年）です。この制限に達すると、HSTS は有効ではなくなります。

アプリケーション プロファイル カスタマイゼーション フレームワークの設定

クライアントレス SSL に組み込まれているアプリケーションプロファイルカスタマイゼーションフレームワーク（APCF）オプションを使用すると、標準以外のアプリケーションや Web リソースを ASA で処理して、クライアントレス SSL VPN 接続で正常に表示できるようになります。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どの（ヘッダー、本文、要求、応答）、何（データ）を変換するかを指定するスクリプトがあり

ます。スクリプトは XML 形式で記述され、sed（ストリーム エディタ）の構文を使用して文字列およびテキストを変換します。

ASA では複数の APCF プロファイルを並行して設定および実行できます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。ASA は、設定履歴に基づいて、最も古いルールを最初に処理し、次に 2 番目に古いルールを処理します。

APCF プロファイルは、ASA のフラッシュメモリ、HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存できます。

APCF プロファイルは、シスコの担当者のサポートが受けられる場合のみ設定することをお勧めします。

APCF プロファイルの管理

APCF プロファイルは、ASA のフラッシュメモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバに保存できます。このペインは、APCF パッケージを追加、編集、および削除する場合と、パッケージを優先順位に応じて並べ替える場合に使用します。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Application Helper] の順に進みます。ここでは、次の機能を実行できます。

- [Add/Edit] をクリックして、新しい APCF プロファイルを作成するか、既存の APCF プロファイルを変更します。
 - [Flash file] を選択して、ASA のフラッシュメモリに保存されている APCF ファイルを指定します。

次に、[Upload] をクリックして、ローカルコンピュータから ASA のフラッシュファイルシステムに APCF ファイルを取得するか、[Browse] をクリックして、フラッシュメモリ内の既存の APCF を選択します。
 - [URL] を選択して、HTTP、HTTPS、FTP、または TFTP サーバから APCF ファイルを取得します。
- [Delete] をクリックして、既存の APCF プロファイルを削除します。確認の画面は表示されず、やり直しもできません。
- [Move Up] または [Move Down] をクリックして、リスト内の APCF プロファイルの順序を入れ替えます。順序は、使用される APCF プロファイルを決定します。

ステップ 2 リストに変更が加えられていない場合は、[Refresh] をクリックします。

APCF パッケージのアップロード

手順

- ステップ 1** コンピュータ上にある APCF ファイルへのパスが表示されます。[Browse Local] をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。
- ステップ 2** APCF ファイルを見つけて、コンピュータに転送するように選択するにはクリックします。[Select File Path] ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。APCF ファイルに移動して選択し、[Open] をクリックします。ASDM が [Local File Path] フィールドにファイルのパスを挿入します。
- ステップ 3** APCF ファイルをアップロードする ASA 上のパスが [Flash File System Path] に表示されます。[Browse Flash] をクリックして、APCF ファイルをアップロードする ASA 上の場所を特定します。[Browse Flash] ダイアログボックスに、フラッシュ メモリの内容が表示されます。
- ステップ 4** ローカルコンピュータで選択した APCF ファイルのファイル名が表示されます。混乱を防ぐために、この名前を使用することをお勧めします。このファイルの名前が正しく表示されていることを確認し、[OK] をクリックします。[Browse Flash] ダイアログボックスが閉じます。ASDM が [Flash File System Path] フィールドにアップロード先のファイルパスを挿入します。
- ステップ 5** 自分のコンピュータ上の APCF ファイルの場所と、APCF ファイルを ASA にダウンロードする場所を特定したら、[Upload File] をクリックします。
- ステップ 6** [Status] ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、[Information] ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されます。[OK] をクリックします。[Upload Image] ダイアログ ウィンドウから、[Local File Path] フィールドと [Flash File System Path] フィールドの内容が削除されます。これは、別のファイルをアップロードできることを表します。別のファイルをアップロードするには、上記の手順を繰り返します。それ以外の場合は、[Close] をクリックします。
- ステップ 7** [Upload Image] ダイアログ ウィンドウを閉じます。APCF ファイルをフラッシュ メモリにアップロードした後、またはアップロードしない場合に、[Close] をクリックします。アップロードする場合には、[APCF] ウィンドウの [APCF File Location] フィールドにファイル名が表示されます。アップロードしない場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる [Close Message] ダイアログボックスが表示されます。ファイルをアップロードしない場合は、[OK] をクリックします。[Close Message] ダイアログボックスと [Upload Image] ダイアログボックスが閉じられ、APCF [Add/Edit] ペインが表示されます。ファイルをアップロードする場合は、[Close Message] ダイアログボックスの [Cancel] をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態です。[Upload Image] ダイアログボックスが再度表示されます。[Upload File] をクリックします。

APCF パケットの管理

手順

ステップ 1 次のコマンドを使用して、APCF パケットを追加、編集、および削除し、パケットを優先順位に応じて並べ替えます。

- [APCF File Location] : APCF パッケージの場所に関する情報を表示します。これは、ASA のフラッシュメモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバのいずれかです。
- [Add/Edit] : 新規または既存の APCF プロファイルを追加または編集します。
- [Delete] : 既存の APCF プロファイルを削除します。確認されず、やり直しもできません。
- [MoveUp] : リスト内の APCF プロファイルを再配置します。リストにより、ASA が APCF プロファイルを使用するときの順序が決まります。

ステップ 2 [Flash File] をクリックして、ASA のフラッシュメモリに保存されている APCF ファイルを指定します。

ステップ 3 フラッシュメモリに保存されている APCF ファイルのパスを入力します。パスをすでに追加している場合は、そのパスを特定するために参照した後、フラッシュメモリに格納された APCF ファイルにリダイレクトします。

ステップ 4 [Browse Flash] をクリックして、フラッシュメモリを参照し、APCF ファイルを指定します。[Browse Flash Dialog] ペインが表示されます。[Folders] および [Files] 列を使用して APCF ファイルを指定します。APCF ファイルを選択して、[OK] をクリックします。ファイルへのパスが [Path] フィールドに表示されます。

(注) 最近ダウンロードした APCF ファイルの名前が表示されない場合には、[Refresh] をクリックします。

- [Upload] : APCF ファイルをローカル コンピュータから ASA フラッシュファイルシステムにアップロードします。[Upload APCF Package] ペインが表示されます。
- [URL] : HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存されている APCF ファイルを使用する場合にクリックします。
- [ftp, http, https, and tftp] (ラベルなし) : サーバタイプを特定します。
- [URL] (ラベルなし) : FTP、HTTP、HTTPS、または TFTP サーバへのパスを入力します。

APCF 構文

APCF プロファイルは、XML フォーマットおよび sed スクリプトの構文を使用します。次の表に、この場合に使用する XML タグを示します。

APCF のガイドライン

APCF プロファイルの使い方を誤ると、パフォーマンスが低下したり、好ましくない表現のコンテンツになる場合があります。シスコのエンジニアリング部では、ほとんどの場合、APCF プロファイルを提供することで特定アプリケーションの表現上の問題を解決しています。

表 8: APCF XML タグ

タグ	使用目的
<APCF>...</APCF>	すべての APCF XML ファイルを開くための必須のルート要素。
<version>1.0</version>	APCF の実装バージョンを指定する必須のタグ。現在のバージョンは 1.0 だけです。
<application>...</application>	XML 記述の本文を囲む必須タグ。
<id> text </id>	この特定の APCF 機能を記述する必須タグ。
<apcf-entities>...</apcf-entities>	単一または複数の APCF エンティティを囲む必須タグ。
<js-object>...</js-object> <html-object>...</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	これらのタグのうちの 1 つが、コンテンツの種類または APCF 処理が実施される段階を指定します。

タグ	使用目的
<conditions>... </conditions>	<p>処理前および処理後の子要素タグで、次の処理基準を指定します。</p> <ul style="list-style-type: none"> • http-version (1.1、1.0、0.9 など) • http-method (get、put、post、webdav) • http-scheme ("http/"、"https/"、その他) • ("a".."z" "A".."Z" "0".."9" "._*[]?") を含む server-regexp 正規表現 • ("a".."z" "A".."Z" "0".."9" "._*[]?+()\{\},") を含む server-fnmatch 正規表現 • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch <p>• 条件タグのうち2つ以上が存在する場合、ASA はすべてのタグに対して論理 AND を実行します。</p>
<action> ... </action>	<p>指定した条件で1つ以上のアクションをコンテンツでラップします。これらのアクションを定義するには、次のタグを使用できます（下記参照）。</p> <ul style="list-style-type: none"> • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

タグ	使用目的
<do>...</do>	<p>次のいずれかのアクションの定義に使用されるアクションタグの子要素です。</p> <ul style="list-style-type: none"> • <no-rewrite/> : リモートサーバから受信したコンテンツを上書きしません。 • <no-toolbar/> : ツールバーを挿入しません。 • <no-gzip/> : コンテンツを圧縮しません。 • <force-cache/> : 元のキャッシュ命令を維持します。 • <force-no-cache/> : オブジェクトをキャッシュできないようにします。 • <downgrade-http-version-on-backend/> : リモートサーバに要求を送信するときに HTTP/1.0 を使用します。
<sed-script> TEXT </sed-script>	<p>テキストベースのオブジェクトのコンテンツの変更に使用されるアクションタグの子要素です。TEXT は有効な Sed スクリプトである必要があります。<sed-script> は、これより前に定義された <conditions> タグに適用されます。</p>
<rewrite-header></rewrite-header>	<p>アクションタグの子要素です。<header> の子要素タグで指定された HTTP ヘッダーの値を変更します <header> (以下を参照してください)。</p>
<add-header></add-header>	<p><header> の子要素タグで指定された新しい HTTP ヘッダーの追加に使用されるアクションタグの子要素です <header> (以下を参照してください)。</p>
<delete-header></delete-header>	<p><header> の子要素タグで指定された特定の HTTP ヘッダーの削除に使用されるアクションタグの子要素です <header> (以下を参照してください)。</p>

タグ	使用目的
<header></header>	<p>上書き、追加、または削除される HTTP ヘッダー名を指定します。たとえば、次のタグは Connection という名前の HTTP ヘッダーの値を変更します。</p> <pre><rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header></pre>

APCF の設定例

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
    <process-request-header>
      <conditions>
        <server-fnmatch>*.example.com</server-fnmatch>
      </conditions>
      <action>
        <do><no-gzip/></do>
      </action>
    </process-request-header>
  </apcf-entities>
</application>
</APCF>

<APCF>
<version>1.0</version>
<application>
  <id>Change MIME type for all .xyz objects</id>
  <apcf-entities>
    <process-response-header>
      <conditions>
        <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
      </conditions>
      <action>
        <rewrite-header>
          <header>Content-Type</header>
          <value>text/html</value>
        </rewrite-header>
      </action>
    </process-response-header>
  </apcf-entities>
</application>
</APCF>
```

セッションの設定

[Clientless SSL VPN Add/Edit Internal Group Policy] > [More Options] > [Session Settings] ウィンドウでは、クライアントレス SSL VPN のセッションからセッションの間にパーソナライズされ

たユーザ情報を指定できます。デフォルトにより、各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設定を継承します。このウィンドウを使用して、デフォルトグループポリシーのパーソナライズされたクライアントレス SSL VPN ユーザ情報、およびこれらの設定値を区別するグループポリシーすべてを指定します。

手順

- ステップ 1** [none] をクリックするか、または [User Storage Location] ドロップダウンメニューからファイルサーバプロトコル (smb または ftp) をクリックします。シスコでは、ユーザストレージに CIFS を使用することを推奨します。ユーザ名/パスワードまたはポート番号を使用せずに CIFS を設定できます。[CIFS] を選択する場合は、次の構文を入力します。

```
cifs//cifs-share/user/data
```

[smb] または [ftp] を選択する場合は、次の構文を使用して、隣のテキストフィールドにファイルシステムの宛先を入力します。

```
username:password@host:port-number/path
```

次に例を示します。 **mike:mysecret@ftpserver3:2323/public**

- (注) このコンフィギュレーションには、ユーザ名、パスワード、および事前共有キーが示されていますが、ASA は内部アルゴリズムにより暗号化した形式でデータを保存し、そのデータを保護します。

- ステップ 2** 必要な場合は、保管場所へユーザがアクセスできるようにするためにセキュリティアプライアンスが渡す文字列を入力します。
- ステップ 3** [Storage Objects] ドロップダウンメニューから次のいずれかのオプションを選択して、ユーザとの関連でサーバが使用するオブジェクトを指定します。ASA は、これらのオブジェクトを保存してクライアントレス SSL VPN 接続をサポートします。

- cookies,credentials
- cookies
- クレデンシャル

- ステップ 4** セッションをタイムアウトするときのトランザクションサイズの限界値を KB 単位で入力します。この属性は、1 つのトランザクションにだけ適用されます。この値よりも大きなトランザクションだけが、セッションの期限切れクロックをリセットします。

エンコーディング

文字エンコーディングは「文字コード」や「文字セット」とも呼ばれ、raw データ (0 や 1 など) を文字と組み合わせ、データを表します。使用する文字エンコード方式は、言語によって決まります。単一の方式を使う言語もあれば、使わない言語もあります。通常は、地域によつ

でブラウザで使用されるデフォルトのコード方式が決まりますが、リモートユーザが変更することもできます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性によりポータル ページで使用される文字コード方式の値を指定することで、ユーザがブラウザを使用している地域や、ブラウザに対する何らかの変更に関係なく、ページが正しく表示されるようにできます。

デフォルトでは、ASA は「Global Encoding Type」を Common Internet File System（共通インターネット ファイル システム）サーバからのページに適用します。CIFS サーバと適切な文字エンコーディングとのマッピングを、[Global Encoding Type] 属性によってグローバルに、そしてテーブルに示されているファイル エンコーディング例外を使用して個別に行うことにより、ファイル名やディレクトリ パス、およびページの適切なレンダリングが問題となる場合に、CIFS ページが正確に処理および表示できるようにします。

文字エンコーディングの表示または指定

エンコーディングを使用すると、クライアントレス SSL VPN ポータル ページの文字エンコーディングを表示または指定できます。

手順

ステップ 1 [Global Encoding Type] によって、表に記載されている CIFS サーバからの文字エンコーディングを除いて、すべてのクライアントレス SSL VPN ポータル ページが継承する文字エンコーディングが決まります。文字列を入力するか、ドロップダウン リストから選択肢を 1 つ選択します。リストには、最も一般的な次の値だけが表示されます。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis
- unicode
- windows-1252
- none

(注) [none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

<http://www.iana.org/assignments/character-sets> で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されま

せん。ASA の設定を保存するときに、コマンドインタプリタによって大文字が小文字に変換されます。

ステップ 2 エンコーディング要件が「Global Encoding Type」属性設定とは異なる CIFS サーバの名前または IP アドレスを入力します。ASA では、ユーザが指定した大文字と小文字の区別は保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

ステップ 3 CIFS サーバがクライアントレス SSL VPN ポータルページに対して指定する必要がある文字エンコーディングを選択します。文字列を入力するか、ドロップダウンリストから選択します。リストには、最も一般的な次の値だけが登録されています。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

(注) 日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do Not Specify] をクリックして、このフォントファミリを削除します。

- unicode
- windows-1252
- none

[none] をクリックするか、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

<http://www.iana.org/assignments/character-sets> で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存するときに、コマンドインタプリタによって大文字が小文字に変換されます。

コンテンツキャッシングの設定

キャッシュにより、クライアントレス SSL VPN のパフォーマンスを強化します。頻繁に再利用されるオブジェクトをシステムキャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。キャッシュを使用することでトラフィック量が減り、結果として多くのアプリケーションがより効率的に実行されます。



- (注) コンテンツキャッシングをイネーブルにすると、一部のシステムの信頼性が低下します。コンテンツキャッシングをイネーブルにした後、ランダムにクラッシュが発生する場合は、この機能をディセーブルにしてください。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Cache] の順に選択します。

ステップ 2 [Enable Cache] がオフの場合は、オンにします。

ステップ 3 キャッシング条件を定義します。

- [Maximum Object Size] : ASA がキャッシュできるドキュメントの最大サイズを KB 単位で入力します。ASA は、オブジェクトの元のコンテンツ（書き換えまたは圧縮されていないコンテンツ）の長さを測定します。範囲は 0 ~ 10,000 KB で、デフォルトは 1,000 KB です。
- [Minimum Object Size] : ASA がキャッシュできるドキュメントの最小サイズを KB 単位で入力します。ASA は、オブジェクトの元のコンテンツ（書き換えまたは圧縮されていないコンテンツ）の長さを測定します。範囲は 0 ~ 10,000 KB で、デフォルトは 0 KB です。

(注) [Maximum Object Size] は、[Minimum Object Size] よりも大きい値にする必要があります。
- [Expiration Time] : 0 ~ 900 の整数を入力して、オブジェクトを再検証しないでキャッシュする分数を設定します。デフォルトは 1 分です。
- [LM Factor] : 1 ~ 100 の整数を入力します。デフォルトは 20 です。
- LM 因数は、最終変更タイムスタンプだけを持つオブジェクトをキャッシュするためのポリシーを設定します。これによって、サーバ設定の変更値を持たないオブジェクトが再検証されます。ASA は、オブジェクトが変更された後の経過時間と、有効期限がコールされた後の経過時間を推定します。推定された期限切れ時刻は、最終変更後の経過時間と LM 因数の積に一致します。LM 因数を 0 に設定すると、ただちに再検証が実行され、100 に設定すると、再検証までの許容最長時間になります。
- この有効期限によって、最終変更タイムスタンプがなく、サーバ設定で有効期限が明示されていないオブジェクトを、ASA がキャッシュする時間の長さを設定します。
- [Cache static content] : たとえば PDF ファイルやイメージなど、リライトされることのないすべてのコンテンツをキャッシュします。
- [Restore Cache Default] : すべてのキャッシュ パラメータをデフォルト値に戻します。

Content Rewrite

[Content Rewrite] ペインには、コンテンツのリライトがイネーブルになっているか、またはオフに切り替わっているすべてのアプリケーションが一覧表示されます。

クライアントレス SSL VPN では、コンテンツ変換およびリライトエンジンによって、JavaScript、VBScript、Java、マルチバイト文字などの高度な要素からプロキシ HTTP へのトラフィックまでを含む、アプリケーショントラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアプリケーションを使用しているか、SSL VPN デバイスに依存せずに使用しているかによって、セマンティックやアクセスコントロールのルールが異なる場合があります。

デフォルトでは、セキュリティアプライアンスはすべてのクライアントレストラフィックをリライト、または変換します。一部のアプリケーションや Web リソース（公開 Web サイトなど）が ASA を通過しないようにしたい場合があります。そのような場合、ASA では、ASA を通過せずに特定のサイトやアプリケーションをブラウズできるようにするリライトルールを作成できます。これは、VPN 接続におけるスプリットトンネリングに似ています。

これらの機能強化は、ASA 9.0 の Content Rewriter に行われました。

- コンテンツリライトは、HTML5 に対するサポートを追加しました。
- クライアントレス SSL VPN リライタエンジンの品質と有効性が大きく向上しました。その結果、クライアントレス SSL VPN ユーザのエンドユーザエクスペリエンスも向上が期待できます。



(注) ASA 9.9.2 のコンテンツリライタは、サードパーティのライブラリを使用して HTML と JavaScript を解析する新しい Service Worker ベースのクライアント側リライタです。また、文法ベースのパーサーは、クライアント側でコンテンツの書き換えプロセスを転送するため、ASA のパフォーマンスが向上します。

文法ベースのパーサーには、古いリライタとは異なり、ファイルサイズの制限や複雑さはありません。

クライアント側のリライタは、JavaScript、CSS、および HTML ファイルのみを書き換えることができます。

コンテンツの書き換えが正しく機能するように、次のガイドラインに従ってください。

- ASA とクライアントシステムに有効な SSL 証明書があることを確認します。
- Service Worker およびキャッシュ機能をサポートする Web ブラウザを使用していることを確認します。
 - 拡張コンテンツリライタは、Chrome および Firefox Web ブラウザのみをサポートします。
 - Firefox を使用している場合は、プライベートブラウジングモードになっていないことを確認します。
- 特定のファイルに適用された *postprocess-response-body* エンティティを持つ Application Profile Customization Framework (APCF) がある場合、ASA はクライアントで APCF をサポートしないため、ファイルはサーバ上で書き換えられます。

コンテンツ書き換えの制限

クライアントレス WebVPN リライタは、実行時に動的に設定されるため、JavaScript ブラケット表記を使用した URL 割り当てを検出できません。

リライトルールの作成

リライトルールは複数作成できます。セキュリティアプライアンスはリライトルールを順序番号に従って検索するため、ルールの番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

[Content Rewrite] テーブルには、次のカラムがあります。

- [Rule Number] : リスト内でのルールの位置を示す整数を表示します。
- [Rule Name] : ルールが適用されるアプリケーションの名前を付けます。
- [Rewrite Enabled] : コンテンツのリライトをイネーブルかオフで表示します。
- [Resource Mask] : リソース マスクを入力します。

手順

- ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Rewrite] の順に移動します。
- ステップ 2 [Add] または [Edit] をクリックして、コンテンツリライトルールを作成または更新します。
- ステップ 3 このルールをイネーブルにするには、[Enable content rewrite] をオンにします。
- ステップ 4 このルールの番号を入力します。この番号は、リストの他のルールに相対的に、そのルールの優先順位を示します。番号がないルールはリストの最後に配置されます。有効な範囲は 1 ~ 65534 です。
- ステップ 5 (任意) ルールについて説明する英数字を指定します。最大 128 文字です。
- ステップ 6 ルールを適用するアプリケーションやリソースに対応する文字列を入力します。文字列の長さは最大で 300 文字です。次のいずれかのワイルドカードを使用できますが、少なくとも 1 つの英数字を指定する必要があります。
- * : すべてに一致します。ASDM では、* または *.* で構成されるマスクは受け付けません。
 - ? : 単一文字と一致します。
 - [!seq] : シーケンスにない任意の文字と一致します。
 - [seq] : シーケンスにある任意の文字と一致します。

コンテンツリライトルールの設定例

表 9: コンテンツリライトルール

機能	コンテンツのリライトをイネーブルにする	ルール番号	ルール名	リソース マスク
youtube.com での HTTP URL のリライトをオフに切り替える	オフ	1	no-rewrite-youtube	*.youtube.com/*
上記のルールに一致しないすべての HTTP URL のリライトをイネーブルにする	Check	65,535	rewrite-all	*

クライアントレス SSL VPN を介した電子メールの使用

Web 電子メールの設定 : MS Outlook Web App

ASA は、Microsoft Outlook Web App to Exchange Server 2010 および Microsoft Outlook Web Access to Exchange Server 2013 をサポートしています。

手順

- ステップ 1 アドレス フィールドに電子メールサービスの URL を入力するか、クライアントレス SSL VPN セッションでの関連するブックマークをクリックします。
- ステップ 2 プロンプトが表示されたら、電子メール サーバのユーザ名を `domain\username` の形式で入力します。
- ステップ 3 電子メール パスワードを入力します。

ブックマークの設定

[Bookmarks] パネルでは、ブックマーク リストを追加、編集、削除、インポート、およびエクスポートできます。

[Bookmarks] パネルを使用して、クライアントレス SSL VPN でアクセスするための、サーバおよび URL のリストを設定します。ブックマーク リストのコンフィギュレーションに続いて、そのリストを 1 つ以上のポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に割り当てることができます。各ポリシーのブックマーク リストは 1 つのみです。リスト名は、各 DAP の [URL Lists] タブのドロップダウン リストに表示されます。

一部の Web ページでの自動サインオンに、マクロ置換を含むブックマークを使用できるようになりました。以前の POST プラグインアプローチは、管理者がサインオンマクロを含む POST ブックマークを指定し、POST 要求のポストの前にロードするキックオフ ページを受信できるようにするために作成されました。この POST プラグインアプローチでは、クッキーまたはその他のヘッダー項目の存在を必要とする要求は排除されました。現在は、管理者は事前ロードページおよび URL を決定し、これによってポストログイン要求の送信場所が指定されます。事前ロードページによって、エンドポイントブラウザは、クレデンシャルを含む POST 要求を使用するのではなく、Web サーバまたは Web アプリケーションに送信される特定の情報を取得できます。

既存のブックマーク リストが表示されます。ブックマーク リストを追加、編集、削除、インポート、またはエクスポートできます。アクセス用のサーバおよび URL のリストを設定し、指定した URL リスト内の項目を配列することができます。

始める前に

ブックマークを設定することでは、ユーザが不正なサイトや会社のアクセプタブルユースポリシーに違反するサイトにアクセスすることを防ぐことはできません。ブックマークリストをグループポリシー、ダイナミックアクセスポリシー、またはその両方に割り当てる以外に、WebACLをこれらのポリシーに割り当てて、トラフィックフローへのアクセスを制御します。これらのポリシー上のURLエントリをオフに切り替えて、ユーザがアクセスできるページについて混乱しないようにします。

手順

ステップ 1 追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。

ブックマークのタイトルおよび実際の関連付けられたURLが表示されます。

ステップ 2 (任意) [Add] をクリックして、新しいサーバまたはURLを設定します。次のいずれかを追加できます。

- GET または Post メソッドによる URL のブックマークの追加
- 定義済みアプリケーションテンプレートに対する URL の追加
- 自動サインオンアプリケーションへのブックマークの追加

ステップ 3 (任意) [Edit] をクリックして、サーバ、URL、または表示名を変更します。

ステップ 4 (任意) [Delete] をクリックして、選択した項目をURLリストから削除します。確認の画面は表示されず、やり直しもできません。

ステップ 5 (任意) ファイルのインポート元またはエクスポート元の場所を選択します。

- [Local computer] : ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Flash file system] : ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Remote server] : ASA からアクセス可能なリモートサーバに常駐するファイルをインポートする場合にクリックします。
- [Path] : ファイルへのアクセス方式 (ftp、http、または https) を指定し、ファイルへのパスを入力します。
- [Browse Local Files/Browse Flash...] : ファイルのパスを参照します。

ステップ 6 (任意) ブックマークを強調表示して [Assign] をクリックし、選択したブックマークを1つ以上のグループポリシー、ダイナミックアクセスポリシー、または LOCAL ユーザに割り当てます。

ステップ 7 (任意) [Move Up] または [Move Down] オプションを使用して、選択した項目の位置をURLリスト内で変更します。

ステップ 8 [OK] をクリックします。

次のタスク

クライアントレス SSL VPN セキュリティ対策について確認してください。

GET または Post メソッドによる URL のブックマークの追加

[Add Bookmark Entry] ダイアログボックスでは、URL リストのリンクまたはブックマークを作成できます。

始める前に

ネットワークの共有フォルダにアクセスするには、`\\server\share\subfolder\<personal folder>` 形式を使用します。ユーザには、`<personal folder>` より上のすべてのポイントに対するリスト権限が必要です。

手順

- ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] に移動し、[Add] ボタンをクリックします。
- ステップ 2 [URL with GET or POST Method] を選択して、ブックマークの作成に使用します。
- ステップ 3 ポータルに表示されるこのブックマークの名前を入力します。
- ステップ 4 [URL] ドロップダウンメニューを使用して、URL タイプ (http、https、cifs、または ftp) を選択します。[URL] ドロップダウンは、標準の URL タイプ、インストールしたすべてのプラグインのタイプを示します。
- ステップ 5 このブックマーク (URL) の DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符 (?) を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。
- server/?Parameter=Value&Parameter=Value*
- 例 :
- 特定のプラグインによって、入力できるオプションのパラメータ/値ペアが決まります。
- host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768*
- プラグインに対してシングルサインオンのサポートを指定するには、パラメータ/値ペア **cscs_sso=1** を使用します。
- ホスト/**?cscs_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**
- ステップ 6 (任意) 事前ロード URL を入力します。事前ロード URL を入力するときに、待機時間も入力できます。待機時間は、実際の POST URL に転送されるまでに、ページのロードに使用できる時間です。

- ステップ 7** サブタイトルとして、ユーザに表示するブックマークエントリについての説明テキストを入力します。
- ステップ 8** [Thumbnail] ドロップダウンメニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
- ステップ 9** [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。
- ステップ 10** ブックマークをクリックして新しいウィンドウで開きます。このウィンドウで、スマートトンネル機能を使用し、ASA を介して宛先サーバとのデータの受け渡しを行います。すべてのブラウザトラフィックは、SSL VPN トンネルで安全に送受信されます。このオプションでは、ブラウザベースのアプリケーションにスマートトンネルのサポートを提供します。一方で、[Smart Tunnels] ([Clientless SSL VPN] > [Portal] メニューにもあり) では、非ブラウザベースのアプリケーションもスマートトンネルリストに追加し、それをグループポリシーとユーザ名に割り当てられます。
- ステップ 11** [Allow the Users to Bookmark the Link] をオンにして、クライアントレス SSL VPN ユーザが、ブラウザの [Bookmarks] または [Favorites] オプションを使用できるようにします。選択を解除すると、これらのオプションを使用できません。このオプションをオフにすると、クライアントレス SSL VPN ポータルの [Home] セクションにブックマークは表示されません。
- ステップ 12** (任意) [Advanced Options] を選択して、ブックマークの特徴の詳細を設定します。
- [URL Method] : 単純なデータ取得の場合には [Get] を選択します。データの保存または更新、製品の注文、電子メールの送信など、データを処理することによってデータに変更が加えられる可能性がある場合には、[Post] を選択します。
 - [Post Parameters] : Post URL 方式の詳細を設定します。

定義済みアプリケーションテンプレートに対する URL の追加

このオプションは、事前に定義された ASDM テンプレートを選択しているユーザのブックマークの作成を簡略化します。ASDM テンプレートには、特定の明確に定義されたアプリケーションに対する事前に入力された必要な値が含まれます。

始める前に

定義済みアプリケーションテンプレートは、次のアプリケーションで現在使用できます。

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

- Microsoft SharePoint 2013

手順

-
- ステップ 1** ユーザに対して表示するブックマークの名前を入力します。
- ステップ 2** サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。
- ステップ 3** [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
- ステップ 4** [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。
- ステップ 5** (任意) [Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。
- ステップ 6** [Select Auto Sign-on Application] リストで、必要なアプリケーションをクリックします。使用可能なアプリケーションは次のとおりです。
- Citrix XenApp
 - Citrix XenDesktop
 - Domino WebAccess
 - Microsoft Outlook Web Access 2010
 - Microsoft Sharepoint 2007
 - Microsoft SharePoint 2010
 - Microsoft SharePoint 2013
- ステップ 7** ログイン ページの前にロードされるページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタクションが必要になります。URL には、任意の数の記号を置き換える * を入力できます (たとえば、`http*://www.example.com/test`) 。
- ステップ 8** [Pre-login Page Control ID] を入力します。これは、ログイン ページに進む前に事前ログイン ページの URL でクリック イベントを取得する制御/タグの ID です。
- ステップ 9** [Application Parameters] を入力します。アプリケーションに応じて、次の内容が含まれる可能性があります。
- プロトコル。HTTP または HTTPS。
 - ホスト名。たとえば、`www.cisco.com` などです。
 - ポート番号。アプリケーションで使用されるポート。
 - [URL Path Appendix]。たとえば、`/Citrix/XenApp` などです。通常これは、自動入力されません。
 - [Domain]。接続するドメイン。

- [User Name]。ユーザ名として使用する SSL VPN 変数。[Select Variable] をクリックして、異なる変数を選択します。
- パスワード。パスワードとして使用する SSL VPN 変数。[Select Variable] をクリックして、異なる変数を選択します。

ステップ 10 (任意) [Preview] をクリックして、テンプレートの出力を表示します。[Edit] をクリックすると、テンプレートを変更できます。

ステップ 11 [OK] をクリックして、変更を行います。または、[Cancel] をクリックして変更を破棄します。

自動サインオンアプリケーションのブックマークの追加

このオプションでは、複雑な自動サインオンアプリケーションのブックマークを作成できます。

自動サインオンアプリケーションの設定には、2つの手順が必要になります。

1. 基本的な初期データがあり、POST パラメータがないブックマークを定義します。ブックマークを保存および割り当てて、グループまたはユーザ ポリシーで使用します。
2. ブックマークを再度編集します。特定のキャプチャ機能を使用して、SSL VPN パラメータをキャプチャし、ブックマークで編集します。

手順

ステップ 1 ユーザに対して表示するブックマークの名前を入力します。

ステップ 2 [URL] ドロップダウンメニューを使用して、URL タイプ (http、https、cifs、または ftp) を選択します。インポートされたすべてのプラグインの URL タイプが、このメニューに表示されます。ポータル ページにリンクとしてプラグインを表示するには、プラグインの URL タイプを選択します。

ステップ 3 ブックマークの DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符 (?) を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。

server/?Parameter=Value&Parameter=Value

例 :

たとえば、入力できるオプションのパラメータ/値ペアは、特定のプラグインによって決まります。

host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

プラグインに対して、シングル サインオン サポートを提供するには、パラメータ/値ペア `cscsso=1` を使用します。

```
host/?cscsso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

- ステップ 4 サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。
- ステップ 5 [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
- ステップ 6 [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。
- ステップ 7 (任意) [Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。
- ステップ 8 [Login Page URL] を入力します。入力する URL には、ワイルドカードを使用できます。たとえば、`http*://www.example.com/myurl*` と入力します。
- ステップ 9 [Landing Page URL] を入力します。ASA では、アプリケーションへの正常なログインを検出するために、ランディング ページを設定する必要があります。
- ステップ 10 (任意) [Post Script] を入力します。Microsoft Outlook Web Access などの一部の Web アプリケーションは、JavaScript を実行して、ログイン フォームを送信する前に、要求パラメータを変更する場合があります。[Post Script] フィールドでは、このようなアプリケーションの JavaScript を入力できます。
- ステップ 11 必要な [Form Parameters] を追加します。必要な SSL VPN 変数ごとに、[Add] をクリックして [Name] を入力し、リストから変数を選択します。パラメータを変更するには [Edit] をクリックし、削除するには [Delete] をクリックします。
- ステップ 12 ログイン ページの前にロードされるページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタラクションが必要になります。URL には、任意の数の記号を置き換える * を入力できます (たとえば、`http*://www.example.com/test`) 。
- ステップ 13 [Pre-login Page Control ID] を入力します。これは、ログイン ページに進む前に事前ログイン ページの URL でクリック イベントを取得する制御/タグの ID です。
- ステップ 14 [OK] をクリックして、変更を行います。または、[Cancel] をクリックして変更を破棄します。次の作業

次のタスク

ブックマークを編集する場合、HTML Parameter Capture 機能を使用して、VPN 自動サインオン パラメータをキャプチャできます。ブックマークは保存され、グループポリシーまたはユーザにまず割り当てられる必要があります。

[SSL VPN Username] を入力してから、[Start Capture] をクリックします。次に、Web ブラウザを使用して、VPN セッションを開始して、イントラネットのページに進みます。プロセスを完了するには、[Stop Capture] をクリックします。パラメータが編集できるようになり、ブックマークに挿入されます。

ブックマーク リストのインポートおよびエクスポート

すでに設定済みのブックマーク リストは、インポートまたはエクスポートできます。使用準備ができていないリストをインポートします。リストをエクスポートして修正または編集してから、再インポートすることもできます。

手順

ステップ 1 ブックマーク リストを名前指定します。最大 64 文字で、スペースは使用できません。

ステップ 2 リスト ファイルをインポートする、またはエクスポートするための方法を選択します。

- [Local computer] : ローカル PC に常駐するファイルをインポートする場合に選択します。
- [Flash file system] : ASA に常駐するファイルをエクスポートする場合に選択します。
- [Remote server] : ASA からアクセス可能なリモート サーバに常駐する URL リスト ファイルをインポートする場合にクリックします。
- [Path] : ファイルへのアクセス方式 (ftp、http、または https) を指定し、ファイルへのパスを入力します。
- [Browse Local Files/Browse Flash] : ファイルのパスを参照します。
- [Import/Export Now] : リスト ファイルをインポートまたはエクスポートします。

Import and Export GUI Customization Objects (Web Contents)

このダイアログボックスでは、Web コンテンツ オブジェクトをインポートおよびエクスポートできます。Web コンテンツ オブジェクトの名前とファイル タイプが表示されます。

Web コンテンツには、全体的に設定されたホームページから、エンドユーザ ポータルをカスタマイズするときに使用するアイコンやイメージまで、さまざまな種類があります。設定済みの Web コンテンツは、インポートまたはエクスポートできます。使用準備ができていない Web コンテンツをインポートします。Web コンテンツをエクスポートして修正または編集してから、再インポートすることもできます。

手順

ステップ 1 ファイルのインポート元またはエクスポート元の場所を選択します。

- [Local computer] : ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
- [Flash file system] : ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。

- [Remote server] : ASA からアクセス可能なリモート サーバに常駐するファイルをインポートする場合にクリックします。
- [Path] : ファイルへのアクセス方式 (ftp、http、または https) を指定し、ファイルへのパスを入力します。
- [Browse Local Files.../Browse Flash...] : ファイルのパスを参照します。

ステップ 2 コンテンツへのアクセスに認証が必要かどうかを決定します。

パスのプレフィックスは、認証を要求するかどうかに応じて異なります。ASA は、認証が必要なオブジェクトの場合には /+CSCOE+/ を使用し、認証が不要なオブジェクトの場合には /+CSCOU+/ を使用します。ASA では、/+CSCOE+/ オブジェクトはポータルページにのみ表示されますが、/+CSCOU+/ オブジェクトはログイン ページまたはポータル ページで表示したり使用することができます。

ステップ 3 クリックして、ファイルをインポートまたはエクスポートします。

POST パラメータの追加および編集

このペインでは、ブックマーク エントリと URL リストのポスト パラメータを設定します。

クライアントレス SSL VPN 変数により、URL およびフォームベースの HTTP post 操作で置換が実行できます。これらの変数はマクロとも呼ばれ、ユーザ ID とパスワード、またはその他の入力パラメータを含む、パーソナル リソースへのユーザアクセスを設定できます。このようなリソースの例には、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

手順

ステップ 1 パラメータの名前と値を、対応する HTML フォームのとおり指定します。たとえば、

`<input name="param_name" value="param_value">` です。

提供されている変数のいずれかをドロップダウンリストから選択できます。また、変数を作成できます。ドロップダウン リストからは、次の変数を選択します。

表 10: クライアントレス SSL VPN の変数

No.	変数置換	定義
1	CSCO_WEBVPN_USERNAME	SSL VPN ユーザ ログイン ID。
2	CSCO_WEBVPN_PASSWORD	SSL VPN ユーザ ログイン パスワード。

No.	変数置換	定義
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN ユーザ内部リソースパスワード。キャッシュされた認定証であり、AAA サーバによって認証されていません。ユーザがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN ユーザ ログイングループ ドロップダウン、接続プロファイル内のグループエイリアス
5	CSCO_WEBVPN_MACRO1	RADIUS/LDAP ベンダー固有属性によって設定。 ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。 RADIUS 経由での変数置換は、VSA#223 によって行われます。
6	CSCO_WEBVPN_MACRO2	RADIUS/LDAP ベンダー固有属性によって設定。 ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。 RADIUS 経由での変数置換は、VSA#224 によって行われます。
7	CSCO_WEBVPN_PRIMARY_USERNAME	二重認証用のプライマリ ユーザのログイン ID
8	CSCO_WEBVPN_PRIMARY_PASSWORD	二重認証用のプライマリ ユーザのログインパスワード

No.	変数置換	定義
9	CSCO_WEBVPN_SECONDARY_USERNAME	二重認証用のセカンダリ ユーザのログイン ID
10	CSCO_WEBVPN_SECONDARY_PASSWORD	二重認証用のセカンダリ ユーザのログイン ID
11	CSCO_WEBVPN_DYNAMIC_URL	ユーザのポータルで複数のブックマーク リンクを生成できる単一のブックマーク。
12	CSCO_WEBVPN_MACROLIST	静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。

ASA はこれら 6 つの変数文字列のいずれかをエンドユーザ要求（ブックマークまたはポストフォーム）で認識すると、リモートサーバに要求を渡す前に、変数をユーザ固有の値に置換します。

(注) プレーンテキストで（セキュリティ アプライアンスを使用せずに）HTTP Sniffer トレースを実行すると、任意のアプリケーションの `http-post` パラメータを取得できます。次のリンクから、無料のブラウザ キャプチャ ツールである HTTP アナライザを入手できます。<http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe>

ステップ 2 該当する変数を選択するには、次の注意事項に従ってください。

- 変数 1 ～ 4 を使用する。ASA は、[SSL VPN Login] ページから最初の 4 つの置き換えの値を取得します。値には、ユーザ名、パスワード、内部パスワード（オプション）、およびグループのフィールドが含まれています。ユーザ要求内のこれらのストリングを認識し、このストリングをユーザ固有の値で置き換えてから、リモートサーバに要求を渡します。

For example, if a URL list contains the link,
`http://someserver/homepage/CSCO_WEBVPN_USERNAME.html`, the ASA translates it to the following unique links:

For USER1, the link becomes `http://someserver/homepage/USER1.html`

For USER2, the link is `http://someserver/homepage/USER2.html`

In the following case, `cifs://server/users/CSCO_WEBVPN_USERNAME` lets the ASA map a file drive to specific users:

For USER1, the link becomes `cifs://server/users/USER1`

For USER 2, the link is `cifs://server/users/USER2`

- 変数 5 と 6 を使用する。マクロ 5 および 6 の値は、RADIUS または LDAP のベンダー固有属性（VSA）です。これらにより、RADIUS または LDAP サーバのいずれかで設定した代わりの設定を使用できるようになります。

- 変数 7～10 を使用する。ASA はこれら 4 つの変数文字列のいずれかをエンドユーザ要求（ブックマークまたはポストフォーム）で認識すると、リモートサーバに要求を渡す前に、変数をユーザ固有の値に置換します。

The following example sets a URL for the homepage:

WebVPN-Macro-Value1 (ID=223), type string, is returned as *wwwin-portal.example.com*
 WebVPN-Macro-Value2 (ID=224), type string, is returned as *401k.com*

To set a home page value, you would configure the variable substitution as

`https://CSCO_WEBVPN_MACRO1`, which would translate to `https://wwwin-portal.example.com`.

- 変数 11 を使用する。これらのブックマークは、`CSCO_WEBVPN_DYNAMIC_URL` がマッピングされている LDAP 属性マップに基づいて生成されます。LDAP から受信した文字列は、デリミタパラメータを使用して解析され、値のリストになります。この変数を url フィールドで使用したり、ブックマーク内で POST パラメータとして使用すると、解析された LDAP 文字列の各値に対してブックマークが生成されます。

`CSCO_WEBVPN_DYNAMIC_URL` を使用するブックマークの設定例を以下に示します。

```
<bookmark>
  <title>Test Bookmark</title>
  <method>post</method>
  <favorite>yes</favorite>
  <url>http://CSCO_WEBVPN_DYNAMIC_URL1(".")</url>
  <subtitle></subtitle>
  <thumbnail></thumbnail>
  <smart-tunnel>no</smart-tunnel>
  <login-page-url></login-page-url>
  <landing-page-url></landing-page-url>
  <pre-login-page-url></pre-login-page-url>
  <control-id></control-id>
  <<post-param>
    <value>value1</value>
    <name>parameter1</name>
  </post-param>
</bookmark>
```

`CSCO_WEBVPN_DYNAMIC_URL` は LDAP 属性マップに設定されており、`host1.cisco.com`、`host2.cisco.com`、`host3.cisco.com` に対応しています。デリミタに従って、`http://host1.cisco.com`、`http://host2.cisco.com`、`http://host3.cisco.com` を含む単一のコンフィギュレーションから生成された、3 つの個別の URL と 3 つのブックマークを取得できます。

さらに、POST パラメータの一部として次のマクロを使用できます。

```
<bookmark>
  <title>Test Bookmark</title>
  <method>post</method>
  <favorite>yes</favorite>
  <url>http://www.myhost.cisco.com</url>
  <subtitle></subtitle>
  <thumbnail></thumbnail>
  <smart-tunnel>no</smart-tunnel>
  <login-page-url></login-page-url>
  <landing-page-url></landing-page-url>
  <pre-login-page-url></pre-login-page-url>
  <control-id></control-id>
  <post-param>
    <value>CSCO_WEBVPN_DYNAMIC_URL(";")</value>
```

```
<name>host</name>
</bookmark>
```

同じマッピングされた LDAP 属性を使用して、ターゲット URL `http://www.myhost.cisco.com` を含む 3 つのブックマークが作成されます。それぞれのブックマークは異なる POST パラメータと、名前 `host` および値 `host1.cisco.com`、`host2.cisco.com`、`host3.cisco.com` を持ちます。

(注) `CSCO_WEBVPN_DYNAMIC_URL` はブックマークでのみ使用できます。マクロをサポートしている別の箇所 (Citrix Mobile Receiver の vdi CLI コンフィギュレーションなど) で使用することはできません。外部ポータルページを定義するために使用することもできません。

- 変数 12 を使用する。このマクロは入力として 3 つのパラメータ (インデックス、デリミタ、エスケープ) を取ります。インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。エスケープは、ASA 要求に置き換える前に LDAP 文字列に適用する条件選択肢です。

たとえば、`CSCO_WEBVPN_MACROLIST(2, ";", url-encode)` は、リストの 2 番目の値を使用すること、および区切り文字として単一のカンマを使用して文字列を区切り、リストにすることを指定しています。値は、バックエンドへの ASA 要求に置換されるときに符号化された URL になります。エスケープルーチンには、次の値が使用されます。

- None* : バックエンド サーバへの送信前に、文字列値に対して変換を行いません。
- url-code* : 解析された各値は符号化された URL になります。ただし、URL で特殊文字列を構成する一連の予約文字は除外されます。
- url-encode-data* : 解析された各値は、URL エンコードで完全に変換されます。
- base64* : 解析された各値は Base 64 で符号化されます。

`CSCO_WEBVPN_MACROLIST1` を使用するブックマークの設定例を以下に示します。

```
<bookmark>
  <title>MyHost</title>
  <method>post</method>
  <favorite>yes</favorite>
  <url>http://www.myhost.cisco.com</url>
  <subtitle></subtitle>
  <thumbnail></thumbnail>
  <smart-tunnel>no</smart-tunnel>
  <login-page-url><login-page-url>
  <landing-page-url></landing-page-url>
  <pre-login-page-url></pre-login-page-url>
  <control-id></control-id>
  <post-param>
    <value>CSCO_WEBVPN_MACROLIST1(1, ";", url-encode-data)</value>
    <name>param1</name>
    <value>CSCO_WEBVON_MACROLIST1(2, ";", url-encode-data)</value>
    <name>param2</name>
    <value>CSCO_WEBVPN_MACROLIST1(3, ";", url-encode-data)</value>
    <name>param3</name>
```

```
</post-param>
</bookmark>
```

このブックマークを使用すると、www.myhost.cisco.com をブラウザして、3 つの POST パラメータ (param1、param2、param3) を自動的にサーバに送信できます。ASA は、CSCO_WEBVPN_MACROLIST1 の値をパラメータに置換してから、バックエンドに送信します。

(注) CSCO_WEBVPN_MACROLIST は、他のマクロが使用される箇所ならどこでも使用できます。

- この場合の最善の方法は、ASDM で Homepage URL パラメータを設定することです。スクリプトを記述したり何かをアップロードしなくても、管理者はグループポリシー内のどのホームページがスマート トンネル経由で接続するかを指定できます。ASDM の Network Client SSL VPN または Clientless SSL VPN Access セクションから、[Add/Edit Group Policy] ペインに移動します。パスは次のとおりです。
 - [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit Group Policy] > [Advanced] > [SSL VPN Client] > [Customization] > [Homepage URL] 属性
 - [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit Group Policy] > [More Options] > [Customization] > [Homepage URL] 属性

ステップ 3 ブックマークまたは URL エントリを設定します。SSL VPN 認証で RSA ワンタイムパスワード (OTP) を使用し、続いて OWA 電子メールアクセスでスタティックな内部パスワードを使用することによって、HTTP Post を使用して OWA リソースにログインできます。この場合の最善の方法は、次のパスのいずれかを使用して ASDM でブックマーク エントリを追加または編集することです。

- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] > [Add/Edit Bookmark Lists] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters] (URL Method 属性の [Post] をクリックすると表示されます)
- [Network (Client) Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [URL Lists] タブ > [Manage] ボタン > [Configured GUI Customization Objects] > [Add/Edit] ボタン > [Add/Edit Bookmark List] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters]

ステップ 4 ファイル共有 (CIFS) URL 置換を設定することによって、より柔軟なブックマーク設定を構成します。URL 「cifs://server/CSCO_WEBVPN_USERNAME」を設定すると、ASA はそれをユーザのファイル共有ホームディレクトリに自動的にマッピングします。この方法では、パスワードおよび内部パスワード置換も行えます。次に、URL 置換の例を示します。

```
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

外部ポートのカスタマイズ

事前設定されたポータルを使用する代わりに、外部ポータル機能を使用して独自のポータルを作成できます。独自のポータルを設定する場合、クライアントレスポータルをバイパスし、POST 要求を送信してポータルを取得できます。

手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Customization] を選択します。必要なカスタマイゼーションを強調表示し、[Edit] を選択します。
 - ステップ 2** [Enable External Portal] チェックボックスをオンにします。
 - ステップ 3** [URL] フィールドに、POST 要求が許可されるように、必要な外部ポータルを入力します。
-



第 16 章

ポリシーグループ

- [スマート トンネル アクセス \(371 ページ\)](#)
- [クライアントレス SSL VPN キャプチャ ツール \(385 ページ\)](#)
- [ポータル アクセス ルールの設定 \(385 ページ\)](#)
- [クライアントレス SSL VPN のパフォーマンスの最適化 \(387 ページ\)](#)

スマート トンネル アクセス

次の項では、クライアントレス SSL VPN セッションでスマート トンネル アクセスをイネーブルにする方法、それらのアクセスを提供するアプリケーションの指定、および使用上の注意について説明します。

スマート トンネル アクセスを設定するには、スマート トンネル リストを作成します。このリストには、スマート トンネル アクセスに適した 1 つ以上のアプリケーション、およびこのリストに関連付けられたエンドポイント オペレーティング システムを含めます。各グループ ポリシーまたはローカル ユーザ ポリシーでは 1 つのスマート トンネル リストがサポートされているため、ブラウザベースではないアプリケーションをサポート対象とするために、グループ化してスマート トンネル リストに加える必要があります。リストを作成したら、1 つ以上のグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

次の項では、スマート トンネル およびその設定方法について説明します。

- [スマート トンネル について \(372 ページ\)](#)
- [スマート トンネル の前提条件 \(373 ページ\)](#)
- [スマート トンネル のガイドライン \(373 ページ\)](#)
- [スマート トンネル の設定 \(Lotus の例\) \(375 ページ\)](#)
- [トンネリングするアプリケーションの設定の簡略化 \(376 ページ\)](#)
- [スマート トンネル リスト について \(381 ページ\)](#)
- [スマート トンネル 自動サインオン サーバ リストの作成 \(381 ページ\)](#)
- [スマート トンネル 自動サインオン サーバ リストへのサーバの追加 \(382 ページ\)](#)

- [スマート トンネル アクセスのイネーブル化とオフへの切り替え \(383 ページ\)](#)
- [スマート トンネルからのログオフの設定 \(384 ページ\)](#)

スマート トンネルについて

スマート トンネルは、TCP ベースのアプリケーションとプライベート サイト間の接続です。このスマート トンネルでは、セキュリティ アプライアンスをパスウェイ、ASA をプロキシ サーバとするクライアントレス (ブラウザベース) SSL VPN セッションが使用されます。スマート トンネル アクセスを許可するアプリケーションを特定し、各アプリケーションのローカルパスを指定できます。Microsoft Windows で実行するアプリケーションの場合は、チェックサム SHA-1 ハッシュの一致を、スマート トンネル アクセスを許可する条件として要求できます。

Lotus SameTime および Microsoft Outlook は、スマート トンネル アクセスを許可するアプリケーションの例です。

スマート トンネルを設定するには、アプリケーションがクライアントであるか、Web 対応アプリケーションであるかに応じて、次の手順のいずれかを実行する必要があります。

- クライアントアプリケーションの1つ以上のスマート トンネル リストを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。
- スマート トンネル アクセスに適切な Web 対応アプリケーションの URL を指定する1つ以上のブックマーク リスト エントリを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

また、クライアントレス SSL VPN セッションを介したスマート トンネル接続でのログイン クレデンシャルの送信を自動化する Web 対応アプリケーションのリストも作成できます。

スマート トンネルのメリット

スマート トンネル アクセスでは、クライアントの TCP ベースのアプリケーションは、ブラウザベースの VPN 接続を使用してサービスにアクセスできます。この方法では、プラグインやレガシーテクノロジーであるポート転送と比較して、ユーザには次のような利点があります。

- スマート トンネルは、プラグインよりもパフォーマンスが向上します。
- ポート転送とは異なり、スマート トンネルでは、ローカルポートへのローカルアプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
- ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。

プラグインの利点は、クライアント アプリケーションをリモート コンピュータにインストールする必要がないという点です。

スマートトンネルの前提条件

スマートトンネルでサポートされるプラットフォームとブラウザについては、『[サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ](#)』を参照してください。

次の要件と制限事項が Windows でのスマートトンネルアクセスには適用されます。

- Windows ではブラウザで ActiveX または Oracle Java ランタイム環境 (JRE 6 以降を推奨) をイネーブルにしておく必要がある。
- Winsock 2 の TCP ベースのアプリケーションだけ、スマートトンネルアクセスに適する。
- Mac OS X の場合に限り、Java Web Start をブラウザでイネーブルにしておく必要がある。
- スマートトンネルは、IE の拡張保護モードと互換性がありません。

スマートトンネルのガイドライン

- スマートトンネルは、Microsoft Windows を実行しているコンピュータとセキュリティアプライアンス間に配置されたプロキシだけをサポートする。スマートトンネルは、Windows でシステム全体のパラメータを設定する Internet Explorer 設定を使用します。この設定がプロキシ情報を含む場合があります。
 - Windows コンピュータで、プロキシが ASA にアクセスする必要がある場合は、クライアントのブラウザにスタティックプロキシエントリが必要であり、接続先のホストがクライアントのプロキシ例外のリストに含まれている必要があります。
 - Windows コンピュータで、プロキシが ASA にアクセスする必要がなく、プロキシがホストアプリケーションにアクセスする必要がある場合は、ASA がクライアントのプロキシ例外のリストに含まれている必要があります。

プロキシシステムはスタティックプロキシエントリまたは自動設定のクライアントの設定、または PAC ファイルによって定義できます。現在、スマートトンネルでは、スタティックプロキシ設定だけがサポートされています。

- スマートトンネルでは、Kerberos Constrained Delegation (KCD) はサポートされない。
- Windows の場合、コマンドプロンプトから開始したアプリケーションにスマートトンネルアクセスを追加する場合は、スマートトンネルリストの1つのエントリの [Process Name] に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。これは「cmd.exe」がアプリケーションの親であるためです。
- HTTP ベースのリモートアクセスによって、いくつかのサブネットが VPN ゲートウェイへのユーザアクセスをブロックすることがある。これを修正するには、Web とエンドユーザの場所との間のトラフィックをルーティングするために ASA の前にプロキシを配置します。このプロキシが CONNECT 方式をサポートしている必要があります。認証が必要なプロキシの場合、スマートトンネルは、基本ダイジェスト認証タイプだけをサポートします。

- スマート トンネルが開始されると、ASA は、ブラウザプロセスが同じである場合に VPN セッション経由ですべてのブラウザトラフィックをデフォルトで送信する。また、`tunnel-all` ポリシーが適用されている場合にのみ、ASA は同じ処理を行います。ユーザがブラウザプロセスの別のインスタンスを開始すると、VPNセッション経由ですべてのトラフィックが送信されます。ブラウザプロセスが同じで、セキュリティアプライアンスが URL へのアクセスを提供しない場合、ユーザはその URL を開くことはできません。回避策として、`tunnel-all` ではないトンネル ポリシーを割り当てます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザはフェールオーバー後に再接続する必要があります。
- スマートトンネルの Mac バージョンは、POST ブックマーク、フォームベースの自動サインオン、または POST マクロ置換をサポートしない。
- macOS ユーザの場合、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッション接続を確立できる。この要件には、Firefox に対するスマート トンネルのサポートも含まれます。スマート トンネルを最初に使用する際に、Firefox を使用して Firefox の別のインスタンスを起動するには、`cscost` という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。
- macOS では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できる。
- macOS では、スマート トンネルは次をサポートしない。
 - サンドボックス化されたアプリケーション ([View] > [Columns] を使用してアクティビティ モニタで確認します)。そのため、macOS 10.14 および 10.15 はスマート トンネリングをサポートしていません。
 - プロキシ サービス
 - 自動サインオン
 - 2 つのレベルの名前スペースを使用するアプリケーション
 - Telnet、SSH、cURL などのコンソールベースのアプリケーション
 - `dlopen` または `dlsym` を使用して `libsocket` コールを見つけ出すアプリケーション
 - `libsocket` コールを見つけ出すスタティックにリンクされたアプリケーション
- macOS では、プロセスへのフルパスが必要です。また、このパスは大文字と小文字が区別されます。各ユーザ名のパスを指定しないようにするには、部分パスの前にチルダ (~) を入力します (例: `~/bin/vnc`) 。
- Mac デバイスや Windows デバイスの Chrome ブラウザでスマート トンネルをサポートするための新しいメソッドが用意されました。Chrome Smart Tunnel Extension は、Netscape プラグインアプリケーションプログラムインターフェイス (NPAPI) に代わるものです。NPAPI は、Chrome ではサポートされなくなりました。

この拡張プログラムをインストールしていない Chrome でスマートトンネルに対応したブックマークをクリックすると、ユーザは拡張プログラムを取得できるように Chrome ウェブストアにリダイレクトされます。Chrome を新規インストールする場合、ユーザは拡張プログラムを取得できるように Chrome ウェブストアに移動されます。この拡張プログラムは、スマートトンネルの実行に必要なバイナリを ASA からダウンロードします。

Chrome のデフォルトのダウンロード場所が、現在のユーザの「ダウンロード」フォルダを指している必要があります。または、Chrome のダウンロード設定が [Ask every time] である場合は、ユーザは尋ねられたときに「ダウンロード」フォルダを選択する必要があります。

スマートトンネルの使用、通常のブックマークおよびアプリケーション設定は、新しい拡張機能のインストールとダウンロード場所指定のプロセス以外は変更されません。

スマートトンネルの設定 (Lotus の例)



- (注) この例では、アプリケーションでのスマートトンネルサポートを追加するために必要な最小限の指示だけを示します。詳細については、以降の各項にあるフィールドの説明を参照してください。

手順

- ステップ 1** [Configuration] > Remote Access VPN > Clientless SSL VPN Access > [Portal] > [Smart Tunnels] を選択します。
- ステップ 2** アプリケーションを追加するスマートトンネルリストをダブルクリックするか、または [Add] をクリックしてアプリケーションのリストを作成し、[List Name] フィールドにそのリストの名前を入力して [Add] をクリックします。
- たとえば、[Smart Tunnels] ペインで [Add] をクリックし、[List Name] フィールドに Lotus と入力して [Add] をクリックします。
- ステップ 3** [Add or Edit Smart Tunnel List] ダイアログボックスで [Add] をクリックします。
- ステップ 4** [Application ID] フィールドに、スマートトンネルリスト内のエントリに対する一意のインデックスとして使用する文字列を入力します。
- ステップ 5** [Process Name] ダイアログボックスに、ファイル名とアプリケーションの拡張子を入力します。

次の表に、[Application ID] 文字列の例と、Lotus をサポートするために必要となる関連付けられたパスを示します。

表 11: スマートトンネルの例 : Lotus 6.0 Thick Client with Domino Server 6.5.5

アプリケーション ID の例	必要最小限のプロセス名
lotusnotes	notes.exe

アプリケーション ID の例	必要最小限のプロセス名
lotuslnotes	lnotes.exe
lotusntaskldr	ntaskldr.exe
lotusfileret	nfileret.exe

ステップ 6 [OS] の横の [Windows] を選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 アプリケーションごとにステップを繰り返してリストに追加します。

ステップ 9 [Add or Edit Smart Tunnel List] ダイアログボックスで [OK] をクリックします。

ステップ 10 次のようにして、関連付けられたアプリケーションへのスマート トンネル アクセスを許可するグループ ポリシーとローカル ユーザ ポリシーにリストを割り当てます。

- グループ ポリシーにリストを割り当てるには、[Configuration] > **Remote Access VPN** > **Clientless SSL VPN Access** > **Group Policies** > **Add** または [**Edit** > **Portal**] を選択し、[Smart Tunnel List] ドロップダウン リストからスマート トンネル名を選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、[Configuration] > **Remote Access VPN** > **AAA Setup** > **Local Users** > **Add** または [**Edit** > **VPN Policy** > **Clientless SSL VPN**] を選択し、[Smart Tunnel List] ドロップダウンリストからスマート トンネル名を選択します。

トンネリングするアプリケーションの設定の簡略化

スマート トンネル アプリケーション リストは、基本的に、トンネルへのアクセスを許可するアプリケーションのフィルタです。デフォルトでは、ブラウザによって開始されるすべてのプロセスに対してアクセスが許可されます。スマート トンネル 対応ブックマークによって、クライアントレス セッションでは Web ブラウザによって開始されるプロセスのみにアクセスが許可されます。ブラウザ以外のアプリケーションでは、管理者はすべてのアプリケーションをトンネリングすることを選択して、エンドユーザがどのアプリケーションを起動するかを知る必要性をなくすことができます。



(注) この設定は、Windows プラットフォームのみに適用されます。

次の表に、アクセスを許可されるプロセスの状況を示します。

状況	スマート トンネル対応ブックマーク	スマート トンネル アプリケーション アクセス
アプリケーションリストが指定される	アプリケーションリストのプロセス名と一致する任意のプロセスにアクセス権が付与されます。	アプリケーションリストのプロセス名と一致するプロセスのみにアクセス権が付与されます。

状況	スマートトンネル対応ブックマーク	スマートトンネルアプリケーションアクセス
スマートトンネルをオフに切り替える	すべてのプロセス（およびその子プロセス）にアクセス権が付与されます。	プロセスにアクセス権は付与されません。
[Smart Tunnel all Applications] チェックボックスをオンにする	すべてのプロセス（およびその子プロセス）にアクセス権が付与されます。 (注) スマートトンネル以外の Web ページによって開始されたプロセスも含まれます (Web ページが同じブラウザプロセスによって処理される場合)。	ブラウザを開始したユーザが所有するすべてのプロセスにアクセス権が付与されますが、その子プロセスには付与されません。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択します。

ステップ 2 [User Account] ウィンドウで、編集するユーザ名を強調表示します。

ステップ 3 [Edit] をクリックします。[Edit User Account] ウィンドウが表示されます。

ステップ 4 [Edit User Account] ウィンドウの左側のサイドバーで、[VPN Policy] > [Clientless SSL VPN] をクリックします。

ステップ 5 次のいずれかの操作を行います。

- [smart_tunnel_all_applications] チェックボックスをオンにします。リストを作成しなくても、または外部アプリケーションについてエンドユーザが起動する可能性がある実行ファイルを知らなくても、すべてのアプリケーションがトンネリングされます。
- または、次のトンネルポリシー オプションから選択します。
 - [Smart Tunnel Policy] パラメータの [Inherit] チェックボックスをオフにします。
 - ネットワーク リストから選択し、トンネル オプションの 1 つを指定します。指定されたネットワークに対してスマートトンネルを使用する、指定されたネットワークに対してスマートトンネルを使用しない、またはすべてのネットワークトラフィックに対してトンネルを使用する、のいずれかです。

スマートトンネルアクセスに適格なアプリケーションの追加

各 ASA のクライアントレス SSL VPN コンフィギュレーションは、スマートトンネルリストをサポートしています。各リストは、スマートトンネルアクセスに適格な 1 つ以上のアプリ

ケーションを示します。各グループ ポリシーまたはユーザ名は1つのスマート トンネル リストのみをサポートするため、サポートされる各アプリケーションのセットをスマート トンネル リストにグループ化する必要があります。

[Add or Edit Smart Tunnel Entry] ダイアログボックスでは、スマート トンネル リストにあるアプリケーションの属性を指定できます。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に移動し、編集するスマート トンネル アプリケーション リストを選択するか、新しいリストを追加します。

ステップ 2 新しいリストの場合は、アプリケーションまたはプログラムのリストに付ける一意の名前を入力します。スペースは使用しないでください。

スマート トンネル リストのコンフィギュレーションに続いて、クライアントレス SSL VPN のグループポリシーとローカル ユーザ ポリシーの [Smart Tunnel List] 属性の横にリスト名が表示されます。他に設定する可能性があるリストと、内容および目的を区別できるような名前を付けてください。

ステップ 3 [Add] をクリックして、このスマート トンネル リストに必要な数のアプリケーションを追加します。以下に、JSON 配列に格納されるパラメータについて説明します。

- [Application ID] : スマート トンネル リストのエントリに命名する文字列を入力します。このユーザ指定の名前は保存され、GUI に戻されます。文字列はオペレーティング システムに対して一意です。通常は、スマート トンネル アクセスを許可されるアプリケーションに付けられる名前です。異なるパスまたはハッシュ値を指定するアプリケーションの複数バージョンをサポートするには、この属性を使用してエントリを差別化し、オペレーティング システム、および各リスト エントリによってサポートされているアプリケーションの名前とバージョンの両方を指定します。文字列は最大 64 文字まで使用できます。
- [Process Name] : アプリケーションのファイル名またはパスを入力します。ストリングには最大 128 文字を使用できます。

Windows では、アプリケーションにスマート トンネル アクセスを許可する場合に、この値とリモート ホストのアプリケーション パスの右側の値が完全に一致している必要があります。Windows でファイル名のみを指定すると、SSL VPN では、アプリケーションにスマート トンネル アクセスを許可する場合に、リモート ホストに対して場所の制限を強制しません。

アプリケーションのパスを指定し、ユーザが別の場所にインストールした場合は、そのアプリケーションは許可されません。アプリケーションは、入力する値と文字列と右側の値が一致している限り、任意のパスに配置できます。

アプリケーションがリモート ホストの複数のパスのいずれかにある場合に、アプリケーションにスマート トンネル アクセスを認可するには、このフィールドにアプリケーションの名前と拡張子だけを指定するか、またはパスごとに固有のスマート トンネル エントリを作成します。

(注) スマートトンネルアクセスで突然問題が発生する場合は、[Process Name] の値がアップグレードされたアプリケーションに対して最新ではない可能性があります。たとえば、アプリケーションへのデフォルトパスは、そのアプリケーションおよび次のアップグレード版を製造する企業が買収されると変更されることがあります。

Windows の場合、コマンドプロンプトから開始したアプリケーションにスマートトンネルアクセスを追加する場合は、スマートトンネルリストの1つのエントリの [Process Name] に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。これは「cmd.exe」がアプリケーションの親であるためです。

- [OS] : [Windows] または [Mac] をクリックし、アプリケーションのホストオペレーティングシステムを指定します。
- [Hash] (任意、Windowsにのみ該当) : この値を取得するには、アプリケーションのチェックサム (つまり、実行ファイルのチェックサム) を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft ファイルチェックサム整合性検証 (FCIV) を挙げることができます。このユーティリティは、<http://support.microsoft.com/kb/841290/> で入手できます。FCIV のインストール後、スペースを含まないパス (c:/fciv.exe など) 上に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe-sha1 application** と入力して (例: **fciv.exe-sha1 c:\msimn.exe**)、SHA-1 ハッシュを表示します。

SHA-1 ハッシュは、常に 16 進数 40 文字です。

クライアントレス SSL VPN は、アプリケーションにスマートトンネルアクセスの認可を与える前に、[Application ID] に一致するアプリケーションのハッシュを計算します。結果が [Hash] の値と一致すると、アプリケーションのスマートトンネルアクセスが認定されます。

ハッシュを入力することにより、[Application ID] で指定した文字列に一致する不正ファイルに対して SSL VPN が資格を与えないようにしています。チェックサムはアプリケーションのバージョンやパッチに応じて異なるため、[Hash] の入力値が、リモートホストの1つのバージョンやパッチにしか一致しないことがあります。アプリケーションの複数のバージョンのハッシュを指定する場合は、それぞれの [Hash] の値に一意的なスマートトンネルエントリを作成します。

(注) [Hash] に値を入力して、スマートトンネルアクセスで今後のアプリケーションのバージョンやパッチをサポートする必要がある場合は、スマートトンネルリストを更新し続ける必要があります。スマートトンネルアクセスで突然問題が発生する場合は、[Hash] の値を含んでいるアプリケーションリストが、アプリケーションのアップグレードに対して最新ではない可能性があります。ハッシュを入力しないことで、この問題を回避できます。

ステップ 4 [OK] をクリックしてアプリケーションを保存し、このスマートトンネルリストに必要な数だけアプリケーションを作成します。

ステップ 5 スマートトンネルリストの作成が終わったら、そのリストをアクティブにするには、次の手順に従って、グループポリシーまたはローカルユーザポリシーにそのリストを割り当てる必要があります。

- グループポリシーにリストを割り当てるには、**Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add** または **Edit > Portal** を選択し、[Smart Tunnel List] 属性の横にあるドロップダウンリストからスマートトンネル名を選択します。
- ローカルユーザポリシーにリストを割り当てるには、**Config > Remote Access VPN > AAA Setup > Local Users > Add** または **Edit > VPN Policy > Clientless SSL VPN** を選択し、[Smart TunnelList] 属性の横にあるドロップダウンリストからスマートトンネル名を選択します。

表 12: スマートトンネル エントリの例

スマートトンネルのサポ ート	アプリケーション ID (一意の文字列であれ ばどれでも OK)	プロセス名	OS
Mozilla Firefox	firefox	firefox.exe	Windows
Microsoft Outlook Express	outlook-express	msimn.exe	Windows
より制限的なオプション: 実行ファイルが事前定義済みのパスにある場合は、Microsoft Outlook Express 専用。	outlook-express	\Program Files\Outlook Express\msimn.exe	Windows
Mac で新しいターミナル ウィンドウを開く (ワンタイムパスワードが 実装されているので、それ 以降、同じターミナルウ ィンドウでのアプリケーション の起動は失敗します)。	terminal	Terminal	Mac
新しいウィンドウでスマ ートトンネルを開始	new-terminal	Terminal open -a MacTelnet	Mac
Mac ターミナルウ ィンドウでアプリケーション を起動	curl	Terminal curl www.example.com	Mac

スマートトンネルリストについて

グループポリシーとユーザ名ごとに、次のいずれかを行うようにクライアントレス SSL VPN を設定できます。

- ユーザのログイン時に自動的にスマートトンネルアクセスを開始する。
- ユーザのログイン時にスマートトンネルアクセスをイネーブルにする。ただし、ユーザはクライアントレス SSL VPN ポータルページの **[Application Access]** > **[Start Smart Tunnels]** ボタンを使用して、スマートトンネルアクセスを手動で開始する必要がある。



(注) スマートトンネルログオンオプションは、各グループポリシーとユーザ名に対して互いに排他的です。1つだけ使用してください。

スマートトンネル自動サインオンサーバリストの作成

[Add Smart Tunnel Auto Sign-on Server List] ダイアログボックスで、スマートトンネルのセットアップ中にログインクレデンシャルの送信を自動化するサーバのリストを追加または編集できます。スマートトンネルの自動サインオンは、Internet Explorer および Firefox で利用可能です。

手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に移動し、[Smart Tunnel Auto Sign-on Server List] が展開されていることを確認します。
- ステップ 2** [Add] をクリックして、リモートサーバのリストの一意の名前を入力します。設定する可能性がある他のリストと内容や目的を区別できるような名前を指定してください。文字列は最大 64 文字まで使用できます。スペースは使用しないでください。

次のタスク



- (注) スマートトンネルの自動サインオンリストを作成した後は、クライアントレス SSL VPN グループポリシーおよびローカルポリシーコンフィギュレーションの下の [Auto Sign-on Server List] 属性の横に、リスト名が表示されます。

スマート トンネル自動サインオン サーバリストへのサーバの追加

次の手順では、スマート トンネル接続での自動サインオンを提供するサーバのリストにサーバを追加し、そのリストをグループ ポリシーまたはローカル ユーザに割り当てる方法について説明します。

手順

ステップ 1 [Configuration]>[Remote Access VPN]>[Clientless SSL VPN Access]>[Portal]>[Smart Tunnels] に移動し、いずれかのリストを選択して、[Edit] をクリックします。

ステップ 2 [Add Smart Tunnel Auto Sign-On Server List] ダイアログで [Add] ボタンをクリックし、スマート トンネル サーバをもう 1 つ追加します。

ステップ 3 自動認証を行うサーバのホスト名または IP アドレスを入力します。

- [Hostname] を選択する場合、自動認証を行うホスト名またはワイルドカードマスクを入力します。次のワイルドカード文字を使用できます。
 - * : 任意の数の文字を一致させる、またはどの文字も一致させません。
 - ? : 単一の文字を一致させます。
 - [] : かつこ内に指定された範囲内の、任意の 1 文字を一致させる。
 - たとえば、*.example.com と入力します。このオプションを使用すると、IP アドレスのダイナミックな変更からコンフィギュレーションを保護します。
- [IP Address] を選択する場合、IP アドレスを入力します。

(注) Firefox では、ワイルドカードを使用したホスト マスク、IP アドレスを使用したサブネット、またはネットマスクをサポートしていません。正確なホスト名または IP アドレスを使用する必要があります。たとえば、Firefox では、*.cisco.com を入力した場合、email.cisco.com をホストする自動サインオンは失敗します。

ステップ 4 [Windows Domain] (オプション) : 認証が必要な場合、クリックして Windows ドメインをユーザ名に追加します。このオプションを使用する場合は、1 つ以上のグループ ポリシーまたはローカルユーザポリシーにスマート トンネルリストを割り当てる際に、ドメイン名を指定する必要があります。

ステップ 5 [HTTP-based Auto Sign-On] (オプション)

- [Authentication Realm] : レルムは Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。ここで自動サインオンが設定され、レルムの文字列が指定されたら、ユーザはレルムの文字列を Web アプリケーション (Outlook Web Access など) で設定し、Web アプリケーションにサインオンすることなくアクセスできます。

イントラネットの Web ページのソース コードで使用されるアドレス形式を使用します。ブラウザ アクセス用にスマート トンネル自動サインオンを設定しており、一部の Web

ページでホスト名が使用され、他の Web ページで IP アドレスが使用されている場合、あるいはどちらが使用されているかわからない場合は、両方を異なるスマートトンネル自動サインオン エントリで指定します。それ以外の場合、Web ページのリンクで、指定されたフォーマットとは異なるフォーマットが使用されると、ユーザがリンクをクリックしても開きません。

(注) 対応するレلمがわからない場合、管理者はログインを一度実行し、プロンプトダイアログから文字列を取得する必要があります。

- [PortNumber] : 対応するホストのポート番号を指定します。Firefox では、ポート番号が指定されていない場合、自動サインオンはデフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。

ステップ 6 [OK] をクリックします。

ステップ 7 スマート トンネル自動サインオン サーバリストのコンフィギュレーションに続いて、そのリストをアクティブにするには、グループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、次の手順を実行します。
 1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] の順に進み、グループ ポリシーを開きます。
 2. [Portal] タブを選択し、[Smart Tunnel] 領域を見つけ、[Auto Sign-on Server List] 属性の横にあるドロップダウン リストから自動サインオン サーバリストを選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、次の手順を実行します。
 1. **Configuration > Remote Access VPN > AAA/Local Users > Local Users** を選択し、自動サインオン サーバリストを割り当てるローカル ユーザを編集します。
 2. [VPN Policy] > [Clientless SSL VPN] の順に進み、[Smart Tunnel] 領域の下の [Auto Sign-on Server] 設定を探します。
 3. [Inherit] をオフにして、[Auto Sign-on Server List] 属性の横にあるドロップダウン リストからサーバリストを選択します。

スマート トンネル アクセスのイネーブル化とオフへの切り替え

デフォルトでは、スマート トンネルはオフになっています。

スマート トンネルアクセスをイネーブルにした場合、ユーザは、クライアントレス SSL VPN ポータルページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、スマート トンネルアクセスを手動で開始する必要があります。

スマート トンネルからのログオフの設定

ここでは、スマートトンネルからの適切なログオフ方法について説明します。すべてのブラウザウィンドウを閉じるか、通知アイコンを右クリックしてログアウトを確認すると、スマートトンネルからログオフできます。



- (注) ポータルにあるログアウトボタンを使用することを強くお勧めします。この方法は、クライアントレス SSL VPN 用であり、スマート トンネルが使用されているかどうかに関係なくログオフが行われます。通知アイコンは、ブラウザを使用しないスタンドアロンアプリケーションを使用する場合に限り使用する必要があります。

親プロセスが終了した場合のスマート トンネルからのログオフの設定

この方法では、ログオフを示すためにすべてのブラウザを閉じることが必要です。スマートトンネルのライフタイムは現在、プロセスのライフタイムの開始に結び付けられています。たとえば、Internet Explorer からスマート トンネルを開始した場合、iexplore.exe が実行されていないとスマート トンネルがオフになります。スマート トンネルは、ユーザがログアウトせずにすべてのブラウザを閉じた場合でも、VPN セッションが終了したと判断します。



- (注) 場合によっては、ブラウザプロセスがエラーの結果として、意図的にではなく残っていることがあります。また、Secure Desktop を使用しているときに、ユーザが Secure Desktop 内ですべてのブラウザを閉じてもブラウザプロセスが別のデスクトップで実行されている場合があります。したがって、スマートトンネルは、現在のデスクトップで表示されているウィンドウがない場合にすべてのブラウザ インスタンスが終了したと見なします。

通知アイコンを使用したスマート トンネルからのログオフの設定

ブラウザを閉じてセッションが失われないようにするために、ペアレントプロセスの終了時にログオフをオフに切り替えることもできます。この方法では、システムトレイの通知アイコンを使用してログアウトします。アイコンは、ユーザがアイコンをクリックしてログアウトするまで維持されます。ユーザがログアウトする前にセッションの期限が切れた場合、アイコンは、次回に接続を試行するまで維持されます。セッション ステータスがシステムトレイで更新されるまで時間がかかることがあります。



- (注) このアイコンが、SSL VPN からログアウトする別の方法です。これは、VPN セッションステータスのインジケータではありません。

手順

-
- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。
- ステップ 2** [Click on smart-tunnel logoff > icon in the system tray] オプション ボタンをイネーブルにします。
- ステップ 3** ウィンドウの [Smart Tunnel Networks] 部分で、[Add] をオンにして、アイコンを含めるネットワークの IP アドレスとホスト名の両方を入力します。
- (注) アイコンを右クリックすると、SSL VPNからのログアウトをユーザに求める単一のメニュー項目が表示されます。
-

クライアントレス SSL VPN キャプチャ ツール

クライアントレス SSL VPN CLI には、WebVPN 接続では正しく表示されない Web サイトに関する情報を記録できるキャプチャツールが含まれています。このツールが記録するデータは、シスコカスタマーサポートの担当者が問題のトラブルシューティングを行う際に役立ちます。

クライアントレス SSL VPN キャプチャ ツールの出力には次の 2 つのファイルが含まれます。

- Web ページのアクティビティに応じて `mangled.1,2,3,4...` など。mangle ファイルは、クライアントレス SSL VPN 接続のページを転送する VPN コンセントレータの html のアクションを記録します。
- Web ページのアクティビティに応じて `original.1,2,3,4...` など。元のファイルは、URL が VPN コンセントレータに送信したファイルです。

キャプチャ ツールによってファイル出力を開き、表示するには、[Administration] > [File Management] に移動します。出力ファイルを圧縮し、シスコサポート担当者に送信します。



- (注) クライアントレス SSL VPN キャプチャ ツールを使用すると、VPN コンセントレータのパフォーマンスが影響を受けます。出力ファイルを生成した後に、キャプチャ ツールを必ずオフに切り替えます。
-

ポータル アクセス ルールの設定

この拡張機能により、カスタマーは、HTTP ヘッダー内に存在するデータに基づいて、クライアントレス SSL VPN セッションを許可または拒否するグローバルなクライアントレス SSL VPN アクセス ポリシーを設定できます。ASA はクライアントレス SSL VPN セッションを拒否する場合、ただちにエンドポイントにエラー コードを返します。

ASA は、このアクセス ポリシーを、エンドポイントが ASA に対して認証する前に評価します。その結果、拒否の場合は、エンドポイントからの追加の接続試行による ASA の処理リソースの消費はより少なくなります。

手順

ステップ 1 ASDM を起動し、**[Configuration]>[Remote Access VPN]>[Clientless SSL VPN Access]>[Portal]>[Portal Access Rule]** を選択します。

[Portal Access Rule] ウィンドウが開きます。

ステップ 2 [Add] をクリックしてポータルアクセスルールを作成するか、既存のルールを選択して **[Edit]>.** をクリックします。

[Add Portal Access Rule] または [Edit Portal Access Rule] ダイアログボックスが開きます。

ステップ 3 1 ~ 65535 のルール番号を [Rule Priority] フィールドに入力します。

ルールは 1 ~ 65535 のプライオリティの順序で処理されます。

ステップ 4 [User Agent] フィールドに、HTTP ヘッダーで検索するユーザ エージェントの名前を入力します。

- 文字列を広範囲に指定するには、文字列をワイルドカード (*) で囲みます。たとえば、*Thunderbird* です。検索文字列でワイルドカードを使用することを推奨します。ワイルドカードを使用しないと、ルールがどの文字列とも一致しないか、予期したよりも大幅に少ない文字列としか一致しない場合があります。

- 文字列にスペースが含まれている場合、ASDM によって、ルールの保存時に文字列の最初と最後に自動的に引用符が追加されます。たとえば、my agent と入力した場合、ASDM によってこの文字列は "my agent" として保存されます。ASA では my agent の一致が検索されます。

スペースを含む文字列に引用符を追加しないでください。ただし、文字列に追加した引用符を ASA で照合させる場合を除きます。たとえば、"my agent" と入力すると、ASDM はその文字列を "\"my agent\" \" として保存するため、"my agent" を検出しようとはしますが、my agent は見つかりません。

- スペースを含む文字列でワイルドカードを使用する場合は、文字列全体をワイルドカードで開始して終了します。たとえば、*my agent* です。ASDM によって、ルールの保存時に、その文字列は自動的に引用符で囲まれます。

ステップ 5 [Action] フィールドで、[Deny] または [Permit] を選択します。

ASA は、この設定に基づいて、クライアントレス SSL VPN 接続を拒否または許可します。

ステップ 6 HTTP メッセージ コードを [Returned HTTP Code] フィールドに入力します。

HTTP メッセージ番号 403 がフィールドにあらかじめ入力されており、これがポータルアクセスルールのデフォルト値です。メッセージコードの有効な範囲は 200 ~ 599 です。

ステップ7 [OK] をクリックします。

ステップ8 [Apply] をクリックします。

クライアントレス SSL VPN のパフォーマンスの最適化

ASA には、クライアントレス SSL VPN のパフォーマンスと機能を最適化する複数の方法があります。パフォーマンスの改善には、Web オブジェクトのキャッシングと圧縮が含まれます。機能性の調整には、コンテンツ変換およびプロキシバイパスの制限の設定が含まれます。その他に、APCF でコンテンツ変換を調整することもできます。

コンテンツ変換の設定

デフォルトでは、ASA は、コンテンツ変換およびリライト エンジンを通じてすべてのクライアントレス SSL VPN トラフィックを処理します。これには、JavaScript や Java などの高度な要素からプロキシHTTPへのトラフィックも含まれますが、そのようなトラフィックでは、ユーザがアプリケーションに SSL VPN デバイス内部からアクセスしているのか、それらのデバイスに依存せずにアクセスしているのかに応じて、セマンティックやアクセス コントロールのルールが異なる場合があります。

Web リソースによっては、高度に個別の処理が要求される場合があります。次の項では、このような処理を提供する機能について説明します。組織や関係する Web コンテンツの要件に応じてこれらの機能のいずれかを使用する場合があります。

プロキシバイパスの使用

プロキシバイパスを使用するように ASA を設定できます。この設定は、プロキシバイパスが提供する特別なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合に行います。プロキシバイパスはコンテンツの書き換えに代わる手法であり、元のコンテンツの変更を最小限に抑えます。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

プロキシバイパスには複数のエントリを設定できます。エントリを設定する順序は重要ではありません。インターフェイスとパスマスク、またはインターフェイスとポートにより、プロキシバイパスルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシバイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートが ASA にアクセスできるようにするために、ファイアウォールコンフィギュレーションの変更が必要になることがあります。この制限を回避するには、パス マスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化の可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、www.example.com/hrbenefits という URL では、hrbenefits がパスになります。同様に、www.example.com/hrinsurance という URL では、hrinsurance がパスです。すべての hr サイトで

プロキシバイパスを使用する場合は、* (ワイルドカード) を /hr* のように使用して、コマンドを複数回使用しないようにできます。

ASA がコンテンツ リライトをほとんどまたはまったく実行しない場合のルールを設定できます。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Proxy Bypass] の順に進みます。

ステップ 2 プロキシバイパスのインターフェイス名を選択します。

ステップ 3 プロキシバイパス用のポートまたは URI を指定します。

- [Port] : (オプション ボタン) プロキシバイパスにポートを使用します。有効なポート番号は 20000 ~ 21000 です。
- [Port] (フィールド) : ASA がプロキシバイパス用に予約する大きな番号のポートを入力します。
- [Path Mask] : (オプション ボタン) プロキシバイパスに URL を使用します。
- [Path Mask] : (フィールド) プロキシバイパス用の URL を入力します。この URL には、正規表現を使用できます。

ステップ 4 プロキシバイパスのターゲット URL を定義します。

- [URL] : (ドロップダウン リスト) プロトコルとして、http または https をクリックします。
- [URL] (テキスト フィールド) : プロキシバイパスを適用する URL を入力します。

ステップ 5 リライトするコンテンツを指定します。選択肢は、なし、または XML、リンク、およびクッキーの組み合わせです。

- [XML] : XML コンテンツをリライトする場合に選択します。
 - [Hostname] : リンクをリライトする場合に選択します。
-



第 17 章

クライアントレス SSL VPN リモート ユーザ

この章では、ユーザ リモート システムの設定要件と作業の概要を説明します。また、ユーザがクライアントレス SSL VPN の使用を開始できるようにします。内容は次のとおりです。



(注) ASA がクライアントレス SSL VPN 用に設定されていることを確認します。

- [クライアントレス SSL VPN リモート ユーザ \(389 ページ\)](#)

クライアントレス SSL VPN リモート ユーザ

この章では、ユーザ リモート システムの設定要件と作業の概要を説明します。また、ユーザがクライアントレス SSL VPN の使用を開始できるようにします。内容は次のとおりです。



(注) ASA がクライアントレス SSL VPN 用に設定されていることを確認します。

ユーザ名とパスワード

ネットワークによっては、リモートセッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業 アプリケーションの一部またはすべてにログインする必要があります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。必要なアクセス権があることを確認してください。

次の表に、クライアントレス SSL VPN ユーザが理解しておく必要のあるユーザ名とパスワードのタイプを示します。

表 13: クライアントレス SSL VPN ユーザに通知するユーザ名とパスワード

ログインユーザ名/パスワードのタイプ		入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
Internet Service Provider : インターネットサービスプロバイダー	インターネットへのアクセス	インターネットサービスプロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN セッションを開始するとき
File Server	リモートファイルサーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモートファイルサーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモートメールサーバへのアクセス	電子メール メッセージの送受信

セキュリティ ヒントの通知

次のセキュリティのヒントを通知してください。

- クライアントレス SSL VPN セッションから必ずログアウトします。ログアウトするには、クライアントレス SSL VPN ツールバーの **logout** アイコンをクリックするか、またはブラウザを閉じます。
- クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。クライアントレス SSL VPN は、企業ネットワーク上のリモートコンピュータやワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。したがって、ユーザが **HTTPS** 以外の Web リソース（インターネット上や内部ネットワーク上にあるリソース）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信はセキュアではありません。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

次の表に、クライアントレス SSL VPN を使用するためのリモート システムの設定に関連するタスク、タスクの要件と前提条件、および推奨される使用法を示します。

各ユーザ アカウントを異なる設定にしたことにより、クライアントレス SSL VPN ユーザがそれぞれに使用できる機能が異なる可能性があります。この表では、情報をユーザ アクティビティ別にまとめています。

表 14: クライアントレス SSL VPN リモート システムの設定およびエンド ユーザの要件

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN の起動	インターネットへの接続	<p>サポートされているインターネット接続は、次のとおりです。</p> <ul style="list-style-type: none"> • 家庭のDSL、ケーブル、ダイヤルアップ • 公共のキオスク • ホテルの回線 • 空港の無線ノード • インターネットカフェ
	クライアントレス SSL VPN がサポートされているブラウザ	<p>クライアントレス SSL VPN には、次のブラウザを推奨します。他のブラウザでは、クライアントレス SSL VPN 機能が完全にサポートされていない可能性があります。</p> <p>Microsoft Windows の場合：</p> <ul style="list-style-type: none"> • Internet Explorer 8 • Firefox 8 <p>Linux の場合：</p> <ul style="list-style-type: none"> • Firefox 8 <p>Mac OS X の場合：</p> <ul style="list-style-type: none"> • Safari 5 • Firefox 8
	ブラウザでイネーブルにされているクッキー	ポートフォワーディングを介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
	クライアントレス SSL VPN の URL	

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
		<p>HTTPS アドレスの形式は次のとおりです。</p> <p><code>https://address</code></p> <p><code>address</code> は、クライアントレス SSL VPN がイネーブルになっている ASA（またはロード バランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、<code>https://10.89.192.163</code> または <code>https://cisco.example.com</code> のようになります。</p>
	クライアントレス SSL VPN のユーザー名とパスワード	
	(任意) ローカル プリンタ	クライアントレス SSL VPN は、Web ブラウザからネットワークプリンタへの印刷をサポートしていません。ローカルプリンタへの印刷はサポートされています。

タスク	リモートシステムまたはエンドユーザの要件	仕様または使用上の推奨事項
クライアントレス SSL VPN 接続でのフローティング ツールバーの使用		<p>フローティングツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。</p> <p>ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。</p> <p>フローティングツールバーは、現在のクライアントレス SSL VPN セッションを表します。[Close] ボタンをクリックすると、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。</p> <p>ヒント テキストフィールドにテキストを貼り付けるには、Ctrl+V キーを使用します（クライアントレス SSL VPN ツールバーでは、右クリックは有効ではありません）。</p>

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
Web ブラウジング	保護されている Web サイトのユーザ名とパスワード	クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。 「 セキュリティ ヒントの通知 (390 ページ) 」を参照してください。
		<p>クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。</p> <ul style="list-style-type: none"> • クライアントレス SSL VPN のタイトルバーが各 Web ページの上部に表示される。 • Web サイトへのアクセス方法： <ul style="list-style-type: none"> • [Clientless SSL VPN Home] ページ上の [Enter Web Address] フィールドに URL を入力する。 • [Clientless SSL VPN Home] ページ上にある設定済みの Web サイトリンクをクリックする。 • 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする。 <p>また、特定のアカウントの設定によっては、次のようになる場合もあります。</p> • 一部の Web サイトがブロックされている。 • アクセス可能な Web サイトが、[Clientless SSL VPN Home] ページにリンクとして表示されるサイトに限定される。

タスク	リモートシステムまたはエンドユーザの要件	仕様または使用上の推奨事項
ネットワークブラウジングとファイル管理	共有リモートアクセス用に設定されたファイルアクセス権	クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。
	保護されているファイルサーバのサーバ名とパスワード	—
	フォルダとファイルが存在するドメイン、ワークグループ、およびサーバ名	ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。
	—	コピー処理の進行中は、 Copy File to Server コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
アプリケーションの使用 (ポートフォワーディングまたはアプリケーション アクセスと呼ばれる)	(注) Mac OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。	
	(注) この機能を使用するには、Oracle Java Runtime Environment (JRE) をインストールし、ローカルクライアントを設定する必要があります。これには、ローカルシステムで管理者の許可が必要であるため、ユーザがパブリックリモートシステムから接続した場合は、アプリケーションを使用できない可能性があります。	
	アプリケーションを使用した後、ユーザは [Close] アイコンをクリックして必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体にアクセスできなくなる可能性があります。	
	インストール済みのクライアントアプリケーション	—
	ブラウザでイネーブルにされているクッキー	—
	管理者特権	ユーザは、DNS 名を使用してサーバを指定する場合、ホストファイルを変更するのに必要になるため、コンピュータに対する管理者アクセス権が必要になります。
Java Runtime Environment (JRE) がインストール済み。 ブラウザで JavaScript をイネーブルにする必要があります。デフォルトでは有効に設定されています。		

タスク	リモートシステムまたはエンドユーザの要件	仕様または使用上の推奨事項
		<p>JRE がインストールされていない場合は、ポップアップウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。</p> <p>まれに、Java 例外エラーで、ポートフォワーディングアプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。 2. Java アイコンがコンピュータのタスクバーに表示されていないことを確認します。Java のインスタンスをすべて閉じます。 3. クライアントレス SSL VPN セッションを確立し、ポートフォワーディング Java アプレットを起動します。

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
	<p>設定済みのクライアント アプリケーション (必要な場合)。</p> <p>(注) Microsoft Outlook クライアントの場合、この設定手順は不要です。</p> <p>Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。</p> <p>Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] の値をチェックします。</p> <ul style="list-style-type: none"> • [Remote Server] にサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。 • [Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。 	<p>クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. リモート システムでクライアントレス SSL VPN を起動し、[Clientless SSL VPN Home] ページで Application Access リンクをクリックします。[Application Access] ウィンドウが表示されます。 2. [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。 3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。 <p>(注) クライアントレス SSL VPN で実行されているアプリケーションで URL (電子メール内の URL など) をクリックしても、クライアントレス SSL VPN ではそのサイトは開きません。クライアントレス SSL VPN でこのようなサイトを開くには、[Enter (URL) Address] フィールドに URL をカット アンド ペーストします。</p>
<p>アプリケーション アクセスを介した電子メールの使用</p>	<p>Application Access の要件を満たす (「アプリケーションの使用」を参照)</p>	<p>電子メールを使用するには、[Clientless SSL VPN Home] ページから Application Access を起動します。これにより、メールクライアントが使用できるようになります。</p>
	<p>(注) IMAP クライアントの使用中にメールサーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。</p>	
	<p>他の電子メールクライアント</p>	<p>Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。</p>

タスク	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
Web アクセスを介した電子メールの使用	インストールされている Web ベースの電子メール製品	サポートされている製品は次のとおりです。 <ul style="list-style-type: none"> • Outlook Web Access 最適な結果を得るために、Internet Explorer 8.x 以上、または Firefox 8 で OWA を使用してください。 • Lotus Notes <p>その他の Web ベースの電子メール製品も動作しますが、動作確認は行っていません。</p>
電子メール プロキシを介した電子メールの使用	インストール済みの SSL 対応メールアプリケーション ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。	サポートされているメールアプリケーションは次のとおりです。 <ul style="list-style-type: none"> • Microsoft Outlook • Microsoft Outlook Express バージョン 5.5 および 6.0 <p>その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。</p>
	設定済みのメールアプリケーション	

クライアントレス SSL VPN データのキャプチャ

CLI capture コマンドを使用すると、クライアントレス SSL VPN 接続では正しく表示されない Web サイトに関する情報を記録できます。このデータは、シスコカスタマーサポートエンジニアによる問題のトラブルシューティングに役立ちます。次の各項では、キャプチャコマンドの使用方法について説明します。

- [キャプチャ ファイルの作成 \(401 ページ\)](#)
- [ブラウザによるキャプチャ データの表示 \(401 ページ\)](#)



(注) クライアントレス SSL VPN キャプチャをイネーブルにすると、ASA のパフォーマンスが影響を受けます。トラブルシューティングに必要なキャプチャ ファイルを生成したら、キャプチャを必ずオフに切り替えます。

キャプチャ ファイルの作成

手順

ステップ 1 クライアントレス SSL VPN キャプチャ ユーティリティを開始してパケットをキャプチャします。

```
capture capture-name type webvpn user csslvpn-username
```

- *capture_name* は、キャプチャに割り当てる名前です。これはキャプチャファイルの名前の先頭にも付加されます。
- *csslvpn-username* は、キャプチャの対象となるユーザ名です。

例 :

```
hostname# capture hr type webvpn user user2
```

ステップ 2 コマンドの **no** バージョンを使用してキャプチャを停止します。

```
no capture capture-name
```

例 :

```
hostname# no capture hr
```

キャプチャ ユーティリティは *capture-name.zip* ファイルを作成します。このファイルはパスワード **koleso** で暗号化されます。

ステップ 3 .zip ファイルをシスコに送信するか、Cisco TAC サービス リクエストに添付します。

ステップ 4 .zip ファイルの内容を確認するには、パスワード **koleso** を使用してファイルを解凍します。

ブラウザによるキャプチャ データの表示

手順

ステップ 1 クライアントレス SSL VPN キャプチャ ユーティリティを開始します。

```
capture capture-name type webvpn user csslvpn-username
```

- *capture_name* は、キャプチャに割り当てる名前です。これはキャプチャファイルの名前の先頭にも付加されます。
- *csslvpn-username* は、キャプチャの対象となるユーザ名です。

例 :

```
hostname# capture hr type webvpn user user2
```

ステップ2 ブラウザを開き、[Address] ボックスに次のように入力します。

https://IP address or hostname of the ASA/webvpn_capture.html

キャプチャされたコンテンツが **sniffer** 形式で表示されます。

ステップ3 コマンドの **no** バージョンを使用してキャプチャを停止します。

no capture capture-name

例：

```
hostname# no capture hr
```



第 18 章

クライアントレス SSL VPN ユーザ

- パスワードの管理 (403 ページ)
- クライアントレス SSL VPN でのシングル サインオンの使用 (405 ページ)
- 自動サインオンの使用 (411 ページ)
- ユーザ名とパスワードの要件 (413 ページ)
- セキュリティ ヒントの通知 (414 ページ)
- クライアントレス SSL VPN の機能を使用するためのリモート システムの設定 (414 ページ)

パスワードの管理

必要に応じて、パスワードの期限切れが近づいたときにエンド ユーザに警告するように ASA を設定できます。

ASA は、RADIUS および LDAP プロトコルのパスワード管理をサポートしています。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネルグループのパスワード管理を設定できます。

パスワード管理を設定すると、ASA はリモート ユーザのログイン時に、現在のパスワードの期限切れ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。

このコマンドは、この通知をサポートしている AAA サーバに対して有効です。

ASA のリリース 7.1 以降では、通常、LDAP による認証時または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPsec VPN クライアント
- クライアントレス SSL VPN

RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバとのみ通信しているように見えます。

始める前に

- 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。
- 認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun 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 サーバにアクセスするために ASA に設定されている DN が、サーバ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。
- MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーにお問い合わせください。
- Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポートされません。
- LDAP でパスワードを変更するには、市販の LDAP サーバ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。
- 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。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] > [Add or Edit] > [Advanced] > [General] > [Password Management] に移動します。

ステップ 2 [Enable password management] オプションをクリックします。

クライアントレス SSL VPN でのシングルサインオンの使用

SAML 2.0 による SSO

SSO および SAML 2.0 について

ASA は SAML 2.0 をサポートしています。これにより、クライアントレス VPN のエンドユーザは、クレデンシャルを1回だけ入力して、クライアントレス VPN とプライベートネットワーク外部のその他の SAAS アプリケーションと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、エンドユーザは一度サインインするだけで、クライアントレス VPN などのあらゆるサービスにアクセスできるようになります。

さらに、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、組み込みブラウザとの SAML 統合が拡張され、これが以前のリリースからのネイティブ (外部) ブラウザ統合に置き換わります。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。

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。クライアントレス VPN のエンドユーザは、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

エンドユーザがクライアントレス VPN を使用して ASA アクセスし、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. クライアントレス VPN のエンドユーザが 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 がエンドユーザのクレデンシャルを確認し、エンドユーザがログインします。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のクレデンシャルを確認します。エンドユーザ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) サーバを IdP NTP サーバ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 とユーザ間のすべてのトラフィックは変換されます。ユーザがログインすると、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、ユーザのユーザ名を特定し、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、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。
- SAML 2.0 SSO は、内部 SAML IdP と SP をサポートしておらず、プライベート ネットワーク外部の SAML IdP と SP のみをサポートしています。
- 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。
- DAP 評価で使用可能な SAML 認証属性は (AAA サーバから RADIUS 認証応答で送信される RADIUS 属性と同様に) サポートされていません。ASA は、DAP ポリシーで SAML 対応トンネルグループをサポートします。ただし、ユーザ名属性は SAML ID プロバイダーによってマスクされるため、SAML 認証の使用中はユーザ名属性を確認できません。
- 既存のクライアントレス VPN のタイムアウト設定は、まだ SAML セッションに適用されます。
- 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。
- AnyConnect で SAML を使用する場合は、次の追加ガイドラインに従ってください。
 - 信頼できないサーバ証明書は、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 で内部サーバにアクセスすることはできません。
 - SAML IdP NameID 属性は、ユーザのユーザ名を特定し、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。
 - VPN ロードバランシングまたは DNS ロードバランシングは使用できません。

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 (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 2 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。

ステップ 3 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Single Sign On Servers] に移動します。

すでに設定されているすべての SAML 2.0 IdP が一覧表示されます。[Add] または [Delete] の次に説明されているように、[Edit] を使用してリストを編集できます。

ステップ 4 [Add] をクリックして、新しい IdP エントリを追加します。

ステップ 5 説明に従って、次のフィールドに入力します。

- [Sign In URL] : IdP にサインインするための URL。url value は 4 ~ 500 文字の範囲で指定します。
- [Sign Out URL] (オプション) : IdP からサインインするときのリダイレクト先 URL。url value は 4 ~ 500 文字の範囲で指定します。
- [Base URL] (オプション) : エンドユーザを 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。

- [Identity Provider Certificate] : 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。すでに設定されているトラストポイントを選択します。

- [Service Provider Certificate] (オプション) : 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) 証明書含むトラストポイントを指定します。すでに設定されているトラストポイントを選択します。
- [Request Signature] : ドロップダウンを使用して、SAML IdP サーバに対して希望する署名方法を選択します。rsa-sha1、rsa-sha256、rsa-sha384、rsa-sha512 から選択できます。
- [Request Timeout] (オプション) : SAML 要求のタイムアウト。
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。
- [Enable the Signature] : 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。
- [Enable the Internal] : IdP が内部ネットワーク内かどうかを決定するには、有効または無効 (デフォルト設定) にします。
(注) 内部 IdP を使用してログインした後に SSO で内部サーバにアクセスすることはできません。
- Enable the Force Re-authentication : SAML 認証要求が発生するときにこの設定を有効にしていると、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なります。再認証の強制有効がデフォルト値です。

ステップ 6 [OK] をクリックします。
新しい IdP エンティティがこのページに一覧表示されます。

例

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 \(410 ページ\)](#) 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

特定のトンネル グループを SAML SP として設定するには、次の手順を実行します。



(注) AnyConnect 4.4 または 4.5 で SAML 認証を使用していて、ASA バージョン 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) (リリース日付: 2018 年 4 月 18 日) を展開している場合、SAML のデフォルトの動作は、AnyConnect 4.4 および 4.5 でサポートされていない組み込みブラウザになります。したがって、[Connection Profiles] 領域で [SAML External Browser] チェックボックスをオンにして、AnyConnect 4.4 および 4.5 クライアントが外部 (ネイティブ) ブラウザを使用して、SAML で認証できるようにする必要があります。

[SAML External Browser] チェックボックスは、AnyConnect 4.6 以降にアップグレードするクライアントの移行のために使用されます。セキュリティ上の制限のため、AnyConnect ソフトウェアをアップグレードする際の一時的な移行の一環としてのみこのソリューションを使用してください。今後、このチェックボックス自体がサポートされなくなります。

手順

- ステップ 1** ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] > [Add/Edit] に移動します。
- ステップ 2** このトンネル グループの認証方式として ([Authentication] [Method]) [Saml] を選択します。
- ステップ 3** [SAML Identity Provider] セクションで、すでに設定されている [SAML Server] を選択するか、[Manage] をクリックして新規に作成します。
既存の SAML 設定を変更した場合、この操作によってトンネル グループの IdP が再度有効になります。
- ステップ 4** [OK] をクリックします。
[Preview CLI Commands] ウィンドウが表示され、承認した変更に基づいて生成された CLI コマンドが示されます。[Send] をクリックすると ASA にコマンドを送信できます。

自動サインオンの使用

[Auto Sign-on] ウィンドウまたはタブでは、クライアントレス SSL VPN ユーザの自動サインオンを設定または編集できます。自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。特定の内部サーバに対して自動サインオンを設定すると、ASA は、クライアントレス SSL VPN ユーザが ASA へのログオン時に入力したログインクレデンシャル (ユーザ名とパスワード) をそれら特定の内部サーバに渡します。特定範囲のサーバの特定の認証方式に応答するように、ASA を設定します。応答するように ASA に設定できる認証方式は、Basic (HTTP) 方式、NTLM 方式、FTP および CIFS 方式を使用する認証、またはこれらの方式すべてを使用する認証から構成されます。

ユーザ名とパスワードのルックアップが ASA で失敗した場合は、空の文字列で置き換えられ、動作は自動サインオンが不可の場合の状態に戻されます。

自動サインオンは、特定の内部サーバに SSO を設定する直接的な方法です。この項では、自動サインオンを行うように SSO をセットアップする手順について説明します。

次のフィールドが表示されます。

- [IP Address] : 次の [Mask] と組み合わせて、認証されるサーバの IP アドレスの範囲を [Add/Edit Auto Sign-on] ダイアログボックスで設定されたとおりに表示します。サーバは、サーバの URI またはサーバの IP アドレスとマスクで指定できます。
- [Mask] : 前の [IP Address] と組み合わせて、[Add/Edit Auto Sign-on] ダイアログボックスで自動サインオンをサポートするように設定されたサーバの IP アドレスの範囲を表示します。
- [URI] : [Add/Edit Auto Sign-on] ダイアログボックスで設定されたサーバを識別する URI マスクを表示します。
- [Authentication Type] : [Add/Edit Auto Sign-on] ダイアログボックスで設定された認証のタイプ (Basic (HTTP) 、NTLM、FTP と CIFS、またはこれらの方式すべて) を表示します。

始める前に

- 認証が不要なサーバ、または ASA とは異なるクレデンシャルを使用するサーバでは、自動サインオンをイネーブルにしないでください。自動サインオンがイネーブルの場合、ASA は、ユーザストレージにあるクレデンシャルに関係なく、ユーザが ASA へのログオン時に入力したログインクレデンシャルを渡します。
- 一定範囲のサーバに対して 1 つの方式 (HTTP Basic など) が設定されているときに、その中の 1 台のサーバが異なる方式 (NTLM など) で認証を試みた場合、ASA はユーザのログインクレデンシャルをそのサーバに渡しません。

手順

-
- ステップ 1** クリックして自動サインオン命令を追加または編集します。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。
- ステップ 2** [Auto Sign-on] テーブルで選択した自動サインオン命令を削除する場合にクリックします。
- ステップ 3** [IP Block] をクリックして、IP アドレスとマスクを使用して内部サーバの範囲を指定します。
- [IP Address] : 自動サインオンを設定する範囲の最初のサーバの IP アドレスを入力します。
 - [Mask] : [subnet mask] メニューで、自動サインオンをサポートするサーバのサーバアドレス範囲を定義するサブネットマスクを選択します。
- ステップ 4** [URI] をクリックして、URI によって自動サインオンをサポートするサーバを指定し、このボタンの横にあるフィールドに URI を入力します。
- ステップ 5** サーバに割り当てられる認証方式を決定します。指定された範囲のサーバに対して、Basic HTTP 認証要求、NTLM 認証要求、FTP および CIFS 認証要求、またはこれら方式のいずれかを使用している要求に応答するように、ASA を設定できます。

- [Basic] : サーバが Basic (HTTP) 認証をサポートする場合は、このボタンをクリックします。
- [NTLM] : サーバが NTLMv1 認証をサポートする場合は、このボタンをクリックします。
- [FTP/CIFS] : サーバが FTP と CIFS の認証をサポートする場合は、このボタンをクリックします。
- [Basic, NTLM, and FTP/CIFS] : サーバが上のすべての方式をサポートする場合は、このボタンをクリックします。

ユーザ名とパスワードの要件

ネットワークによっては、リモートセッション中にユーザが、コンピュータ、インターネットサービスプロバイダー、クライアントレス SSL VPN、メールサーバ、ファイルサーバ、企業アプリケーションの一部またはすべてにログインする必要があることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。次の表に、クライアントレス SSL VPN ユーザが理解しておく必要のあるユーザ名とパスワードのタイプを示します。

ログインユーザ名/パスワードのタイプ		入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
Internet Service Provider : インターネットサービスプロバイダー	インターネットへのアクセス	インターネットサービスプロバイダーへの接続
クライアントレス SSL VPN	リモートネットワークへのアクセス	クライアントレス SSL VPN の起動
File Server	リモートファイルサーバへのアクセス	クライアントレス SSL VPN ファイルブラウジング機能を使用して、リモートファイルサーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メールサーバ	クライアントレス SSL VPN 経路によるリモートメールサーバへのアクセス	電子メールメッセージの送受信

セキュリティヒントの通知

ユーザはいつでもツールバーの[Logout]アイコンをクリックして、クライアントレス SSL VPN セッションを閉じることができます（ブラウザ ウィンドウを閉じてもセッションは閉じません）。

クライアントレス SSL VPN は、企業ネットワーク上のリモート PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるリソース）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信は暗号化されていないため、プライベートではありません。

クライアントレス SSL VPN の機能を使用するためのリモートシステムの設定

この項では、クライアントレス SSL VPN を使用するようにリモートシステムを設定する方法について説明します。

- [クライアントレス SSL VPN について](#) (414 ページ)
- [クライアントレス SSL VPN の前提条件](#) (415 ページ)
- [クライアントレス SSL VPN フローティング ツールバーの使用](#) (415 ページ)
- [Web のブラウズ](#) (416 ページ)
- [ネットワークのブラウズ \(ファイル管理\)](#) (416 ページ)
- [ポート転送の使用](#) (418 ページ)
- [ポート転送を介した電子メールの使用](#) (419 ページ)
- [Web アクセスを介した電子メールの使用](#) (420 ページ)
- [電子メール プロキシを介した電子メールの使用](#) (420 ページ)
- [スマート トンネルの使用](#) (420 ページ)

ユーザ アカウントを別々に設定でき、各ユーザは異なるクライアントレス SSL VPN の機能を使用できます。

クライアントレス SSL VPN について

次のようなサポートされている接続を使用して、インターネットに接続できます。

- 家庭の DSL、ケーブル、ダイヤルアップ。

- 公共のキオスク。
- ホテルのホットスポット。
- 空港の無線ノード。
- インターネット カフェ。



(注) クライアントレス SSL VPN がサポートしている Web ブラウザのリストについては、『サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ』を参照してください。

クライアントレス SSL VPN の前提条件

- ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
- クライアントレス SSL VPN の URL が必要です。URL は、`https://address` 形式の `https` アドレスでなければなりません。`address` は、SSL VPN がイネーブルになっている ASA (またはロードバランシング クラスタ) のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、`https://cisco.example.com` などです。
- クライアントレス SSL VPN のユーザ名とパスワードが必要です。



(注) クライアントレス SSL VPN ではローカル印刷がサポートされていますが、VPN 経由による企業ネットワーク上のプリンタへの印刷はサポートされていません。

クライアントレス SSL VPN フローティング ツールバーの使用

フローティングツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。

フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。**[Close]** ボタンをクリックすると、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。



ヒント テキスト フィールドにテキストを貼り付けるには、**Ctrl+V** を使用します (クライアントレス SSL VPN セッション中は、表示されるツールバー上での右クリックはオフになっています)。



- (注) ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。

Web のブラウズ

クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。[セキュリティ ヒントの通知 \(414 ページ\)](#) を参照してください。

クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。

- クライアントレス SSL VPN のタイトル バーが各 Web ページの上部に表示される。
- Web サイトへのアクセス方法：
 - クライアントレス SSL VPN ホーム ページ上の [Enter Web Address] フィールドに URL を入力する
 - クライアントレス SSL VPN ホーム ページ上にある設定済みの Web サイト リンクをクリックする
 - 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする
 - 保護されている Web サイトのユーザ名とパスワードが必要です。

特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN ホーム ページ上にリンクとして表示されるものに限られる

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN ホーム ページ上にリンクとして表示されるものに限られる

ネットワークのブラウズ (ファイル管理)

ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。



- (注) コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

重要なポイントは次のとおりです。

- 共有リモート アクセス用にファイル アクセス権を設定する必要があります。
- 保護されているファイル サーバのサーバ名とパスワードが必要です。
- フォルダとファイルが存在するドメイン、ワークグループ、およびサーバの名前が必要です。



- (注) クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。

Remote File Explorer の使用

ユーザは、Remote File Explorer を使用して、Web ブラウザから企業ネットワークをブラウズできます。ユーザが Cisco SSL VPN ポータル ページの [Remote File System] アイコンをクリックすると、ユーザのシステムでアプレットが起動し、ツリーおよびフォルダ ビューにリモート ファイル システムが表示されます。



- (注) この機能を使用するには、ユーザのマシンに Oracle Java ランタイム環境 (JRE) がインストールされ、Web ブラウザで Java がイネーブルになっている必要があります。リモート ファイルの起動には、JRE 8u131 b11、7u141 b11、6u151 b10 以降が必要です。

ユーザはブラウザで次を実行できます。

- リモート ファイル システムのブラウズ。
- ファイルの名前の変更。
- リモートファイルシステム内、およびリモートとローカルのファイルシステム間でのファイルの移動またはコピー。
- ファイルのバルク アップロードおよびダウンロードの実行。

ファイルをダウンロードするには、ブラウザでファイルをクリックして、[Operations] > [Download] を選択し、[Save] ダイアログで場所と名前を指定してファイルを保存します。

ファイルをアップロードするには、宛先フォルダをクリックして、[Operations] > [Upload] を選択し、[Open] ダイアログでファイルの場所と名前を指定します。

この機能には次の制限があります。

- ユーザは、アクセスを許可されていないサブフォルダを表示できません。
- ユーザがアクセスを許可されていないファイルは、ブラウザに表示されても移動またはコピーできません。
- ネストされたフォルダの最大の深さは 32 です。
- ツリー ビューでは、ドラッグ アンド ドロップのコピーがサポートされていません。
- Remote File Explorer の複数のインスタンスの間でファイルを移動するときは、すべてのインスタンスが同じサーバを探索する必要があります（ルート共有）。
- Remote File Explorer は、1 つのフォルダに最大 1500 のファイルおよびフォルダを表示できます。フォルダがこの制限を超えた場合、フォルダは表示されません。

ポート転送の使用

ポート フォワーディングを使用するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用してクライアント アプリケーションを設定する必要があります。

- アプリケーションを使用した後、ユーザは[Close]アイコンをクリックして必ず[Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がオフに切り替わる可能性があります。

始める前に

- macOS では、この機能をサポートしているのは Safari 11 以前のブラウザだけです。
- クライアント アプリケーションがインストールされている必要があります。
- ブラウザでクッキーをイネーブルにする必要があります。
- DNS 名を使用してサーバを指定する場合、ホスト ファイルの変更に必要なため、PC に対する管理者アクセス権が必要です。
- Oracle Java Runtime Environment (JRE) をインストールしておく必要があります。

JRE がインストールされていない場合は、ポップアップウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。まれに、Java 例外エラーで、ポートフォワーディングアプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。

1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。
2. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。
3. Java のインスタンスをすべて閉じます。
4. クライアントレス SSL VPN セッションを確立し、ポート フォワーディング Java アプレットを起動します。

- ブラウザで javascript をイネーブルにする必要があります。デフォルトでは有効に設定されています。
- 必要に応じて、クライアント アプリケーションを設定する必要があります。



(注) Microsoft Outlook クライアントの場合、この設定手順は不要です。Windows 以外のすべてのクライアントアプリケーションでは、設定が必要です。Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] フィールドの値をチェックします。[Remote Server] フィールドにサーバホスト名が含まれている場合、クライアントアプリケーションの設定は不要です。[Remote Server] フィールドに IP アドレスが含まれている場合、クライアントアプリケーションを設定する必要があります。

手順

-
- ステップ 1** クライアントレス SSL VPN セッションを開始して、[Home] ページの [Application Access] リンクをクリックします。[Application Access] ウィンドウが表示されます。
- ステップ 2** [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。
- ステップ 3** この IP アドレスとポート番号を使用して、クライアントアプリケーションを設定します。設定手順は、クライアントアプリケーションによって異なります。

(注) クライアントレス SSL VPN セッション上で実行しているアプリケーションで URL (電子メールメッセージ内のものなど) をクリックしても、サイトがそのセッションで開くわけではありません。サイトをセッション上で開くには、その URL を [Enter Clientless SSL VPN (URL) Address] フィールドに貼り付けます。

ポート転送を介した電子メールの使用

電子メールを使用するには、クライアントレス SSL VPN のホームページから Application Access を起動します。これにより、メールクライアントが使用できるようになります。



(注) IMAP クライアントの使用中にメールサーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。

アプリケーション アクセスおよびその他のメールクライアントの要件を満たしている必要があります。

Web アクセスを介した電子メールの使用

次の電子メールアプリケーションがサポートされています。

- Microsoft Outlook Web App to Exchange Server 2010

OWA には、Internet Explorer 11（以降）、または最新の Firefox が必要です。

- Exchange Server 2013 への Microsoft Outlook Web アクセス。

最適な結果を得るために、Internet Explorer 11（以降）または最新の Firefox で OWA を使用してください。

- Louts iNotes



(注) Web ベースの電子メール製品がインストールされており、その他の Web ベースの電子メールアプリケーションも動作する必要がありますが、検証されていません。

電子メール プロキシを介した電子メールの使用

メールアプリケーションの使用法と例については、「[クライアントレス SSL VPN を介した電子メールの使用（355 ページ）](#)」を参照してください。

はじめる前に

SSL 対応メールアプリケーションがインストールされている必要があります。

ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。

メールアプリケーションが正しく設定されている必要があります。

その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。

スマート トンネルの使用

スマート トンネルの使用に管理権限は必要ありません。



(注) ポートフォワーダの場合と異なり、Java は自動的にダウンロードされません。

- スマート トンネルを使用する場合、Windows では ActiveX または JRE、Mac OS X では Java Web Start が必要です。
- ブラウザでクッキーをイネーブルにする必要があります。

- ブラウザで javascript をイネーブルにする必要があります。
- Mac OS X では、フロントサイドプロキシはサポートされていません。
- サポートされているオペレーティング システムとブラウザだけを使用してください。
- TCP ソケットベースのアプリケーションだけがサポートされています。



第 19 章

モバイル デバイスでのクライアントレス SSL VPN

- [モバイルデバイスでのクライアントレス SSL VPN の使用 \(423 ページ\)](#)

モバイル デバイスでのクライアントレス SSL VPN の使用

Pocket PC または他の認定されたモバイルデバイスからクライアントレス SSL VPN にアクセスできます。認定されたモバイルデバイスでクライアントレスの SSL VPN を使用するために、ASA 管理者またはクライアントレス SSL VPN ユーザは特別なことを行う必要はありません。

クライアントレス SSL VPN のモバイルデバイスバージョンに応じて、次のような相違点があります。

- ポップアップのクライアントレス SSL VPN ウィンドウはバナー Web ページに置き換わっています。
- 標準のクライアントレス SSL VPN フローティング ツールバーがアイコンバーに置き換わっています。このバーには、[Go]、[Home]、および [Logout] の各種ボタンが表示されます。
- メインのクライアントレス SSL VPN ポータル ページに [Show Toolbar] アイコンがありません。
- クライアントレス SSL VPN のログアウト時に、警告メッセージで PIE ブラウザを正しく閉じる手順が表示されます。この手順に従わないで通常の方法でブラウザのウィンドウを閉じると、クライアントレス SSL VPN または HTTPS を使用するすべてのセキュア Web サイトから PIE が切断されません。

モバイルでのクライアントレス SSL VPN の制限

- クライアントレス SSL VPN は OWA 2010 の基本認証をサポートする。OWA サーバに基本認証を設定せずにクライアントレス SSL VPN ユーザがこのサーバにアクセスしようとするとアクセスは拒否されます。

- サポートされていないクライアントレス SSL VPN の機能
 - Application Access および他の Java 依存の各種機能
 - HTTP プロキシ
 - Citrix Metaframe 機能 (PDA に対応する Citrix ICA クライアント ソフトウェアが装備されていない場合)



第 20 章

クライアントレス SSLVPN のカスタマイズ

- [クライアントレス SSL VPN ユーザ エクスペリエンスのカスタマイズ \(425 ページ\)](#)
- [クライアントレス SSL VPN エンド ユーザの設定 \(430 ページ\)](#)
- [ブックマーク ヘルプのカスタマイズ \(468 ページ\)](#)

クライアントレス SSLVPN ユーザ エクスペリエンスのカスタマイズ

ログインページ、ポータルページ、ログアウトページなどの、クライアントレス SSL VPN ユーザ エクスペリエンスをカスタマイズできます。2つの方式を使用できます。[Add/Edit Customization Object] ウィンドウで、事前定義されたページ コンポーネントをカスタマイズできます。このウィンドウでは、ページをカスタマイズするために使用される、XML ファイル（カスタマイゼーション オブジェクト）を ASA に追加したり、ASA に保存されている XML ファイルを変更します。または、XML ファイルをローカル コンピュータまたはサーバにエクスポートし、XML タグを変更して、ファイルを ASA に再インポートできます。どちらの方式でも、接続プロファイルまたはグループ ポリシーに適用するカスタマイゼーション オブジェクトが作成されます。

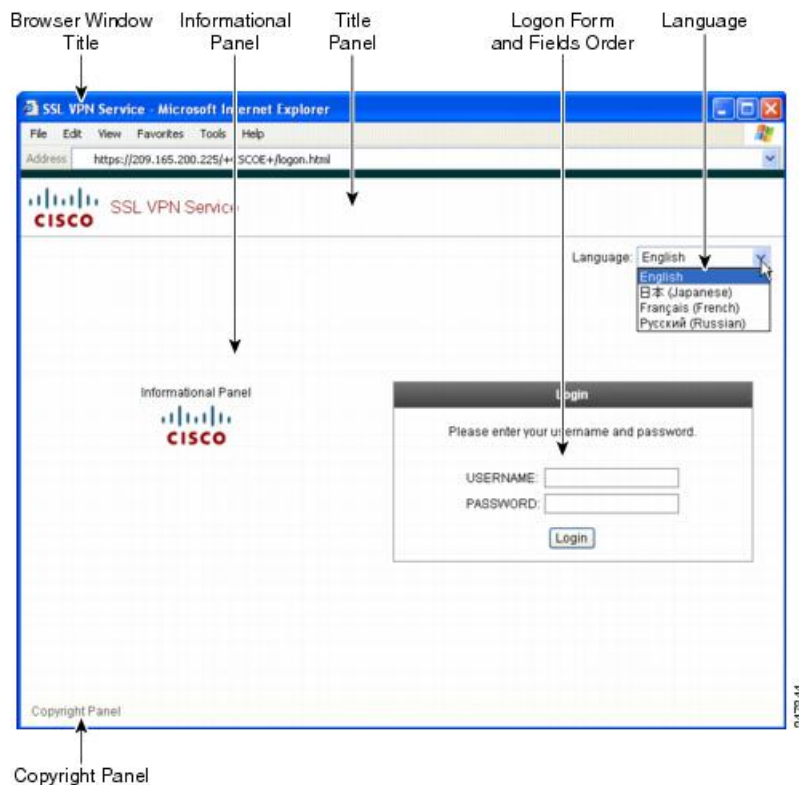
ログインページの事前定義されたコンポーネントをカスタマイズするのではなく、独自のページを作成して ASA にインポートできます（フル カスタマイゼーション）。

タイトル、言語オプション、ユーザへのメッセージなど、ログインページの事前定義されたコンポーネントをカスタマイズできます。または、独自のカスタムページでページを完全に置き換えることができます（フル カスタマイゼーション）。

Customization Editor によるログイン ページのカスタマイズ

次の図に、ログイン ページとカスタマイズ可能な事前定義のコンポーネントを示します。

図 10: クライアントレス ログイン ページのコンポーネント



ログインページのすべてのコンポーネントをカスタマイズするには、次の手順を実行します。
[Preview] ボタンをクリックして、各コンポーネントに対する変更をプレビューできます。

手順

- ステップ 1** 事前定義されたカスタマイゼーションを指定します。[Logon Page] に移動し、[Customize pre-defined logon page components] を選択します。ブラウザ ウィンドウのタイトルを指定します。
- ステップ 2** タイトルパネルを表示し、カスタマイズします。[Logon Page]>[Title Panel] に移動し、[Display title panel] をオンにします。タイトルとして表示するテキストを入力し、ロゴを指定します。フォント スタイルを指定します。
- ステップ 3** 表示する言語オプションを指定します。[Logon Page]>[Language] に移動し、[Enable Language Selector] をオンにします。リモートユーザに表示する言語を追加または削除します。リスト内の言語には、[Configuration]>[Remote Access VPN]>[Language Localization] で設定する変換テーブルが必要です。
ユーザ名とパスワードフィールドのラベルは、ユーザが選択した言語に従って変更されます。
- ステップ 4** ログインフォームをカスタマイズします。[Logon Page]>[Logon Form] に移動します。フォームのテキストおよびパネル内のフォントスタイルをカスタマイズします。接続プロファイルでセカンダリ認証サーバが設定されている場合にのみ、セカンダリパスワードフィールドがユーザに表示されます。

- ステップ 5** ログインフォームのフィールドを配置します。[Logon Page]>[Form Fields Order] に移動します。上矢印ボタンと下矢印ボタンを使用して、フィールドが表示される順序を変更します。
- ステップ 6** ユーザへのメッセージを追加します。[Logon Page]>[Informational Panel] に移動し、[Display informational panel] をオンにします。パネルに表示するテキストを追加し、ログインフォームに対してパネルの位置を変更し、このパネルに表示するロゴを指定します。
- ステップ 7** 著作権宣言文を表示します。[Logon Page]>[Copyright Panel] に移動し、[Display copyright panel] をオンにします。著作権のために表示するテキストを追加します。
- ステップ 8** [OK] をクリックしてから、編集したカスタマイゼーションオブジェクトに変更を適用します。

次のタスク

独自の完全にカスタマイズしたページでのログインページの置き換えについて確認してください。

独自のフルカスタマイズしたページへのログインページの置き換え

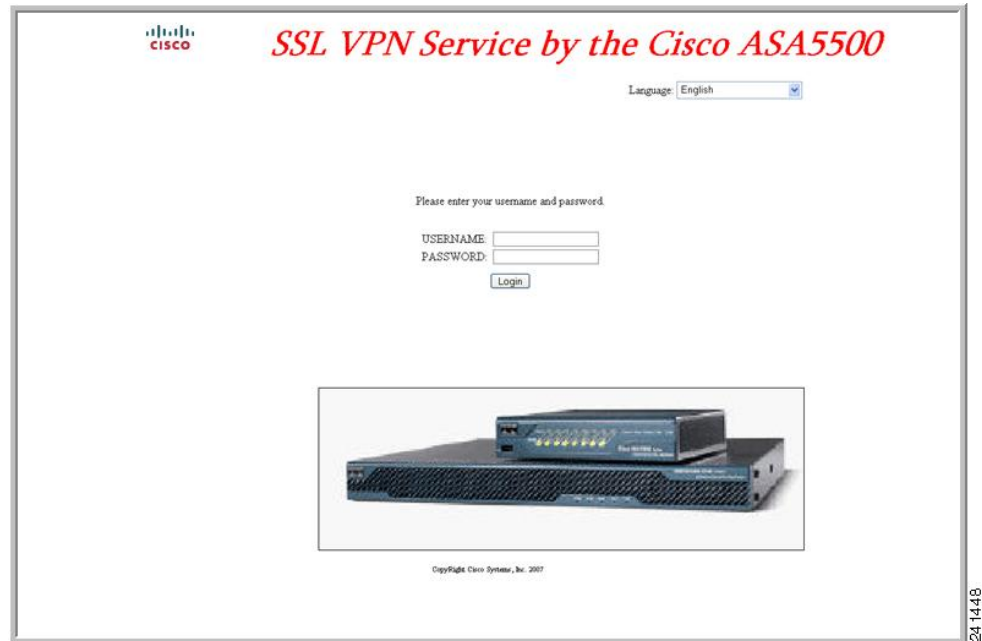
提供されるログインページの特定のコンポーネントを変更するのではなく、独自のカスタムログイン画面を使用する場合は、フルカスタマイゼーション機能を使用してこの高度なカスタマイゼーションを実行できます。

フルカスタマイゼーション機能を使用して、独自のログイン画面に HTML を配置し、ASA で関数を呼び出す Cisco HTML コードを挿入します。これにより、Login フォームと言語セレクトドロップダウンリストが作成されます。

このマニュアルでは、独自の HTML コードを作成するために必要な修正、および ASA でユーザ独自のコードを使用するために設定する必要があるタスクについて説明します。

次の図に、フルカスタマイゼーション機能によって有効化される簡単なカスタムログイン画面の例を示します。

図 11: ログイン ページのフル カスタマイゼーション例



カスタム ログイン画面ファイルの作成

次の HTML コードは例として使用され、表示するコードです。

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font color="#FF0000"
size="7" face="Sylfaen"> SSL VPN Service by the Cisco ASA5500</font></b></i></p>

<body onload="cscs_ShowLoginForm('lform');cscs_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
```



```

</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

</td></tr>
</table>

```

字下げされたコードは、画面に Login フォームと言語セクタを挿入します。関数 **cscs_ShowLoginForm('lform')** はログオン フォームを挿入します。**cscs_ShowLanguageSelector('selector')** は言語セクタを挿入します。

手順

-
- ステップ 1** ファイルに **login.inc** という名前を付けます。ファイルをインポートすると、ASA はこのファイル名をログイン画面として認識します。
- ステップ 2** このファイルで使用されるイメージのパスを変更して、**/+CSCOU+/** を含めます。認証前にリモートユーザに表示するファイルは、パス **/+CSCOU+/** で表される ASA キャッシュメモリの特定の領域に配置する必要があります。そのため、このファイルにある各イメージのソースはこのパスに含める必要があります。次に例を示します。
- src="/+CSCOU+/asa5520.gif"**
- ステップ 3** 下記の特別な HTML コードを挿入します。このコードには、Login フォームと言語セクタを画面に挿入する前述のシスコの関数が含まれています。

```

<body onload="cscs_ShowLoginForm('lform');cscs_ShowLanguageSelector('selector')">
<table>
<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

</td></tr>

```

</table>

ファイルおよびイメージのインポート

手順

ステップ 1 [Clientless SSL VPN Access] > [Portal] > [Web Contents] の順に選択します。

ステップ 2 [Import] をクリックします。

- a) [Source] オプションを選択し、Web コンテンツをファイルのパスを入力します。
- b) [Destination] 領域で、[Require Authentication to access its content] に対して [No] を選択します。これにより、ファイルは、認証の前にユーザがアクセスできるフラッシュメモリの領域に保存されます。

ステップ 3 [Import Now] をクリックします。

カスタム ログイン画面を使用するセキュリティ アプライアンスの設定

手順

ステップ 1 [Clientless SSL VPN Access] > [Portal] > [Customization] のテーブルで、カスタマイゼーション オブジェクトを選択し、[Edit] をクリックします。

ステップ 2 ナビゲーション ペインで、[Logon Page] を選択します。

ステップ 3 [Replace pre-defined logon page with a custom page] を選択します。

ステップ 4 [Manage] をクリックして、ログイン ページ ファイルをインポートします。

ステップ 5 [Destination] 領域で、[No] を選択し、認証前にユーザに対してログイン ページが表示されるようにします。

ステップ 6 [Edit Customization Object] ウィンドウに戻り、[General] をクリックして、必要な接続プロファイルやグループ ポリシーのカスタマイゼーション オブジェクトをイネーブルにします。

クライアントレス SSL VPN エンド ユーザの設定

この項は、エンド ユーザのためにクライアントレス SSL VPN を設定するシステム管理者を対象にしています。ここでは、エンド ユーザ インターフェイスをカスタマイズする方法、およびリモート システムの設定要件と作業の概要を説明します。ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報を明確にします。

エンドユーザインターフェイスの定義

クライアントレス SSL VPN エンドユーザインターフェイスは一連の HTML パネルから構成されています。ユーザは、ASA インターフェイスの IP アドレスを `https://address` 形式で入力することにより、クライアントレス SSL VPN にログインします。最初に表示されるパネルは、ログイン画面です。

クライアントレス SSL VPN ホーム ページの表示

ユーザがログインすると、ポータル ページが開きます。

ホームページには設定済みのクライアントレス SSL VPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプルホームページには、特定のファイル共有の指定機能以外のすべてのクライアントレス SSL VPN 機能が表示されています。ユーザはこのホームページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、および Application Access（ポート転送とスマート トンネル）による TCP アプリケーションへのアクセスを実行できます。

クライアントレス SSL VPN の [Application Access] パネルの表示

ポート転送またはスマート トンネルを開始するには、[Application Access] ボックスの [Go] ボタンをクリックします。[Application Access] ウィンドウが開き、このクライアントレス SSL VPN 接続用に設定された TCP アプリケーションが表示されます。このパネルを開いたままでアプリケーションを使用する場合は、通常の方法でアプリケーションを起動します。

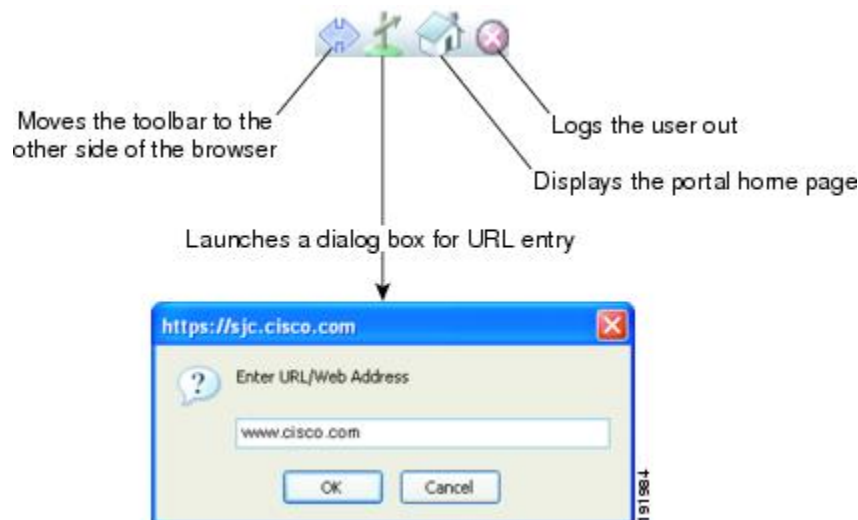


(注) ステートフル フェールオーバーでは、Application Access を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。

フローティング ツールバーの表示

次の図のフローティング ツールバーには、現在のクライアントレス SSL VPN セッションが表示されます。

図 12: クライアントレス SSL VPN フローティング ツールバー



フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティングツールバーは表示できません。
- ツールバーを閉じると、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。

クライアントレス SSL VPN ページのカスタマイズ

クライアントレス SSL VPN ユーザに表示されるポータル ページの外観を変えることができます。変更できる外観には、ユーザがセキュリティ アプライアンスに接続するときに表示される [Login] ページ、セキュリティ アプライアンスのユーザ認証後に表示される [Home] ページ、ユーザがアプリケーションを起動するときに表示される [Application Access] ウィンドウ、およびユーザがクライアントレス SSL VPN セッションからログアウトするときに表示される [Logout] ページが含まれます。

ポータル ページのカスタマイズ後は、このカスタマイゼーションを保存して、特定の接続プロファイル、グループ ポリシー、またはユーザに適用できます。ASA をリロードするまで、またはクライアントレス SSL をオフに切り替えてから再度イネーブルにするまで、変更は適用されません。

いくつものカスタマイゼーションオブジェクトを作成、保存して、個々のユーザまたはユーザグループに応じてポータル ページの外観を変更するようにセキュリティ アプライアンスをイネーブル化できます。

カスタマイゼーションについて

ASA は、カスタマイゼーション オブジェクトを使用して、ユーザ画面の外観を定義します。カスタマイゼーション オブジェクトは、リモート ユーザに表示されるカスタマイズ可能なすべての画面項目に対する XML タグを含む XML ファイルからコンパイルされます。ASA ソフトウェアには、リモート PC にエクスポートできるカスタマイゼーション テンプレートが含まれています。このテンプレートを編集し、新しいカスタマイゼーション オブジェクトとして再び ASA にインポートできます。

カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは、変更したりキャッシュメモリから削除したりすることはできませんが、エクスポートして編集し、新しいカスタマイゼーション オブジェクトとして再び ASA にインポートできます。

カスタマイゼーション オブジェクト、接続プロファイル、およびグループ ポリシー

ユーザが初めて接続するときには、接続プロファイル（トンネルグループ）で指定されたデフォルトのカスタマイゼーション オブジェクト (*DfltCustomization*) がログイン画面の表示方法を決定します。接続プロファイルリストがイネーブルになっている場合に、独自のカスタマイゼーションがある別のグループをユーザが選択すると、その新しいグループのカスタマイゼーション オブジェクトを反映して画面が変わります。

リモート ユーザが認証された後は、画面の外観は、そのグループ ポリシーにカスタマイゼーション オブジェクトが割り当てられているかどうかによって決まります。

カスタマイゼーション テンプレートの編集

この項では、カスタマイゼーション テンプレートの内容を示して、便利な図を提供しています。これらを参照して、正しい XML タグをすばやく選択して、画面表示を変更できます。

テキスト エディタまたは XML エディタを使用して、XML ファイルを編集できます。次の例は、カスタマイゼーション テンプレートの XML タグを示しています。一部の冗長タグは、見やすくするために削除してあります。

```
<custom>
  <localization>
    <languages>en,ja,zh,ru,ua</languages>
    <default-language>en</default-language>
  </localization>
  <auth-page>
    <window>
      <title-text l10n="yes"><![CDATA[SSL VPN Service</title-text>
    </window>
    <full-customization>
      <mode>disable</mode>
      <url></url>
    </full-customization>
    <language-selector>
      <mode>disable</mode>
```

```

<title l10n="yes">Language:</title>
<language>
  <code>en</code>
  <text>English</text>
</language>
<language>
  <code>zh</code>
  <text>(Chinese)</text>
</language>
<language>
  <code>ja</code>
  <text>(Japanese)</text>
</language>
<language>
  <code>ru</code>
  <text>(Russian)</text>
</language>
<language>
  <code>ua</code>
  <text>(Ukrainian)</text>
</language>
</language-selector>
<logon-form>
  <title-text l10n="yes"><![CDATA[Login</title-text>
  <title-background-color><![CDATA[#666666</title-background-color>
  <title-font-color><![CDATA[#ffffff</title-font-color>
  <message-text l10n="yes"><![CDATA[Please enter your username and
password.</message-text>
  <username-prompt-text l10n="yes"><![CDATA[USERNAME:</username-prompt-text>
  <password-prompt-text l10n="yes"><![CDATA[PASSWORD:</password-prompt-text>
  <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
  <internal-password-first>no</internal-password-first>
  <group-prompt-text l10n="yes"><![CDATA[GROUP:</group-prompt-text>
  <submit-button-text l10n="yes"><![CDATA[Login</submit-button-text>
  <title-font-color><![CDATA[#ffffff</title-font-color>
  <title-background-color><![CDATA[#666666</title-background-color>
  <font-color>#000000</font-color>
  <background-color>#ffffff</background-color>
  <border-color>#858A91</border-color>
</logon-form>
<logout-form>
  <title-text l10n="yes"><![CDATA[Logout</title-text>
  <message-text l10n="yes"><![CDATA[Goodbye.<br>

For your own security, please:<br>

<li>Clear the browser's cache

<li>Delete any downloaded files

<li>Close the browser's window</message-text>
  <login-button-text l10n="yes">Logon</login-button-text>
  <hide-login-button>no</hide-login-button>
  <title-background-color><![CDATA[#666666</title-background-color>
  <title-font-color><![CDATA[#ffffff</title-font-color>
  <title-font-color><![CDATA[#ffffff</title-font-color>
  <title-background-color><![CDATA[#666666</title-background-color>
  <font-color>#000000</font-color>
  <background-color>#ffffff</background-color>
  <border-color>#858A91</border-color>
</logout-form>
<title-panel>
  <mode>enable</mode>

```

```

    <text l10n="yes"><![CDATA[SSL VPN Service</text>
    <logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
    <gradient>yes</gradient>
    <style></style>
    <background-color><![CDATA[#ffffff</background-color>
    <font-size><![CDATA[larger</font-size>
    <font-color><![CDATA[#800000</font-color>
    <font-weight><![CDATA[bold</font-weight>
</title-panel>
<info-panel>
  <mode>disable</mode>
  <image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
  <image-position>above</image-position>
  <text l10n="yes"></text>
</info-panel>
<copyright-panel>
  <mode>disable</mode>
  <text l10n="yes"></text>
</copyright-panel>
</auth-page>
<portal>
  <title-panel>
    <mode>enable</mode>
    <text l10n="yes"><![CDATA[SSL VPN Service</text>
    <logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
    <gradient>yes</gradient>
    <style></style>
    <background-color><![CDATA[#ffffff</background-color>
    <font-size><![CDATA[larger</font-size>
    <font-color><![CDATA[#800000</font-color>
    <font-weight><![CDATA[bold</font-weight>
  </title-panel>
  <browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
  <access-network-title l10n="yes">Start AnyConnect</access-network-title>
  <application>
    <mode>enable</mode>
    <id>home</id>
    <tab-title l10n="yes">Home</tab-title>
    <order>1</order>
  </application>
  <application>
    <mode>enable</mode>
    <id>web-access</id>
    <tab-title l10n="yes"><![CDATA[Web Applications</tab-title>
    <url-list-title l10n="yes"><![CDATA[Web Bookmarks</url-list-title>
    <order>2</order>
  </application>
  <application>
    <mode>enable</mode>
    <id>file-access</id>
    <tab-title l10n="yes"><![CDATA[Browse Networks</tab-title>
    <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks</url-list-title>
    <order>3</order>
  </application>
  <application>
    <mode>enable</mode>
    <id>app-access</id>
    <tab-title l10n="yes"><![CDATA[Application Access</tab-title>
    <order>4</order>
  </application>
  <application>
    <mode>enable</mode>
    <id>net-access</id>
    <tab-title l10n="yes">AnyConnect</tab-title>

```

```

    <order>4</order>
</application>
<application>
  <mode>enable</mode>
  <id>help</id>
  <tab-title l10n="yes">Help</tab-title>
  <order>1000000</order>
</application>
<toolbar>
  <mode>enable</mode>
  <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
  <prompt-box-title l10n="yes">Address</prompt-box-title>
  <browse-button-text l10n="yes">Browse</browse-button-text>
  <username-prompt-text l10n="yes"></username-prompt-text>
</toolbar>
<column>
  <width>100%</width>
  <order>1</order>
</column>
<pane>
  <type>TEXT</type>
  <mode>disable</mode>
  <title></title>
  <text></text>
  <notitle></notitle>
  <column></column>
  <row></row>
  <height></height>
</pane>
<pane>
  <type>IMAGE</type>
  <mode>disable</mode>
  <title></title>
  <url l10n="yes"></url>
  <notitle></notitle>
  <column></column>
  <row></row>
  <height></height>
</pane>
<pane>
  <type>HTML</type>
  <mode>disable</mode>
  <title></title>
  <url l10n="yes"></url>
  <notitle></notitle>
  <column></column>
  <row></row>
  <height></height>
</pane>
<pane>
  <type>RSS</type>
  <mode>disable</mode>
  <title></title>
  <url l10n="yes"></url>
  <notitle></notitle>
  <column></column>
  <row></row>
  <height></height>
</pane>
<url-lists>
  <mode>group</mode>
</url-lists>
<home-page>
  <mode>standard</mode>

```



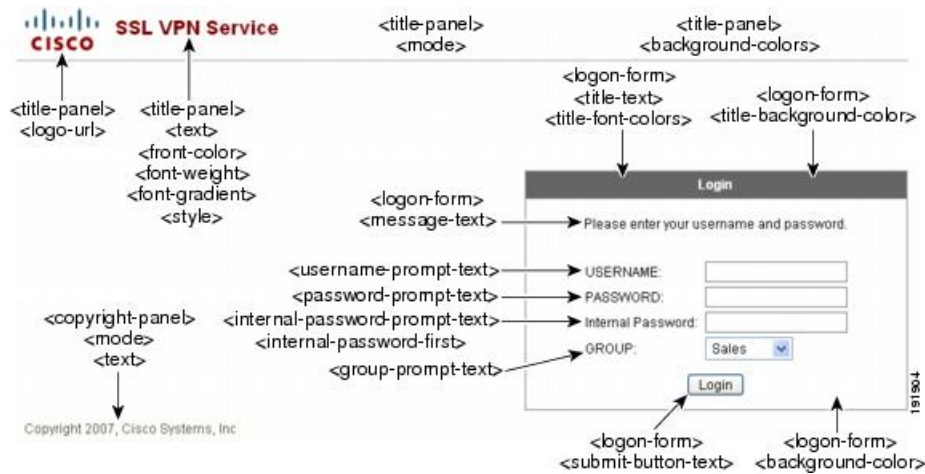
```

        <url></url>
    </home-page>
</portal>
</custom>

```

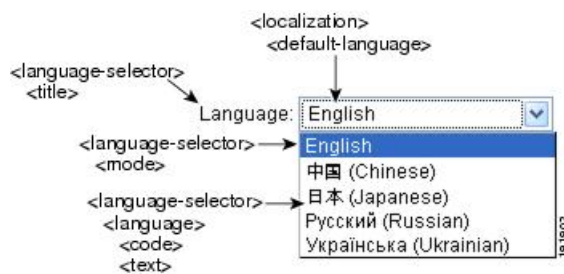
次の図に、[Login] ページとページをカスタマイズする XML タグを示します。これらのタグはすべて、上位レベルのタグ <auth-page> にネストされています。

図 13: [Login] ページと関連 XML タグ



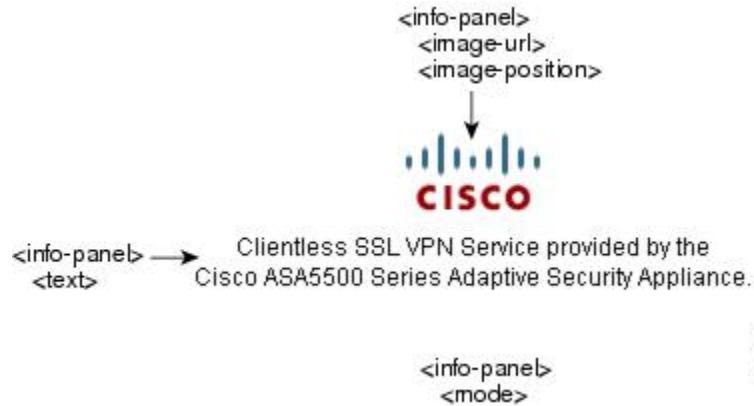
次の図に、[Login] ページで使用可能な言語セクタ ドロップダウンリストと、この機能をカスタマイズするための XML タグを示します。これらのタグはすべて、上位レベルの <auth-page> タグにネストされています。

図 14: [Login] 画面の言語セクタと関連 XML タグ



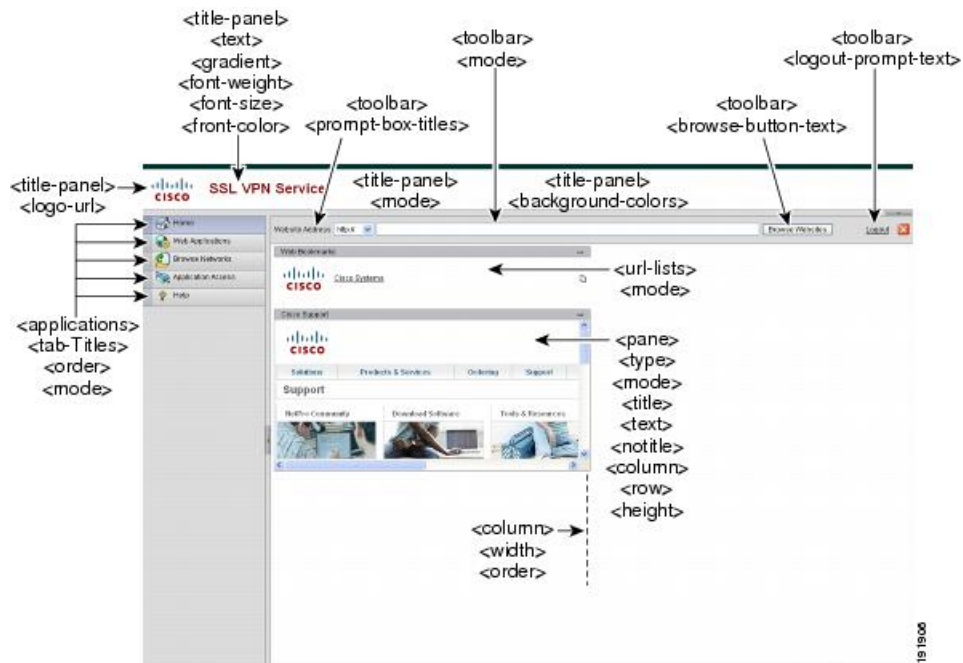
次の図に、[Login] ページで使用できる Information Panel とこの機能をカスタマイズするための XML タグを示します。この情報は [Login] ボックスの左側または右側に表示されます。これらのタグは、上位レベルの <auth-page> タグにネストされています。

図 15: [Login] 画面の [Information Panel] と関連 XML タグ



次の図に、ポータルページとこの機能をカスタマイズするための XML タグを示します。これらのタグは、上位レベルの `<auth-page>` タグにネストされています。

図 16: [Portal] ページと関連 XML タグ



ログイン画面の高度なカスタマイゼーション

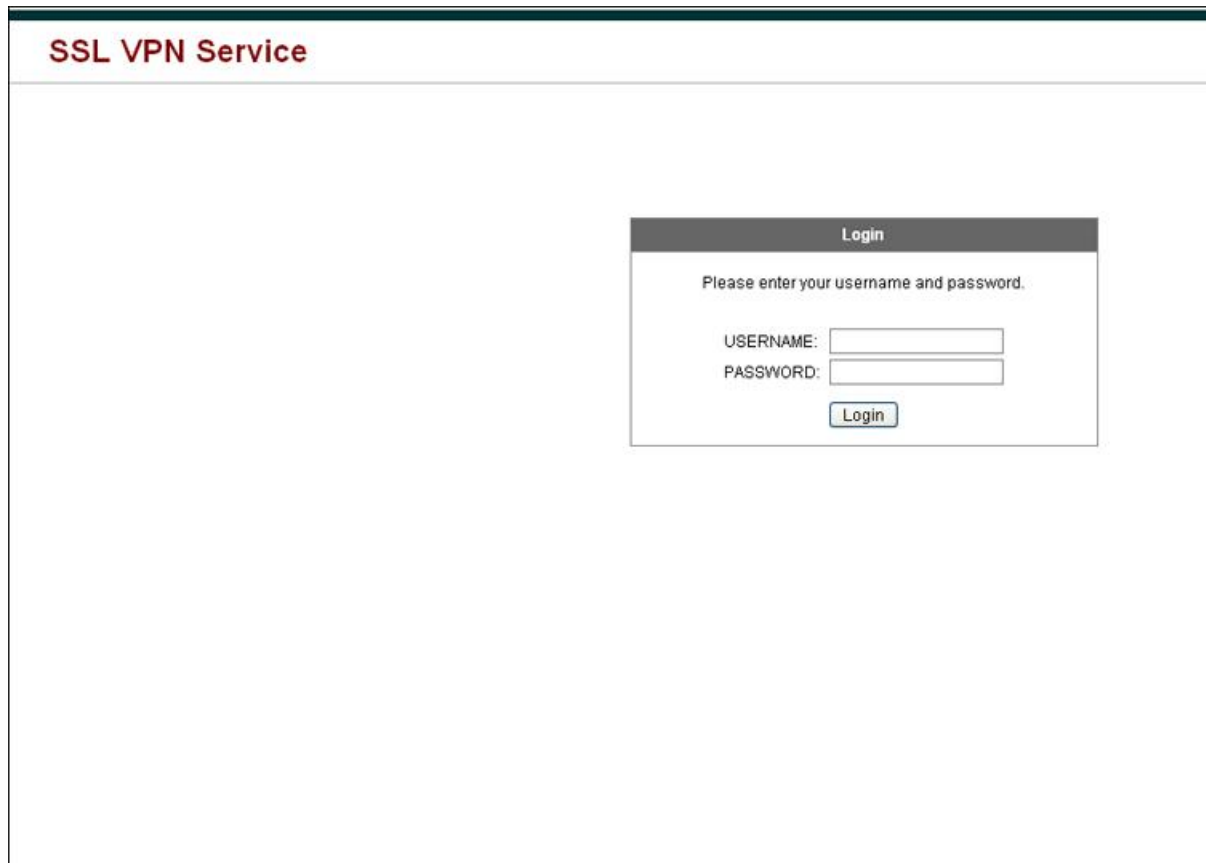
提供されるログイン画面の特定の画面要素を変更するのではなく、独自のカスタムログイン画面を使用する場合は、フルカスタマイゼーション機能を使用してこの高度なカスタマイゼーションを実行できます。

フルカスタマイゼーション機能を使用して、独自のログイン画面に HTML を配置し、ASA で関数を呼び出す Cisco HTML コードを挿入します。これにより、Login フォームと言語セレクトア ドロップダウン リストが作成されます。

この項では、独自の HTML コードを作成するために必要な修正、および ASA でユーザ独自のコードを使用するために設定する必要があるタスクについて説明します。

次の図に、クライアントレス SSL VPN ユーザに表示される標準の Cisco ログイン画面を示します。Login フォームは、HTML コードで呼び出す関数によって表示されます。

図 17: 標準の Cisco [Login] ページ



The screenshot shows a web page titled "SSL VPN Service". In the center, there is a login form with a dark header bar containing the word "Login". Below the header, the text "Please enter your username and password." is displayed. There are two input fields: "USERNAME:" followed by a text box, and "PASSWORD:" followed by a text box. Below the password field is a "Login" button.

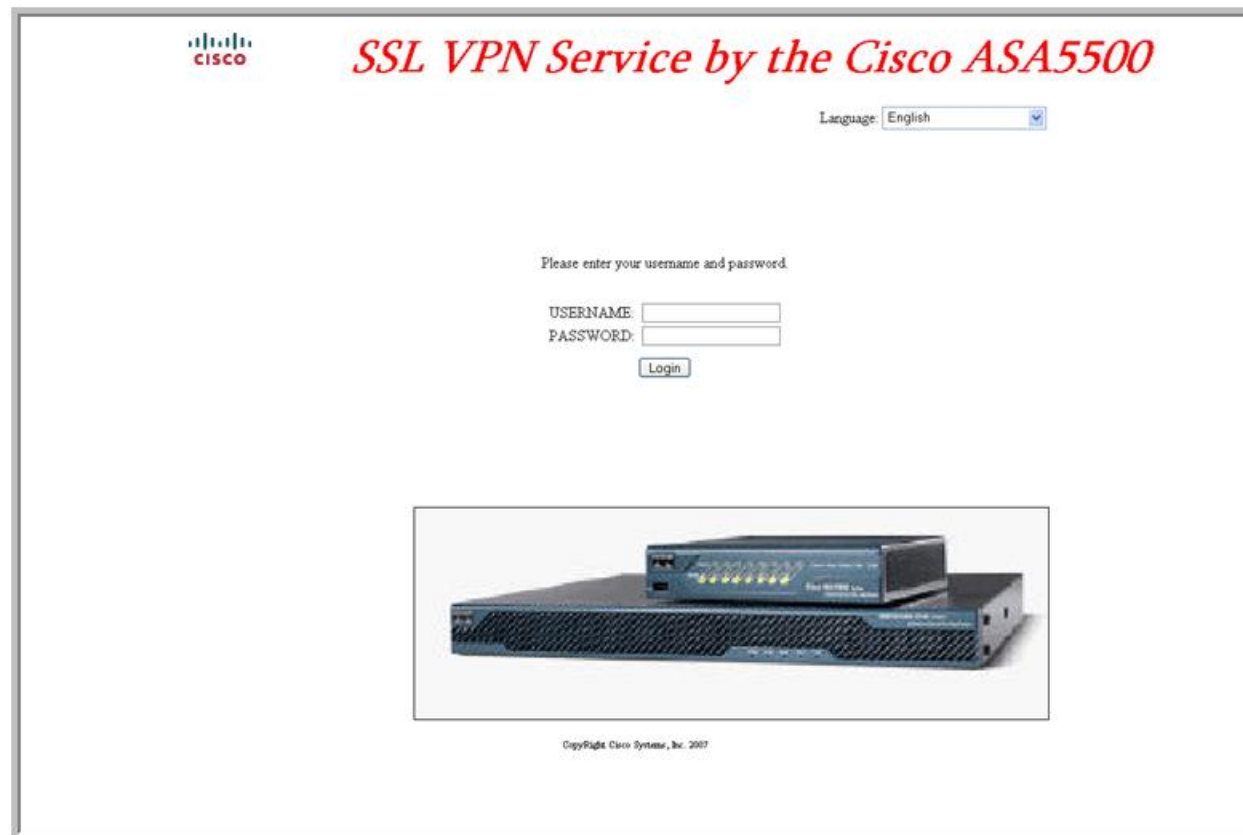
次の図に、[Language Selector] ドロップダウン リストを示します。この機能は、クライアントレス SSL VPN ユーザにはオプションとなっており、ログイン画面の HTML コード内の関数によっても呼び出されます。

図 18: 言語セレクト ドロップダウン リスト



次の図に、フル カスタマイゼーション機能によって有効化される簡単なカスタム ログイン画面の例を示します。

図 19: ログイン画面のフル カスタマイゼーション例



次の HTML コードは例として使用され、表示するコードです。

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>New Page 3</title>
<base target="_self">
</head>
```

```

<p align="center">
<font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font color="#FF0000"
size="7" face="Sylfaen"> SSL VPN Service by the Cisco ASA5500</font></b></i></p>

<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

</td></tr>

</table>

```

字下げされたコードは、画面に Login フォームと言語セレクトを挿入します。関数 **csco_ShowLoginForm('lform')** はログオンフォームを挿入します。**csco_ShowLanguageSelector('selector')** は言語セレクトを挿入します。

HTML ファイルの変更

手順

- ステップ 1** ファイルに `login.inc` という名前を付けます。ファイルをインポートすると、ASA はこのファイル名をログイン画面として認識します。
- ステップ 2** このファイルで使用されるイメージのパスを変更して、`/+CSCOU+/` を含めます。
- 認証前にリモートユーザに表示するファイルは、パス `/+CSCOU+/` で表される ASA キャッシュメモリの特定の領域に配置する必要があります。そのため、このファイルにある各イメージのソースはこのパスに含める必要があります。
- 次に例を示します。
- ```
src="/+CSCOU+/asa5520.gif"
```

**ステップ 3** 下記の特別な HTML コードを挿入します。このコードには、Login フォームと言語セレクトを画面に挿入する前述のシスコの関数が含まれています。

```
<body onload="cscs_ShowLoginForm('lform');cscs_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

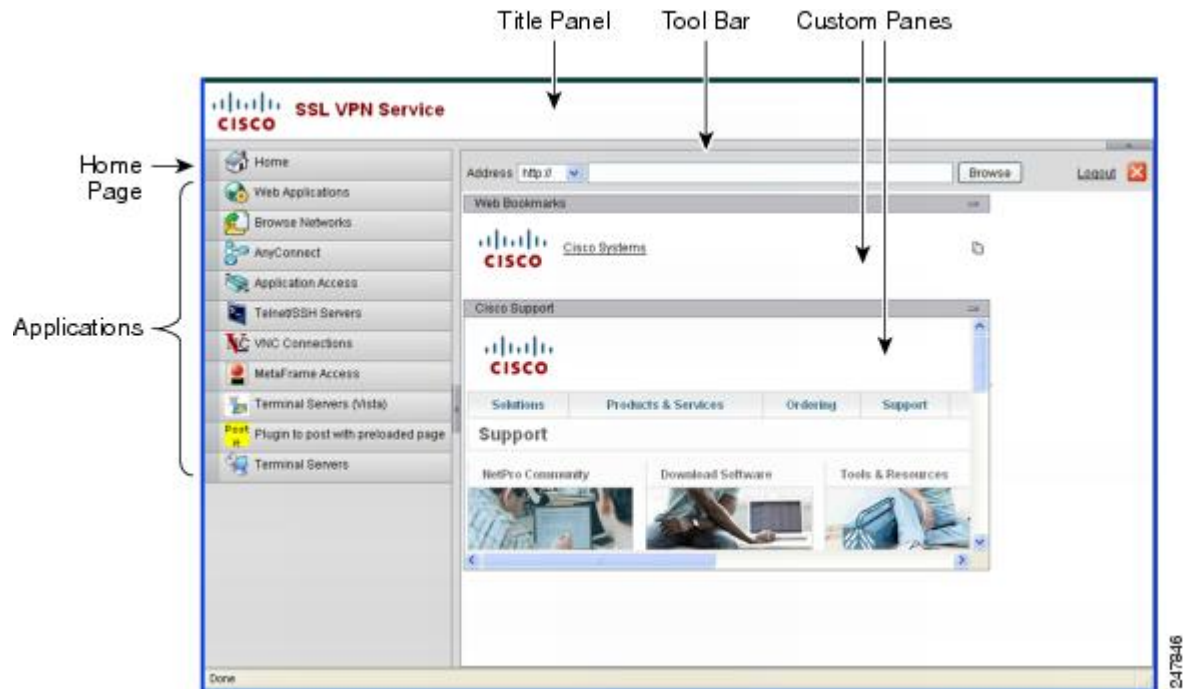
</td></tr>

</table>
```

## ポータル ページのカスタマイズ

次の図に、ポータル ページとカスタマイズ可能な事前定義のコンポーネントを示します。

図 20:ポータル ページのカスタマイズ可能なコンポーネント



ページのコンポーネントをカスタマイズする以外に、ポータル ページを、テキスト、イメージ、RSS フィード、または HTML を表示するカスタム ペインに分割できます。

ポータル ページをカスタマイズするには、次の手順を実行します。[Preview] ボタンをクリックすると、各コンポーネントに対する変更をプレビューできます。

#### 手順

- ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Customization] の順に選択します。
- ステップ 2 [Add] をクリックします。
- ステップ 3 [Customization Object Name] フィールドに、カスタマイズの名前を入力します。
- ステップ 4 左側のペインで、[Portal Page] をクリックします。
- ステップ 5 [Browser Window Title] フィールドにタイトルを入力します。
- ステップ 6 タイトルパネルを表示してカスタマイズするには、[Title Panel] をクリックし、[Display title panel] チェックボックスをオンにします。タイトルとして表示するテキストを入力し、ロゴを指定します。フォントスタイルを指定することもできます。
- ステップ 7 ツールバーを有効にしてカスタマイズするには、[Toolbar] をクリックし、[Display toolbar] チェックボックスをオンにします。[Prompt Box Title]、[Browse Button Text]、[Logout Prompt] を必要に応じてカスタマイズします。  
ツールバーを有効にすると、ログインに使用されたユーザ名も表示されます。[Username] フィールドには、有効なキーワードとして **Username** を含める必要があります。

- ステップ 8** アプリケーションリストをカスタマイズするには、[Applications] をクリックし、[Show navigation panel] チェックボックスをオンにします。クライアント/サーバのプラグインとポートフォワードリング アプリケーションを含む、ASA 設定で有効になっているアプリケーションが表に示されます。この表では、これらのアプリケーションを必要に応じて有効または無効にします。
- ステップ 9** ポータルページのスペースにカスタム ペインを作成するには、[Custom Panes] をクリックします。カラムの数および幅を設定します。必要に応じて、カスタム ペインを作成し、ウィンドウをテキスト、イメージ、RSS フィード、または HTML ページの行およびカラムに分割します。
- ステップ 10** ホーム ページ URL を指定するには、[Home Page] をクリックし、[Enable custom intranet web page] チェックボックスをオンにします。ブックマークの構成を定義するブックマーク モードを選択します。
- ステップ 11** タイムアウト アラート メッセージとツールチップを設定するには、[Timeout Alerts] をクリックします。
- ステップ 12** [OK] をクリックします。

### 次のタスク

カスタム ポータル タイムアウト アラートの設定について確認してください。

## カスタム ポータル タイムアウト アラートの設定

クライアントレス SSL VPN 機能のユーザが VPN セッションで時間を管理できるように、クライアントレス SSL VPN ポータルページには、クライアントレス VPN セッションが終了するまでの合計残り時間を示すカウントダウンタイマーが表示されます。セッションは、非アクティブ状態によって、または設定された最大許容接続時間が終了したために、タイムアウトします。

ユーザのセッションが、アイドル タイムアウトまたはセッション タイムアウトにより終了することをユーザに警告するカスタム メッセージを作成できます。デフォルトのアイドル タイムアウトメッセージはカスタム メッセージによって置き換えられます。デフォルトのメッセージは、「Your session will expire in %s.」です。メッセージ内の %s プレースホルダーは、進行するカウントダウン タイマーで置き換えられます。

### 手順

- ステップ 1** ASDM を起動し、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Customization] を選択します。
- ステップ 2** [Add] をクリックして新しいカスタマイゼーション オブジェクトを追加するか、既存のカスタマイゼーション オブジェクトを選択して [Edit] をクリックし、カスタム アイドル タイムアウト メッセージを既存のカスタマイゼーション オブジェクトに追加します。
- ステップ 3** [Add / Edit Customization Object] ペインで、ナビゲーション ツリーの [Portal Page] ノードを展開して、[Timeout Alerts] をクリックします。
- ステップ 4** [Enable alert visual tooltip (red background for timer countdown)] をオンにします。これにより、カウントダウン タイマーがツール ヒントとして赤の背景に表示されます。ユーザが [Time left]



領域をクリックすると、時間領域が拡大されて、カスタム タイムアウト アラート メッセージが表示されます。このボックスをオフのままにしておくと、カスタム タイムアウト アラートはポップアップ ウィンドウに表示されます。

**ステップ 5** [Idle Timeout Message] ボックスおよび [Session Timeout Message] ボックスにメッセージを入力します。メッセージの例は、次のとおりです。「Warning: Your session will end in %s. Please complete your work and prepare to close your applications.」

**ステップ 6** [OK] をクリックします。

**ステップ 7** [Apply] をクリックします。

## カスタマイゼーションオブジェクト ファイルでのカスタム タイムアウト アラートの指定

必要に応じて、ASA の外部の既存のカスタマイゼーションオブジェクト ファイルを編集し、ASA にインポートできます。

タイムアウト メッセージは、XML カスタマイゼーションオブジェクト ファイルの <timeout-alerts> XML 要素で設定されます。<timeout-alerts> 要素は <portal> 要素の子です。<portal> 要素は <custom> 要素の子です。

<timeout-alerts> 要素は、<portal> の子要素の順序では、<home-page> 要素の後、<application> 要素の前に配置します。

<timeout-alerts> の次の子要素を指定する必要があります。

- <alert-tooltip> : 「yes」に設定されると、カウントダウン タイマーはユーザにツール ヒントとして赤の背景に表示されます。カウントダウン タイマーをクリックすると、ツールチップが展開されて、カスタムメッセージが表示されます。「no」に設定されるか未定義の場合、カスタムメッセージはポップアップ ウィンドウでユーザに表示されます。
- <session-timeout-message> : この要素にカスタムセッションタイムアウトメッセージを入力します。設定されており、空ではない場合は、デフォルトメッセージの代わりに、カスタムメッセージを受け取ります。メッセージ内の %s プレースホルダは、進行するカウントダウンタイマーで置き換えられます。
- <idle-timeout-message> : この要素にカスタムアイドルタイムアウトメッセージを入力します。設定されており、空ではない場合は、デフォルトメッセージの代わりに、カスタムメッセージを受け取ります。 %s プレースホルダは、進行するカウントダウンタイマーで置き換えられます。

### 次の作業

カスタマイゼーションオブジェクトのインポートおよびエクスポートと、XML ベースのポータルカスタマイゼーションオブジェクトと URL リストの作成について確認してください。

### タイムアウトアラート要素および子要素の設定例

この例では、<portal> 要素の <timeout-alerts> 要素のみを示します。

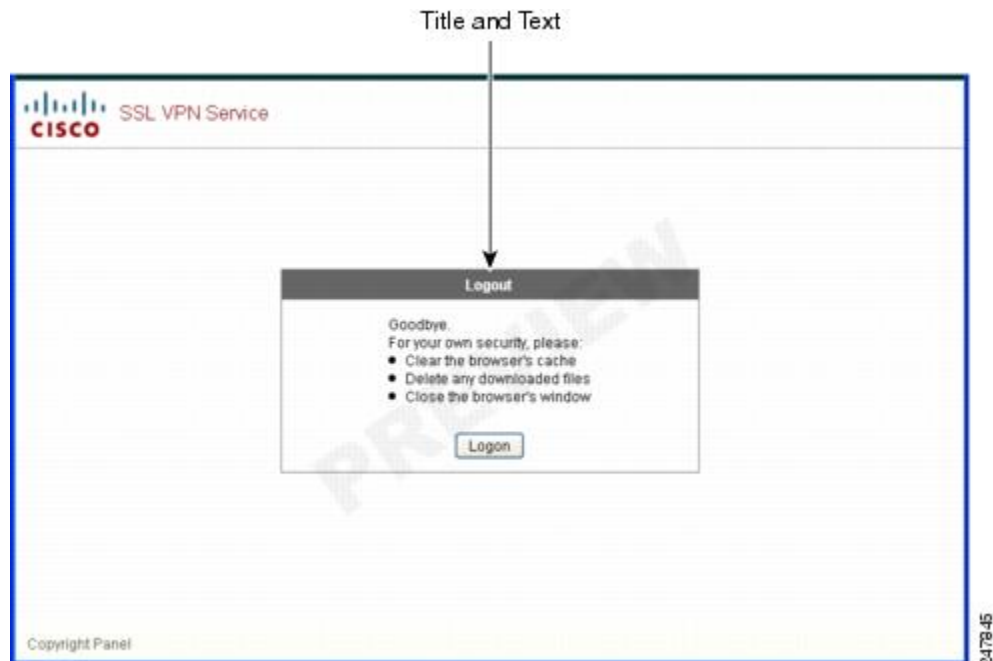
この例を既存のカスタマイゼーションオブジェクトにカットアンドペーストしないでください。

```
<portal>
 <window></window>
 <title-panel></title-panel>
 <toolbar></toolbar>
 <url-lists></url-lists>
 <navigation-panel></navigation-panel>
 <home-page>
 <timeout-alerts>
 <alert-tooltip>yes</alert-tooltip>
 <idle-timeout-message>You session expires in %s due to
idleness.</idle-timeout-message>
 <session-timeout-message>Your session expires in %s.</session-timeout-message>
 </timeout-alerts>
 <application></application>
 <column></column>
 <pane></pane>
 <external-portal></external-portal>
</portal>
```

## ログアウトページのカスタマイズ

次の図に、カスタマイズ可能なログアウトページを示します。

図 21: ログアウトページのコンポーネント



ログアウトページをカスタマイズするには、次の手順を実行します。[Preview] ボタンをクリックして、各コンポーネントに対する変更をプレビューできます。

## 手順

- ステップ 1 [Logout Page]に移動します。必要に応じて、タイトルまたはテキストをカスタマイズします。
- ステップ 2 ユーザに便利のように、ログアウト ページに [Login] ボタンを表示できます。そのためには、[Show logon button]をオンにします。必要に応じて、ボタンのテキストをカスタマイズします。
- ステップ 3 必要に応じて、タイトルのフォントまたは背景をカスタマイズします。
- ステップ 4 [OK]をクリックしてから、編集したカスタマイゼーションオブジェクトに変更を適用します。

# カスタマイゼーションオブジェクトの追加

## 手順

- ステップ 1 [Add]をクリックし、新しいカスタマイゼーションオブジェクトの名前を入力します。最大 64 文字で、スペースは使用できません。
- ステップ 2 (任意) [Find]をクリックして、カスタマイゼーションオブジェクトを検索します。このフィールドへの入力を開始すると、各フィールドの先頭部分の文字が検索され、一致するものが検出されます。ワイルドカードを使用すると、検索範囲が広がります。たとえば、[Find] フィールドに *sal* と入力すると、*sales* という名前のカスタマイゼーション オブジェクトは一致しますが、*wholesalers* という名前のカスタマイゼーションオブジェクトは一致しません。[Find] フィールドに *\*sal* と入力した場合は、テーブル内の *sales* と *wholesalers* のうち、最初に出現するものが検出されます。  
  
上矢印と下矢印を使用して、上または下にある、一致する次の文字列に移動します。[Match Case] チェックボックスをオンにして、大文字と小文字が区別されるようにします。
- ステップ 3 ログイン時にポータルページの [Password] フィールドをクリックすると、オンスクリーンキーボードによってキーボードがイネーブルになります。これは、[Username] ボックスではイネーブルになりません。オンスクリーン キーボードをポータル ページに表示するタイミングを指定します。次の選択肢があります。
  - Do not show OnScreen Keyboard
  - Show only for the login page
  - Show for all portal pages requiring authentication
- ステップ 4 (任意) カスタマイゼーション オブジェクトを強調表示して [Assign] をクリックし、選択したオブジェクトを 1 つ以上のグループポリシー、接続プロファイル、または LOCAL ユーザに割り当てます。

## カスタマイゼーションオブジェクトのインポートおよびエクスポート

既存のカスタマイゼーションオブジェクトをインポートまたはエクスポートできます。エンドユーザーに適用するオブジェクトをインポートします。ASA 上の既存のカスタマイゼーションオブジェクトをエクスポートして編集し、その後再びインポートできます。

### 手順

- 
- ステップ 1** カスタマイゼーションオブジェクトを名前指定します。最大 64 文字で、スペースは使用できません。
- ステップ 2** カスタマイゼーションファイルをインポートする、またはエクスポートするための方法を選択します。
- [Local computer] : ローカル PC に常駐するファイルをインポートするには、この方式を選択します。
  - [Path] : ファイルへのパスを入力します。
  - [Browse Local Files] : ファイルのパスを参照します。
  - [Flash file system] : ASA に常駐するファイルをエクスポートするには、この方式を選択します。
  - [Path] : ファイルへのパスを入力します。
  - [Browse Flash] : ファイルのパスを参照します。
  - [Remote server] : ASA からアクセス可能なリモートサーバに常駐するカスタマイゼーションファイルをインポートするには、このオプションを選択します。
  - [Path] : ファイルへのアクセス方式 (ftp、http、または https) を指定し、ファイルへのパスを入力します。

- ステップ 3** クリックして、ファイルをインポートまたはエクスポートします。
- 

## XML カスタマイゼーションファイルの構成について

次の図に、XML カスタマイゼーションオブジェクトのファイル構造を示します。



- 
- (注) パラメータ/タグが指定されなければデフォルト/継承値が使用されます。存在する場合は、空の文字列であってもパラメータ/タグ値が設定されます。
-

表 15: XML ベース カスタマイゼーション ファイルの構成

タグ	タイプ	値	プリセット値	説明
custom	ノード	—	—	ルート タグ
auth-page	ノード	—	—	認証ページ コンフィギュレーションのタグ コンテナ
window	ノード	—	—	ブラウザ ウィンドウ
title-text	string	任意の文字列	空の文字列	—
title-panel	ノード	—	—	ロゴおよびテキストを表示したページの先頭パネル
mode	text	enable disable	disable	—
text	text	任意の文字列	空の文字列	—
logo-url	text	任意の URL	空のイメージ URL	—
copyright-panel	ノード	—	—	著作権情報を示したページの下部ペイン
mode	text	enable disable	disable	—
text	text	任意の URL	空の文字列	—
info-panel	ノード	—	—	カスタム テキストとイメージを表示したペイン
mode	string	enable disable	disable	—
image-position	string	above below	above	テキストに対する相対的なイメージの位置
image-url	string	任意の URL	空のイメージ	—
text	string	任意の文字列	空の文字列	—

logon-form	ノード	—	—	ユーザ名、パスワード、グループプロンプトのフォーム
title-text	string	任意の文字列	Logon	—
message-text	string	任意の文字列	空の文字列	—
username-prompt-text	string	任意の文字列	ユーザ名	—
password-prompt-text	string	任意の文字列	Password	—
internal-password-prompt-text	string	任意の文字列	Internal Password	—
group-prompt-text	string	任意の文字列	グループ	—
submit-button-text	string	任意の文字列	Logon	
logout-form	ノード	—	—	ログアウトメッセージと、ログインまたはウィンドウを閉じるためのボタンを表示したフォーム
title-text	string	任意の文字列	Logout	—
message-text	string	任意の文字列	空の文字列	—
login-button-text	string	任意の文字列	ログイン	
close-button-text	string	任意の文字列	Close window	—
language-selector	ノード	—	—	言語を選択するドロップダウンリスト
mode	string	enable disable	disable	—
title	text	—	言語	言語を選択するよう求めるプロンプトテキスト
language	ノード (複数)	—	—	—
code	string	—	—	—
text	string	—	—	—

portal	ノード	—	—	ポータルページ コンフィギュレーションのタグコンテナ
window	ノード	—	—	認証ページの説明を参照
title-text	string	任意の文字列	空の文字列	—
title-panel	ノード	—	—	認証ページの説明を参照
mode	string	enable disable	Disable	—
text	string	任意の文字列	空の文字列	—
logo-url	string	任意の URL	空のイメージ URL	—
navigation-panel	ノード	—	—	アプリケーション タブの左側のペイン
mode	string	enable disable	イネーブル化	—
application	ノード (複数)	—	該当なし	ノードは (ID によって) 設定されているアプリケーションのデフォルトを変更する
id	string	ストック アプリケーションの場合： web-access file-access app-access net-access help ins の場合： 固有のプラグイン	該当なし	—
tab-title	string	—	該当なし	—

order	number	—	該当なし	エレメントの並べ替えで使用する値。デフォルトのエレメント順の値には、1000、2000、3000などの段階があります。たとえば、最初と2番目のエレメントの間にエレメントを挿入するには、1001～1999の値を使用します。
url-list-title	string	—	該当なし	アプリケーションにブックマークがある場合は、グループ化されたブックマークを表示したパネルのタイトル
mode	string	enable disable	該当なし	v
toolbar	ノード	—	—	—
mode	string	enable disable	Enable	—
prompt-box-title	string	任意の文字列	住所	URL プロンプトリストのタイトル
browse-button-text	string	任意の文字列	ブラウザ	[Browse] ボタンのテキスト
logout-prompt-text	string	任意の文字列	Logout	—
column	ノード (複数)	—	—	デフォルトで1列を表示
width	string	—	該当なし	—
order	number	—	該当なし	エレメントの並べ替えで使用する値。



url-lists	ノード	—	—	URL リストは、明示的にオフに切り替えられていない場合、ポータルホームページのデフォルト エlement と見なされる
mode	string	group   nogroup	group	モード： group : Web Bookmarks や File Bookmarks などのアプリケーションタイプによってグループ化されたエlement no-group : URL リストを別々のペインに表示する disable : デフォルトで URL リストを表示しない
panel	ノード (複数)	—	—	追加ペインの設定を許可
mode	string	enable disable	—	コンフィギュレーションを削除せずにパネルを一時的にオフに切り替える場合に使用する
title	string	—	—	—
type	string	—	—	Supported types: RSS IMAGE TEXT HTML
url	string	—	—	RSS、IMAGE、または HTML タイプのペインの URL

url-mode	string	—	—	モード : mangle、no-mangle
text	string	—	—	TEXT タイプ ペインのテキスト
column	number	—	—	—

## カスタマイゼーションの設定例

次の例は、次のカスタマイゼーション オプションを示しています。

- File アクセス アプリケーションのタブを非表示にする。
- Web Access アプリケーションのタイトルと順序を変更する。
- ホーム ページで 2 つのカラムを定義する。
- RSS ペインを追加する。
- 2 番目のペインの上部に 3 つのペイン (テキスト、イメージ、および html) を追加する。

```
<custom name="Default">
 <auth-page>

 <window>
 <title-text l10n="yes">title WebVPN Logon</title>
 </window>

 <title-panel>
 <mode>enable</mode>
 <text l10n="yes">EXAMPLE WebVPN</text>
 <logo-url>http://www.example.com/images/EXAMPLE.gif</logo-url>
 </title-panel>

 <copyright>
 <mode>enable</mode>
 <text l10n="yes">(c) Copyright, EXAMPLE Inc., 2006</text>
 </copyright>

 <info-panel>
 <mode>enable</mode>
 <image-url>/+CSCOE+/custom/EXAMPLE.jpg</image-url>
 <text l10n="yes">
 <![CDATA[
 <div>
 Welcome to WebVPN !.
 </div>
]>
 </text>
 </info-panel>
 <logon-form>
 <form>
 <title-text l10n="yes">title WebVPN Logon</title>
 <message-text l10n="yes">message WebVPN Logon</title>
 <username-prompt-text l10n="yes">Username</username-prompt-text>
 <password-prompt-text l10n="yes">Password</password-prompt-text>
 <internal-password-prompt-text l10n="yes">Domain
```

```

password</internal-password-prompt-text>
 <group-prompt-text l10n="yes">Group</group-prompt-text>
 <submit-button-text l10n="yes">Logon</submit-button-text>
</form>
</logon-form>
<logout-form>
 <form>
 <title-text l10n="yes">title WebVPN Logon</title>
 <message-text l10n="yes">message WebVPN Logon</title>
 <login-button-text l10n="yes">Login</login-button-text>
 <close-button-text l10n="yes">Logon</close-button-text>
 </form>
</logout-form>

<language-selector>
 <language>
 <code l10n="yes">code1</code>
 <text l10n="yes">text1</text>
 </language>
 <language>
 <code l10n="yes">code2</code>
 <text l10n="yes">text2</text>
 </language>
</language-selector>

</auth-page>
<portal>

 <window>
 <title-text l10n="yes">title WebVPN Logon</title>
 </window>

 <title-panel>
 <mode>enable</mode>
 <text l10n="yes">EXAMPLE WebVPN</text>
 <logo-url>http://www.example.com/logo.gif</logo-url>
 </title-panel>

 <navigation-panel>
 <mode>enable</mode>
 </navigation-panel>

 <application>
 <id>file-access</id>
 <mode>disable</mode>
 </application>
 <application>
 <id>web-access</id>
 <tab-title>EXAMPLE Intranet</tab-title>
 <order>3001</order>
 </application>

 <column>
 <order>2</order>
 <width>40%</width>
 </column>
 <column>
 <order>1</order>
 <width>60%</width>
 </column>

 <url-lists>
 <mode>no-group</mode>
 </url-lists>

```

```

<pane>
 <id>rss_pane</id>
 <type>RSS</type>
 <url>rss.example.com?id=78</url>
</pane>
<pane>
 <type>IMAGE</type>
 <url>http://www.example.com/logo.gif</url>
 <column>1</column>
 <row>2</row>
</pane>

<pane>
 <type>HTML</type>
 <title>EXAMPLE news</title>
 <url>http://www.example.com/news.html</url>
 <column>1</column>
 <row>3</row>
</pane>

</portal>

</custom>

```

## カスタマイゼーションテンプレートの使用

Template という名前のカスタマイゼーションテンプレートには、現在使用されているすべてのタグと、その使用法を示す対応するコメントが含まれています。export コマンドを使用し、次のようにして ASA からカスタマイゼーションテンプレートをダウンロードします。

```

hostname# export webvpn customization Template tftp://webserver/default.xml
hostname#

```

Template ファイルは、変更することも削除することもできません。エクスポートする場合は、この例のように、default.xml という新しい名前で作成して保存します。このファイルで変更を行った後、組織のニーズに合致するカスタマイゼーションオブジェクトを作成し、default.xml または選択した別名のファイルとして ASA にインポートします。次に例を示します。

```

hostname# import webvpn customization General tftp://webserver/custom.xml
hostname#

```

ここでは、custom.xml という名前の XML オブジェクトをインポートし、ASA で General と命名します。

## カスタマイゼーションテンプレート

Template という名前のカスタマイゼーションテンプレートを以下に示します。

```

<?xml version="1.0" encoding="UTF-8" ?>
- <!-- Copyright (c) 2008,2009 by Cisco Systems, Inc. All rights reserved. Note: all
white spaces in tag values are significant and preserved. Tag: custom Description:
Root customization tag Tag: custom/languages Description: Contains list of languages,
recognized by ASA Value: string containing comma-separated language codes. Each language

```

code is a set dash-separated alphanumeric characters, started with alpha-character (for example: en, en-us, irokese8-language-us) Default value: en-us Tag: custom/default-language Description: Language code that is selected when the client and the server were not able to negotiate the language automatically.

For example the set of languages configured in the browser is "en,ja", and the list of languages, specified by 'custom/languages' tag is "cn,fr", the default-language will be used. Value: string, containing one of the language coded, specified in 'custom/languages' tag above. Default value: en-us  
 \*\*\*\*\* Tag: custom/auth-page  
 Description: Contains authentication page settings  
 \*\*\*\*\* Tag: custom/auth-page/window  
 Description: Contains settings of the authentication page browser window Tag: custom/auth-page/window/title-text Description: The title of the browser window of the authentication page Value: arbitrary string Default value: Browser's default value  
 \*\*\*\*\* Tag: custom/auth-page/title-panel Description: Contains settings for the title panel Tag: custom/auth-page/title-panel/mode Description: The title panel mode Value: enable|disable Default value: disable Tag: custom/auth-page/title-panel/text Description: The title panel text. Value: arbitrary string Default value: empty string Tag: custom/auth-page/title-panel/logo-url Description: The URL of the logo image (imported via "import webvpn webcontent") Value: URL string Default value: empty image URL Tag: custom/auth-page/title-panel/background-color Description: The background color of the title panel Value: HTML color format, for example #FFFFFF Default value: #FFFFFF Tag: custom/auth-page/title-panel/font-color Description: The background color of the title panel Value: HTML color format, for example #FFFFFF Default value: #000000 Tag: custom/auth-page/title-panel/font-weight Description: The font weight Value: CSS font size value, for example bold, bolder, lighter etc. Default value: empty string Tag: custom/auth-page/title-panel/font-size Description: The font size Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc. Default value: empty string Tag: custom/auth-page/title-panel/gradient Description: Specifies using the background color gradient Value: yes|no Default value: no Tag: custom/auth-page/title-panel/style Description: CSS style of the title panel Value: CSS style string Default value: empty string \*\*\*\*\* Tag: custom/auth-page/copyright-panel Description: Contains the copyright panel settings Tag: custom/auth-page/copyright-panel/mode Description: The copyright panel mode Value: enable|disable Default value: disable Tag: custom/auth-page/copyright-panel/text Description: The copyright panel text Value: arbitrary string Default value: empty string \*\*\*\*\* Tag: custom/auth-page/info-panel Description: Contains information panel settings Tag: custom/auth-page/info-panel/mode Description: The information panel mode Value: enable|disable Default value: disable Tag: custom/auth-page/info-panel/image-position Description: Position of the image, above or below the informational panel text Values: above|below Default value: above Tag: custom/auth-page/info-panel/image-url Description: URL of the information panel image (imported via "import webvpn webcontent") Value: URL string Default value: empty image URL Tag: custom/auth-page/info-panel/text Description: Text of the information panel Text: arbitrary string Default value: empty string \*\*\*\*\* Tag: custom/auth-page/logon-form Description: Contains logon form settings Tag: custom/auth-page/logon-form/title-text Description: The logon form title text Value: arbitrary string Default value: "Logon" Tag: custom/auth-page/logon-form/message-text Description: The message inside of the logon form Value: arbitrary string Default value: empty string Tag: custom/auth-page/logon-form/username-prompt-text Description: The username prompt text Value: arbitrary string Default value: "Username" Tag: custom/auth-page/logon-form/password-prompt-text Description: The password prompt text Value: arbitrary string Default value: "Password" Tag: custom/auth-page/logon-form/internal-password-prompt-text Description: The internal password prompt text Value: arbitrary string Default value: "Internal Password" Tag: custom/auth-page/logon-form/group-prompt-text Description: The group selector prompt text Value: arbitrary string Default value: "Group" Tag: custom/auth-page/logon-form/submit-button-text Description: The submit button text Value: arbitrary string Default value: "Logon" Tag: custom/auth-page/logon-form/internal-password-first Description: Sets internal password first in the order Value: yes|no Default value: no Tag: custom/auth-page/logon-form/title-font-color Description: The font color of the logon

```

form title Value: HTML color format, for example #FFFFFF Default value: #000000 Tag:
custom/auth-page/logon-form/title-background-color Description: The background color of the
 logon form title Value: HTML color format, for example #FFFFFF Default value: #000000
 Tag: custom/auth-page/logon-form/font-color Description: The font color of the logon
 form Value: HTML color format, for example #FFFFFF Default value: #000000 Tag:
custom/auth-page/logon-form/background-color Description: The background color of the
 logon form Value: HTML color format, for example #FFFFFF Default value: #000000
 ***** Tag:
custom/auth-page/logout-form Description: Contains the logout form settings Tag:
custom/auth-page/logout-form/title-text Description: The logout form title text Value:
 arbitrary string Default value: "Logout" Tag: custom/auth-page/logout-form/message-text
 Description: The logout form message text Value: arbitrary string Default value: Goodbye.
 For your own security, please: Clear the browser's cache
 Delete any downloaded files Close the browser's window
Tag: custom/auth-page/logout-form/login-button-text Description: The text of the button
 sending the user to the logon page Value: arbitrary string Default value: "Logon"
 ***** Tag:
custom/auth-page/language-selector Description: Contains the language selector settings
 Tag: custom/auth-page/language-selector/mode Description: The language selector mode
 Value: enable|disable Default value: disable Tag: custom/auth-page/language-selector/title
 Description: The language selector title Value: arbitrary string Default value: empty
 string Tag: custom/auth-page/language-selector/language (multiple) Description: Contains
 the language settings Tag: custom/auth-page/language-selector/language/code Description:
 The code of the language Value (required): The language code string Tag:
custom/auth-page/language-selector/language/text Description: The text of the language
 in the language selector drop-down box Value (required): arbitrary string
 ***** Tag: custom/portal Description:
 Contains portal page settings *****
 Tag: custom/portal/window Description: Contains the portal page browser window settings
 Tag: custom/portal/window/title-text Description: The title of the browser window of
 the portal page Value: arbitrary string Default value: Browser's default value
 ***** Tag: custom/portal/title-panel
 Description: Contains settings for the title panel Tag: custom/portal/title-panel/mode
 Description: The title panel mode Value: enable|disable Default value: disable Tag:
custom/portal/title-panel/text Description: The title panel text. Value: arbitrary string
 Default value: empty string Tag: custom/portal/title-panel/logo-url Description: The
 URL of the logo image (imported via "import webvpn webcontent") Value: URL string Default
 value: empty image URL Tag: custom/portal/title-panel/background-color Description:
 The background color of the title panel Value: HTML color format, for example #FFFFFF
 Default value: #FFFFFF Tag: custom/auth-pa/title-panel/font-color Description: The
 background color of the title panel Value: HTML color format, for example #FFFFFF Default
 value: #000000 Tag: custom/portal/title-panel/font-weight Description: The font weight
 Value: CSS font size value, for example bold, bolder, lighter etc. Default value: empty
 string Tag: custom/portal/title-panel/font-size Description: The font size Value: CSS
 font size value, for example 10pt, 8px, x-large, smaller etc. Default value: empty
 string Tag: custom/portal/title-panel/gradient Description: Specifies using the background
 color gradient Value: yes|no Default value: no Tag: custom/portal/title-panel/style
 Description: CSS style for title text Value: CSS style string Default value: empty string
 ***** Tag: custom/portal/application
 (multiple) Description: Contains the application setting Tag:
custom/portal/application/mode Description: The application mode Value: enable|disable
 Default value: enable Tag: custom/portal/application/id Description: The application
 ID. Standard application ID's are: home, web-access, file-access, app-access,
 network-access, help Value: The application ID string Default value: empty string Tag:
 custom/portal/application/tab-title Description: The application tab text in the
 navigation panel Value: arbitrary string Default value: empty string Tag:
custom/portal/application/order Description: The order of the application's tab in the
 navigation panel. Applications with lesser order go first. Value: arbitrary number Default
 value: 1000 Tag: custom/portal/application/url-list-title Description: The title of
 the application's URL list pane (in group mode) Value: arbitrary string Default value:
 Tab title value concatenated with "Bookmarks"
 ***** Tag:
custom/portal/navigation-panel Description: Contains the navigation panel settings Tag:
 custom/portal/navigation-panel/mode Description: The navigation panel mode Value:

```

```

enable|disable Default value: enable
***** Tag: custom/portal/toolbar
Description: Contains the toolbar settings Tag: custom/portal/toolbar/mode Description:
The toolbar mode Value: enable|disable Default value: enable Tag:
custom/portal/toolbar/prompt-box-title Description: The universal prompt box title Value:
arbitrary string Default value: "Address" Tag: custom/portal/toolbar/browse-button-text
Description: The browse button text Value: arbitrary string Default value: "Browse"
Tag: custom/portal/toolbar/logout-prompt-text Description: The logout prompt text Value:
arbitrary string Default value: "Logout"
***** Tag: custom/portal/column
(multiple) Description: Contains settings of the home page column(s) Tag:
custom/portal/column/order Description: The order the column from left to right. Columns
with lesser order values go
first Value: arbitrary number Default value: 0 Tag: custom/portal/column/width
Description: The home page column width Value: percent Default value: default value set
by browser Note: The actual width may be increased by browser to accommodate content
***** Tag: custom/portal/url-lists
Description: Contains settings for URL lists on the home page Tag:
custom/portal/url-lists/mode Description: Specifies how to display URL lists on the home
page:
group URL lists by application (group) or show individual
URL lists (nogroup). URL lists fill out cells of the configured columns,
which are not taken by custom panes. Use the attribute value
"nodisplay" to not show URL lists on the home page. Value: group|nogroup|nodisplay
Default value: group ***** Tag:
custom/portal/pane (multiple) Description: Contains settings of the custom pane on the
home page Tag: custom/portal/pane/mode Description: The mode of the pane Value:
enable|disable Default value: disable Tag: custom/portal/pane/title Description: The
title of the pane Value: arbitrary string Default value: empty string Tag:
custom/portal/pane/notitle Description: Hides pane's title bar Value: yes|no Default
value: no Tag: custom/portal/pane/type Description: The type of the pane. Supported
types:
TEXT - inline arbitrary text, may contain HTML tags;
HTML - HTML content specified by URL shown in the individual iframe; IMAGE
- image specified by URL RSS - RSS feed specified by URL Value:
TEXT|HTML|IMAGE|RSS Default value: TEXT Tag: custom/portal/pane/url Description: The
URL for panes with type HTML,IMAGE or RSS Value: URL string Default value: empty string
Tag: custom/portal/pane/text Description: The text value for panes with type TEXT
Value: arbitrary string Default value:empty string Tag: custom/portal/pane/column
Description: The column where the pane located. Value: arbitrary number Default value:
1 Tag: custom/portal/pane/row Description: The row where the pane is located Value:
arbitrary number Default value: 1 Tag: custom/portal/pane/height Description: The height
of the pane Value: number of pixels Default value: default value set by browser
***** Tag:
custom/portal/browse-network-title Description: The title of the browse network link
Value: arbitrary string Default value: Browse Entire Network Tag:
custom/portal/access-network-title Description: The title of the link to start a network
access session Value: arbitrary string Default value: Start AnyConnect -->
- <custom>
- <localization>
<languages>en, ja, zh, ru, ua</languages>
<default-language>en</default-language>
</localization>
- <auth-page>
- <window>
- <title-text l10n="yes">
- <![CDATA[
WebVPN Service

</title-text>
</window>
- <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
- <language>
<code>en</code>

```

```

<text>English</text>
</language>
- <language>
<code>zh</code>
<text>?? (Chinese)</text>
</language>
- <language>
<code>ja</code>
<text>?? (Japanese)</text>
</language>
- <language>
<code>ru</code>
<text>?????? (Russian)</text>
</language>
- <language>
<code>ua</code>
<text>???????? (Ukrainian)</text>
</language>
</language-selector>
- <logon-form>
- <title-text l10n="yes">
- <![CDATA[
Login

</title-text>
- <title-background-color>
- <![CDATA[
#666666

</title-background-color>
- <title-font-color>
- <![CDATA[
#ffffff

</title-font-color>
- <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.

</message-text>
- <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:

</username-prompt-text>
- <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:

</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:

</group-prompt-text>
- <submit-button-text l10n="yes">
- <![CDATA[
Login

</submit-button-text>
- <title-font-color>
- <![CDATA[

```



```
#ffffff

</title-font-color>
- <title-background-color>
- <![CDATA[
#666666

</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout

</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.

</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service

</text>
<logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff

</background-color>
- <font-size>
- <![CDATA[
larger

</font-size>
- <font-color>
- <![CDATA[
#800000

</font-color>
- <font-weight>
- <![CDATA[
bold

</font-weight>
</title-panel>
- <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
- <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
```

```

</auth-page>
- <portal>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service

</text>
<logo-url l10n="yes">/+CSCOU+/cscsco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff

</background-color>
- <font-size>
- <![CDATA[
larger

</font-size>
- <font-color>
- <![CDATA[
#800000

</font-color>
- <font-weight>
- <![CDATA[
bold

</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
- <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
- <application>
<mode>enable</mode>
<id>web-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Web Applications

</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks

</url-list-title>
<order>2</order>
</application>
- <application>
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks

</tab-title>

```

```

- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks

</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access

</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
- <column>
<width>100%</width>
<order>1</order>
</column>
- <pane>
<type>TEXT</type>
<mode>disable</mode>
<title />
<text />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>IMAGE</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />

```

```

<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>

```

## ヘルプのカスタマイズ

ASA は、クライアントレスセッションの間、アプリケーションペインにヘルプ コンテンツを表示します。それぞれのクライアントレスアプリケーションペインには、事前設定されたファイル名を使用する独自のヘルプファイルのコンテンツが表示されます。たとえば、[Application Access] パネルに表示されるヘルプ コンテンツは、`app-access-hlp.inc` というファイルの内容です。次の図に、クライアントレス アプリケーション パネルと、ヘルプのコンテンツの事前設定されたファイル名を示します。

表 16: クライアントレス アプリケーション

アプリケーション タイプ	パネル	ファイル名
規格	Application Access	app-access-hlp.inc
規格	Browse Networks	file-access-hlp.inc
規格	AnyConnect Client	net-access-hlp.inc
規格	Web Access	web-access-hlp.inc
プラグイン	MetaFrame Access	ica-hlp.inc
プラグイン	Terminal Servers	rdp-hlp.inc
プラグイン	Telnet/SSH Servers	ssh,telnet-hlp.inc
プラグイン	VNC Connections	vnc-hlp.inc

<sup>3</sup> このプラグインは、`sshv1` と `sshv2` の両方を実行できます。

シスコが提供するヘルプ ファイルをカスタマイズするか、または別の言語でヘルプ ファイルを作成できます。その後、[Import] ボタンをクリックして、それらのファイルを ASA のフラッ

シュ メモリにコピーし、後続のクライアントレス セッション中に表示します。また、以前にインポートしたヘルプコンテンツ ファイルをエクスポートし、カスタマイズして、フラッシュメモリに再インポートすることもできます。

#### 手順

- ステップ 1** [Import] をクリックして、[Import Application Help Content] ダイアログを起動します。このダイアログでは、クライアントレスセッション中に表示する新しいヘルプコンテンツをフラッシュメモリにインポートできます。
- ステップ 2** (任意) インポート済みのヘルプコンテンツをテーブルから選択し、取得するには、[Export] をクリックします。
- ステップ 3** (任意) インポート済みのヘルプコンテンツをテーブルから選択し、削除するには、[Delete] をクリックします。
- ステップ 4** ブラウザに表示される言語の省略形が表示されます。このフィールドは、ファイル変換には使用されません。ファイル内で使用される言語を示します。テーブル内の略語に関連付ける言語名を特定するには、ブラウザで表示される言語のリストを表示します。たとえば、次の手順のいずれかを使用すると、ダイアログ ウィンドウに言語と関連の言語コードが表示されます。
  - Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。
  - Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

ヘルプコンテンツ ファイルがインポートされたときのファイル名が表示されます。

## シスコが提供するヘルプ ファイルのカスタマイズ

シスコが提供するヘルプ ファイルをカスタマイズするには、まず、フラッシュメモリカードからファイルのコピーを取得する必要があります。

#### 手順

- ステップ 1** ブラウザを使用して、ASA とのクライアントレスセッションを確立します。
- ステップ 2** 次の表の項目「セキュリティアプライアンスのフラッシュメモリ内のヘルプファイルのURL」に示されている文字列を ASA のアドレスに追加し、表の下の説明に従って *language* の部分を置き換え、その後 **Enter** を押してヘルプファイルを表示します。

表 17: シスコ提供のクライアントレス アプリケーション用ヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリ内のヘルプ ファイルの URL
規格	Application Access	/+CSCO+/help/language/app-access-hlp.inc
規格	Browse Networks	/+CSCO+/help/language/file-access-hlp.inc
規格	AnyConnect Client	/+CSCO+/help/language/net-access-hlp.inc
規格	Web Access	/+CSCO+/help/language/web-access-hlp.inc
プラグイン	Terminal Servers	/+CSCO+/help/language/rdp-hlp.inc
プラグイン	Telnet/SSH Servers	/+CSCO+/help/language/ssh,telnet-hlp.inc
プラグイン	VNC Connections	/+CSCO+/help/language/vnc-hlp.inc

*language* は、ブラウザで表示される言語の略語です。略語はファイル変換では使用されません。これは、ファイルで使用される言語を示します。シスコが提供する英語版のヘルプ ファイルを表示する場合は、略語として **en** と入力します。

次のアドレス例は、Terminal Servers のヘルプの英語版を表示します。

**https://address\_of\_security\_appliance/+CSCO+/help/en/rdp-hlp.inc**

**ステップ 3** [File] > [Save (Page) As] を選択します。

(注) [File name] ボックスの内容は変更しないでください。

**ステップ 4** [Save as type] オプションを [Web Page, HTML only] に変更して、[Save] をクリックします。

**ステップ 5** 任意の HTML エディタを使用してファイルをカスタマイズします。

(注) ほとんどの HTML タグを使用できますが、ドキュメントとその構造を定義するタグは使用しないでください (たとえば、<html>, <title>, <body>, <head>, <h1>, <h2> など)。<b> タグのような文字のタグや、<p>, <ol>, <ul>, および <li> のようなコンテンツを構造化するタグは使用できます。

**ステップ 6** オリジナルのファイル名と拡張子を指定して、HTML only としてファイルを保存します。ファイル名に余分なファイル拡張子がないことを確認します。

### 次のタスク

ASDM に戻り、[Configuration] > **Remote Access VPN > Clientless SSL VPN Access** > [Portal] > [Help Customization] > [Import] を選択して、修正したヘルプ ファイルをフラッシュ メモリにインポートします。

## シスコが提供していない言語用のヘルプ ファイルの作成

標準 HTML を使用して他の言語のヘルプ ファイルを作成します。サポートするそれぞれの言語に別のフォルダを作成することをお勧めします。



- (注) ほとんどの HTML タグを使用できますが、ドキュメントとその構造を定義するタグは使用しないでください（たとえば、<html>, <title>, <body>, <head>, <h1>, <h2> など）。<b> タグのような文字のタグや、<p>, <ol>, <ul>, および <li> のようなコンテンツを構造化するタグは使用できません。

HTML only としてファイルを保存します。[Filename] カラムにあるファイル名を使用してください。

ASDM に戻り、[Configuration] > **Remote Access VPN > Clientless SSL VPN Access** > [Portal] > [Help Customization] > [Import] を選択して、新しいヘルプ ファイルをフラッシュ メモリにインポートします。

## アプリケーションのヘルプコンテンツのインポートおよびエクスポート

[Import Application Help Content] ダイアログボックスを使用して、クライアントレス セッション中にポータル ページに表示するために、ヘルプ ファイルをフラッシュ メモリにインポートします。[Export Application Help Content] ダイアログボックスを使用して、以前にインポートしたヘルプ ファイルをその後の編集のために取得します。

### 手順

- ステップ 1** [Language] フィールドによってブラウザに表示される言語が指定されますが、このフィールドはファイル変換には使用されません（このフィールドは、[Export Application Help Content] ダイアログボックスでは非アクティブです）。[Language] フィールドの横にあるドット（複数）をクリックし、[Browse Language Code] ダイアログボックスで、表示される言語を含む行をダブルクリックします。[Language Code] フィールドの略語がその行の略語と一致することを確認して、[OK] をクリックします。
- ステップ 2** ヘルプ コンテンツを提供する言語が [Browse Language Code] ダイアログボックスにない場合は、次の手順を実行します。
- ブラウザに表示される言語および略語のリストを表示します。
  - 言語の略語を [Language Code] フィールドに入力し、[OK] をクリックします。

または

ドット（複数）の左にある [Language] テキスト ボックスに入力することもできます。

次のいずれかの操作を実行すると、ダイアログボックスに言語および関連付けられた言語コードが表示されます。

- Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。
- Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

**ステップ 3** インポートしている場合は、新しいヘルプ コンテンツ ファイルを [File Name] ドロップダウン リストから選択します。エクスポートする場合は、このフィールドは使用できません。

**ステップ 4** ソース ファイル（インポートの場合）または転送先ファイル（エクスポートの場合）のパラメータを設定します。

- [Local computer] : ソースまたは転送先ファイルがローカルコンピュータにある場合に指定します。
  - [Path] : ソースまたは転送先ファイルのパスを指定します。
  - [Browse Local Files] : ソースまたは転送先ファイルのローカル コンピュータを参照します。
- [Flash file system] : ソースまたは宛先ファイルが ASA のフラッシュ メモリ内にある場合に指定します。
  - [Path] : フラッシュ メモリ内のソースまたは転送先ファイルのパスを指定します。
  - [Browse Flash] : ソースまたは転送先ファイルのあるフラッシュ メモリを参照します。
- [Remote server] : ソースまたは転送先ファイルがリモートサーバにある場合に指定します。
  - [Path] : ftp、tftp、または http（インポートの場合のみ）の中からファイル転送（コピー）方式を選択し、パスを指定します。

## ブックマーク ヘルプのカスタマイズ

ASA は、選択された各ブックマークのアプリケーションパネルにヘルプの内容を表示します。これらのヘルプ ファイルをカスタマイズしたり、他の言語でヘルプ ファイルを作成したりできます。次に、後続のセッション中に表示するために、ファイルをフラッシュ メモリにインポートします。事前にインポートしたヘルプ コンテンツ ファイルを取得して、変更し、フラッシュ メモリに再インポートすることもできます。

各アプリケーションのパネルには、事前に設定されたファイル名を使用して独自のヘルプ ファイル コンテンツが表示されます。今後、各ファイルは、ASA のフラッシュ メモリ内の `/+CSCOE+/help/language/` という URL に置かれます。次の表に、VPN セッション用に保守できる各ヘルプ ファイルの詳細を示します。



表 18: VPN アプリケーションのヘルプ ファイル

アプリケーションタイプ	パネル	セキュリティアプライアンスのフラッシュメモリ内のヘルプファイルの URL	シスコが提供するヘルプファイルに英語版があるか
規格	Application Access	#CSCOE#help#ug#appaccess#pic	あり
規格	Browse Networks	#CSCOE#help#ug#bncs#pic	あり
規格	AnyConnect Client	#CSCOE#help#ug#accs#pic	あり
規格	Web Access	#CSCOE#help#ug#wbas#pic	あり
プラグイン	MetaFrame Access	#CSCOE#help#ug#mfah#pic	なし
プラグイン	Terminal Servers	#CSCOE#help#ug#tph#pic	あり
プラグイン	Telnet/SSH Servers	#CSCOE#help#ug#shs#pic	あり
プラグイン	VNC Connections	#CSCOE#help#ug#vnc#pic	あり

*language* は、ブラウザに表示される言語の省略形です。このフィールドは、ファイル変換には使用されません。ファイル内で使用される言語を示します。特定の言語コードを指定するには、ブラウザに表示される言語のリストからその言語の省略形をコピーします。たとえば、次の手順のいずれかを使用すると、ダイアログウィンドウに言語と関連の言語コードが表示されます。

- Internet Explorer を起動して、[Tools] > [Internet Options] > [Languages] > [Add] を選択します。
- Mozilla Firefox を起動して、[Tools] > [Options] > [Advanced] > [General] を選択し、[Languages] の隣にある [Choose] をクリックして、[Select a language to add] をクリックします。

## 言語変換について

ASA は、クライアントレス SSL VPN セッション全体に対する言語変換機能を備えています。これには、ログイン、ログアウト バナー、およびプラグインおよび AnyConnect などの認証後に表示されるポータル ページが含まれます。リモート ユーザ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。次の表に、変換ドメインおよび、変換される機能領域を示します。

言語変換ドメインのオプション

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN クライアントのユーザ インターフェイスに表示されるメッセージ。

変換ドメイン	変換される機能エリア
バナー	クライアントレス接続でVPNアクセスが拒否される場合に表示されるメッセージ。
CSD	Cisco Secure Desktop (CSD) のメッセージ。
customization	ログインページ、ログアウトページ、ポータルページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-rdp2	Java Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。
PortForwarder	ポートフォワーディングユーザに表示されるメッセージ。
url-list	ユーザがポータルページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータルメッセージ。

ASA には、標準機能の一部である各ドメイン用の変換テーブルテンプレートが含まれています。プラグインのテンプレートはプラグインともに含まれており、独自の変換ドメインを定義します。

変換ドメインのテンプレートをエクスポートできます。これで、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、新しいバージョンの変換テーブルが作成され、以前のメッセージが上書きされます。

一部のテンプレートはスタティックですが、ASA の設定に基づいて変化するテンプレートもあります。クライアントレスユーザのログオンおよびログアウトページ、ポータルページ、および URL ブックマークはカスタマイズが可能のため、**ASA generates the customization** および

**url-list** は変換ドメインテンプレートを動的に生成し、テンプレートは変更内容をこれらの機能エリアに自動的に反映させます。

変換テーブルを作成した後、このテーブルを使用して、カスタマイゼーションオブジェクトを作成し、グループポリシーまたはユーザ属性に適用できます。AnyConnect 変換ドメイン以外では、カスタマイゼーションオブジェクトを作成し、そのオブジェクトで使用する変換テーブルを識別し、グループポリシーまたはユーザに対してそのカスタマイゼーションを指定するまで、変換テーブルは影響を及ぼすことなく、ユーザ画面のメッセージは変換されません。AnyConnect ドメインの変換テーブルに対する変更は、ただちに AnyConnect クライアントユーザに表示されます。

## 変換テーブルの編集

### 手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Language Localization] の順に移動します。[Language Localization] ペインが表示されたら、[Add] をクリックします。
- ステップ 2** ドロップダウン ボックスから言語ローカリゼーションテンプレートを選択します。このボックスのエントリは、変換する機能エリアに対応します。
- ステップ 3** テンプレートの言語を指定します。テンプレートはキャッシュメモリ内の変換テーブルになり、指定した名前が付きます。ブラウザの言語オプションと互換性のある短縮形を使用してください。たとえば、中国語のテーブルを作成するときに IE を使用している場合は、IE によって認識される *zh* という略語を使用します。
- ステップ 4** 変換テーブルを編集します。msgid フィールドで表される変換対象のメッセージごとに、対応する msgstr フィールドの引用符の間に変換済みテキストを入力します。次の例では、メッセージ Connected の msgstr フィールドにスペイン語テキストを入力しています。

```
msgid "Connected"
msgstr "Conectado"
```

- ステップ 5** [OK] をクリックします。

## 変換テーブルの追加

テンプレートに基づいて新しい変換テーブルを追加するか、またはこのペインですでにインポートされた変換テーブルを修正できます。

### 手順

- ステップ 1** 修正するテンプレートを選択し、新しい変換テーブルの基礎として使用します。テンプレートは変換ドメインに構成され、特定の機能領域に影響します。

- ステップ2** ドロップダウン リストから変換ドメインを選択します
- ステップ3** 言語を指定します。ブラウザの言語オプションと互換性のある略語を使用してください。ASA はこの名前で新しい変換テーブルを作成します。
- ステップ4** エディタを使用してメッセージ変換を変更します。メッセージIDフィールド (msgid) には、デフォルトの変換が含まれています。msgid に続くメッセージ文字列フィールド (msgstr) で変換を指定します。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、「Connected」というメッセージをスペイン語に変換するには、msgstr の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"
```

変更を行った後、[Apply] をクリックして変換テーブルをインポートします。

---



## 第 21 章

# クライアントレス SSL VPN のトラブルシューティング

- [Application Access 使用時の hosts ファイル エラーからの回復 \(473 ページ\)](#)
- [WebVPN 条件付きデバッグ \(477 ページ\)](#)
- [管理者によるクライアントレス SSL VPN ユーザへのアラートの送信 \(478 ページ\)](#)
- [クライアントレス SSL VPN セッションクッキーの保護 \(478 ページ\)](#)

## Application Access 使用時の hosts ファイル エラーからの回復

Application Access の実行の妨げになる hosts ファイル エラーを回避するために、Application Access を使用し終わったら、Application Access ウィンドウを必ず閉じるようにします。ウィンドウを閉じるには、[Close] アイコンをクリックします。

Application Access が正しく終了しなかった場合は、hosts ファイルは、クライアントレス SSL VPN 用にカスタマイズされた状態のままになっています。ユーザが次に Application Access を起動するときに、クライアントレス SSL VPN は hosts.webvpn ファイルを検索することで、Application Access の状態をチェックします。hosts.webvpn ファイルが検出されると、「Backup HOSTS File Found」というエラーメッセージが表示され、Application Access が一時的にオフに切り替わります。

Application Access が異常終了した場合は、リモートアクセスクライアント/サーバアプリケーションが不安定な状態になります。クライアントレス SSL VPN を使用せずにこれらのアプリケーションを起動しようとすると、正しく動作しない場合があります。通常の接続先のホストが使用できなくなる場合があります。一般にこのような状況は、自宅からリモートでアプリケーションを実行し、Application Access ウィンドウを終了せずにコンピュータをシャットダウンし、その後職場でそのアプリケーションを実行しようとした場合に発生します。

Application Access ウィンドウを正しく閉じないと、次のエラーが発生する可能性があります。

- 次に Application Access を起動しようとしたときに、Application Access がオフに切り替わっている可能性があり、「Backup HOSTS File Found」エラーメッセージが表示される。

- アプリケーションをローカルで実行している場合でも、アプリケーション自体がオフに切り替わっているか、または動作しない。

このようなエラーは、Application Access ウィンドウを不適切な方法で終了したことが原因です。次に例を示します。

- Application Access の使用中に、ブラウザがクラッシュした。
- Application Access の使用中に、停電またはシステム シャットダウンが発生した。
- 作業中に Application Access ウィンドウを最小化し、このウィンドウがアクティブな状態（ただし最小化されている）でコンピュータをシャットダウンした。

## Hosts ファイルの概要

ローカルシステム上の hosts ファイルには、IP アドレスとホスト名がマッピングされています。Application Access を起動すると、クライアントレス SSL VPN は hosts ファイルを修正し、クライアントレス SSL VPN 固有のエントリを追加します。Application Access ウィンドウを正しく閉じて Application Access を終了すると、hosts ファイルは元の状態に戻ります。

Application Access の起動前	hosts ファイルは元の状態です。
Application Access の起動時	<ul style="list-style-type: none"> <li>• クライアントレス SSL VPN は hosts ファイルを hosts.webvpn にコピーして、バックアップを作成します。</li> <li>• 次に、クライアントレス SSL VPN は hosts ファイルを編集し、クライアントレス SSL VPN 固有の情報を挿入します。</li> </ul>
Application Access の終了時	<ul style="list-style-type: none"> <li>• クライアントレス SSL VPN はバックアップファイルを hosts ファイルにコピーして、hosts ファイルを元の状態に戻します。</li> <li>• クライアントレス SSL VPN は、hosts.webvpn を削除します。</li> </ul>
Application Access の終了後	hosts ファイルは元の状態です。



(注) Microsoft 社のアンチスパイウェア ソフトウェアは、ポート転送 Java アプレットによる hosts ファイルの変更をブロックします。アンチスパイウェア ソフトウェアの使用時に hosts ファイルの変更を許可する方法の詳細については、[www.microsoft.com](http://www.microsoft.com) を参照してください。

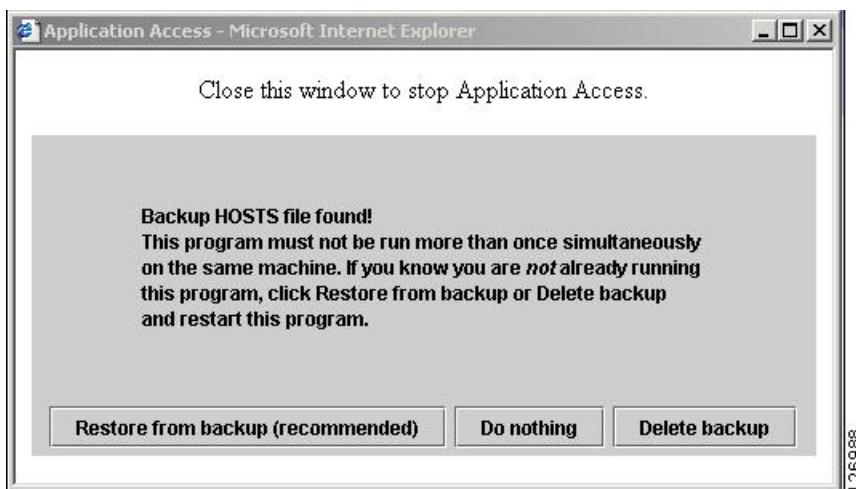
## クライアントレス SSL VPN による hosts ファイルの自動再設定

リモートアクセス サーバに接続できる場合は、hosts ファイルを再設定し、Application Access やアプリケーションを再度イネーブルにするために、次の手順を実行します。

### 手順

**ステップ 1** クライアントレス SSL VPN を起動してログインします。

[Applications Access] リンクをクリックします。



**ステップ 2** 次のいずれかのオプションを選択します。

- [Restore from backup] : クライアントレス SSL VPN は強制的に正しくシャットダウンされます。クライアントレス SSL VPN は hosts.webvpn backup ファイルを hosts ファイルにコピーし、hosts ファイルを元の状態に戻してから、hosts.webvpn を削除します。その後、Application Access を再起動する必要があります。
- [Do nothing] : Application Access は起動しません。リモートアクセスのホームページが再び表示されます。
- [Delete backup] : クライアントレス SSL VPN は hosts.webvpn ファイルを削除し、hosts ファイルをクライアントレス SSL VPN 用にカスタマイズされた状態にしておきます。元の hosts ファイル設定は失われます。Application Access は、クライアントレス SSL VPN 用にカスタマイズされた hosts ファイルを新しいオリジナルとして使用して起動します。このオプションは、hosts ファイル設定が失われても問題がない場合にだけ選択してください。Application Access が不適切にシャットダウンされた後に、ユーザまたはユーザが使用するプログラムによって hosts ファイルが編集された可能性がある場合は、他の 2 つのオプションのどちらかを選択するか、または hosts ファイルを手動で編集します

## 手動による hosts ファイルの再設定

現在の場所からリモートアクセス サーバに接続できない場合や、カスタマイズした hosts ファイルの編集内容を失いたくない場合は、次の手順に従って、hosts ファイルを再設定し、Application Access とアプリケーションを再度イネーブルにします。

### 手順

**ステップ 1** hosts ファイルを見つけて編集します。最も一般的な場所は、c:\windows\system32\drivers\etc\hosts です。

**ステップ 2** # added by WebVpnPortForward という文字列が含まれている行があるかどうかをチェックします。この文字列を含む行がある場合、hosts ファイルはクライアントレス SSL VPN 用にカスタマイズされています。hosts ファイルがクライアントレス SSL VPN 用にカスタマイズされている場合、次の例のようになっています。

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

Copyright (c) 1993-1999 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to hostnames. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding hostname.
The IP address and the hostname should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97 cisco.example.com # source server
38.25.63.10 x.example.com # x client host

123.0.0.1 localhost
```

**ステップ 3** # added by WebVpnPortForward という文字列が含まれている行を削除します

**ステップ 4** ファイルを保存して、閉じます。

**ステップ 5** クライアントレス SSL VPN を起動してログインします。

**ステップ 6** [Application Access] リンクをクリックします。



## WebVPN 条件付きデバッグ

リモートアクセス VPN 上で複数のセッションを実行すると、ログのサイズを考慮するとトラブルシューティングが困難になることがあります。 **debug webvpn condition** コマンドを使用して、デバッグプロセスをより正確に絞り込むためのフィルタを設定できます。

```
debug webvpn condition { group name | p-ipaddress ip_address [{ subnet subnet_mask | prefix length}]
| reset | user name}
```

それぞれの説明は次のとおりです。

- **group name** は、グループポリシー（トンネルグループまたは接続プロファイルではない）でフィルタ処理を行います。
- **p-ipaddress ip\_address** [{**subnet subnet\_mask** | **prefix length**}] は、クライアントのパブリック IP アドレスでフィルタ処理を行います。サブネットマスク（IPv4）またはプレフィックス（IPv6）はオプションです。
- **reset** すべてのフィルタをリセットします。 **no debug webvpn condition** コマンドを使用して、特定のフィルタをオフにできます。
- **user name** は、ユーザ名でフィルタ処理を行います。

複数の条件を設定すると、条件が結合（AND で連結）され、すべての条件が満たされた場合にのみデバッグが表示されます。

条件フィルタを設定したら、基本の **debug webvpn** コマンドを使用してデバッグをオンにします。条件を設定するだけではデバッグは有効になりません。デバッグの現在の状態を表示するには、**show debug** および **show webvpn debug-condition** コマンドを使用します。

ASA VPN で複数のセッションが実行されている場合、単一のユーザセッションをトラブルシューティングすることが煩わしくなります。条件付きデバッグを使用すると、フィルタ条件のセットに基づいて特定のセッションのログを検証できます。条件付きデバッグをサポートするモジュールは、SAML、WebVPN 要求および応答、Anyconnect です。



(注) IPv4 および IPv6 サブネットの「any, any」のサポートが提供されます。

次に、ユーザ `jdoe` で条件付きデバッグを有効にする例を示します。

```
asa3(config)# debug webvpn condition user jdoe

asa3(config)# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

asa3(config)# debug webvpn
INFO: debug webvpn enabled at level 1.

asa3(config)# show debug
```

```
debug webvpn enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

## 管理者によるクライアントレスSSLVPNユーザへのアラートの送信

### 手順

- ステップ1** メイン ASDM アプリケーション ウィンドウで、[Tools] > [Administrator's Alert Message to Clientless SSL VPN Users] を選択します。
- ステップ2** 送信する新規または編集済みのアラート内容を入力して、[Post Alert] をクリックします。
- ステップ3** 現在のアラート内容を削除して新しいアラート内容を入力するには、[Cancel Alert] をクリックします。

## クライアントレス SSL VPN セッションクッキーの保護

FlashアプリケーションやJavaアプレットなどの組み込みオブジェクト、および外部アプリケーションは、通常は既存のセッションのクッキーに依存してサーバと連携しています。これらの組み込みオブジェクトは、初期化時にいくつかの Javascript を使用してブラウザからクッキーを取得します。クライアントレス SSL VPN セッションクッキーに `httponly` フラグを追加すると、セッションクッキーがブラウザのみで認識され、クライアント側のスクリプトでは認識されなくなり、セッションの共有は不可能になります。

### 始める前に

- VPN セッションのクッキー設定は、アクティブなクライアントレス SSL VPN セッションがない場合にだけ変更してください。
- クライアントレス SSL VPN セッションのステータスを確認するには、`show vpn-sessiondb webvpn` コマンドを使用します。
- `vpn-sessiondb logoff webvpn` コマンドを使用して、すべてのクライアントレス SSL VPN セッションからログアウトします。
- 次のクライアントレス SSL VPN 機能は、`http-only-cookie` コマンドがイネーブルの場合に動作しません。
  - Java プラグイン

- Java リライタ
- ポートフォワーディング。
- ファイルブラウザ
- デスクトップアプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能
- AnyConnect Web 起動
- Citrix Receiver、XenDesktop、および Xenon
- その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション

クライアントレス SSL VPN セッション Cookie が JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにするには、次の手順を実行します。

#### 手順

---

**ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [HTTP Cookie] を選択します。

**ステップ 2** [Enable HTTP-only VPN cookies] チェックボックスをオンにします。

(注) この設定は、Cisco TAC から指示された場合にのみ使用してください。このコマンドをイネーブルにすると、「ガイドライン」に記載されているクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。

**ステップ 3** [Apply] をクリックして変更内容を保存します。

---

