



Cisco Firepower Threat Defense コンフィギュレーションガイド (Firepower Device Manager バージョン 6.2.3 用)

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: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). 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)

© 2015–2018 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

使用する前に 1

このガイドの対象読者	1
Firepower Device Manager/FTD 6.2 の新機能	2
Firepower Device Manager/FTD 6.2.1 の新機能	6
Firepower Device Manager/FTD 6.2.2 の新機能	7
Firepower Device Manager/FTD バージョン 6.2.3 の新機能	7
システムへのログイン	13
Firepower Device Manager へのログイン	14
CLI (コマンドライン インターフェイス) へのログイン	15
パスワードの変更	16
ユーザ プロファイルの設定	16
FTD CLI のローカルユーザ アカウントの作成	17
システムの設定	19
インターフェイスの接続	20
ASA 5506-X、5506W-X および 5506H-X の配線	20
ASA 5508-X および 5516-X の配線	22
ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の配線	22
Firepower 2100の配線	23
仮想ケーブル接続：Firepower Threat Defense Virtual	24
ISA 3000 のケーブル配線	26
初期設定の完了	27
外部インターフェイスの IP アドレスを取得できない場合の対処方法	29
ワイヤレス アクセス ポイント (ASA 5506W-X) の設定	31
初期設定前のデフォルト設定	34

初期セットアップ後の設定	37
設定の基本	40
デバイスの設定	40
セキュリティ ポリシーの設定	42
変更の展開	43
インスペクション エンジンを再起動する設定の変更	44
インターフェイスと管理ステータスの表示	45
システム タスク ステータスの表示	46
CLI コンソールを使用した設定の監視およびテスト	47

第 2 章

Firepower Threat Defense の使用例	51
Firepower Device Manager でデバイスを設定する方法	51
ネットワーク トラフィックを調べる方法	56
脅威をブロックする方法	65
マルウェアをブロックする方法	72
アクセプタブルユース ポリシー (URL フィルタリング) の実装方法	76
アプリケーションの使用を制御する方法	81
サブネットを追加する方法	85
その他の例	92

第 3 章

システムのライセンス	95
Firepower システムのスマート ライセンス	95
Cisco Smart Software Manager	95
ライセンス認証局との定期通信	96
スマート ライセンスのタイプ	96
期限切れまたは無効なオプション ライセンスの影響	98
スマート ライセンスの管理	99
デバイスの登録	100
オプション ライセンスの有効化と無効化	101
Cisco Smart Software Manager との同期	102
デバイスの登録解除	103

第 4 章

デバイスのモニタリング 105

- トラフィック統計情報を取得するためにロギングを有効にする 105
 - イベント タイプ 105
 - 設定可能な接続ロギング 107
 - 自動接続ロギング 107
 - 接続ロギングのためのヒント 107
 - 外部の Syslog サーバへのイベントの送信 108
- トラフィックのモニタリングおよびシステム ダッシュボード 109
- コマンドラインを使用したその他の統計情報のモニタリング 112
- イベントの表示 113
 - カスタム ビューの設定 114
 - イベントのフィルタリング 115
 - イベント フィールドの説明 117

第 5 章

オブジェクト 129

- オブジェクト タイプ 129
- オブジェクトの管理 132
 - ネットワーク オブジェクトとグループの設定 133
 - ポート オブジェクトとグループの設定 134
 - セキュリティ ゾーンの設定 136
 - アプリケーションフィルタ オブジェクトの設定 137
 - URL オブジェクトとグループの設定 139
 - 地理位置情報オブジェクトの設定 141
 - Syslog サーバの設定 142
 - AD アイデンティティ レルムの設定 143
 - ディレクトリ サーバ接続のトラブルシューティング 146
 - ユーザ数の制限 147
 - サポートされるディレクトリ サーバ 148
 - ディレクトリ ベースの DN の決定 148

第 6 章

証明書 151

- 証明書について 151
 - 公開キー暗号化 152
 - 各機能で使用される証明書タイプ 152
 - 例：OpenSSL を使用した内部証明書の生成 153
- 証明書の設定 154
 - 内部および内部 CA 証明書のアップロード 155
 - 自己署名内部および内部 CA 証明書の生成 157
 - 信頼できる CA 証明書のアップロード 158

第 1 部 :

基本 161

第 7 章

インターフェイス 163

- FTD インターフェイスについて 163
 - インターフェイス モード 164
 - 管理/診断インターフェイス 164
 - 個別の管理ネットワークの設定に関する推奨事項 165
 - 別の管理ネットワークのための管理/診断インターフェイス設定に関する制限事項 166
 - セキュリティ ゾーン 166
 - IPv6 アドレス指定 166
 - Auto-MDI/MDIX 機能 167
- インターフェイスに関する注意事項と制限事項 167
 - インターフェイス設定の制限事項 168
 - デバイス モデルによる VLAN サブインターフェイスの最大数 169
- 物理インターフェイスの設定 170
- ブリッジ グループの設定 174
- VLAN サブインターフェイスと 802.1Q トランキングの設定 179
- 高度なインターフェイス オプションの設定 183
 - MTU について 183
 - パス MTU ディスカバリ 183

MTU およびフラグメンテーション	183
MTU とジャンボ フレーム	183
詳細オプションの設定	184
Firepower Threat Defense Virtual へのインターフェイスの追加	186
モニタリング インターフェイス	188
インターフェイスの例	189

第 8 章

ルーティング 191

ルーティングの概要	191
ルートのタイプ	191
ルーティング テーブルとルート選択	192
ルーティング テーブルへの入力方法	192
転送の決定方法	195
管理トラフィック用ルーティングテーブル	196
等コスト マルチパス (ECMP) ルーティング	197
スタティック ルート	197
スタティック ルートとデフォルト ルートについて	197
デフォルト ルート	198
スタティック ルート	198
スタティック ルーティングのガイドライン	198
スタティック ルートの設定	199
ルーティングのモニタリング	200

第 11 部 :

セキュリティ ポリシー 203

第 9 章

SSL 復号 205

SSL 復号について	205
SSL 復号を実装する理由	206
暗号化されたトラフィックに適用できるアクション	206
再署名の復号	206
既知のキーの復号	207

復号禁止	208
ブロック	208
自動的に生成された SSL 復号ルール	208
復号できないトラフィックの処理	208
SSL 復号のためのライセンス要件	209
SSL 復号のガイドライン	209
SSL 復号ポリシーの実装および管理方法	210
SSL 復号ポリシーの設定	212
SSL 復号ポリシーの有効化	213
SSL 復号のデフォルトアクションの設定	214
SSL 復号ルールの設定	215
SSL 復号ルールの送信元/送信先基準	218
SSL 復号ルールのアプリケーション基準	220
SSL 復号ルールの URL 基準	221
SSL 復号ルールのユーザ基準	222
SSL 復号ルールの詳細条件	223
既知のキーと復号の再署名の証明書の設定	224
再署名の復号ルールの CA 証明書のダウンロード	225
例：ネットワークからの古い SSL/TLS バージョンのブロック	227
SSL 復号のモニタリングとトラブルシューティング	229
SSL 復号のモニタリング	229
復号再署名がブラウザでは機能するがアプリでは機能しない Web サイトの処理 (SSL または認証局ピンング)	229

第 10 章

アイデンティティ ポリシー	231
アイデンティティ ポリシーの概要	231
アクティブ認証によるユーザ ID の確立	231
不明なユーザの対処	232
アイデンティティ ポリシーの設定	232
アイデンティティ ポリシーの設定	233
アイデンティティ ルールの設定	235

トランスペアレント ユーザ認証の有効化	239
トランスペアレント認証の要件	240
トランスペアレント認証用の Internet Explorer の設定	241
トランスペアレント認証用の Firefox の設定	242
アイデンティティ ポリシーのモニタリング	243
アイデンティティ ポリシーの例	243

第 11 章

セキュリティ インテリジェンス	245
セキュリティ インテリジェンスについて	245
ブラックリストの例外の作成	246
セキュリティ インテリジェンス フィード カテゴリ	246
セキュリティ インテリジェンスのためのライセンス要件	247
セキュリティ インテリジェンスの設定	247
セキュリティ インテリジェンスのモニタリング	249
セキュリティ インテリジェンスの例	249

第 12 章

アクセス制御	251
アクセス コントロールの概要	251
アクセス コントロール ルールとデフォルト アクション	251
アプリケーションフィルタリング	252
暗号化および復号トラフィックのアプリケーション制御	252
アプリケーションフィルタリングのベスト プラクティス	253
URL フィルタリング	253
カテゴリ別とレピュテーション別の URL のフィルタリング	254
カテゴリとレピュテーションでの URL の検索	254
手動 URL フィルタリング	254
HTTPS トラフィックのフィルタリング	256
URL フィルタリングとアプリケーションフィルタリングの比較	257
効果的な URL フィルタリングのベスト プラクティス	257
Web サイトのブロック時にユーザに表示される内容	258
侵入、ファイル、マルウェアのインスペクション	259

アクセス制御ルールの順序のベスト プラクティス	260
NAT とアクセス ルール	260
その他のセキュリティ ポリシーがアクセス制御に影響する仕組み	260
アクセス制御のためのライセンス要件	261
アクセス コントロール ポリシーに関する注意事項と制限事項	261
アクセス コントロール ポリシーを設定する	263
デフォルト アクションの設定	263
アクセス コントロール ルールの設定	264
送信元/宛先基準	266
アプリケーション基準	268
URL 基準	270
ユーザ基準	271
侵入ポリシーの設定	272
ファイル ポリシーの設定	273
ロギングの設定	275
アクセス コントロール ポリシーのモニタリング	276
ダッシュボードでのアクセス制御統計情報のモニタリング	276
CLI でのアクセス コントロール ポリシーのモニタリング	277
アクセス制御の例	278
第 13 章	
侵入ポリシー	279
侵入ポリシーとネットワーク分析ポリシーについて	279
システム定義のネットワーク分析および侵入ポリシー	280
侵入ルールおよびプリプロセッサ ルール	281
侵入ルール属性	281
デフォルトの侵入変数セット	282
ジェネレータ識別子	283
ネットワーク分析ポリシー	285
システムによる NAP ルールを使用したネットワーク分析ポリシーの選択方法	285
NAP の処理を最適化する侵入のポリシーを適用するためのベスト プラクティス	287
侵入ポリシーのためのライセンス要件	287

侵入ポリシーの管理	288
アクセス制御ルールでの侵入ポリシーの適用	288
侵入ルールのアクションの変更	289
侵入イベントの Syslog の設定	290
侵入ポリシーのモニタリング	291
侵入ポリシーの例	291

第 14 章

ネットワーク アドレス変換 (NAT)	293
NAT を使用する理由	293
NAT の基本	294
NAT の用語	294
NAT タイプ	295
ルーテッドモードの NAT	295
自動 NAT および 手動 NAT	296
自動 NAT	296
手動 NAT	297
自動 NAT と 手動 NAT の比較	297
NAT ルールの順序	298
NAT インターフェイス	300
NAT のルーティング設定	301
マッピング インターフェイスと同じネットワーク上のアドレス	301
一意のネットワーク上のアドレス	301
実際のアドレスと同じアドレス (アイデンティティ NAT)	301
NAT のガイドライン	302
インターフェイスのガイドライン	302
IPv6 NAT のガイドライン	302
IPv6 NAT のベスト プラクティス	303
インスペクション対象プロトコルに対する NAT サポート	303
NAT のその他のガイドライン	305
NAT の設定	307
ダイナミック NAT	308

ダイナミック NAT について	308
ダイナミック NAT の欠点と利点	309
ダイナミック自動 NAT の設定	310
ダイナミック手動 NAT の設定	311
ダイナミック PAT	314
ダイナミック PAT について	314
ダイナミック PAT の欠点と利点	315
ダイナミック自動 PAT の設定	316
ダイナミック手動 PAT の設定	317
スタティック NAT	320
スタティック NAT について	320
スタティック自動 NAT の設定	324
スタティック手動 NAT の設定	327
アイデンティティ NAT	330
アイデンティティ自動 NAT の設定	331
アイデンティティ手動 NAT の設定	333
Firepower Threat Defense の NAT ルールプロパティ	336
自動 NAT のパケット変換プロパティ	336
手動 NAT のパケット変換プロパティ	338
詳細 NAT プロパティ	340
IPv6 ネットワークの変換	341
NAT64/46 : IPv6 アドレスの IPv4 への変換	341
NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット	342
NAT64/46 の例 : 外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク	344
NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換	349
NAT66 の例 : ネットワーク間のスタティック変換	350
NAT66 の例 : シンプルな IPv6 インターフェイス PAT	352
NAT のモニタリング	356
NAT の例	356
内部 Web サーバへのアクセスの提供 (スタティック自動 NAT)	356

FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック自動 NAT）	359
宛先に応じて異なる変換（ダイナミック手動 PAT）	366
宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）	371
NAT を使用した DNS クエリと応答の書き換え	377
DNS 64 応答修正	378
DNS 応答修正：外部の DNS サーバ	384
DNS 応答修正：ホスト ネットワーク上の DNS サーバ	388

第 III 部：	バーチャル プライベート ネットワーク（VPN）	391
----------	--------------------------	-----

第 15 章	サイト間 VPN	393
	VPN の基本	393
	インターネット キー エクスチェンジ（IKE）	394
	VPN 接続の安全性を確保する方法	395
	使用する暗号化アルゴリズムの決定	395
	使用するハッシュ アルゴリズムの決定	396
	使用する Diffie-Hellman 係数グループの決定	397
	VPN トポロジ	398
	サイト間 VPN の管理	398
	サイト間 VPN 接続の設定	399
	グローバル IKE ポリシーの設定	403
	IKEv1 ポリシーの設定	404
	IKEv2 ポリシーの設定	406
	IPsec プロポーザルの設定	408
	IKEv1 の IPsec プロポーザルの設定	409
	IKEv2 の IPsec プロポーザルの設定	410
	サイト間 VPN 接続の確認	411
	サイト間 VPN のモニタリング	414
	サイト間 VPN の例	415
	NAT からのサイト間 VPN トラフィックの除外	415

外部インターフェイスで外部のサイト間 VPN ユーザにインターネット アクセスを提供する
方法 (ヘア ピニング) 422

第 16 章**リモート アクセス VPN 429**

リモート アクセス VPN の概要 429

デバイス モデル別の同時 VPN セッションの最大数 429

AnyConnect クライアント ソフトウェアのダウンロード 430

AnyConnect ソフトウェアのインストール方法 431

リモート アクセス VPN のライセンス要件 432

リモート アクセス VPN に関する注意事項と制限事項 432

リモート アクセス VPN の設定 432

クライアント プロファイルの設定およびアップロード 434

リモート アクセス VPN 接続の設定 435

リモート アクセス VPN グループによるリソースへのアクセスを制御する 439

リモート アクセス VPN 設定の確認 441

リモート アクセス VPN のモニタリング 443

リモート アクセス VPN のトラブルシューティング 443

SSL 接続問題のトラブルシューティング 444

AnyConnect のダウンロードおよびインストールの問題のトラブルシューティング 444

AnyConnect 接続問題のトラブルシューティング 445

RA VPN トラフィック フローの問題のトラブルシューティング 445

リモート アクセス VPN の例 446

外部インターフェイスでリモート アクセス VPN ユーザにインターネット アクセスを提供
する方法 (ヘアピニング) 446

リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバを使用する方
法 453

第 IV 部 :**システム管理 473**

第 17 章**システム設定 475**

管理アクセス リストの設定 475

診断ロギングの設定 477

重大度	478
DHCP サーバの設定	479
DNS の設定	481
管理インターフェイスの設定	482
デバイスのホスト名の設定	484
Network Time Protocol (NTP) の設定	484
URL フィルタリングの設定	485
クラウドサービスの設定	486
クラウド管理の設定 (Cisco Defense Orchestrator)	486
Cisco Success Network への接続	487

第 18 章

システム管理	489
ソフトウェアアップデートのインストール	489
システム データベースおよびフィードの更新	489
システム データベースおよびフィードの更新の概要	489
システム データベースの更新	491
Cisco Security Intelligence フィードの更新	492
Firepower Threat Defense ソフトウェアのアップグレード	493
デバイスの再イメージ化	495
システムのバックアップと復元	496
システムの即時バックアップ	496
スケジュールされた時間でのシステムのバックアップ	497
定期的なバックアップ スケジュールの設定	498
バックアップの復元	499
バックアップ ファイルの管理	500
システムの再起動	501
システムのトラブルシューティング	501
接続をテストするための ping アドレス	501
ホストまでのルートの追跡	503
Firepower Threat Defense デバイスのトレースルートへの表示	505
NTP のトラブルシューティング	507

管理インターフェイスの DNS のトラブルシューティング	508
CPU およびメモリ使用率の分析	512
ログの表示	512
トラブルシューティング ファイルの作成	514
一般的でない管理タスク	515
ローカル管理とリモート管理の切り替え	515
ファイアウォール モードの変更	518
設定のリセット	521
<hr/>	
付録 A :	詳細設定 523
Smart CLI と FlexConfig について	523
Smart CLI と FlexConfig の推奨される使用法	524
Smart CLI および FlexConfig オブジェクトの CLI コマンド	525
ASA ソフトウェアのバージョンおよび現在の CLI 設定の特定	525
禁止された CLI コマンド	525
Smart CLI テンプレート	531
Smart CLI および FlexConfig に関する注意事項と制限事項	532
Smart CLI オブジェクトの設定	532
FlexConfig ポリシーの設定	534
FlexConfig オブジェクトの設定	536
FlexConfig オブジェクトの変数の作成	538
FlexConfig 変数の参照と値の取得	540
変数参照 : {{variable}}	540
セクション {{#key}} {{/key}} と逆セクション {{^key}} {{/key}}	543
秘密キー オブジェクトの設定	545
FlexConfig ポリシーのトラブルシューティング	546
FlexConfig の例	547
グローバル デフォルト インспекションを有効/無効にする方法	547
FlexConfig の変更を元に戻す方法	553
一意のトラフィック クラスのインспекションを有効にする方法	555



第 1 章

使用する前に

ここでは、Firepower Threat Defense の設定を開始する方法について説明します。

- [このガイドの対象読者](#) (1 ページ)
- [Firepower Device Manager/FTD 6.2 の新機能](#) (2 ページ)
- [システムへのログイン](#) (13 ページ)
- [システムの設定](#) (19 ページ)
- [設定の基本](#) (40 ページ)

このガイドの対象読者

このガイドでは、Firepower Threat Defense デバイスに含まれている Firepower Device Manager の Web ベースのインターフェイスを使用して Firepower Threat Defense を設定する方法について説明します。

Firepower Device Manager を使うことで、小～中規模なネットワークで最も一般的に使用されるソフトウェアの基本機能の設定が行えます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合、統合 Firepower Device Manager の代わりに Firepower Management Center デバイスを使用します。

Firepower Device Manager は次のデバイスで使用できます。

表 1: Firepower Device Manager がサポートされるモデル

デバイス モデル	Firepower Threat Defense の最小ソフトウェア バージョン
Firepower 2110、2120、2130、2140	6.2.1
Firepower Threat Defense Virtual VMware 用	6.2.2

デバイス モデル	Firepower Threat Defense の最小ソフトウェアバージョン
Firepower Threat Defense Virtual カーネルベース仮想マシン (KVM) ハイパーバイザ用	6.2.3
ASA 5508-X、5516-X	6.1
ASA 5525-X、5545-X、5555-X	6.1
ASA 5506-X、5506H-X、5506W-X、5512-X	6.1
ASA 5515-X	6.1
ISA 3000 (Cisco 3000 シリーズ産業用セキュリティ アプライアンス)	6.2.3

Firepower Device Manager/FTD 6.2 の新機能

リリース : 2017 年 1 月 23 日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2 で使用できる新機能を示します。

機能	説明
Cisco Defense Orchestrator のクラウド管理	Cisco Defense Orchestrator のクラウドベースのポータルを使用してデバイスを管理できます。[デバイス (Device)] > [システム設定 (System Settings)] > [クラウド管理 (Cloud Management)] を選択します。Cisco Defense Orchestrator の詳細については、 http://www.cisco.com/go/cdo を参照してください。
アクセスルールのドラッグアンドドロップ	ルールテーブルで、アクセスルールをドラッグアンドドロップして移動できます。
FTD ソフトウェア アップグレード	Firepower Device Manager 経由でソフトウェア アップグレードをインストールできます。[デバイス (Device)] > [更新 (Updates)] を選択します。

機能	説明
<p>FTD のデフォルト設定の変更</p>	<p>新しいデバイスまたは再イメージ化されたデバイスでは、デフォルト設定に次の重要な変更が含まれます。</p> <ul style="list-style-type: none"> • (ASA 5506-X、5506W-X、5506H-X) 最初のデータ インターフェイスと ASA 5506W-X の Wi-Fi インターフェイスを除き、これらのデバイス モデルのその他すべてのデータ インターフェイスは、「内部」ブリッジグループに構造化され、有効化されます。DHCP サーバは内部のブリッジグループにあります。ブリッジド インターフェイスに エンドポイントまたはスイッチを接続することができ、エンドポイントは 192.168.1.0/24 ネットワーク上のアドレスを取得します。 • 内部 インターフェイス IP アドレスは 192.168.1.1 です。DHCP サーバは、アドレス プールの 192.168.1.5 ~ 192.168.1.254 の インターフェイスで定義されます。 • HTTPS アクセスは内部 インターフェイスで有効なため、デフォルト アドレス (192.168.1.1) で内部 インターフェイスを介して Firepower Device Manager を開くことができます。ASA 5506-X モデルでは、内部ブリッジグループ メンバー インターフェイス経由でこれを実行できます。 • 管理ポートは、192.168.45.0/24 ネットワークの DHCP サーバをホストします。ワークステーションを管理ポートに直接接続して、IP アドレスを取得し、Firepower Device Manager を開いてデバイスを設定できます。 • OpenDNS のパブリック DNS サーバは、現在、管理 インターフェイスのデフォルト DNS サーバです。以前は、デフォルト DNS サーバはありませんでした。デバイスの設定時に、別の DNS サーバを設定できます。 • 管理 IP アドレスのデフォルト ゲートウェイでは、データ インターフェイスを使用してインターネットにルーティングします。したがって、Management 物理 インターフェイスをネットワークに配線する必要はありません。

機能	説明
管理インターフェイスおよびアクセスの変更	<p>管理アドレス機能および Firepower Device Manager へのアクセス方法に対するいくつかの変更：</p> <ul style="list-style-type: none"> • HTTPS (Firepower Device Manager 用) および SSH (CLI 用) 接続に対するデータ インターフェイスを開くことができます。デバイスを管理するために、別の管理ネットワークを必要としたり、管理/診断物理ポートを内部ネットワークに接続したりする必要はありません。[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス リスト (Management Access List)] を選択します。 • システムは、外部インターフェイスのゲートウェイ経由でシステムデータベースのアップデートを取得できます。管理インターフェイスまたはネットワークからインターネットへの明示的なルートは必要ありません。デフォルトでは、データ インターフェイスを介して内部ルートを使用します。ただし、別の管理ネットワークを使用する場合、特定のゲートウェイを設定できます。[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択します。 • Firepower Device Manager を使用して、DHCP を介して IP アドレスを取得するように管理インターフェイスを設定できます。[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択します。 • スタティック アドレスを設定する場合、管理アドレスで DHCP サーバを設定できます。[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択します。

機能	説明
<p>さまざまなユーザ インターフェイスの変更</p>	<p>次に、Firepower Device Manager ユーザ インターフェイスの注目すべき変更を示します。</p> <ul style="list-style-type: none"> • [デバイス (Device)]メインメニュー項目。以前のリリースでは、このメニュー項目はデバイスのホスト名でした。また、開くページは、[デバイスダッシュボード (Device Dashboard)]ではなく [デバイスサマリー (Device Summary)]と呼ばれます。 • デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。 • [デバイス (Device)]> [システム設定 (System Settings)]> [クラウド設定 (Cloud Preferences)]は、[デバイス (Device)]> [システム設定 (System Settings)]> [URLフィルタリング設定 (URL Filtering Preferences)]と呼ばれます。 • [システム設定 (System Settings)]> [DHCP サーバ (DHCP Server)] ページは 2 つのタブで構成され、グローバルパラメータとは異なる DHCP サーバテーブルが表示されます。
<p>サイト間 VPN 接続</p>	<p>事前共有キーを使用して、サイト間のバーチャルプライベート ネットワーク (VPN) 接続を設定できます。IKEv1 および IKEv2 接続を設定できます。</p>

機能	説明
統合ルーティングおよびブリッジングのサポート	<p>統合ルーティングおよびブリッジングによって、ブリッジグループとルーテッドインターフェイスの間でルーティングする機能が提供されます。ブリッジグループは、FTD デバイスがルーティングではなくブリッジするインターフェイスのグループです。FTD デバイスは、FTD デバイスがファイアウォールとして継続的に機能する本当のブリッジではありません。インターフェイス間のアクセス コントロールは管理され、すべての通常のファイアウォールチェックが実行されます。</p> <p>この機能によって、ブリッジグループを設定したり、ブリッジグループ間およびブリッジグループとルーテッドインターフェイスの間でルーティングするようにブリッジグループを設定したりできます。ブリッジグループは、ブリッジ仮想インターフェイス (BVI) を使用して、ブリッジグループのゲートウェイとして機能することによってルーティングに参加します。FTD デバイスにブリッジグループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ 2 スイッチを使用するのではない別の方法が提供されます。BVI は、名前付きインターフェイスにすることができ、メンバー インターフェイスとは別にいくつかの機能 (DHCP サーバなど) に参加できます。ここで、ブリッジグループ メンバー インターフェイスで他の機能 (NAT、アクセスコントロールルールなど) を設定します。</p> <p>[デバイス (Device)] > [インターフェイス (Interfaces)] を選択して、ブリッジグループを設定します。</p>

Firepower Device Manager/FTD 6.2.1 の新機能

リリース日 : 2017 年 5 月 15 日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.1 で使用できる新機能を示します。



(注) このリリースは、Firepower 2100 シリーズ のみに適用されます。

機能	説明
リモートアクセスVPNの設定	AnyConnect クライアントのリモートアクセス SSL VPN を設定できます。[デバイス (Device)] > [リモート アクセス VPN (Remote Access VPN)] グループから RA VPN を設定します。[デバイス (Device)] > [スマート ライセンス (Smart License)] グループから RA VPN ライセンスを設定します。
Firepower 2100 シリーズ デバイス設定	Firepower Device Manager を使用して、Firepower 2100 シリーズ デバイスで FTD を設定できます。

Firepower Device Manager/FTD 6.2.2 の新機能

リリース：2017年9月5日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.2 で使用できる新機能を示します。

機能	説明
ASA 5500-X シリーズ デバイスのリモートアクセスVPNの設定	ASA 5500-X シリーズ デバイスでは、AnyConnect クライアント用にリモートアクセス SSL VPN を設定できます。[デバイス (Device)] > [リモート アクセス VPN (Remote Access VPN)] グループから RA VPN を設定します。[デバイス (Device)] > [スマート ライセンス (Smart License)] グループから RA VPN ライセンスを設定します。
Firepower Threat Defense Virtual for VMware デバイス設定。	Firepower Device Manager を使用して Firepower Threat Defense Virtual for VMware デバイス上の FTD を設定できます。その他の仮想プラットフォームは、Firepower Device Manager ではサポートされません。 (注) Firepower Device Manager でサポートされるようにするには、新しい 6.2.2 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Firepower Device Manager に切り替えることはできません。

Firepower Device Manager/FTD バージョン 6.2.3 の新機能

リリース：2018年3月29日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.3 で使用できる新機能を示します。

機能	説明
SSL/TLS の復号	<p>接続の内容を調べることができるように、SSL/TLS 接続を復号できます。復号しないと、暗号化された接続は、侵入およびマルウェアの脅威を識別したり、URL およびアプリケーション使用状況ポリシーへの準拠を強制したりするための効果的な検査が行えません。[Policies] > [SSL Decryption] ページおよび [Monitoring] > [SSL Decryption] ダッシュボードが追加されました。</p> <p>注目 アクティブな認証を実装するアイデンティティポリシーは、SSL 復号ルールを自動的に生成します。SSL 復号をサポートしていないリリースからアップグレードする場合、SSL 復号ポリシーは、この種類のルールがある場合、自動的に有効になります。ただし、アップグレードの完了後、再署名の復号ルールで使用する証明書を指定する必要があります。アップグレード後すぐに SSL 復号設定を編集してください。</p>
セキュリティ インテリジェンスのブラックリスト登録	<p>新しい [ポリシー (Policies)] > [セキュリティインテリジェンス (Security Intelligence)] ページから設定できるセキュリティインテリジェンスポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセスコントロールポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティインテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。</p> <p>また、[ポリシー (Policies)] ダッシュボードの名前を [アクセスおよびSIルール (Access And SI Rules)] に変更し、セキュリティインテリジェンス同等のルールがアクセスルールとともにダッシュボードに含まれるようになりました。</p>
侵入ルールの調整	<p>アクセス制御ルールを適用する事前に定義された侵入ポリシー内の侵入ルールのアクションを変更できます。トラフィックに一致するイベント（警告）をドロップまたは生成する各ルールを設定したり、ルールを無効にしたりできます。有効になっているルールのアクション（ドロップまたは警告に設定）のみ変更できます。デフォルトで無効になっているルールを有効にはできません。侵入ルールを調整するには、[ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。</p>

機能	説明
<p>侵入ポリシーに基づく自動ネットワーク分析ポリシー (NAP) 割り当て</p>	<p>以前のリリースでは、[Balanced Security and Connectivity] ネットワーク分析ポリシーが、特定の送信元/送信先のセキュリティゾーンとネットワークオブジェクトの組み合わせに割り当てられた侵入ポリシーに関係なく、プリプロセッサ設定で常に使用されました。システムは自動的に NAP ルールを生成し、同じ名前の NAP と侵入ポリシーをそれらの基準に基づいてトラフィックに割り当てるようになりました。レイヤ 4 または 7 の基準を使用して異なる侵入ポリシーをトラフィック（それ以外は同じ送信元/送信先のセキュリティゾーンおよびネットワークオブジェクトと一致する）に割り当てる場合、完全に一致する NAP および侵入ポリシーは取得されないことに注意してください。カスタムネットワーク分析ポリシーは作成できません。</p>
<p>脅威、攻撃、およびターゲットのダッシュボード用のドリルダウンレポート</p>	<p>脅威、攻撃、およびターゲットのダッシュボードに移動して、報告された項目についての詳細を表示できるようになりました。これらのダッシュボードは [Monitoring] ページで使用できます。</p> <p>これらの新しいレポートのため、6.2.3 より前のリリースからアップグレードする場合は、これらのダッシュボードのレポートデータが失われます。</p>
<p>[Web Applications] ダッシュボード</p>	<p>新しい [Web Applications] ダッシュボードは、Google など、ネットワークで使用されている上位の Web アプリケーションを示します。このダッシュボードはアプリケーションのダッシュボードを強化し、HTTP の使用率などのプロトコル指向の情報を提供します。</p>
<p>新しいゾーンのダッシュボードが入力ゾーンと出力ゾーンのダッシュボードを置き換え</p>	<p>新しいゾーンのダッシュボードは、デバイスに入ってから出るトラフィックに対する上位セキュリティゾーンのペアを示します。このダッシュボードは、入力および出力ゾーンに対する個別のダッシュボードを置き換えます。</p>
<p>新しいマルウェア ダッシュボード</p>	<p>新しいマルウェア ダッシュボードは、上位のマルウェアのアクションと判定結果の組み合わせを示します。ドリルダウンして、関連付けられているファイルタイプの情報を参照できます。この情報を表示するには、アクセスルールにファイルポリシーを設定する必要があります。</p>
<p>自己署名入りの内部証明書、および内部 CA 証明書</p>	<p>自己署名入りの内部アイデンティティ証明書を生成できるようになりました。また、SSL 復号ポリシーで使用するための、自己署名付きの内部 CA 証明書を生成し、アップロードできるようになりました。これらの機能を、[Objects] > [Certificates] ページで設定します。</p>

機能	説明
インターフェイスのプロパティ編集時に DHCP サーバの設定を編集する機能	インターフェイスのプロパティを編集すると同時に、インターフェイスに設定されている DHCP サーバの設定を編集できるようになりました。これにより、インターフェイスの IP アドレスを別のサブネットに変更する必要がある場合に、DHCP アドレスプールを簡単に再定義できます。
製品を改善し、効果的な技術サポートを提供するための、Cisco Success Network によるシスコへの利用状況や統計データの送信	<p>Cisco Success Network に接続し、シスコにデータを送信できます。Cisco Success Network を有効にすることで、テクニカルサポートを提供するために不可欠な、使用状況の情報と統計情報をシスコに提供します。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。Cisco Smart Software Manager でデバイスを登録するとき、または後から好きなきときに、接続を有効にできます。接続はいつでも無効にできます。</p> <p>Cisco Success Network はクラウドサービスです。[Device] > [System Settings] > [Cloud Management] ページの名前が [Cloud Services] に変更されました。同じページから、Cisco Defense Orchestrator を設定できます。</p>
Firepower Threat Defense Virtual for Kernel-based Virtual Machine (KVM) ハイパーバイザデバイス設定	<p>Firepower Device Manager を使用して Firepower Threat Defense Virtual for KVM デバイス上の FTD を設定できます。以前は、VMware のみがサポートされていました。</p> <p>(注) Firepower Device Manager のサポートを得るには、新しい 6.2.3 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Firepower Device Manager に切り替えることはできません。</p>
ISA 3000 (Cisco 3000 シリーズ産業用セキュリティアプライアンス) デバイスの設定	Firepower Device Manager を使用して ISA 3000 デバイス上の FTD を設定できます。ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。

機能	説明
<p>ルール データベースまたは VDB の更新でのオプションの展開</p>	<p>侵入ルール データベースまたは VDB を更新する、または更新スケジュールを設定する際に、更新が即時展開しないようにすることができます。更新プログラムは検査エンジンを再起動するため、展開時に瞬間的なトラフィックのドロップが発生します。自動的に展開しないことにより、トラフィックのドロップの影響が最小になる場合に展開を開始できます。</p> <p>(注) VDB ダウンロードは、単独で Snort を再起動することもできますが、展開時に再起動が発生します。ダウンロード時の再起動を止めることはできません。</p>
<p>展開が Snort を再起動するかどうかを示す、改善されたメッセージ。さらに、展開時の Snort を再起動する必要性の低下</p>	<p>展開を開始する前に、Firepower Device Manager により、設定の更新で Snort の再起動が必要かどうかを示されます。Snort の再起動は、トラフィックの瞬間的なドロップを発生させます。したがって、展開がトラフィックに影響を与えず、すぐに実行できるかどうか分かるようになったため、混乱が少ないときに展開できます。</p> <p>さらに、以前のリリースでは展開の実行の度に Snort が再起動されていました。Snort は、次の理由でのみ再起動されるようになりました。</p> <ul style="list-style-type: none"> • ユーザが SSL 復号ポリシーを有効または無効にする • 更新されたルール データベースまたは VDB がダウンロードされた • ユーザが 1 つまたは複数の物理インターフェイス（ただしサブインターフェイスではない）で MTU を変更した
<p>Firepower Device Manager の CLI コンソール</p>	<p>Firepower Device Manager から CLI コンソールを開くことができるようになりました。CLI コンソールは SSH またはコンソールセッションを模倣していますが、コマンドのサブセットのみ (show、ping、traceroute、および packet-tracer) を許可します。トラブルシューティングとデバイスのモニタリングに CLI コンソールを使用します。</p>

機能	説明
管理アドレスへのアクセスのブロックのサポート	<p>プロトコルが管理 IP アドレスにアクセスできないようにするために、すべての管理アクセスリストのエントリを削除できるようになりました。以前は、すべてのエントリを削除すると、すべてのクライアント IP アドレスからのアクセスを許可するようにシステムのデフォルトが設定されていました。6.2.3 へのアップグレードでは、以前からのプロトコル (HTTPS または SSH) 用の空の管理アクセスリストがあった場合、システムはすべての IP アドレス用のデフォルトの許可ルールを作成します。必要に応じて、これらのルールを削除できます。</p> <p>また、SSH または HTTPS アクセスを無効にする場合を含み、Firepower Device Manager は CLI から管理アクセスリストに加えられた変更を認識します。</p> <p>少なくとも 1 つのインターフェイスに対する HTTPS アクセスを有効にしてください。そうしないとデバイスを設定および管理することができません。</p>

機能	説明
デバイス CLI を使用した、機能の設定のための Smart CLI および FlexConfig	<p>Smart CLI と FlexConfig により、まだ Firepower Device Manager ポリシーおよび設定では直接サポートされていない機能を設定できます。Firepower Threat Defense は、ASA 設定コマンドを使用していくつかの機能を実装します。ASA 設定コマンドの知識があり、専門家ユーザの場合、次の方法を使用して、デバイスでこれらの機能を設定できます。</p> <ul style="list-style-type: none"> • Smart CLI : (推奨される方法です。) Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。このリリースでは、Smart CLI を使用して、OSPFv2 を設定できます。 • FlexConfig : FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI 変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。 <p>注意 Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。ブラックリストに登録されていない任意のコマンドも設定できます。Smart CLI または FlexConfig を介して機能を有効にすると、その他の設定済みの機能に予期しない結果が発生する可能性があります。</p>
Firepower Threat Defense REST API、および API Explorer	<p>REST API を使用して、Firepower Device Manager を介してローカルで管理している Firepower Threat Defense デバイスをプログラムで操作できます。オブジェクトモデルを表示し、クライアントプログラムから作成できるさまざまな呼び出しのテストに使用できる API エクスプローラがあります。API エクスプローラを開くには、Firepower Device Manager にログインし、URL のパスを <code>/#/api-explorer</code> (https://ftd.example.com/#/api-explorer など) に変更します。</p>

システムへのログイン

Firepower Threat Defense デバイスには、次の 2 つのインターフェイスがあります。

Firepower Device Manager Web インターフェイス

Firepower Device Manager はお使いの Web ブラウザで実行されます。このインターフェイスを使用して、システムを設定、管理、モニタできます。

コマンドライン インターフェイス (CLI、コンソール)

CLIはトラブルシューティングに使用します。Firepower Device Manager の代わりに、初期設定にも使用できます。

次に、これらのインターフェイスにログインし、ユーザアカウントを管理する方法を説明します。

Firepower Device Manager へのログイン

Firepower Device Manager を使用して、システムを設定、管理、およびモニタします。ブラウザで設定可能な機能を、コマンドラインインターフェイス (CLI) で設定することはできません。セキュリティ ポリシーを実装するには、Web インターフェイスを使用する必要があります。

Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。



(注) 誤ったパスワードを入力し、3 回連続してログインに失敗した場合、アカウントは 5 分間ロックされます。再度ログインを試みる前に待つ必要があります。

始める前に

Firepower Device Manager には、**admin** ユーザ名のみを使用してログインできます。Firepower Device Manager アクセスするための追加ユーザは作成できません。

手順

ステップ 1 ブラウザを使用して、システムのホームページ (<https://ftd.example.com> など) を開きます。

次のいずれかのアドレス使用できます。設定済みのものであれば、IPv4 アドレス、IPv6 アドレス、または DNS 名を使用できます。

- 管理アドレス。デフォルトでは、これは管理/診断インターフェイスの 192.168.45.45 です。
- HTTPS アクセス用に開いたデータ インターフェイスのアドレス。デフォルト (ほとんどのハードウェアプラットフォーム) では、「内部」インターフェイスで HTTPS アクセスが許可されているため、デフォルトの内部アドレス 192.168.1.1 に接続できます。内部インターフェイスがブリッジグループであるデバイス モデルでは、任意のブリッジグループメンバー インターフェイスを介してこのアドレスに接続できます。

ヒント ブラウザがサーバ証明書を認識するように設定されていない場合、信頼できない証明書に関する警告が表示されます。証明書を例外として受け入れるか、または信頼できるルート証明書ストアの証明書を受け入れます。

ステップ 2 **admin** のユーザ名とパスワードを入力して、[ログイン (Login)] をクリックします。

デフォルトの **admin** パスワードは **Admin123** です。

セッションは非アクティブの状態が 30 分間続くと期限切れになり、再度ログインするように求められます。ページの右上にある [ユーザ (user)] アイコンのドロップダウンリストから [ログアウト (Log Out)] を選択するとログアウトできます。



CLI (コマンドライン インターフェイス) へのログイン

コマンドライン インターフェイス (CLI) を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。

CLI にログインするには、次のいずれかを実行します。

- デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナルエミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。



(注) Firepower 2100 デバイスでは、コンソールポートの CLI は FXOS です。connect ftd コマンドを使用して FTD CLI にアクセスできます。FXOS CLI はシャード レベルのトラブルシューティングのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには FTD CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

- Firepower Threat Defense Virtual の場合は、仮想コンソールを開きます。
- SSH クライアントを使用して、管理 IP アドレスに接続します。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます ([管理アクセス リストの設定 \(475 ページ\)](#) を参照)。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。admin ユーザ名 (デフォルトのパスワードは Admin123 です) または別の CLI ユーザ アカウントを使用してログインします。

ヒント

- ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法の情報については、『Cisco Firepower Threat Defense コマンドリファレンス』（http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）を参照してください。
- **configure user add** コマンドを使用して、CLI にログインできるローカルユーザアカウントを作成できます。ただし、これらのユーザは CLI のみにログインできます。Firepower Device Manager の Web インターフェイスにはログインできません。

パスワードの変更

パスワードは定期的に変更する必要があります。次の手順では、Firepower Device Manager にログインしているときにパスワードを変更する方法について説明します。



- (注) CLI にログインしている場合は、**configure password** コマンドを使用してパスワードを変更できます。別の CLI ユーザのパスワードを変更するには、**configure user password username** コマンドを使用します。

手順

- ステップ 1** メニューの右上にある [ユーザ (user)] アイコンのドロップダウンリストから、[プロファイル (Profile)] を選択します。



- ステップ 2** [パスワード (Password)] タブをクリックします。
ステップ 3 現在のパスワードを入力します。
ステップ 4 新しいパスワードを入力して確認します。
ステップ 5 [変更 (Change)] をクリックします。

ユーザ プロファイルの設定

ユーザ インターフェイスの設定を行い、パスワードを変更できます。

手順

ステップ 1 メニューの右上にある [ユーザ (user)] アイコンのドロップダウンリストから、[プロファイル (Profile)] を選択します。



ステップ 2 [プロファイル (Profile)] タブで次の設定を行い、[保存 (Save)] をクリックします。

- [スケジュールするタスクのタイムゾーン (Time Zone for Scheduling Tasks)] : バックアップや更新などのタスクのスケジュールに使用するタイムゾーンを選択します。別のゾーンを設定すると、ブラウザのタイムゾーンはダッシュボードやイベントに使用されます。
- [カラー テーマ (Color Theme)] : ユーザ インターフェイスで使用するカラー テーマを選択します。

ステップ 3 [パスワード (Password)] タブで新しいパスワードを入力し、[変更 (Change)] をクリックします。

FTD CLI のローカル ユーザ アカウントの作成

FTD デバイスで CLI にアクセスするユーザを作成できます。これらのアカウントは管理アプリケーションへのアクセスは許可されず、CLI へのアクセスのみが有効になります。CLI はトラブルシューティングやモニタリング用に役立ちます。

複数のデバイス上にローカルユーザアカウントを一度に作成することはできません。デバイスごとに固有のローカルユーザ CLI アカウントのセットがあります。

手順

ステップ 1 config 権限を持つアカウントを使用してデバイスの CLI にログインします。

管理者ユーザアカウントには必要な権限がありますが、config 権限を持っていただどのアカウントでも問題ありません。SSH セッションまたはコンソール ポートを使用できます。

特定のデバイス モデルでは、コンソール ポートから FXOS CLI に移動します。connect ftd を使用して FTD の CLI にアクセスします。

ステップ 2 ユーザ アカウントを作成します。

```
configure user add username {basic | config}
```

次の権限レベルを持つユーザを定義できます。

- **config** : ユーザに設定アクセス権を付与します。すべてのコマンドの管理者権限がユーザに与えられます。

- **basic** : ユーザに基本的なアクセス権を付与します。ユーザはコンフィギュレーション コマンドを入力することはできません。

例 :

次の例では、**config** アクセス権を使用して、**joecool** という名前のユーザアカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login          UID   Auth Access  Enabled Reset   Exp Warn  Str Lock Max
admin          1000 Local Config Enabled No   Never N/A  Dis  No N/A
joecool        1001 Local Config Enabled No   Never N/A  Dis  No  5
```

- (注) 自分のパスワードを **configure password** コマンドを使用して変更できることをユーザに伝えます。

ステップ 3 (オプション) セキュリティ要件を満たすようにアカウントの性質を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging** *username max_days warn_days*

ユーザパスワードの有効期限を設定します。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も 1~9999 ですが、警告までの日数は最大日数以内にする必要があります。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** *username*

次回ログイン時にユーザにパスワードを強制的に変更するよう要求します。

- **configure user maxfailedlogins** *username number*

アカウントがロックされる前の連続したログイン失敗の最大回数を 1~9999 までで設定します。**configure user unlock** コマンドを使用してアカウントのロックを解除します。新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

- **configure user minpasswlen** *username number*

パスワードの最小長を 1~127 までで設定します。

- **configure user strengthcheck** *username {enable | disable}*

パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

ステップ 4 必要に応じてユーザアカウントを管理します。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりしなければならない可能性があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

- **configure user access** *username* {**basic** | **config**}

ユーザアカウントの権限を変更します。

- **configure user delete** *username*

指定したアカウントを削除します。

- **configure user disable** *username*

指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。

- **configure user enable** *username*

指定したアカウントを有効にします。

- **configure user password** *username*

指定したユーザのパスワードを変更します。ユーザは通常、**configure password** コマンドを使用して自分のパスワードを変更する必要があります。

- **configure user unlock** *username*

ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザアカウントをロック解除します。

システムの設定

ネットワークでシステムが正しく機能するためには、初期設定を完了する必要があります。展開を成功させるには、ケーブルを正しく接続し、デバイスをネットワークに挿入し、インターネットや他のアップストリームルータに接続するために必要なアドレスを設定する必要があります。次の手順で、このプロセスについて説明します。

始める前に

初期設定を開始する前に、デバイスにはいくつかのデフォルト設定が含まれています。詳細は、[初期設定前のデフォルト設定 \(34 ページ\)](#) を参照してください。

手順

ステップ 1 [インターフェイスの接続 \(20 ページ\)](#)

ステップ 2 [初期設定の完了 \(27 ページ\)](#)

設定の結果の詳細については、[初期セットアップ後の設定 \(37ページ\)](#) を参照してください。

ステップ3 ワイヤレスアクセスポイント (ASA 5506W-X) の設定 (31ページ)

インターフェイスの接続

デフォルト設定では、特定のインターフェイスが内部および外部ネットワークに使用されると仮定しています。これらの前提に基づいてネットワークケーブルをインターフェイスに接続すると、初期設定の実行が容易になります。

ハードウェアモデルのデフォルト設定は、内部インターフェイスにワークステーションを直接接続できるように設計されています。内部インターフェイスがブリッジグループであるデバイスモデルでは、すべてのメンバーインターフェイスに接続できます。あるいは、管理ポートに直接ワークステーションを接続することもできます。正しいネットワークでアドレスを取得するには、DHCPを使用します。インターフェイスはさまざまなネットワーク上にあるため、内部インターフェイスと管理ポートを同じネットワークに接続しようとしないでください。

内部インターフェイスまたは管理インターフェイスを、アクティブなDHCPサーバがあるネットワークに接続しないでください。接続すると、内部ポートおよび管理ポートに対して実行されている既存のDHCPサーバとの競合が生じます。ネットワークに別のDHCPサーバを使用する必要がある場合、ワークステーションを直接管理ポートに接続し、初期設定を完了してから、不要なDHCPサーバを無効にします。その後、デバイスをネットワークに接続できます。

次に、デバイスを設定するために内部インターフェイスを使用するときの、このトポロジでのシステムの配線方法を示します。

ASA 5506-X、5506W-X および 5506H-X の配線

図 1: ASA 5506W-X (Wi-Fi あり)、5506-X (Wi-Fi なし)

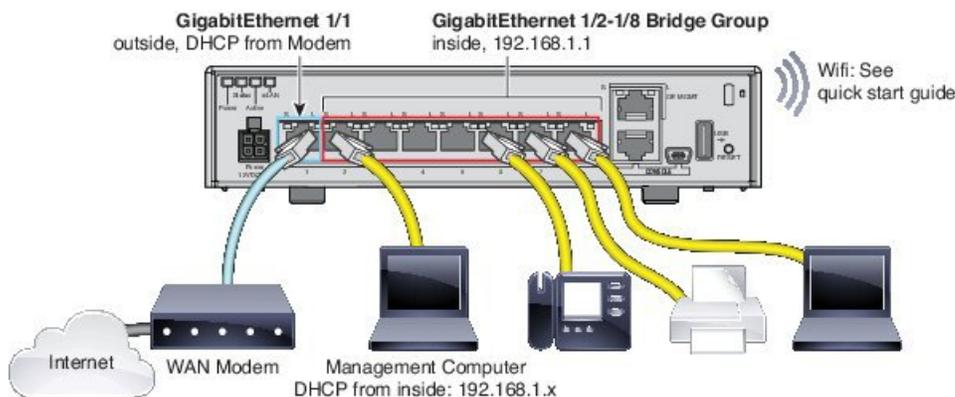
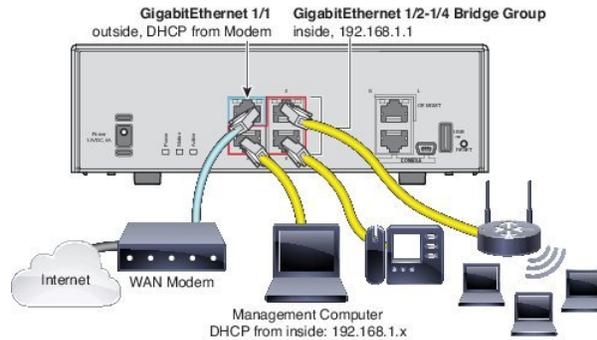


図 2 : ASA 5506H-X



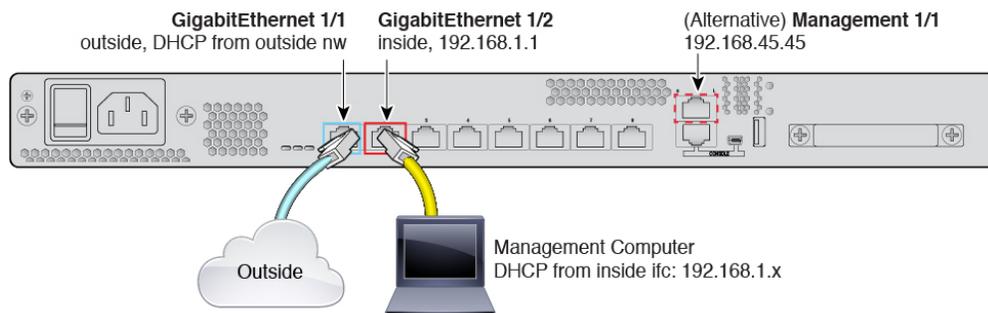
- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- デバイスを設定するために使用するワークステーションに、GigabitEthernet 1/2（または別の内部ブリッジグループのメンバー ポート）を接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



(注) 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 1/2 などの内部ポートの 1 つにそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが内部ブリッジグループ 192.168.1.1 で実行中のデバイスと競合するためです。

- 必要に応じて、内部ブリッジグループ内の別のポートに別のエンドポイントまたはスイッチを接続します。デバイスの初期設定が完了するのを待ってからエンドポイントを追加してもよいでしょう。スイッチを追加する場合、内部ブリッジグループで実行中の DHCP サーバと競合するため、それらのネットワークで他の DHCP サーバが実行中でないことを確認します。

ASA 5508-X および 5516-X の配線

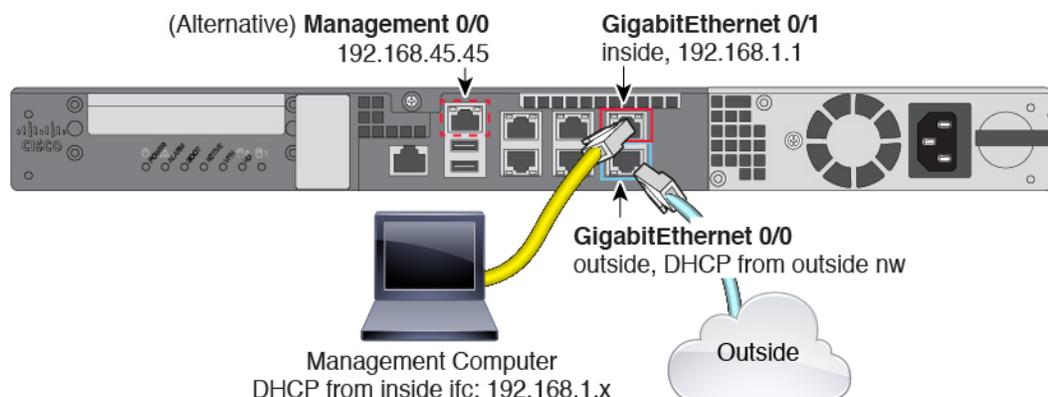


- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック IP アドレスを設定することもできます。
- GigabitEthernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



(注) 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 1/2 にそのスイッチを接続することです。ただし、スイッチのネットワーク上の他のデバイスが DHCP サーバを実行しないように徹底する必要があります。内部インターフェイス 192.168.1.1 上で実行されているデバイスと競合するためです。

ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の配線

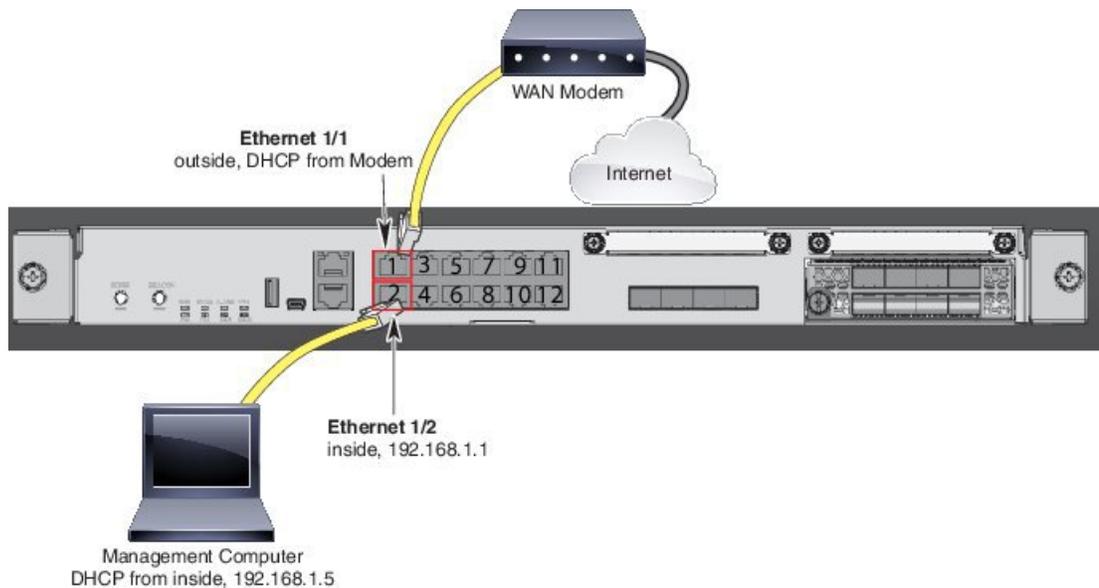


- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 0/0 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- GigabitEthernet 0/1 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



(注) 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 0/1 にそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが内部インターフェイス 192.168.1.1 で実行中のデバイスと競合するためです。

Firepower 2100の配線



- ISP/WAN モデムまたはその他の外部デバイスに Ethernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- Ethernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



- (注) 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、Ethernet 1/2 にそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが Ethernet 1/2、192.168.1.1 で実行中のデバイスと競合するためです。

仮想ケーブル接続：Firepower Threat Defense Virtual

Firepower Threat Defense Virtual をインストールするには、<http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html> でお使いの仮想プラットフォームに対応した『Cisco Firepower Threat Defense Virtual Quick Start Guid』を参照してください。Firepower Device Manager は、VMware、KVM の各仮想プラットフォームでサポートされています。

Firepower Threat Defense Virtual のデフォルト設定では、管理インターフェイスと内部インターフェイスは同じサブネットに配置されます。スマート ライセンスを使用する場合やシステム データベースへの更新プログラムを取得する場合は、管理インターフェイスにインターネット接続が必要です。

そのため、デフォルト設定は、Management 0/0 と GigabitEthernet 0/1（内部）の両方を仮想スイッチ上の同じネットワークに接続できるように設計されています。デフォルトの管理アドレスは、内部 IP アドレスをゲートウェイとして使用します。したがって、管理インターフェイスは内部インターフェイスを介してルーティングし、その後、外部インターフェイスを介してルーティングして、インターネットに到達します。

また、インターネットにアクセスできるネットワークを使用している限り、内部インターフェイス用に使用されているサブネットとは異なるサブネットに Management 0/0 を接続するオプションもあります。ネットワークに適切な管理インターフェイスの IP アドレスとゲートウェイが設定されていることを確認してください。

管理インターフェイスの IP 設定は、[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で定義されている点に注意してください。[デバイス (Device)] > [インターフェイス (Interfaces)] > [設定の表示 (View Configuration)] に一覧されている Management0/0 (診断) インターフェイスの IP アドレスと同じではありません。

Firepower Threat Defense の物理インターフェイスへの VMware ネットワークアダプタとインターフェイスのマッピング方法

VMware Firepower Threat Defense Virtual デバイス用に最大 10 のインターフェイスを設定できます。少なくとも 4 つのインターフェイスを設定する必要があります。

Management0-0 送信元ネットワークが、インターネットにアクセスできる VM ネットワークに関連付けられていることを確認します。これは、システムが Cisco Smart Software Manager にアクセスしてシステムデータベース更新をダウンロードすることを可能にするために必要です。

OVFをインストールするときにネットワークを割り当てます。インターフェイスを設定しておけば、後でVMwareクライアントを介して仮想ネットワークを変更できます。ただし、新しいインターフェイスを追加する必要がある場合は、で説明しているように、プロセスがさらに複雑になります[Firepower Threat Defense Virtual へのインターフェイスの追加 \(186 ページ\)](#)。

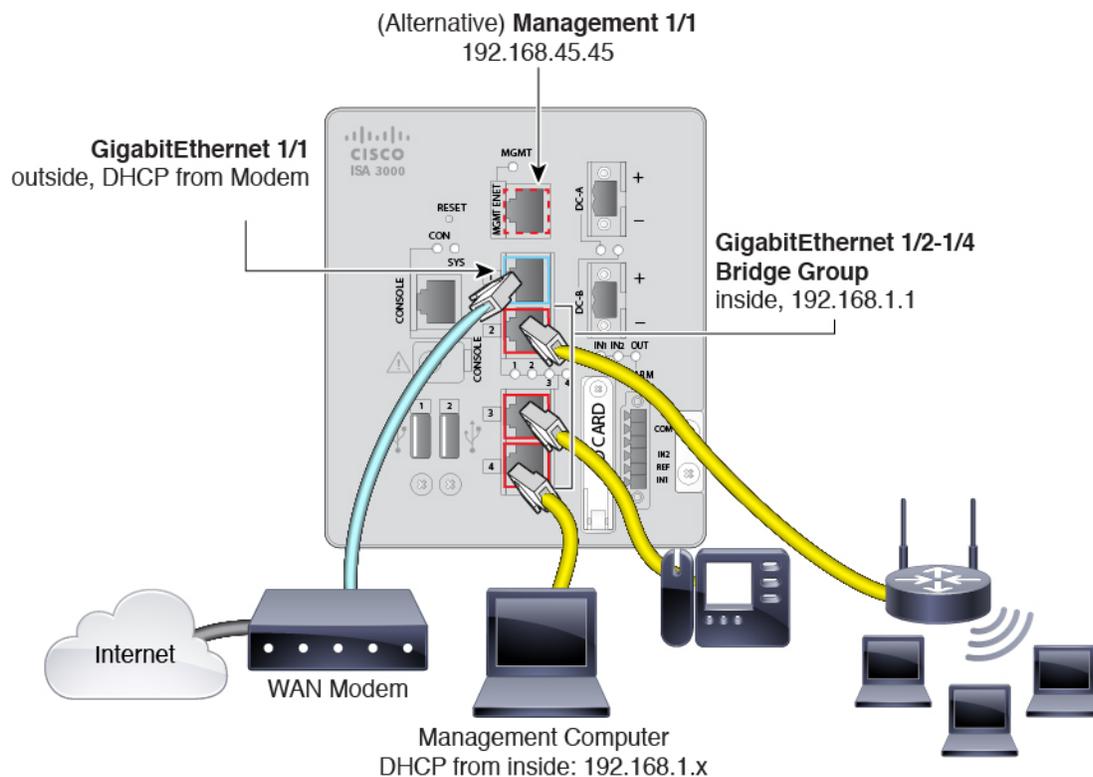
次の表は、VMware ネットワーク アダプタおよび送信元インターフェイスの、Firepower Threat Defense Virtual の物理インターフェイス名へのマッピングを示しています。追加のインターフェイスについては、命名は同じパターンに従い、関連する数字を1つずつ増やします。すべての追加インターフェイスはデータインターフェイスです。仮想ネットワークの仮想マシンへの割り当ての詳細については、VMware のオンライン ヘルプを参照してください。

表 2: 送信元から宛先ネットワークへのマッピング

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク (物理インターフェイス名)	機能
Network adapter 1	Management0-0	Diagnostic0/0	管理と診断
Network adapter 2	GigabitEthernet0-0	GigabitEthernet 0/0	内部データ
Network adapter 3	GigabitEthernet0-1	GigabitEthernet 0/1	外部データ
Network adapter 4	GigabitEthernet0-2	GigabitEthernet0/2	データ トラフィック
Network adapter 5	GigabitEthernet0-3	GigabitEthernet 0/3	データ トラフィック
Network adapter 6	GigabitEthernet0-4	GigabitEthernet 0/4	データ トラフィック
Network adapter 7	GigabitEthernet0-5	GigabitEthernet 0/5	データ トラフィック
Network adapter 8	GigabitEthernet0-6	GigabitEthernet 0/6	データ トラフィック
Network adapter 9	GigabitEthernet0-7	GigabitEthernet 0/7	データ トラフィック
Network adapter 10	GigabitEthernet0-8	GigabitEthernet 0/8	データ トラフィック

ISA 3000 のケーブル配線

図 3: ISA 3000



- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- デバイスを設定するために使用するワークステーションに、GigabitEthernet 1/2（または別の内部ブリッジグループのメンバーポート）を接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。



(注) 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 1/2 などの内部ポートの 1 つにそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが内部ブリッジグループ 192.168.1.1 で実行中のデバイスと競合するためです。

- 必要に応じて、内部ブリッジグループ内の別のポートに別のエンドポイントまたはスイッチを接続します。デバイスの初期設定が完了するのを待ってからエンドポイントを追加してもよいでしょう。スイッチを追加する場合、内部ブリッジグループで実行中の DHCP サーバと競合するため、それらのネットワークで他の DHCP サーバが実行中でないことを確認します。

初期設定の完了

Firepower Device Manager に初めてログインする際には、デバイスのセットアップ ウィザードを使用してシステムの初期設定を完了します。

始める前に

データ インターフェイスがゲートウェイデバイス（たとえば、ケーブルモデムやルータなど）に接続されていることを確認します。エッジの導入では、これはインターネット向けのゲートウェイになります。データセンター導入の場合は、これがバックボーンルータになります。使用モデルのデフォルトの「外部」インターフェイスを使用します（[インターフェイスの接続（20 ページ）](#)）および[初期設定前のデフォルト設定（34 ページ）](#)を参照）。

次に、使用ハードウェアモデルの「内部」インターフェイスにワークステーションを接続します。内部インターフェイスがブリッジグループであるモデルの場合、外部インターフェイス以外のデータポートである任意のブリッジグループメンバーインターフェイスに接続できます。また、管理/診断物理インターフェイスに接続できます。Firepower Threat Defense Virtual については、管理 IP アドレスに接続できることを確認するだけで十分です

（管理 IP アドレスからインターネットへの接続が必要な Firepower Threat Defense Virtual を除く）。管理/診断用の物理インターフェイスは、ネットワークに接続する必要はありません。デフォルトでは、インターネットに接続するデータ インターフェイス（通常、外部インターフェイス）を介してシステムのライセンスとデータベースおよびその他の更新が取得されます。代わりに別の管理ネットワークを使用する場合は、初期設定の完了後、管理/診断インターフェイスをネットワークに接続して、別の管理ゲートウェイを設定できます。

手順

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

- a) CLI で初期設定を完了していない場合、<https://ip-address> にアクセスして Firepower Device Manager を開きます。アドレスは以下のいずれかになります。
 - 内部インターフェイス、またはデフォルトの内部ブリッジグループがあるモデルのいずれかの内部ブリッジグループのデータ インターフェイスに接続している場合は、[\[https://192.168.1.1\]](https://192.168.1.1)。
 - (Firepower Threat Defense Virtual に必要) Management 物理インターフェイスに接続されている場合は <https://192.168.45.45>。
- b) ユーザ名 **admin**、およびパスワード **Admin123** を使用してログインします。

ステップ 2 これがシステムへの初めてのログインであり、CLI セットアップウィザードを使用していない場合、エンドユーザ ライセンス契約を読んで承認し、管理パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 3 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ (Next)] をクリックします。

注意 [次へ (Next)] をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

外部インターフェイス

- [IPv4 の設定 (Configure IPv4)] : 外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動で静的 IP アドレス、サブネット マスク、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv4 アドレスを設定しないという選択肢もあります。デフォルトの内部アドレスと同じサブネットに (静的に、または DHCP を介して) IP アドレスを設定しないでください ([初期設定前のデフォルト設定 \(34 ページ\)](#) を参照)。
- [IPv6 の設定 (Configure IPv6)] : 外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動で静的 IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

管理インターフェイス

- [DNS サーバ (DNS Servers)] : システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNS を使用 (Use OpenDNS)] をクリックすると、フィールドに適切な IP アドレスがリロードされます。ISP は、特定の DNS サーバを使用するよう要求する場合があります。ウィザードを完了した後、DNS 解決が機能しない場合は、[管理インターフェイスの DNS のトラブルシューティング \(508 ページ\)](#) を参照してください。
- [ファイアウォールホスト名 (Firewall Hostname)] : システムの管理アドレスのホスト名です。

ステップ 4 システム時刻を設定し、[次へ (Next)] をクリックします。

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

ステップ 5 システムのスマート ライセンスを設定します。

スマートライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマートライセンスを設定できます。

デバイスを今すぐ登録するには、リンクをクリックして Smart Software Manager (SSM) のアカウントにログインし、新しいトークンを作成して、編集ボックスにそのトークンをコピーします。

デバイスをまだ登録しない場合は、評価モード オプションを選択します。評価期間は 90 日です。後でデバイスを登録してスマートライセンスを取得する場合は、[デバイス (Device)] をクリックしてから、[スマートライセンス (Smart Licenses)] グループでリンクをクリックします。

ステップ 6 [終了 (Finish)] をクリックします。

次のタスク

- オプションライセンスでカバーされている機能 (カテゴリベースの URL フィルタリング、侵入インスペクション、マルウェア対策など) を使用する場合は、必要なライセンスを有効にします。 [オプションライセンスの有効化と無効化 \(101 ページ\)](#) を参照してください。
- 新しいシステムの場合、デフォルトの内部ブリッジグループがあるデバイス モデル上のその他のインターフェイスは、内部ブリッジグループのメンバーとして使用可能な状態になっています。エンドポイントをインターフェイスに直接接続できます。デフォルトの単一の物理インターフェイスがあるモデルの場合、その他のデータインターフェイスを異なるネットワークに接続して、インターフェイスを設定できます。ブリッジグループメンバー インターフェイスの場合、ブリッジグループからそれらのインターフェイスを削除して、追加の固有ネットワークを設定することもできます。インターフェイスの設定の詳細については、 [サブネットを追加する方法 \(85 ページ\)](#) および [インターフェイス \(163 ページ\)](#) を参照してください。
- 内部インターフェイスまたはブリッジグループメンバー インターフェイスを介してデバイスを管理し、内部インターフェイスを介して CLI セッションを開きたい場合は、SSH 接続に対して内部インターフェイスまたはブリッジグループを開きます。 [管理アクセスリストの設定 \(475 ページ\)](#) を参照してください。
- 製品の使用方法については、使用例で学習してください。 [Firepower Threat Defense の使用例 \(51 ページ\)](#) を参照してください。

外部インターフェイスの IP アドレスを取得できない場合の対処方法

デフォルトのデバイス設定には内部インターフェイスのスタティック IPv4 アドレスが含まれています。初期デバイスセットアップ ウィザードを使用してこのアドレスを変更することはできません。ただし、後で変更することはできます。

デフォルトの内部 IP アドレスが、デバイスに接続されている他のネットワークと競合する可能性があります。これは特に、外部インターフェイスで DHCP を使用してインターネットサービスプロバイダー（ISP）からアドレスを取得する場合に該当します。一部の ISP は、内部ネットワークと同じサブネットをアドレスプールとして使用しています。同じサブネットのアドレスを持つ 2 つのデータインターフェイスを持つことはできないため、ISP からの競合するアドレスを外部インターフェイスに設定することはできません。

内部スタティック IP アドレスと外部インターフェイスの DHCP が提供するアドレスの間に競合がある場合は、接続図には、外部インターフェイスは管理上動作しているが IPv4 アドレスが割り当てられていないことが示されます。

この場合セットアップウィザードは正常に完了し、デフォルト NAT、アクセス、およびその他のポリシーや設定がすべて設定されます。競合を解消するには、次の手順に従います。

始める前に

ISP に正常に接続できることを確認します。サブネット競合がある場合外部インターフェイスのアドレスを取得できませんが、単に ISP への接続がない場合にも外部インターフェイスのアドレスを取得できません。

手順

-
- ステップ 1** [デバイス (Device)] をクリックして、[インターフェイス (Interfaces)] サマリーのリンクをクリックします。
- ステップ 2** 内部インターフェイス行の [操作 (Actions)] カラムにカーソルを置き、[編集 (edit)] アイコン  をクリックします。
- ステップ 3** [IPv4 アドレス (IPv4 Address)] タブで、一意のサブネットのスタティックアドレス (192.168.2.1/24、192.168.46.1/24 など) を入力します。デフォルトの管理アドレスは 192.168.45.45/24 であるため、このサブネットは使用しないでください。
- 内部ネットワークで DHCP サーバがすでに実行されている場合、DHCP を使用してアドレスを取得することもできます。ただし最初に、[このインターフェイスに DHCP サーバを定義済み (DHCP SERVER IS DEFINED FOR THIS INTERFACE)] グループで [削除 (Delete)] をクリックして、インターフェイスから DHCP サーバを削除する必要があります。
- ステップ 4** [このインターフェイスに DHCP サーバを定義済み (DHCP SERVER IS DEFINED FOR THIS INTERFACE)] 領域で [編集 (Edit)] をクリックして、DHCP プールを新しいサブネットの範囲に変更します (たとえば、192.168.2.5-192.168.2.254)。
- ステップ 5** [OK] をクリックしてインターフェイスの変更を保存します。
- ステップ 6** 変更を展開するには、メニューの [展開 (Deploy)] ボタンをクリックします。



- ステップ 7** [今すぐ展開 (Deploy Now)] をクリックします。

展開が完了すると、外部インターフェイスに IP アドレスが割り当てられていることが接続グラフィックで示されるはずですが、内部ネットワークのクライアントを使用して、インターネットまたはその他のアップストリーム ネットワークに接続できることを確認します。

ワイヤレス アクセス ポイント (ASA 5506W-X) の設定

ASA 5506W-X には、デバイスに統合されている Cisco Aironet 702i ワイヤレス アクセス ポイントが付属します。ワイヤレス アクセス ポイントは、デフォルトでは無効になっています。ワイヤレス無線を有効化し、SSID およびセキュリティの設定を行うには、アクセス ポイント Web インターフェイスに接続してください。

アクセス ポイントは、GigabitEthernet 1/9 インターフェイスを介して内部的に接続します。すべての Wi-Fi クライアントは GigabitEthernet 1/9 ネットワークに属します。セキュリティ ポリシーにより、Wi-Fi ネットワークが他のインターフェイス上の任意のネットワークにアクセスする方法が決まります。アクセス ポイントには、外部インターフェイスやスイッチ ポートは含まれません。

次の手順では、アクセス ポイントを設定する方法について説明します。この手順では、デバイス セットアップ ウィザードが完了していると仮定します。代わりに手動でデバイスを設定した場合、設定に基づいて手順を調整する必要があります。

詳細については、次のマニュアルを参照してください。

- ワイヤレス LAN コントローラの使用の詳細については、『[Cisco Wireless LAN Controller Software documentation](#)』を参照してください。
- ワイヤレス アクセス ポイントのハードウェアおよびソフトウェアの詳細については、『[Cisco Aironet 700 Series documentation](#)』を参照してください。

始める前に

アクセス ポイントに到達できず、FTD デバイス推奨設定になっていて、他のネットワークの問題が見つからない場合、アクセス ポイントをデフォルト設定に復元できます。FTDCLI にアクセス (コンソール ポートに接続、または SSH アクセスを設定) する必要があります。FTD CLI から、次のコマンドを入力します。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <press enter, by default, the password is blank>
firepower# hw-module module wlan recover configuration
```

アクセス ポイントのトラブルシューティングをさらに行う必要がある場合、`session wlan console` コマンドを使用して、アクセス ポイント CLI に接続します。

手順

ステップ1 ワイヤレス インターフェイス GigabitEthernet1/9 を設定して有効化します。

- a) [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] グループでリンクをクリックしてインターフェイスのリストを表示します。
- b) GigabitEthernet 1/9 インターフェイスの [編集 (edit)] アイコン () をクリックします。
- c) 次のオプションを設定します。

- [インターフェイス名 (Interface Name)] : インターフェイスの名前 (たとえば **wifi** など) を入力します。
- [ステータス (Status)] : インターフェイスを有効にするには、スライダをクリックします。
- [IPv4アドレス (IPv4 Address)] : アドレス タイプに [スタティック (Static)] を選択し、アドレスおよびサブネット マスクを入力します。たとえば、192.168.10.1/24 などと入力します。

- d) [保存 (Save)] をクリックします。

ステップ2 内部インターフェイスと同じセキュリティ ゾーンに Wi-Fi インターフェイスを追加します。

デバイスのセットアップ ウィザードでは、[inside_zone] というセキュリティ ゾーンの [内部 (inside)] ブリッジグループのメンバーを設定します。Wi-Fi インターフェイスは、アクセスポイントの Web インターフェイスに到達できるよう、同じゾーンに存在する必要があります (デフォルトの Inside_Inside_Rule アクセスルールによって可能になりました)。

- a) メニューの [オブジェクト (Objects)] をクリックし、コンテンツ テーブルから [セキュリティ ゾーン (Security Zones)] を選択します。
- b) [inside_zone] の [編集 (edit)] アイコン () をクリックします。
- c) [インターフェイス (Interfaces)] の下の [+] をクリックし、[wifi] インターフェイスを選択します。

ステップ3 Inside_zone セキュリティゾーン内のインターフェイスの間でトラフィックを許可するアクセス制御ルールが存在することを確認します。

デバイスのセットアップ ウィザードでは、トラフィックが [inside_zone] から [outside_zone] に流れるようにするためのルールを作成します。これにより、内部ユーザがインターネットにアクセスできます。

またウィザードでは、内部ホストが互いに到達できるよう、[inside_zone] と [inside_zone] の間のトラフィックが流れるようにするためのルールも作成します。

[Inside_zone] に [wifi] インターフェイスを追加することで、Wi-Fi ユーザはこれらの両方のルールにも含まれるため、インターネットおよびその他の社内ユーザに到達できます。

ウィザードを完了していなかった場合、これらのルールが存在しない可能性があります。デフォルトのアクションではすべてのトラフィックをブロックするため、これらのルールを作成

する必要があります。次の手順では、[inside_zone]セキュリティゾーン内のインターフェイス間のトラフィックを有効にするルールを作成する方法について説明します。

- a) メニューの [ポリシー (Policies)] をクリックします。
- b) ルールを追加するには、[アクセスコントロール (Access Control)] テーブルの上の [+] をクリックします。
- c) 少なくとも、ルール内の以下のオプションを設定します。
 - [タイトル (Title)] : ルールの名前を入力します。たとえば、「Inside_Inside」と入力します。
 - [アクション (Action)] : 許可または信頼。
 - [送信元/宛先 (Source/Destination)] > [送信元ゾーン (Source Zones)] : inside_zone を選択します。
 - [送信元/宛先 (Source/Destination)] > [宛先ゾーン (Destination Zones)] : inside_zone を選択します。
- d) [OK] をクリックします。

ステップ 4 ワイヤレス インターフェイスで、DHCP サーバを設定します。

DHCP サーバはアクセスポイントに接続するデバイスに IP アドレスを供給します。また、アクセスポイント自体にもアドレスを提供します。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device)]
- b) [システム設定 (System Settings)] > [DHCPサーバ (DHCP Server)] をクリックします。
- c) [DHCPサーバ (DHCP Servers)] タブをクリックします。
- d) DHCP サーバテーブルの上の [+] をクリックします。
- e) 以下の DHCP サーバプロパティを設定します。
 - [DHCPサーバの有効化 (Enable DHCP Server)] : DHCP サーバを有効にするには、スライダをクリックします。
 - [インターフェイス (Interface)] : [wifi] インターフェイスを選択します。
 - [アドレスプール (Address Pool)] : DHCP クライアントのアドレスプールを入力します。たとえば、ワイヤレスインターフェイスのアドレス例を使用している場合、プールは 192.168.10.2-192.168.10.254 になります。プールは、インターフェイスの IP アドレスと同じサブネット上にある必要があり、インターフェイスのアドレスやブロードキャストアドレスをプールに含めることはできません。
- f) [追加 (Add)] [OK] をクリックします。

ステップ 5 メニューの [展開 (Deploy)] ボタンをクリックし、[今すぐ展開 (Deploy Now)] ボタンをクリックし、変更をデバイスに展開します。



導入が完了するまで待機してから続行します。

ステップ6 ワイヤレス アクセス ポイントを設定します。

ワイヤレス アクセス ポイントは、ワイヤレス インターフェイス用に定義された DHCP プールからアドレスを取得します。プール内の最初のアドレスを取得する必要があります。アドレスの例を使用した場合、これは「192.168.10.2」です。（最初のアドレスが機能しない場合は、プール内の次のアドレスを試します）。

- a) 新しいブラウザ ウィンドウを使用し、ワイヤレス アクセス ポイントの IP アドレス、たとえば [http://192.168.10.2] に移動します。

アクセスポイントの Web インターフェイスが表示されます。

このアドレスを開くには、内部ネットワークまたはそのネットワークにルーティングできるネットワーク上にいる必要があります。

- b) ユーザ名 **cisco**、パスワード **Cisco** を使用してログインします。
- c) 左側の [簡易設定 (Easy Setup)] > [ネットワーク設定 (Network Configuration)] をクリックします。
- d) [無線設定 (Radio Configuration)] 領域で、[無線2.4GHz (Radio 2.4GHz)] および [無線5GHz (Radio 5GHz)] セクションのそれぞれに対して、少なくとも次のパラメータを設定し、セクションごとに [適用 (Apply)] をクリックします。

- [SSID] : サービスセット識別子。ワイヤレス ネットワークの名前です。ユーザが Wi-Fi 接続用のワイヤレス ネットワークを選択する際に、この名前が表示されます。
- [ビーコンのブロードキャストSSID (Broadcast SSID in Beacon)] : このオプションを選択します。
- [ユニバーサル管理モード (Universal Admin Mode)] : 無効。
- [セキュリティ (Security)] : どのセキュリティ オプションを使用するかを選択します。

ステップ7 ワイヤレス アクセス ポイントの Web インターフェイスで、無線を有効化します。

- a) 左側の [サマリー (Summary)] をクリックし、メインページの [ネットワークインターフェイス (Network Interfaces)] で、2.4 GHz 無線に対応するリンクをクリックします。
- b) [設定 (Settings)] タブをクリックします。
- c) [無線の有効化 (Enable Radio)] の設定では、[有効化 (Enable)] ラジオ ボタンをクリックし、ページ下部の [適用 (Apply)] をクリックします。
- d) 5 Ghz 無線についてこの手順を繰り返します。

初期設定前のデフォルト設定

ローカル マネージャ (Firepower Device Manager) を使用して Firepower Threat Defense デバイスの初期設定を行う前、デバイスには次のデフォルト設定が含まれています。

多数のモデルにおいて、この設定では、Firepower Device Manager を内部インターフェイス経由で開き（通常、コンピュータをインターフェイスに直接接続する）、内部インターフェイス上に定義された DHCP サーバを使用してコンピュータに IP アドレスを提供することを前提としています。または、管理/診断用物理インターフェイスにコンピュータを接続し、DHCP を使用してアドレスを取得することもできます。ただし、一部のモデルではデフォルト設定や管理要件が異なります。詳細については、次の表を参照してください。

デフォルト設定

設定	デフォルト	初期設定時に変更できるか
管理者ユーザのパスワード	Admin123	可。デフォルトパスワードを変更する必要があります。
管理 IP アドレス	192.168.45.45	不可
管理ゲートウェイ	デバイスのデータインターフェイス。 通常、外部インターフェイスがインターネットへのルートになります。このゲートウェイは、 <code>from-the-device</code> （デバイスからの出力）トラフィックのみで機能します。 Firepower Threat Defense Virtual192.168.45.1	不可
管理インターフェイスの DHCP サーバ	アドレス プール 192.168.45.46 ~ 192.168.45.254 で有効です。 Firepower Threat Defense Virtual : DHCP サーバが有効になっていません。	不可
管理インターフェイスの DNS サーバ	OpenDNS のパブリック DNS サーバ、 208.67.220.220 および 208.67.222.222。	可
内部インターフェイスの IP アドレス	192.168.1.1/24 Firepower Threat Defense Virtual192.168.45.1/24	不可
内部クライアントの DHCP サーバ	アドレス プール 192.168.1.5 ~ 192.168.1.254 の内部インターフェイスで実行されます。 Firepower Threat Defense Virtual : 内部 インターフェイスのアドレスプールは 192.168.45.46 ~ 192.168.45.254 です。	不可

設定	デフォルト	初期設定時に変更できるか
内部クライアントの DHCP 自動設定 (自動設定では、WINS サーバおよび DNS サーバのアドレスをクライアントに提供)	外部インターフェイスで有効です。	可 (ただし間接的)。外部インターフェイスにスタティック IPv4 アドレスを設定した場合、DHCP サーバの自動設定が無効になります。
外部インターフェイスの IP アドレス	インターネットサービスプロバイダー (ISP) または上流に位置するルータから DHCP 経由で取得されます。	可

デバイス モデル別のデフォルト インターフェイス

初期設定時に異なる内部および外部インターフェイスを選択することはできません。設定後にインターフェイスの割り当てを変更するには、インターフェイス設定と DHCP 設定を編集します。非交換インターフェイスとして設定するには、ブリッジグループからインターフェイスを削除する必要があります。

Firepower Threat Defense デバイス	外部インターフェイス	内部インターフェイス
ASA 5506-X ASA 5506H-X ASA 5506W-X	GigabitEthernet 1/1	BVI1 (外部インターフェイスを除く他のデータインターフェイスをすべて含む)。5506W-X ではワイヤレス インターフェイス GigabitEthernet 1/9。
ASA 5508-X ASA 5516-X	GigabitEthernet 1/1	GigabitEthernet 1/2
ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet 0/0	GigabitEthernet 0/1
Firepower 2100 シリーズ	Ethernet1/1	Ethernet1/2
Firepower Threat Defense Virtual	GigabitEthernet 0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet 1/1	BVI1 (すべてのデータ インターフェイスを含む、ただし、外部インターフェイスは除く)。

初期セットアップ後の設定

セットアップ ウィザードを完了すると、デバイス設定は次のようになります。この表では、個々の設定項目の値が、ユーザが明示的に選択したものとなるのか、または他の項目の設定に基づき自動的に定義されたものかを示します。「暗黙的」な設定を検証し、ニーズに合わない場合は編集します。

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
管理者ユーザのパスワード	任意の入力値	明示的
管理 IP アドレス	192.168.45.45	デフォルト
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。管理ゲートウェイは、 from-the-device (デバイスからの出力) トラフィックのみで機能します。 Firepower Threat Defense Virtual 192.168.45.1	デフォルト
管理インターフェイス上の DHCP サーバ	アドレス プール 192.168.45.46 ~ 192.168.45.254 で有効です。 Firepower Threat Defense Virtual : DHCP サーバが有効になっていません。	デフォルト
管理インターフェイスの DNS サーバ	任意の入力値	明示的
管理ホスト名	firepower または任意の入力値	明示的
データ インターフェイスを通過する管理アクセス	データ インターフェイスの管理アクセス リスト ルールにより、内部インターフェイスを通過する HTTPS アクセスが許可されます。内部ブリッジグループを持つモデルでは、内部ブリッジグループの全メンバー インターフェイスがこの対象となります。SSH 接続は許可されません。IPv4 および IPv6 接続はいずれも許可されます。 Firepower Threat Defense Virtual: デフォルトの管理アクセスルールを持つデータ インターフェイスはありません。	暗黙的
システム時間	選択したタイム ゾーンおよび NTP サーバ。	明示的
スマート ライセンス	基本ライセンスとともに登録したか、または評価期間を開始したか、いずれか選択した方法。 サブスクリプションライセンスは有効化されていません。スマート ライセンスのページに移動して、スマート ライセンスを有効化してください。	明示的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
内部インターフェイスの IP アドレス	192.168.1.1/24 Firepower Threat Defense Virtual 192.168.45.1/24	デフォルト
内部クライアントの DHCP サーバ	アドレス プール 192.168.1.5 ~ 192.168.1.254 の内部インターフェイスで実行されます。 Firepower Threat Defense Virtual : 内部インターフェイスのアドレスプールは 192.168.45.46 ~ 192.168.45.254 です。	デフォルト
内部クライアントに対する DHCP 自動設定 (自動設定では、WINS サーバおよび DNS サーバ用のアドレスがクライアントに提供)	DHCP を使用して外部インターフェイスの IPv4 アドレスを取得している場合、DHCP 自動設定は外部インターフェイスに対して有効化されます。 静的アドレッシングを使用している場合は、DHCP 自動設定は無効になります。	明示的 (ただし間接的)
データ インターフェイスの設定	<ul style="list-style-type: none"> • ASA 5506-X、ISA 3000 : 外部インターフェイスを除くすべてのデータ インターフェイス (GigabitEthernet1/2 など) が有効になり、内部ブリッジグループの一部となります。これらのポートにエンドポイントまたはスイッチを接続すると、内部インターフェイスのアドレスを DHCP サーバから取得できます。これらのインターフェイスには inside_1、inside_2 などと名前が付けられます。 • それ以外のすべてのモデル : 外部および内部インターフェイスのみが設定され有効になります。他のすべてのデータ インターフェイスは無効になります。 	デフォルト
外部の物理インターフェイスおよび IP アドレス	デバイス モデルに基づくデフォルトの外部ポート。初期設定前のデフォルト設定 (34 ページ) を参照してください。 IP アドレスは DHCP によって取得するか、入力したスタティックアドレスです (IPv4、IPv6、またはその両方)。	インターフェイスはデフォルト、 アドレッシングは明示的
スタティック ルート	外部インターフェイスに対してスタティック IPv4 または IPv6 アドレスを設定すると、スタティックなデフォルトルートも IPv4 または IPv6 用に適宜設定され、このアドレスタイプ用に定義されたゲートウェイをポイントします。DHCP を選択した場合は、デフォルトルートは DHCP サーバから取得されます。 ネットワーク オブジェクトもこのゲートウェイ、および「any」アドレス (IPv4 の場合は 0.0.0.0/0、IPv6 の場合は ::/0) に合わせて作成されます。	暗黙的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
セキュリティゾーン	<p>内部インターフェイスを含む inside_zone。内部ブリッジグループを持つモデルでは、内部ブリッジグループインターフェイスの全メンバーがゾーンに含まれます。</p> <p>外部インターフェイスを含む outside_zone。</p> <p>(これらのゾーンを編集して他のインターフェイスを追加することも、独自のゾーンを作成することも可能)。</p>	暗黙的
アクセスコントロールポリシー	<p>inside_zone から outside_zone に送信されるすべてのトラフィックを信頼するルール。これにより、インスペクションなしで、ネットワーク内のユーザからのすべてのトラフィックを外部に出すことができ、これらの接続のすべてのリターントラフィックが許可されます。</p> <p>内部ブリッジグループを持つモデルでは、inside_zone 内のインターフェイス間を伝送されるすべてのトラフィックを信頼する2番目のルールが作成されます。これにより、内部ネットワーク内のユーザ間で伝送されるすべてのトラフィックが、インスペクションを受けることなく許可されます。</p> <p>他のすべてのトラフィックに対するデフォルトアクションは、ブロックです。つまり、外部から開始され、ネットワークに進入しようとするすべてのトラフィックが阻止されます。</p>	暗黙的
NAT	<p>(内部ブリッジグループがないモデル) インターフェイスの動的 PAT ルールは、外部インターフェイスへの任意の IPv4 トラフィックの発信元アドレスを、外部インターフェイスの IP アドレス上の一意のポートに変換します。</p> <p>(内部ブリッジグループを持つモデル) 内部ブリッジグループの各メンバーに対し、インターフェイスのダイナミック PAT ルールにより、外部インターフェイスを宛先とするすべての IPv4 トラフィックの発信元アドレスは、外部インターフェイスの IP アドレス上の一意のポートに変換されます。これらは NAT ルールテーブルに表示されるため、必要に応じて後から編集できます。</p> <p>補足的な非表示の PAT ルールにより、内部インターフェイスを通過する HTTPS アクセス、およびデータインターフェイスを経由する管理アドレスのルーティングが有効化されます。これらは NAT テーブルには含まれませんが、CLI で show nat コマンドを使用すれば確認することができます。</p>	暗黙的

設定の基本

ここでは、デバイスの設定に関する基本的な手順について説明します。

デバイスの設定

Firepower Device Managerに最初にログインするとき、基本設定の構成のセットアップウィザードを利用できます。ウィザードを完了したら、次の方法を使用してその他の機能を設定し、デバイス設定を管理します。

各項目が視覚的に区別しにくい場合、ユーザ プロファイルから異なるカラー スキームを選択します。ページ右上の [ユーザ (user)] アイコンのドロップダウンメニューから、[プロファイル (Profile)] を選択します。



手順

ステップ 1 [デバイス (Device)] をクリックして[**デバイス概要 (Device Summary)**] に移動します。

ダッシュボードには、有効なインターフェイスやキー設定が設定されているか (緑色) またはまだ設定が必要であるかなど、デバイスの視覚的なステータスが表示されます。詳細については、[インターフェイスと管理ステータスの表示 \(45 ページ\)](#) を参照してください。

ステータス イメージの上にはデバイス モデルの概要、ソフトウェア バージョン、VDB (システムと脆弱性のデータベース) バージョンがあり、前回の侵入ルールは更新されています。

イメージの下には設定可能なさまざまな機能のグループがあり、各グループの設定の概要、およびシステム設定を管理するために行うことができるアクションが表示されます。

ステップ 2 設定を行うか、またはアクションを実行するには、各グループのリンクをクリックします。

次に、グループの概要を示します。

- [インターフェイス (Interface)] : 管理インターフェイスに加えて、少なくとも2つのデータインターフェイスを設定する必要があります。[インターフェイス \(163 ページ\)](#) を参照してください。
- [ルーティング (Routing)] : ルーティングの設定。デフォルト ルートを定義する必要があります。他のルートは設定に応じて必要になります。[ルーティング \(191 ページ\)](#) を参照してください。
- [更新 (Updates)] : 地理位置情報、侵入ルールと脆弱性のデータベースの更新、およびシステムソフトウェアのアップグレード。これらの機能を使用する場合、最新のデータベースの更新情報を確実にするため、定期的な更新スケジュールを設定します。定期的なスケジュールの更新が発生する前に更新をダウンロードする必要がある場合にも、このページ

にアクセスできます。[システムデータベースおよびフィードの更新 \(489 ページ\)](#) を参照してください。

- [システム設定 (System Settings)]: このグループにはさまざまな設定が含まれます。デバイスの初期設定時に構成し、その後ほとんど変更しない基本設定などがあります。[システム設定 \(475 ページ\)](#) を参照してください。
- [スマートライセンス (Smart License)]: システム ライセンスの現在のステータスを示します。システムを使用するには、適切なライセンスをインストールする必要があります。一部の機能では追加のライセンスが必要です。[システムのライセンス \(95 ページ\)](#) を参照してください。
- [バックアップと復元 (Backup and Restore)]: システム設定をバックアップするか、以前のバックアップを復元します。[システムのバックアップと復元 \(496 ページ\)](#) を参照してください。
- [トラブルシューティング (Troubleshoot)]: Cisco Technical Assistance Center の依頼により、トラブルシューティング ファイルを生成します。[トラブルシューティング ファイルの作成 \(514 ページ\)](#) を参照してください。
- [サイト間VPN (Site-to-Site VPN)]: このデバイスとリモート デバイス間のサイト間バーチャルプライベート ネットワーク (VPN) 接続。[サイト間 VPN の管理 \(398 ページ\)](#) を参照してください。
- [リモートアクセスVPN (Remote Access VPN)]: 内部ネットワークへの外部クライアントの接続を可能にするリモートアクセス仮想プライベートネットワーク (VPN) 構成です。[リモート アクセス VPN の設定 \(432 ページ\)](#) を参照してください。
- [詳細設定 (Advanced Configuration)]: FlexConfig および Smart CLI を使用して、Firepower Device Manager を使用して設定できない機能を設定します。[詳細設定 \(523 ページ\)](#) を参照してください。

ステップ 3 変更を展開するには、メニューの [展開 (Deploy)] ボタンをクリックします。



変更は、それらを展開するまでデバイスで有効になりません。[変更の展開 \(43 ページ\)](#) を参照してください。

次のタスク

メインメニューの [ポリシー (Policies)] をクリックし、システムのセキュリティ ポリシーを設定します。また、これらのポリシーで必要なオブジェクトを設定するには、[オブジェクト (Objects)] をクリックします。

セキュリティポリシーの設定

組織のアクセプタブルユースポリシーを実装して不正侵入やその他の脅威からネットワークを保護するにはセキュリティポリシーを使用します。

手順

ステップ1 [ポリシー (Policies)] をクリックします。

[セキュリティポリシー (Security Policies)] ページには、システムを経由する接続の一般的な流れ、およびセキュリティポリシーが適用される順序が表示されます。

ステップ2 ポリシーの名前をクリックして構成します。

アクセス制御ポリシーは常に必要ですが、各ポリシータイプを構成する必要はない場合があります。次に、ポリシーの概要を示します。

- [SSL復号 (SSL Decryption)] : 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号化するかを判断するにはSSL復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。[SSL復号ポリシーの設定 \(212 ページ\)](#) を参照してください。
- [アイデンティティ (Identity)] : 個々のユーザにネットワークアクティビティを関連付ける、またはユーザまたはユーザグループのメンバーシップに基づいてネットワークアクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティポリシーを使用します。[アイデンティティポリシーの設定 \(232 ページ\)](#) を参照してください。
- [セキュリティインテリジェンス (Security Intelligence)] : ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティインテリジェンスポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。[セキュリティインテリジェンスの設定 \(247 ページ\)](#) を参照してください。
- [NAT] (ネットワークアドレス変換) : 内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。[NAT の設定 \(307 ページ\)](#) を参照してください。
- [アクセス制御 (Access Control)] : ネットワーク上で許可する接続の決定にアクセスコントロールポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル (マルウェア) ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。[アクセスコントロールポリシーを設定する \(263 ページ\)](#) を参照してください。

- [侵入 (Intrusion)]: 侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。[侵入ポリシーの管理 \(288 ページ\)](#) を参照してください。

ステップ 3 変更を展開するには、メニューの [展開 (Deploy)] ボタンをクリックします。



変更は、それらを展開するまでデバイスで有効になりません。[変更の展開 \(43 ページ\)](#) を参照してください。

変更の展開

ポリシーまたは設定を更新した場合、変更がすぐにはデバイスに適用されません。設定の変更には、次の 2 つの手順を実行します。

1. 変更を行います。
2. 変更を展開します。

この手順により、デバイスを「部分的に設定された」状態で実行することなく、関連する変更のグループ化を行えるようになります。ほとんどの場合、展開には自分の変更内容のみが含まれています。ただし、必要に応じて、システムが設定全体を再適用し、これがネットワークに悪影響を及ぼす可能性があります。さらに、いくつかの変更ではインスペクションエンジンの再起動が必要であり、この再起動中にトラフィックがドロップされます。したがって、発生し得る混乱の影響が最小限になるタイミングで変更を展開するように検討してください。

目的の変更を完了した後、次の手順を使用して変更を展開します。



注意

Firepower Device Manager を使用する Firepower Threat Defense デバイスは、インスペクションエンジンがソフトウェアのリソースの問題が原因でビジー状態である、または設定の展開中にエンジンの再起動が必要なためダウンしているときに、トラフィックをドロップします。再起動が必要な変更の詳細については、[インスペクションエンジンを再起動する設定の変更 \(44 ページ\)](#) を参照してください。

手順

ステップ 1 Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。

このアイコンは、展開されていない変更がある場合にドットマークで強調表示されます。



[展開サマリー (Deployment Summary)] ページが開きます。このウィンドウには、前回の展開リストに、展開の開始時点と完了時点での変更内容（「変更されたオブジェクト」）に関するサマリー情報と、各展開のステータスを記載したものが表示されます。

展開でインスペクションエンジンの再起動が必要な場合は、再起動を必要とする変更の詳細を示すメッセージがページに表示されます。この時点で一時的なトラフィック損失を許容できない場合は、ダイアログを閉じ、変更を展開する良いタイミングを待ちます。

アイコンが強調表示されていない場合でも、クリックすればこれまでの展開ジョブの結果を表示できます。



ステップ 2 [今すぐ展開 (Deploy Now)] をクリックします。

インスペクションエンジンを再起動する設定の変更

設定の変更を展開した場合、次の設定またはアクションはいずれもインスペクションエンジンを再起動します。



注意 展開時に、リソース需要が高まった結果、いくつかの packets がインスペクションなしでドロップされることがあります。さらに、一部の設定の展開では、インスペクションエンジンを再起動する必要があり、トラフィックインスペクションが中断され、トラフィックがドロップされます。

展開

一部の変更ではインスペクションエンジンの再起動が必要で、これにより一時的なトラフィック損失が発生します。インスペクションエンジンの再起動が必要な変更は、次のとおりです。

- SSL 復号ポリシーが有効化または無効化された。
- 1 つ以上の物理インターフェイス上（サブインターフェイスではありません）で MTU が変更された。
- アクセス制御ルールのファイル ポリシーを追加または削除します。
- ルール データベースが更新された。
- VDB が更新された。

さらに、Snort プロセスがビジー状態で CPU の合計使用率が 60% を超えている場合、展開中に一部の packets がドロップされることがあります。 `show asp inspect-dp snort` コマンドを使用して、Snort の現在の CPU 使用率を確認できます。

システム データベースの更新

ルール データベースまたは VDB に更新プログラムをダウンロードした場合は、それらをアクティブにするために更新プログラムを展開する必要があります。この展開により、インスペクションエンジンが再起動される場合があります。手動で更新プログラムをダウンロードする、または更新プログラムのスケジュールを設定する場合は、ダウンロードが完了した後に、システムが変更を自動で展開する必要があるかどうかを指定できます。更新プログラムを自動的に展開するシステムがない場合は、次に変更を展開したときに更新プログラムが適用され、その際にインスペクションエンジンが再起動される場合があります。

システム アップデート

システムを再起動せずに、バイナリの変更が含まれるシステム更新プログラムまたはパッチをインストールする場合は、インスペクションエンジンを再起動する必要があります。バイナリの変更には、インスペクションエンジン、プリプロセッサ、脆弱性データベース (VDB) または共有オブジェクトルールの変更が含まれることがあります。場合によって、バイナリの変更を含まないパッチで、Snort の再起動が必要になることもある点に注意してください。

インターフェイスと管理ステータスの表示

[デバイスの概要 (Device Summary)] には、デバイスのグラフィカルビューと管理アドレス用の設定が含まれています。[デバイスの概要 (Device Summary)] を開くには、[デバイス (Device)] をクリックします。

このグラフィックの要素は、要素のステータスに基づいて色が変わります。要素をマウスオーバーすると、追加情報が提供される場合があります。このグラフィックを使用して、次の項目をモニタできます。



- (注) インターフェイスステータス情報を含む、グラフィックのインターフェイス部分は、[インターフェイス (Interfaces)] ページおよび [モニタリング (Monitoring)] > [システム (System)] ダッシュボードでも使用可能です。

インターフェイス ステータス

ポートをマウスオーバーすると、その IP アドレスと有効なリンクステータスが表示されます。IP アドレスはスタティックに割り当てることができれば、DHCP を使用して取得することもできます。ブリッジ仮想インターフェイス (BVI) をマウスオーバーすると、メンバーインターフェイスのリストが表示されます。

インターフェイスポートは、次のカラーコーディングを使用します。

- 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
- グレー：インターフェイスは無効です。

- オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。

内部、外部ネットワーク接続

グラフィックは、次の条件に従い、外部（またはアップストリーム）ネットワークおよび内部ネットワークに接続されているポートを示します。

- 内部ネットワーク：「inside」という名前のインターフェイスの場合のみ、内部ネットワークのポートが表示されます。その他に内部ネットワークが存在する場合、それらは表示されません。いずれのインターフェイスにも「inside」と命名していない場合は、ポートは内部ポートとしてマークされません。
- 外部ネットワーク：「outside」という名前のインターフェイスの場合のみ、外部ネットワークのポートが表示されます。内部ネットワークと同様に、この名前は必須であり、存在しない場合は、ポートは外部ポートとしてマークされません。

管理設定のステータス

グラフィックは、管理アドレス用にゲートウェイ、DNS サーバ、NTP サーバ、スマートライセンスが設定されているかどうか、さらに、それらの設定が正常に機能しているかどうかを示します。

緑は機能が設定され正常に動作していることを示し、グレーは機能が設定されていないか、正常に動作していないことを示しています。たとえば、サーバに到達不能な場合は、DNS ボックスがグレーになります。要素をマウス オーバーすると、詳細が表示されます。

問題が見つかった場合は、次のように修正します。

- 管理ポートおよびゲートウェイ：[システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択します。
- DNSサーバ：[システム設定 (System Settings)] > [DNSサーバ (DNS Server)] を選択します。
- NTPサーバ：[システム設定 (System Settings)] > [NTP] を選択します。[NTP のトラブルシューティング \(507 ページ\)](#) も参照してください。
- スマートライセンス：[スマートライセンス (Smart License)] グループ内の [設定の表示 (View Configuration)] リンクをクリックします。

システム タスク ステータスの表示

システムタスクには、さまざまなデータベースの更新の取得や適用など、直接関与することなく実行されるアクションが含まれます。これらのタスクのリストとそのステータスを表示し、これらのシステムタスクが正常に完了したことを確認できます。

手順

ステップ 1 メインメニューの [タスクリスト (Task List)] ボタンをクリックします。



タスク リストが開き、システム タスクのステータスと詳細が表示されます。

ステップ 2 タスクのステータスを評価します。

永続的な問題がある場合は、デバイス設定を修正する必要があります。たとえば、データベースの更新を永続的に取得できない場合、デバイスの管理 IP アドレスにインターネットへのパスがないと示される場合があります。タスクの説明に挙げられている問題については、Cisco Technical Assistance Center (TAC) に問い合わせる必要があります。

タスク リストでは、次の操作を実行できます。

- これらのステータスに基づいてリストをフィルタするには、[成功 (Success)] または [失敗 (Failures)] ボタンをクリックします。
- タスクをリストから削除するには、[削除 (delete)] アイコン () をクリックします。
- 進行中でないすべてのタスクのリストを空にするには、[完了したタスクをすべて削除 (Remove All Completed Tasks)] をクリックします。

CLI コンソールを使用した設定の監視およびテスト

FTD デバイスには、監視およびトラブルシューティングに使用できるコマンドラインインターフェイス (CLI) が組み込まれています。SSH セッションを開いてすべてのシステムコマンドにアクセスすることができますが、Firepower Device Manager で CLI コンソールを開いて、さまざまな **show** コマンド、**ping**、**traceroute**、および **packet-tracer** などの読み取り専用コマンドを使用することもできます。

ページ間の移動、設定、および機能の展開を行っている間、CLI コンソールを開いたままにしておくことができます。たとえば、新しいスタティックルートを展開した後で、CLI コンソールで **ping** を使用して、ターゲットネットワークに到達できることを確認できます。

CLI コンソールは基本 FTD CLI を使用します。CLI コンソールを使用して、診断 CLI、エキスパートモード、および FXOS CLI (FXOS を使用するモデル) に入ることはできません。このような他の CLI モードに入る必要がある場合は、SSH を使用します。

コマンドの詳細については、Cisco Firepower Threat Defense コマンドリファレンス、https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html を参照してください。

注：

- **ping** は CLI コンソールでサポートされていますが、**ping system** コマンドはサポートされていません。
- システムは最大で2つのコマンドを同時に処理できます。そのため、別のユーザが（たとえば、REST API を使用して）コマンドを発行している場合は、その他のコマンドの完了を待ってからコマンドを入力する必要があります。問題が解決しない場合は、CLI コンソールの代わりに SSH セッションを使用します。
- コマンドは、展開された設定に基づいて情報を返します。FDM で設定を変更しても、展開していない場合は、コマンド出力に変更の結果が表示されません。たとえば、新しいスタティックルートを作成しても展開していない場合、そのルートは **show route** 出力に表示されません。

手順

ステップ 1 Web ページの右上にある [CLIコンソール (CLI Console)] ボタンをクリックします。



ステップ 2 プロンプトにコマンドを入力し、[Enter] を押します。

コマンドの中には他より出力まで時間がかかるものもありますが、しばらくお待ちください。コマンドの実行がタイムアウトになったというメッセージが表示されたら、もう一度試してください。 **show perfstats** など、対話型の応答が必要なコマンドを入力した場合にも、タイムアウトエラーが発生します。問題が解決しない場合は、CLI コンソールの代わりに SSH クライアントを使用する必要があります。

このウィンドウを使用する方法について、いくつかのヒントを次に示します。

- コマンドの一部を入力した後で [Tab] キーを押すと、オート コンプリートが作動します。また、Tab はコマンド内のその位置で使用可能なパラメータをリストします。また、Tab は3つのレベルまでキーワードを示します。3つのレベルを過ぎると、コマンドリファレンスを使用して詳細を確認する必要があります。
- コマンドの実行を停止するには、Ctrl+C を押します。
- ウィンドウを移動するには、ヘッダー内の任意の箇所をクリックしたままウィンドウを目的の位置にドラッグします。
- ウィンドウサイズを変更するには、[展開 (Expand)]  または [折りたたみ (Collapse)]  ボタンをクリックします。
- [別のウィンドウに切り離す (Undock Into Separate Window)]  ボタンをクリックすると、ウィンドウが Web ページから独自のブラウザウィンドウに切り離されます。再度ドッキングするには、[メインウィンドウにドッキング (Dock to Main Window)]  ボタンをクリックします。

- クリックしてドラッグすると、テキストが強調表示されます。次に Ctrl+C を押すと、出力がクリップボードにコピーされます。
- すべての出力を消去するには、[CLIのクリア (Clear CLI)] () ボタンをクリックします。
- [最後の出力のコピー (Copy Last Output)] () ボタンをクリックすると、最後に入力したコマンドからの出力がクリップボードにコピーされます。

ステップ 3 完了したら、コンソール ウィンドウを閉じます。 **exit** コマンドは使用しないでください。

Firepower Device Manager へのログインに使用するクレデンシャルにより CLI へのアクセスが検証されますが、コンソール使用時は実際には CLI にログインしていません。



第 2 章

Firepower Threat Defense の使用例

ここでは、Firepower Device Manager を使用して、Firepower Threat Defense で実行する共通のタスクについていくつか説明します。これらの使用例は、デバイス設定ウィザードが完了しており、この初期設定が保持されていることを前提としています。初期設定を変更した場合でも、これらの例を使用して、製品の使用方法を理解できます。

- [Firepower Device Manager でデバイスを設定する方法 \(51 ページ\)](#)
- [ネットワーク トラフィックを調べる方法 \(56 ページ\)](#)
- [脅威をブロックする方法 \(65 ページ\)](#)
- [マルウェアをブロックする方法 \(72 ページ\)](#)
- [アクセプタブルユース ポリシー \(URL フィルタリング\) の実装方法 \(76 ページ\)](#)
- [アプリケーションの使用を制御する方法 \(81 ページ\)](#)
- [サブネットを追加する方法 \(85 ページ\)](#)
- [その他の例 \(92 ページ\)](#)

Firepower Device Manager でデバイスを設定する方法

セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- (ASA 5506-X および ISA 3000 を除く)。外部インターフェイスと内部インターフェイス。その他のデータ インターフェイスは設定されません。
- (ASA 5506-X、ISA 3000 のみ)。外部インターフェイスと、他のすべてのデータのインターフェイスが含まれる内部ブリッジグループ。
- 内部インターフェイスおよび外部インターフェイスのセキュリティゾーン。
- 内部から外部へのトラフィックをすべて信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスまたはブリッジグループで実行されている DHCP サーバ。

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

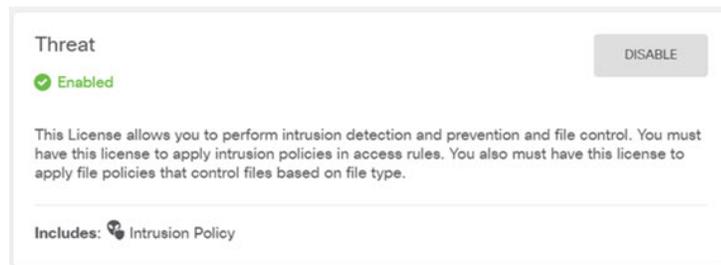
手順

ステップ 1 [デバイス (Device)] を選択し、[スマートライセンス (Smart License)] グループで [設定の表示 (View Configuration)] をクリックします。

使用するオプションのライセンス ([脅威 (Threat)], [マルウェア (Malware)], [URL]) でそれぞれ [有効化 (Enable)] をクリックします。必要かどうかわからない場合は、各ライセンスの説明を確認します。

登録していない場合は、このページから登録できます。[Request Register] をクリックして、説明に従います。評価ライセンスの有効期限が切れる前に登録してください。

たとえば、有効な脅威ライセンスは次のようになります。



ステップ 2 他のインターフェイスに接続している場合は、[デバイス (Device)] を選択し、[インターフェイス (Interfaces)] サマリーにあるリンクをクリック。

- ASA 5506-X および ISA 3000 は外部以外のすべてのデータ インターフェイスが含まれるブリッジグループが事前に設定された状態で出荷されるため、これらのインターフェイスを設定する必要はありません。ブリッジグループを分割する場合は、ブリッジグループを編集して個別に扱うインターフェイスを除去できます。その後、別々のネットワークをホストするインターフェイスとしてそれらを設定できます。

他のモデルでは、他のインターフェイスのブリッジグループを作成、別々のネットワークを設定、または両方の組み合わせを設定できます。

各インターフェイスの編集アイコン (🔗) をクリックして、IP アドレスなどの設定を定義します。

次の例では、Web サーバなどのパブリックアクセス可能な資産を配置する「非武装地帯」(DMZ) として使用するためのインターフェイスを構成します。完了したら [保存 (Save)] をクリックします。

Edit Physical Interface

Interface Name Status

dmz

Description

[IPv4 Address](#) [IPv6 Address](#) [Advanced Options](#)

Type

Static

IP Address and Subnet Mask

192.168.6.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

ステップ 3 新しいインターフェイスを構成する場合は、[オブジェクト (Objects)] を選択し、目次から[セキュリティゾーン (Security Zones)] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後は常にゾーン オブジェクトを編集する必要があります。

次の例では、DMZインターフェイスのために新しいDMZゾーンを作成する方法を示します。

Add Security Zone

Name

dmz-zone

Description

Interfaces

dmz

ステップ 4 内部クライアントが DHCP を使用してデバイスから IP アドレスを取得するようにする場合は、[デバイス (Device)]、次に [システム設定 (System Settings)] > [DHCP サーバ (DHCP Server)] を選択します。[DHCP サーバ (DHCP Servers)] タブを選択します。

すでに内部インターフェイス用に構成されている DHCP サーバがありますが、アドレス プールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上に DHCP サーバをセットアップするのがごく一般的です。各内部インターフェイスのサーバおよびアドレス プールを設定するには、[+] をクリックします。

クライアントに対して提供される WINS および DNS リストを [設定 (Configuration)] タブで調整することもできます。

次の例では、アドレス プールの 192.168.4.50 ~ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバを設定する方法を示しています。



ステップ 5 [[デバイス (Device)]] を選択し、次に [設定の表示 (View Configuration)] (または [最初のスタティックルートの作成 (Create First Static Route)]) を [ルーティング (Routing)] グループでクリックし、デフォルト ルートを設定します。

デフォルト ルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4 (0.0.0.0/0)、デフォルトの IPv6 ルートは任意の ipv6 (::0/0) です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルト ルートをすでに持っていることがあります。

このページで定義したルートは、データインターフェイス用のみです。管理インターフェイスには影響しません。管理ゲートウェイは [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で設定します。

次の例に、IPv4 のデフォルト ルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです (アドレスは ISP から取得する必要があります)。[ゲートウェイ (Gateway)] の下部の [新しいネットワークを作成する (Create New Network)] ドロップダウン リストをクリックしてこのオブジェクトを作成することができます。

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and values:

- Protocol:** IPv4 (selected), IPv6
- Gateway:** isp-gateway
- Interface:** outside
- Metric:** 1
- Networks:** any-ipv4

ステップ 6 [ポリシー (Policies)] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間でのトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーンオブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

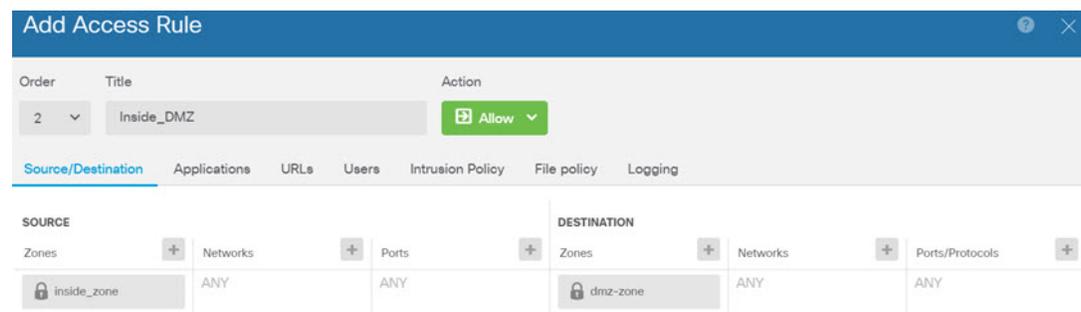
ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィック フローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

- [SSL 復号 (SSL Decryption)]: 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ (Identity)]: 個々のユーザにネットワーク アクティビティを関連付ける、またはユーザまたはユーザ グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティ ポリシーを使用します。
- [セキュリティインテリジェンス (Security Intelligence)]: ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンスポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。

- [NAT] (ネットワーク アドレス変換) : 内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御 (Access Control)]: ネットワーク上で許可する接続の決定にアクセスコントロールポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル (マルウェア) ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。
- [侵入 (Intrusion)]: 侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーン間のトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection)] が選択されている場合、[ロギング (Logging)] を除いて他のいずれのタブでもオプションは設定されません。



ステップ7 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

ネットワークトラフィックを調べる方法

デバイスの初期設定を完了すると、インターネットまたはその他のアップストリーム ネットワークへのすべての内部トラフィックアクセスを許可するアクセスコントロールポリシーと、他のすべてのトラフィックをブロックするデフォルトアクションが設定されます。追加のアクセスコントロールルールを作成する前に、ネットワークで実際に発生しているトラフィックを調べると役立ちます。

Firepower Device Manager のモニタリング機能を使用して、ネットワークトラフィックを分析できます。Firepower Device Manager のレポートの内容は、次のとおりです。

- ネットワークの用途
- 最も多くネットワークを使用しているユーザ
- ユーザの接続先
- ユーザが使用しているデバイス
- ヒット数が最も多いアクセスコントロールルール（ポリシー）

初期のアクセスルールでは、ポリシー、宛先、セキュリティゾーンなどのトラフィックについての情報が明らかになります。しかし、ユーザ情報を取得するには、ユーザを認証（識別）する必要があるアイデンティティポリシーの設定が必要です。ネットワークで使用されるアプリケーションの情報を取得するには、追加でいくつかの調整を行う必要があります。

次の手順で、トラフィックをモニタするように Firepower Threat Defense デバイスを設定する方法を説明し、設定ポリシーおよびモニタリングポリシーのエンドツーエンドプロセスの概要を示します。



- (注) この手順では、ユーザがアクセスしたサイトの Web サイトカテゴリとレピュテーションの情報は取得されないため、URL カテゴリダッシュボードに有用な情報は表示されません。カテゴリおよびレピュテーションのデータを取得するには、カテゴリベースの URL フィルタリングを実装し、URL ライセンスを有効化する必要があります。この情報のみ取得する場合は、許可するカテゴリ（金融サービスなど）へのアクセスを許可する新規のアクセス制御ルールを追加して、アクセス制御ポリシーで最初のルールに設定できます。URL フィルタリングの実装の詳細については、[アクセプタブルユースポリシー（URL フィルタリング）の実装方法（76 ページ）](#)を参照してください。

手順

- ステップ 1** ユーザの動作を調べるには、接続に関連付けられているユーザを識別するアイデンティティポリシーの設定が必要です。

アイデンティティポリシーを有効化すると、ネットワークを使用するユーザおよびそのユーザが使用しているリソースに関する情報を収集できます。この情報は、ユーザの監視ダッシュボードに表示されます。ユーザ情報は、イベントビューアに表示される接続イベントにも表示されます。

ユーザは、HTTP 接続に Web ブラウザを使用する場合にのみ認証されます。

ユーザが認証に失敗した場合でも、そのユーザは Web 接続を確立することはできます。これは、単に、接続に関するユーザのアイデンティティ情報がないことを意味します。必要に応じて、認証に失敗したユーザのトラフィックをドロップするアクセスコントロールルールを作成できます。

- a) メインメニューで、[ポリシー (Policies)] をクリックして、[アイデンティティ (Identity)] をクリックします。

アイデンティティポリシーは、最初は無効化されています。アイデンティティポリシーはアクティブディレクトリサーバを使用してユーザを認証し、ユーザが使用しているワークステーションの IP アドレスとユーザを関連付けます。その後、システムはその IP アドレスのトラフィックをユーザのトラフィックとして識別します。

- b) [アイデンティティポリシーの有効化 (Enable Identity Policy)] をクリックします。

このアクションで [アイデンティティポリシーの設定 (Identity Policy Configuration)] ダイアログボックスが開きます。

- c) [レルムサーバ (Realm Server)] をクリックしてドロップダウンリストを開き、[新規アイデンティティレルムの作成 (Create New Identity Realm)] を選択します。

レルムサーバオブジェクトをすでに作成している場合は、それを選択して、サーバの設定手順をスキップします。

- d) 次のフィールドに入力して、[OK] をクリックします。

- [名前 (Name)] : ディレクトリレルムの名前。
- [タイプ (Type)] : ディレクトリサーバのタイプ。サポートされるタイプは **Active Directory** のみで、このフィールドを変更することはできません。
- [ディレクトリユーザ名 (Directory Username)]、[ディレクトリパスワード (Directory Password)] : 取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格された特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は **Administrator@example.com** (Administrator だけでなく) などの完全修飾名である必要があります。

(注) この情報から `ldap-login-dn` と `ldap-login-password` が生成されます。たとえば、`Administrator@example.com` は `cn=adminisntrator,cn=users,dc=example,dc=com` に変換されます。 `cn=users` は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN (Base DN)] : ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリツリー。(`dc=example,dc=com` など)。ベース DN の検索の詳細については、[ディレクトリベースの DN の決定 \(148 ページ\)](#) を参照してください。
- [ADプライマリドメイン (AD Primary Domain)] : デバイスが参加する必要がある完全修飾 Active Directory ドメイン名。(`example.com` など)。
- [ホスト名/IPアドレス (Hostname/IP Address)] : ディレクトリサーバのホスト名または IP アドレス。サーバへの暗号化された接続を使用する場合、IP アドレスではなく完全修飾ドメイン名を入力する必要があります。

- [ポート (Port)] : サーバとの通信に使用するポート番号。デフォルトは389です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化 (Encryption)] : ユーザおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法 ([STARTTLS] または [LDAPS]) を選択します。デフォルトでは [なし (None)] になっており、ユーザおよびグループの情報がクリアテキストでダウンロードされます。
 - [STARTTLS] では、暗号化方式をネゴシエートし、ディレクトリサーバでサポートされる最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモートアクセス VPN にレルムを使用する場合はサポートされません。
 - [LDAPS] では、LDAP over SSL が必要です。ポート 636 を使用します。
- [信頼できるCA証明書 (Trusted CA Certificate)] : 暗号化方式を選択する場合、認証局 (CA) の証明書をアップロードして、システムとディレクトリサーバの間で信頼できる接続を有効化します。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス (Hostname/IP Address)] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

例 :

たとえば、次のイメージには、ad.example.com サーバの暗号化されていない接続の作成方法が示されています。プライマリドメインは example.com で、ディレクトリユーザ名は Administrator@ad.example.com です。すべてのユーザおよびグループの情報は、識別名 (DN) ou=user,dc=example,dc=com の下にあります。

Name	Type
AD	Active Directory (AD) ▼
Directory Username	Directory Password
Administrator@ad.example.com
<i>e.g. user@example.com</i>	
Base DN	AD Primary Domain
ou=user,dc=example,dc=com	example.com
<i>e.g. ou=user, dc=example, dc=com</i>	<i>e.g. example.com</i>

Directory Server Configuration

Hostname / IP Address	Port
ad.example.com	389
<i>e.g. ad.example.com</i>	
Encryption	Trusted CA certificate
NONE ▼	Please select a certificate ▼

- e) [アイデンティティポリシーの設定 (Identity Policy Configuration)] ダイアログボックスの [レルムサーバ (Realm Server)] リストで、作成したレルムサーバを選択します。
- f) [アイデンティティポリシーの設定 (Identity Policy Configuration)] ダイアログボックスで、アクティブ認証のキャプティブポータル設定を行います。

アイデンティティルールにユーザのアクティブ認証が必要な場合、ユーザは接続されているインターフェイスのキャプティブポータルポートにリダイレクトされ、その後、認証を要求されます。

- [サーバ証明書 (Server Certificate)] : アクティブ認証時にユーザに提示する内部証明書を選択します。事前定義された自己署名の DefaultInternalCertificate を選択するか、[新規内部証明書の作成 (Create New Internal Certificate)] をクリックして、ブラウザが信頼している証明書をアップロードできます。

ブラウザが信頼している証明書をアップロードしない場合、ユーザは証明書を許可する必要があります。

- [ポート (Port)] : キャプティブポータルポート。デフォルトは885 (TCP) です。別のポートを設定する場合は、1025 ~ 65535 の範囲にする必要があります。

例 :

[アイデンティティポリシーの設定 (Identity Policy Configuration)] ダイアログは、次のようになります。

Identity Policy Configuration

Realm Server

AD

ACTIVE AUTHENTICATION

Server Certificate

DefaultInternalCertificate

Port

885

e.g. 885 or 1025-65535

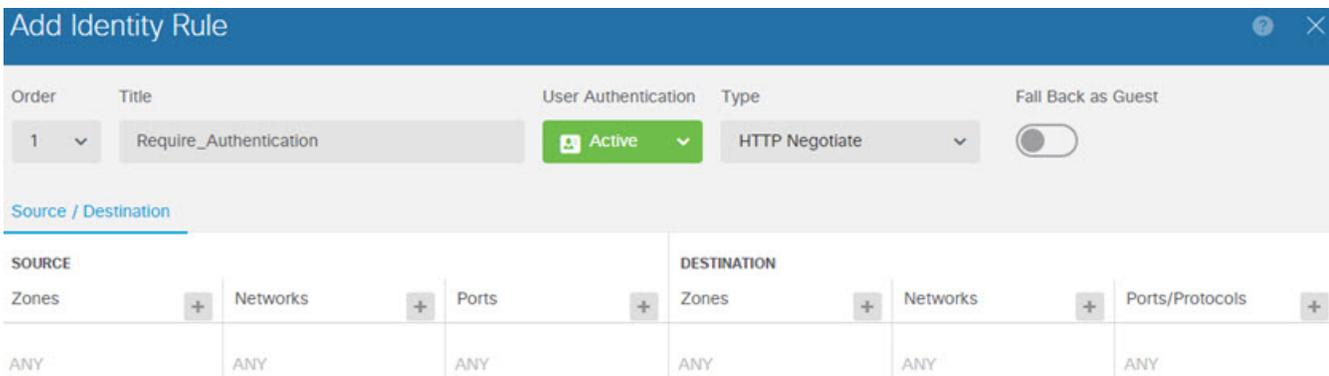
CANCEL SAVE

- g) [保存 (Save)] をクリックします。
- 次に、アクティブ認証に必要なルールを作成します。
- h) [アイデンティティルールの作成 (Create Identity Rule)] ボタンをクリックするか、[+] ボタンをクリックします。
- i) アイデンティティルールのプロパティを入力します。
- 全員を認証する必要があることを前提として、次の設定を使用できます。
- [名前 (Name)] : 任意の選択 (Require_Authentication など) 。
 - [ユーザ認証 (User Authentication)] : [アクティブ (Active)] が選択されているため、そのままにします。
 - [タイプ (Type)] : [HTTP ネゴシエート (HTTP Negotiate)] を選択します。これにより、ブラウザおよびディレクトリサーバは最も強力な認証プロトコルを、NTLM、HTTP ベーシックの順にネゴシエートできます。

(注) HTTP Basic、HTTP 応答ページ、および NTLM 認証方式では、ユーザはインターフェイスの IP アドレスを使用してキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名 `firewall-hostname.AD-domain-name` を使用してリダイレクトされます。HTTP ネゴシエートを使用する場合、アクティブ認証を必要としているすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要があります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。DNS サーバを更新できない、または更新を望まない場合は、その他の認証方式のいずれかを選択します。

- [送信元/宛先 (Source/Destination)] : すべてのフィールドをデフォルトの [すべて (Any)] のままにします。

より制限されているトラフィックに合わせて、ポリシーに制約を加えることができます。ただし、アクティブ認証は HTTP トラフィックに対してのみ試行されるため、非 HTTP トラフィックが送信元/宛先条件に一致していることは重要ではありません。アイデンティティポリシーのプロパティの詳細については、[アイデンティティルールの設定 \(235 ページ\)](#) を参照してください。



- j) [OK] をクリックしてルールを追加します。

ウィンドウの右上を見ると、[展開 (Deploy)] アイコン ボタンにドットが表示されていることがあります。これは、展開されていない変更があることを示します。ユーザインターフェイスを変更するだけでは、デバイスに変更を設定するには不十分です。変更を展開する必要があります。部分的に設定された変更がデバイスで実行される潜在的な問題を避けるために、一連の関連する変更を加えてから変更を展開できます。この手順で、後から変更を展開します。



ステップ 2 Inside_Outside_Rule アクセス コントロール ルールのアクションを [許可 (Allow)] に変更します。

Inside_Outside_Rule アクセスルールは、信頼できるルールとして作成されます。ただし、信頼できるトラフィックのインスペクションは実行されないため、トラフィック一致基準にアプリ

ケーションやその他の条件（ゾーン、IPアドレス、およびポートを除く）が含まれない場合、システムは信頼できるトラフィックの一部の特性（アプリケーションなど）を学習できません。信頼できるトラフィックではなく許可にルールを変更すると、システムはすべてのトラフィックのインスペクションを実行します。

(注) (ASA 5506-X、ISA 3000)。また、`Inside_Inside_Rule` を [信頼性 (Trust)] から [許可 (Allow)] に変更することも検討してください。このルールは、内部インターフェイス間を移動するトラフィックに対応しています。

- [ポリシー (Policies)] ページの [アクセスコントロール (Access Control)] をクリックします。
- `Inside_Outside_Rule` 行の右側にある [アクション (Actions)] セルにマウスを合わせると、[編集 (edit)] アイコンと [削除 (delete)] アイコンが表示されます。ルールを開くには、[編集 (edit)] アイコン (🔍) をクリックします。
- [アクション (Action)] の [許可 (Allow)] を選択します。



- [OK] をクリックして変更を保存します。

ステップ3 アクセスコントロールポリシーのデフォルトアクションでロギングを有効化します。

接続のロギングが有効なアクセスコントロールルールと接続が一致する場合にのみ、ダッシュボードに接続情報が表示されます。`Inside_Outside_Rule` ではロギングが有効ですが、デフォルトアクションのロギングは無効化されています。そのため、ダッシュボードには `Inside_Outside_Rule` の情報のみが表示され、ルールと一致しない接続は反映されません。

- アクセスコントロールポリシー ページの下部のデフォルトアクションで、任意の場所をクリックします。



- [ログアクションの選択 (Select Log Action)] > [接続の開始時と終了時 (At Beginning and End of Connection)] を選択します。
- [OK] をクリックします。

ステップ4 脆弱性データベース (VDB) の更新スケジュールを設定します。

シスコはVDBの更新を定期的にリリースしています。これには、接続で使用されるアプリケーションを特定できるアプリケーションディテクタが含まれています。定期的にVDBを更新する必要があります。更新を手動でダウンロードするか、または定期的なスケジュールを設定できます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、VDBの更新は無効化されているため、VDBの更新を取得するには操作を実行する必要があります。

- [the name of the device in the menu] をクリックします。[デバイス (Device)]
- [更新 (Updates)] グループで [設定の表示 (View Configuration)] をクリックします。

Updates

[View Configuration](#) >

- c) [VDB] グループで [設定 (Configure)] をクリックします。

VDB 265.0

Configure
Set recurring VDB updates

UPDATE NOW

- d) 更新スケジュールを定義します。

ネットワークを妨害しない時間および頻度を選択します。また、更新をダウンロードすると、システムが自動的に展開することも理解しておいてください。これは、新しいディテクタを有効化するために必要です。そのため、実行して保存したが、展開していない設定変更も展開されます。

たとえば、次のスケジュールでは、VDB が週に 1 回、日曜日の午前 0:00 (24 時間方式を使用) に更新されます。

Set recurring VDB Update

Frequency

Weekly

Days of Week

Sundays *

Time

at 00 : 00

(-07:00) America/Los_Angeles

- e) [保存 (Save)] をクリックします。

ステップ 5 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックして、展開が完了するまで待ちます。

展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

Deployment Summary

DEPLOY NOW

You have successfully deployed.

Deployment History

Modified Objects	Initiated	Completed	Status
<ul style="list-style-type: none"> > AccessPolicy > AccessRule > ActiveDirectoryRealm > IdentityPolicy > IdentityRule 	11 May 2016 01:24:35 PM	11 May 2016 01:27:06 PM	✔ Deployed

次のタスク

この時点から、監視ダッシュボードおよびイベントにユーザおよびアプリケーションの情報が表示されます。望ましくないパターンがないかこの情報を評価し、許容できない使用を制限するための新しいアクセスルールを展開できます。

侵入およびマルウェアに関する情報の収集を開始する場合、1つまたは複数のアクセスルールで侵入ポリシーとファイルポリシーの有効化が必要です。また、これらの機能のライセンスも有効化する必要があります。

URL カテゴリに関する情報の収集を開始するには、URL フィルタリングを実装する必要があります。

脅威をブロックする方法

侵入ポリシーをアクセスコントロールルールに追加することによって、次世代侵入防御システム (IPS) のフィルタリングを実装できます。侵入ポリシーはネットワークトラフィックを分析して、トラフィックの内容を既知の脅威と比較します。接続がモニタリング中の脅威と一致した場合、システムはその接続をドロップして攻撃を阻止します。

その他すべてのトラフィックの処理は、ネットワークトラフィックに侵入の形跡がないかどうかを調べる前に実行されます。侵入ポリシーをアクセスコントロールルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシーを使用してトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを [許可 (allow)] するルールに侵入ポリシーを設定できます。インスペクションは、トラフィックを [信頼 (trust)] または [ブロック (block)] するよう設定されたルールでは実行されません。また、デフォルトアクションが [許可 (allow)] の場合、デフォルトアクションの一部として侵入ポリシーを設定できます。

Firepower システムには複数の侵入ポリシーが付属しています。これらのポリシーは Cisco Talos Intelligence Group (Talos) によって設計されており、侵入ルール、プリプロセッサルール状態、詳細設定が設定されています。

潜在的な侵入を許可するトラフィックの検査に加え、セキュリティインテリジェンスポリシーを使用することで、既知の不正 IP アドレスとのすべてのトラフィック、または既知の不正 URL へのすべてのトラフィックを先制的にブロックできます。

手順

ステップ 1 まだ有効化していない場合は、[脅威 (Threat)] ライセンスを有効化します。

侵入ポリシーおよびセキュリティインテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

- [the name of the device in the menu] をクリックします。[デバイス (Device)]
- [スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。



- [脅威 (Threat)] グループで [有効化 (Enable)] をクリックします。

必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化 (Disable)] ボタンに変わります。



ステップ 2 1 つまたは複数のアクセス ルールの侵入ポリシーを選択します。

脅威がないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside_Outside_Rule に侵入インスペクションを追加します。ASA 5506-X モデルでは、Inside_Inside_Rule に追加することもできます。

- メインメニューで [ポリシー (Policies)] をクリックします。

[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。

- b) Inside_Outside_Rule 行の右側にある [アクション (Actions)] セルにマウスを合わせると、[編集 (edit)] アイコンと [削除 (delete)] アイコンが表示されます。ルールを開くには、[編集 (edit)] アイコン (🔗) をクリックします。
- c) まだ選択していない場合は、[アクション (Action)] の [許可 (Allow)] を選択します。

Order	Title	Action
1	Inside_Outside_Rule	🔗 Allow

- d) [侵入ポリシー (Intrusion Policy)] タブをクリックします。
- e) [侵入ポリシー (Intrusion Policy)] トグルをクリックしてから、侵入ポリシーを選択します。

ポリシーは、安全性の低いものから高いものへの順で表示されています。[バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] ポリシーは、ほとんどのネットワークに適しています。ドロップしたくないトラフィックをドロップする可能性がある、過度に強力な防御ではなく、侵入に対する適切な防御を実現します。ドロップされるトラフィックが多すぎると判断した場合は、[セキュリティより接続を優先する (Connectivity over Security)] ポリシーを選択することによって侵入インスペクションを緩和できます。

セキュリティを強力にする必要がある場合は、[接続性よりもセキュリティを優先 (Security over Connectivity)] ポリシーを試します。[最大検出 (Maximum Detection)] ポリシーでは、ネットワークインフラストラクチャのセキュリティがよりいっそう重視され、動作にさらに大きな影響を及ぼす可能性があります。

Edit Access Rule

Order	Title	Action
1	Inside_Outside_Rule	🔗 Allow

Source/Destination Applications URLs Users **Intrusion Policy** File

INTRUSION POLICY

LEVEL OF INTRUSION POLICY

Balanced Security and Connectivity

BALANCED SECURITY AND CONNECTIVITY

This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.

f) [OK] をクリックして変更を保存します。

ステップ 3 侵入ルール データベースの更新スケジュールを設定します。

シスコは、接続をドロップするかどうかを決定する侵入ポリシーで使用される、侵入ルール データベースの更新を定期的リリースしています。ルールデータベースは定期的に更新する必要があります。更新は手動でダウンロードするか、定期的なスケジュールを設定できます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、データベースの更新は無効化されているため、更新されたルールを取得するには操作が必要です。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device)]
- b) [更新 (Updates)] グループで [設定の表示 (View Configuration)] をクリックします。

Updates

[View Configuration](#) >

- c) [ルール (Rule)] グループで [設定 (Configure)] をクリックします。

Rule

2016-03-28-001-vrt

[Configure](#)
Set recurring Rule updates

[UPDATE NOW](#)



- d) 更新スケジュールを定義します。

ネットワークを妨害しない時間および頻度を選択します。また、更新をダウンロードすると、システムが自動的に展開することも理解しておいてください。これは、新しいルールを有効化するために必要です。そのため、実行して保存したが、展開していない設定変更も展開されます。

たとえば、次のスケジュールでは、ルール データベースが週に 1 回、月曜日の午前 0:00 (24 時間方式を使用) に更新されます。

Set recurring Rule Update

Frequency

Weekly

Days of Week

Mondays *

Time

at 00 : 00

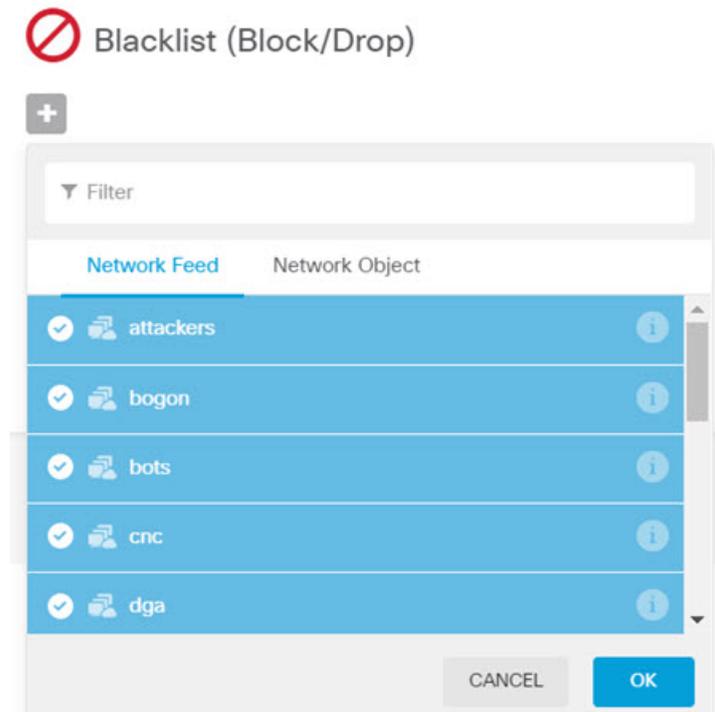
(-07:00) America/Los_Angeles

e) [保存 (Save)]をクリックします。

ステップ 4 既知の不正ホストやサイトとの接続を先制的にドロップするためのセキュリティインテリジェンス ポリシーを設定します。

セキュリティインテリジェンスを使用して、脅威だとわかっているホストやサイトとの接続をブロックすることで、接続ごとに脅威を特定するためのディープ パケット インスペクションに必要な時間を節約できます。セキュリティインテリジェンスにより、不必要なトラフィックを早期にブロックして、実際に関心があるトラフィックの処理により多くのシステム時間を残すことができます。

- [デバイス (Device)]をクリックし、[更新 (Updates)]グループで[設定の表示 (View Configuration)]をクリックします。
- [セキュリティインテリジェンスフィード (Security Intelligence Feeds)]グループで[今すぐ更新 (Update Now)]をクリックします。
- または、[設定 (Configure)] をクリックして、フィードの定期更新を設定します。デフォルトの [毎時 (Hourly)] はほとんどのネットワークに適していますが、必要に応じて頻度を減らすことができます。
- [ポリシー (Policies)] をクリックして、[セキュリティインテリジェンス (Security Intelligence)] ポリシーをクリックします。
- ポリシーをまだ有効化していない場合は、[セキュリティインテリジェンスの有効化 (Enable Security Intelligence)] をクリックします。
- [ネットワーク (Network)] タブで、[ブラックリスト (Blacklist)] の下にある [+] をクリックして、[ネットワークフィード (Network Feeds)] タブにあるすべてのフィードを選択します。フィードの横にある [i] ボタンをクリックして、各フィードの説明を確認できます。



フィードが存在しないというメッセージが表示される場合は、後でもう一度試してください。フィードのダウンロードはまだ完了していません。この問題が解決しない場合は、管理 IP アドレスとインターネット間にパスがあることを確認してください。

- g) [OK] をクリックして、選択したフィードを追加します。

他にも不正 IP アドレスがある場合は、[+] > [ネットワークオブジェクト (Network Objects)] をクリックして、それらのアドレスを含むオブジェクトを追加できます。リストの下部にある [新規ネットワークオブジェクトの作成 (Create New Network Object)] をクリックして、すぐに追加することもできます。

- h) [URL] タブをクリックし、[ブラックリスト (Blacklist)] の下にある [+] > [URL フィード (URL Feeds)] をクリックして、すべての URL フィードを選択します。[OK] をクリックして、それらをブラックリストに追加します。

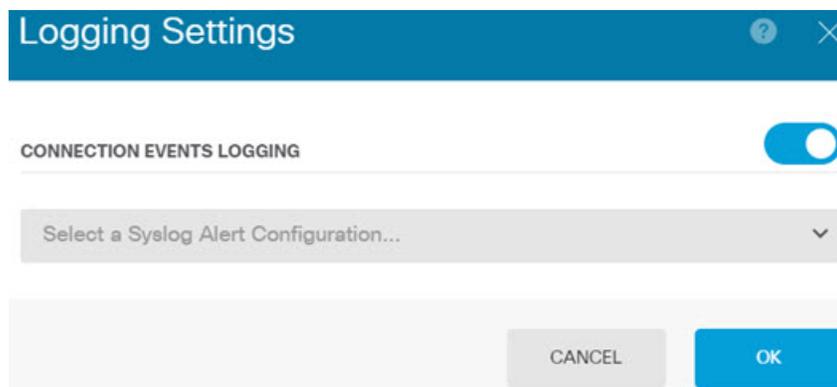
ネットワークリストと同様に、独自の URL オブジェクトをブラックリストに追加して、フィードに含まれていないその他のサイトをブロックできます。[+] > [URL オブジェクト (URL Objects)] をクリックします。リストの最後にある [新規 URL オブジェクトの作成 (Create New URL Object)] をクリックして、新しいオブジェクトを追加できます。

Blacklist (Block/Drop)



- i) [歯車 (gear)]アイコンをクリックし、[接続イベントロギング (Connection Events Logging)]を有効にして、一致した接続のセキュリティインテリジェンスイベントをポリシーが生成できるようにします。[OK] をクリックして変更を保存します。

接続ロギングを有効にしない場合、ポリシーが予想どおりに機能しているかどうかの評価に使用するためのデータを得られません。外部 syslog サーバを定義している場合は、ここで選択することで、そのサーバにもイベントを送信できます。



- j) 必要に応じて、各タブの [ブロックしない (Do Not Block)] リストにネットワーク オブジェクトまたは URL オブジェクトを追加して、ブラックリストに対する例外を作成できます。

[ブロックしない (Do Not Block)] リストは、ホワイトリストではなく、例外リストです。例外リストにあるアドレスや URL がブラックリストにも表示されている場合、そのアドレスや URL の接続はアクセスコントロールポリシーの通過を許可されます。フィードはこのようにしてブロックできますが、後で必要なアドレスやサイトがブロックされていることに気付いた場合は、例外リストを使用して、フィードを完全に削除することなく、そのブロックをオーバーライドできます。その後、それらの接続はアクセス制御、および侵入ポリシー (設定されている場合) によって評価される点に注意してください。

したがって、接続に脅威が含まれている場合は、侵入検査中に特定されてブロックされます。

[アクセスおよびSIルール (Access and SI Rules)]ダッシュボード、およびイベントビューアのセキュリティインテリジェンスビューアを使用して、ポリシーによって実際にドロップされているトラフィックを特定し、[ブロックしない (Do Not Block)]リストにアドレスや URL を追加する必要があるかどうかを決めます。

ステップ 5 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)]アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

次のタスク

この時点から、侵入が特定された場合は、監視ダッシュボードおよびイベントに攻撃者、ターゲット、および脅威に関する情報が表示されます。この情報を評価して、ネットワークにさらにセキュリティ対策が必要かどうか、または使用中の侵入ポリシーのレベルを下げる必要があるかどうかを決定できます。

セキュリティインテリジェンスの場合、[アクセスおよびSIルール (Access and SI Rules)]ダッシュボードでポリシーのヒット数を確認できます。セキュリティインテリジェンス イベントはイベントビューアでも確認できます。セキュリティインテリジェンスのブロック数は侵入の脅威情報には反映されません。これは、検査する前にトラフィックがブロックされるためです。

マルウェアをブロックする方法

ユーザは、インターネットサイトまたは電子メールなどのその他の通信方法から、悪意のあるソフトウェア (マルウェア) を取得する危険に常にさらされています。信頼できる Web サイトでも、乗っ取られて、無警戒なユーザにマルウェアを配布することがあります。Web ページには、別の送信元からのオブジェクトを含めることができます。このオブジェクトには、イメージ、実行可能ファイル、Javascript、広告などがあります。改ざんされた Web サイトには頻繁に、外部の送信元でホストされているオブジェクトが組み込まれます。真のセキュリティとは、最初の要求だけではなく、各オブジェクトを個別に調べることです。

Firepower の高度なマルウェア防御 (AMP for Firepower) を使用してマルウェアを検出するには、ファイルポリシーを使用します。ファイル制御を実行するファイルポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

AMP for Firepower は AMP クラウドを使用して、ネットワーク トラフィックで検出された潜在的なマルウェアの性質を取得します。AMP クラウドにアクセスし、マルウェア ルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドに問い合わせます。可能性のある性質は、[クリーン (clean)]、[マルウェア (malware)]、または [不明 (unknown)] (明確な判定を下せない) になります。AMP クラウドに到達できない場合、性質は [不明 (unknown)] になります。

ファイルポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、接続時にファイルのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを [許可 (allow)] するルールにファイル ポリシーを設定できます。インスペクションは、トラフィックを [信頼 (trust)] または [ブロック (block)] するよう設定されたルールでは実行されません。

手順

ステップ 1 まだ有効化していない場合は、[マルウェア (Malware)] ライセンスを有効化します。

マルウェア制御にファイル ポリシーを使用するには、マルウェア ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

- [the name of the device in the menu] をクリックします。[デバイス (Device)]
- [スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。



- [マルウェア (Malware)] グループで [有効化 (Enable)] をクリックします。

必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化 (Disable)] ボタンに変わります。



ステップ 2 1 つまたは複数のアクセス ルールのファイル ポリシーを選択します。

マルウェアがないかスキャンされるトラフィックに対応するルールを決定します。この例では、`Inside_Outside_Rule` にファイルインスペクションを追加します。ASA 5506-X モデルでは、`Inside_Inside_Rule` に追加することもできます。

- a) メインメニューで [ポリシー (Policies)] をクリックします。
[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。
- b) `Inside_Outside_Rule` 行の右側にある [アクション (Actions)] セルにマウスを合わせると、[編集 (edit)] アイコンと [削除 (delete)] アイコンが表示されます。ルールを開くには、[編集 (edit)] アイコン (🔍) をクリックします。
- c) まだ選択していない場合は、[アクション (Action)] の [許可 (Allow)] を選択します。

Order	Title	Action
1	Inside_Outside_Rule	Allow

- d) [ファイルポリシー (File Policy)] タブをクリックします。
- e) 使用するファイルポリシーをクリックします。

主な選択は、マルウェアと見なされるすべてのファイルをドロップする [マルウェアをすべてブロック (Block Malware All)]、または AMP クラウドにクエリしてファイルの性質を判断するがブロックはしない [クラウドをすべてルックアップ (Cloud Lookup All)] です。ファイルがどのように評価されるかを確認する場合は、クラウドルックアップを使用します。ファイルが評価される方法に納得したら、後でブロッキングポリシーに切り替えることができます。

他にも、マルウェアをブロックするために使用できるポリシーがあります。これらのポリシーは、ファイル制御や Microsoft Office、または Office および PDF ドキュメントのアップロードのブロックと関連しています。つまり、これらのポリシーを使用すると、マルウェアがブロックされるだけでなく、ユーザはこれらのファイルタイプを他のネットワークに送信できなくなります。ニーズに合う場合は、これらのポリシーを選択できます。

この例では、[マルウェアをすべてブロック (Block Malware All)] を選択します。

The screenshot shows the 'Edit Access Rule' interface. At the top, there's a blue header with the title 'Edit Access Rule'. Below it is a table with three columns: 'Order', 'Title', and 'Action'. The first row contains '1', 'Inside_Outside_Rule', and a green 'Allow' button. Underneath the table are several tabs: 'Source/Destination', 'Applications', 'URLs', 'Users', 'Intrusion Policy', and 'File policy'. The 'File policy' tab is active. Below the tabs, there's a section titled 'SELECT THE FILE POLICY' with a dropdown menu showing 'Block Malware All'. To the right of this section, there's a 'CONTROL' section with a checkbox and text: 'Use file pol Malware Pr policies to regardless'.

- f) [ロギング (Logging)] タブをクリックして、[ファイルイベント (File Events)] の下にある [ファイルのロギング (Log Files)] が選択されていることを確認します。

デフォルトでは、ファイルポリシーを選択するとファイルロギングは有効化されます。イベントおよびダッシュボードにファイルおよびマルウェア情報を表示するには、ファイルロギングを有効化が必要です。

FILE EVENTS

Log Files

- g) [OK] をクリックして変更を保存します。

ステップ 3 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスクステータスが [展開済み (Deployed)] になります。

次のタスク

この時点から、ファイルまたはマルウェアが送信される場合に、監視ダッシュボードおよびイベントにファイルタイプやファイルおよびマルウェアのイベントに関する情報が表示されます。この情報を評価し、ファイルの送信に関してネットワークにさらにセキュリティ対策が必要かどうかを決定できます。

アクセプタブルユース ポリシー (URL フィルタリング) の実装方法

ネットワークのアクセプタブルユース ポリシーを設定できます。アクセプタブルユース ポリシーは、組織で適切とされるネットワークアクティビティと、不適切とされるアクティビティを区別します。通常、これらのポリシーはインターネットの使用に注目し、生産性の維持、法的責任の回避（敵対的でない作業場所の維持など）、Web トラフィックの制御を目的としています。

URL フィルタリングを使用して、アクセス ポリシーと共にアクセプタブルユース ポリシーを定義できます。広範なカテゴリ（ジャンルなど）でフィルタリングできるため、ブロックする Web サイトを個別に識別する必要はありません。カテゴリの照合では、サイトの関連レピュテーションを指定して、許可またはブロックすることもできます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとする、セッションがブロックされます。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、脅威インテリジェンスは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して、要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と出没する可能性があります。

次の手順で、URL フィルタリングを使用してアクセプタブルユース ポリシーを実装する方法について説明します。この例では、複数のカテゴリのあらゆるレピュテーションのサイト、高リスクのソーシャルネットワーキングサイト、および未分類サイトである `badsite.example.com` をブロックします。

手順

ステップ 1 まだ有効化していない場合は、[URL] ライセンスを有効化します。

URL カテゴリとレピュテーションの情報を使用する場合、またはこれらの情報をダッシュボードとイベントに表示する場合には、URL ライセンスを有効にする必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device)]
- b) [スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。



- c) [URLライセンス (URL License)]グループの [有効化 (Enable)]をクリックします。
- 必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化 (Disable)] ボタンに変わります。



ステップ2 URL フィルタリングのアクセス コントロール ルールを作成します。

ブロッキングルールの作成前に、ユーザがアクセスしているサイトのカテゴリを最初に確認できます。その場合、許可するカテゴリ (金融サービスなど) に [許可 (Allow)] アクションを設定したルールを作成できます。すべての Web 接続のインスペクションを実行して、URL がこのカテゴリに属しているかどうかを判断する必要があるため、金融サービスサービス以外のサイトのカテゴリ情報も取得します。

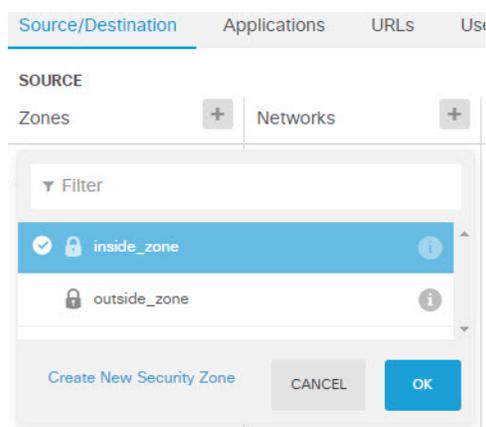
ただし、ブロック対象とすることがすでに判明している URL カテゴリが存在する場合があります。ブロッキングポリシーでもインスペクションが強制されるため、ブロックされるカテゴリだけでなく、ブロックされないカテゴリへの接続に関するカテゴリ情報も取得します。

- a) メインメニューで [ポリシー (Policies)] をクリックします。
- [アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。
- b) [+] をクリックして新しいルールを追加します。
- c) 順序、タイトル、およびアクションを設定します。
- [順序 (Order)] : デフォルトで、新しいルールはアクセスコントロールポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル内で最初に照合されるルールの1つのみです)。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセスコントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。
 - [タイトル (Title)] : ルールに Block_Web_Sites などの意味のある名前を付けます。
 - [アクション (Action)] : [ブロック (Block)] を選択します。

Order	Title	Action
1	Block_Web_Sites	Block

- d) [送信元/接続先 (Source/Destination)] タブで、[送信元 (Source)] > [ゾーン (Zones)] の [+] をクリックし、[inside_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。

条件の追加も同じ方法です。 [+] をクリックすると小さいダイアログボックスが開くため、追加する項目をクリックします。複数の項目をクリックできます。選択した項目をクリックすると選択が解除されます。チェックマークは、選択済みの項目を示します。ただし、 [OK (OK)] ボタンをクリックするまでポリシーには何も追加されません。項目を選択するだけでは不十分です。

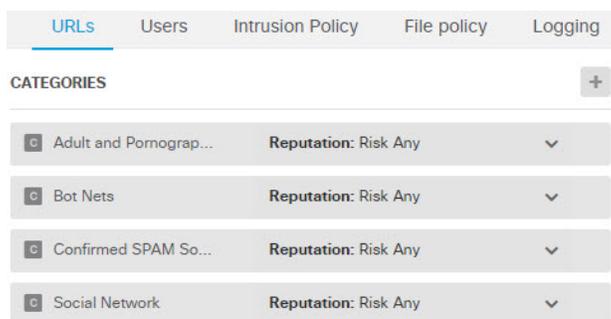


- e) 同じ技術を使用して、[接続先 (Destination)] > [ゾーン (Zones)] で [outside_zone] を選択します。

Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
SOURCE			DESTINATION			
Zones	Networks	Ports	Zones			
inside_zone	ANY	ANY	outside_zone			

- f) [URLs] タブをクリックします。
 g) [カテゴリ (Categories)] の [+] をクリックして、完全または部分的にブロックするカテゴリを選択します。

この例では、[アダルトおよびポルノ (Adult and Pornography)]、[ボットネット (Bot Nets)]、[確認済みのスパム送信元 (Confirmed SPAM Sources)]、および[ソーシャルネットワーク (Social Network)] を選択します。ブロックすることが必要な可能性が高い追加カテゴリがあります。



- h) レピュテーションに影響されるブロッキングを [ソーシャルネットワーク (Social Network)] カテゴリに実装するには、そのカテゴリの [レピュテーション: すべてのリスク (Reputation: Risk Any)] をクリックして、[すべて (Any)] の選択を解除してからスライダを [セキュリティリスクがある無害なサイト (Benign sites with security risks)] に移動します。閉じるには、スライダをクリックします。



レピュテーションスライダの左側は許可されるサイトを示し、右側はブロックされるサイトを示します。この場合、レピュテーションが [疑わしいサイト (Suspicious Sites)] と [高リスク (High Risk)] の範囲内にあるソーシャル ネットワーキング サイトのみがブロックされます。したがって、ユーザは、リスクの少ない、一般的に使用されるソーシャル ネットワーキング サイトにはアクセスできます。

レピュテーションを使用すると、別の方法で許可したカテゴリ内のサイトを選択的にブロックできます。

- i) カテゴリ リストの左側にある [URLS] リストの横の [+] をクリックします。
- j) ポップアップダイアログボックスの下部で、[新規URLの作成 (Create New URL)] リンクをクリックします。
- k) 名前と URL の両方に「badsite.example.com」と入力して、[追加 (Add)]、[OK] の順にクリックしてオブジェクトを作成します。

オブジェクトに URL と同じ名前を付けるか、またはオブジェクトに別の名前を付けることができます。URL には、URL のプロトコル部分を含めず、サーバ名のみを追加します。

New URL Object

Name
badsite.example.com

Description

URL
badsite.example.com

- l) 新規オブジェクトを選択して、[OK] をクリックします。

ポリシーの編集時に新規オブジェクトを追加するだけで、リストにオブジェクトが追加されます。新規オブジェクトは、自動的に選択されません。

Order	Title	Action
1	Block_Web_Sites	Block

Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
URLS		CATEGORIES				
badsite.example.com		Adult and Pornograp...	Reputation: Risk Any			
		Bot Nets	Reputation: Risk Any			
		Confirmed SPAM So...	Reputation: Risk Any			
		Social Network	Reputation: Benign sites with sec...			

- m) [ロギング (Logging)] タブをクリックして、[ログアクションの選択 (Select Log Action)] > [接続の開始時と終了時 (At Beginning and End of Connection)] を選択します。

Web カテゴリ ダッシュボードおよび接続イベントにカテゴリおよびレピュテーションの情報を表示するには、ロギングを有効化する必要があります。

- n) [OK] をクリックしてルールを保存します。

ステップ 3 (オプション) URL フィルタリングを設定します。

URL ライセンスが有効化されている場合、システムは Web カテゴリ データベースへの更新を自動的に有効化します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。何らかの理由で更新を希望しない場合は、更新をオフにできます。

また、分類されていない URL を分析のためにシスコに送信するよう選択することもできます。したがって、インストールされている URL データベースにはサイトのカテゴリがなく、Cisco CSI にカテゴリが含まれていることがあります。Cisco CSI からカテゴリとレピュテーションが返されると、カテゴリベースのルールを URL 要求に正しく適用できます。メモリ制限により

インストールされる URL データベースが小さいローエンドのシステムでは、このオプションを選択することが重要です。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device)]
- b) [システム設定 (System Settings)] > [トラフィック設定 (Traffic Settings)] > [URL フィルタリングの設定 (URL Filtering Preferences)] をクリックします。
- c) [未知の URL 用 Cisco CSI のクエリー (Query Cisco CSI for Unknown URLs)] を選択します。
- d) [保存 (Save)] をクリックします。

ステップ 4 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

次のタスク

この時点で、URL カテゴリとレピュテーション、およびドロップされた接続に関する情報が監視ダッシュボードとイベントに表示され始めます。この情報を評価して、URL フィルタリングによって好ましくないサイトのみがドロップされているかどうか、または特定カテゴリのレピュテーション設定を緩和する必要があるかどうかを判断できます。

分類およびレピュテーションに基づいて Web サイトへのアクセスをブロックすることを、ユーザに事前に通知することについて検討します。

アプリケーションの使用を制御する方法

ブラウザ ベースのアプリケーション プラットフォームか、企業ネットワークの内部および外部で転送として Web プロトコルを使用するリッチ メディア アプリケーションかにかかわらず、Web は企業内でアプリケーションを配信するユビキタス プラットフォームになっています。

Firepower Threat Defense では、接続のインスペクションを実行して、使用するアプリケーションを決定します。これにより、特定の TCP/UDP ポートをターゲットにするのではなく、アプリケーションをターゲットとしたアクセスコントロールルールを記述できるようになります。したがって、Web ベース アプリケーションが同じポートを使用している場合でも、それらを選択的にブロックまたは許可できます。

特定のアプリケーションを許可またはブロックするよう選択できますが、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性に基づいてルールを記述することもできます。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロック

する、アクセスコントロールルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとする、セッションがブロックされます。

シスコは、システムおよび脆弱性データベース (VDB) の更新を通じて頻繁にアプリケーションディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

この使用例では、[アノマイザー/プロキシ (anonymizer/proxy)] カテゴリに属するアプリケーションをブロックします。

始める前に

この使用例では、使用例 [ネットワークトラフィックを調べる方法 \(56 ページ\)](#) を完了していることを前提としています。その使用例では、[アプリケーション (Applications)] ダッシュボードで分析できる、アプリケーションの使用状況に関する情報を取得する方法について説明しています。実際に使用されているアプリケーションを理解することで、効率的なアプリケーションベースのルールを設計できます。また、その使用例では、VDB の更新をスケジュールする方法についても説明しています (ここでは繰り返しません)。アプリケーションを正しく識別できるように、定期的に VDB を更新してください。

手順

ステップ 1 アプリケーションベースのアクセスコントロールルールを作成します。

- a) メインメニューで [ポリシー (Policies)] をクリックします。

[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。

- b) [+] をクリックして新しいルールを追加します。
- c) 順序、タイトル、およびアクションを設定します。

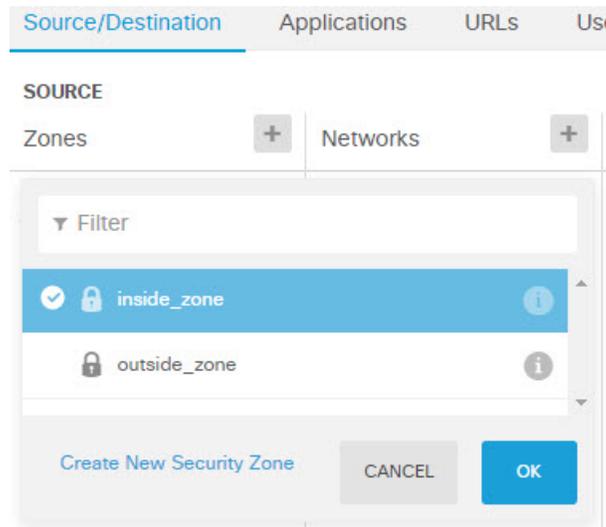
- [順序 (Order)] : デフォルトで、新しいルールはアクセスコントロールポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです)。このルールでは、デバイスの初期設定時に作成した `Inside_Outside_Rule` と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセスコントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。

- [タイトル (Title)] : ルールに `Block_Anonymizers` などの意味のある名前を付けます。

- [アクション (Action)] : [ブロック (Block)] を選択します。

Order	Title	Action
1	Block_Anonymizers	Block

- d) [送信元/接続先 (Source/Destination)] タブで、[送信元 (Source)] > [ゾーン (Zones)] の [+] をクリックし、[inside_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。



- e) 同じ技術を使用して、[接続先 (Destination)] > [ゾーン (Zones)] で [outside_zone] を選択します。

Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
<p>SOURCE</p> <p>Zones + Networks +</p> <p>inside_zone ANY ANY</p>					<p>DESTINATION</p> <p>Zones +</p> <p>outside_zone</p>	

- f) [アプリケーション (Applications)] タブをクリックします。
g) [アプリケーション (Applications)] の [+] をクリックして、ポップアップダイアログボックスの下部にある [高度なフィルタ (Advanced Filter)] リンクをクリックします。

事前にアプリケーションフィルタオブジェクトを作成して、ここの [アプリケーションフィルタ (Application Filters)] リストで選択できますが、アクセスコントロールルールで条件を直接指定して、オプションで条件をフィルタオブジェクトとして保存することもできます。単一のアプリケーションにルールを記述していない場合は、[高度なフィルタ (Advanced Filter)] ダイアログボックスを使用して、より簡単にアプリケーションを検索して適切な条件を生成できます。

条件を選択すると、ダイアログボックスの下部にある [アプリケーション (Applications)] リストが更新され、条件に一致するアプリケーションが表示されます。記述したルールは、これらのアプリケーションに適用されます。

このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、Facebook および TFPT は非常に高リスクに分類されています。ほとんどの組織は、これらのアプリケーションをブロックすることを希望しません。さまざまなフィルタ条件を試して、選択に一致するアプリケーションを確認するには時間がかかります。これらのリストは VDB の更新で変更できることを覚えておいてください。

この例では、[カテゴリ (Categories)] リストからアノニマイザー/プロキシを選択します。

Filter Applications ? RESET FILTER

Risks: Any

Business Relevance: Any

Types: Any

Categories: 1 selected ×

- Search Categories
- anonymizer/proxy
- mobile application
- VoIP
- web services provider
- e-commerce

Tags: Any selected

- Search Tags
- displays ads
- not work related
- high bandwidth
- file sharing/transfer
- share media

Filter the list of applications 33 Applications

Application	Description
<input checked="" type="checkbox"/> All applications that match the filters (33)	
<input type="checkbox"/> ASProxy	ASProxy open-source web proxy
<input type="checkbox"/> After School	Anonymous messaging app.
<input type="checkbox"/> Avocent	Registered with IANA on port 1078 tcp/udp.
<input type="checkbox"/> Avoidr	Web based proxy compatible with many popular social networking sites.

- h) [高度なフィルタ (Advanced Filters)] ダイアログボックスで、[追加 (Add)] をクリックします。

フィルタが追加され、[アプリケーション (Applications)] タブに表示されます。

Source/Destination **Applications** URLs Users Intrusion Policy

APPLICATIONS SAVE AS FILTER +

Categories: anonymizer/proxy

- i) [ロギング (Logging)] タブをクリックして、[ログアクションの選択 (Select Log Action)] > [接続の開始時と終了時 (At Beginning and End of Connection)] を選択します。

このルールによってブロックされる接続の情報を取得するには、ロギングを有効化する必要があります。

- j) [OK] をクリックしてルールを保存します。

ステップ 2 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

ステップ 3 [モニタリング (Monitoring)] をクリックして、結果を評価します。

これで、[ネットワークの概要 (Network Overview)] ダッシュボードのアプリケーション ウィジェットにドロップされた接続が表示されます。[すべて (All)]/[拒否 (Denied)]/[許可 (Allowed)] ドロップダウン オプションを使用して、ドロップされたアプリケーションのみに焦点を当てます。

アプリケーションに関する情報は、[Webアプリケーション (Web Applications)] ダッシュボードで検索することもできます。[アプリケーション (Applications)] ダッシュボードにプロトコル関連の結果が表示されます。これらのアプリケーションを使用しようとするユーザがいる場合、アイデンティティ ポリシーが有効で認証が必要なことを前提として、接続を試行しているユーザとアプリケーションを関連付けることができます。

サブネットを追加する方法

デバイスに使用可能なインターフェイスがある場合、スイッチ（または別のルータ）に接続して、別のサブネットにサービスを提供できます。

サブネットを追加する潜在的な理由は多数あります。この使用例では、次の一般的なシナリオに対処します。

- サブネットは、プライベート ネットワーク 192.168.2.0/24 を使用する内部ネットワークです。
- ネットワークのインターフェイスには、スタティック アドレス 192.168.2.1 があります。この例では、物理インターフェイスはこのネットワーク専用です。別の方法では、すでに接続されているインターフェイスを使用して、新しいネットワークのサブインターフェイスを作成します。

- デバイスは、DHCPを使用してネットワーク上のワークステーションにアドレスを提供します。アドレスプールとして 192.168.2.2 ~ 192.168.2.254 を使用します。
- 他の内部ネットワークおよび外部ネットワークへのネットワークアクセスは、許可されず。外部ネットワークに移動するトラフィックでは、NAT を使用してパブリックアドレスを取得します。



(注) この例では、ブリッジグループに未使用のインターフェイスは含まれていないことを前提としています。現在、未使用のインターフェイスがブリッジグループメンバーである場合、次の手順に進む前にこれをブリッジグループから削除する必要があります。

始める前に

ネットワークケーブルを新しいサブネットのインターフェイスおよびスイッチに物理的に接続します。

手順

ステップ1 インターフェイスを設定します。

- a) [デバイス (Device)] をクリックしてから、[インターフェイス (Interface)] サマリーにあるリンクをクリックします。
- b) 接続しているインターフェイスの行の右側にある [アクション (Actions)] セルにマウスを合わせて、[編集 (edit)] アイコン (🔍) をクリックします。
- c) 基本的なインターフェイスのプロパティを設定します。
 - [名前 (Name)] : インターフェイスに固有の名前 ([Inside_2] など)。
 - [ステータス (Status)] : ステータストグルをクリックして、インターフェイスを有効化します。
 - [IPv4アドレス (IPv4 Address)] タブ : [タイプ (Type)] に [スタティック (Static)] を選択して、[192.168.2.1/24] を入力します。

Edit Physical Interface

Interface Name: Status:

Description:

IPv4 Address IPv6 Address Advanced Options

Type: IP Address and Subnet Mask: /

- d) [保存 (Save)] をクリックします。

インターフェイス リストに、更新されたインターフェイス ステータスと設定された IP アドレスが表示されます。

GigabitEthernet1/3	inside_2	<input checked="" type="checkbox"/>	192.168.2.1	STATIC
--------------------	----------	-------------------------------------	-------------	--------

ステップ 2 インターフェイスの DHCP サーバを設定します。

- [the name of the device in the menu] をクリックします。[デバイス (Device)]
- [システム設定 (System Settings)] > [DHCPサーバ (DHCP Server)] をクリックします。
- [DHCPサーバ (DHCP Servers)] タブをクリックします。

表に、既存の DHCP サーバが表示されます。デフォルト設定を使用している場合、リストには内部インターフェイスのいずれかが含まれます。

- 表の上部の [+] をクリックします。
- サーバのプロパティを設定します。
 - [DHCPサーバの有効化 (Enable DHCP Server)] : このトグルをクリックして、サーバを有効化します。
 - [インターフェイス (Interface)] : DHCP サービスを提供しているインターフェイスを選択します。この例では、inside_2 を選択します。
 - [アドレスプール (Address Pool)] : サーバがネットワーク上のデバイスに供給できるアドレス。192.168.2.2 ~ 192.168.2.254 を入力します。ネットワークアドレス (.0) 、インターフェイスアドレス (.1) 、またはブロードキャストアドレス (.255) が含まれないようにしてください。また、ネットワーク上のデバイスにスタティックアドレスが必要な場合は、プールからそれらのアドレスを除外します。プールは単一の連続したアドレスである必要があるため、範囲の最初または最後からスタティックアドレスを選択します。

Add Server

Enabled DHCP Server

Interface

inside_2

Address Pool

192.168.2.2-192.168.2.254

e.g. 192.168.45.46-192.168.45.254

- f) [追加 (Add)] をクリックします。

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

ステップ3 内部セキュリティゾーンにインターフェイスを追加します。

インターフェイスにポリシーを記述するには、インターフェイスはセキュリティゾーンに属している必要があります。セキュリティゾーンのポリシーを記述します。そのため、ゾーンでインターフェイスを追加および削除すると、インターフェイスに適用されたポリシーは自動的に変更されます。

- メインメニューで [オブジェクト (Objects)] をクリックします。
- オブジェクトの目次から、[セキュリティゾーン (Security Zones)] を選択します。
- [inside_zone] オブジェクトの行の右側にある [アクション (Actions)] セルにマウスを合わせて、[編集 (edit)] アイコン (🔗) をクリックします。
- [インターフェイス (Interfaces)] の下にある [+] をクリックして、inside_2 インターフェイスを選択し、インターフェイスリストで [OK] をクリックします。

Interfaces

+

🔗 inside

🔗 inside_2

- e) [保存 (Save)] をクリックします。

Security Zones		
2 objects		
#	NAME	INTERFACES
1	inside_zone	inside, inside_2
2	outside_zone	outside

ステップ 4 内部ネットワーク間のトラフィックを許可するアクセス コントロール ルールを作成します。

トラフィックは、すべてのインターフェイス間で自動的に許可されません。希望のトラフィックを許可するには、アクセスコントロールルールを作成する必要があります。唯一の例外は、アクセスコントロールルールのデフォルトアクションでトラフィックを許可している場合です。この例では、デバイスのセットアップウィザードで設定したブロックのデフォルトアクションを保持していることを前提としています。したがって、内部インターフェイス間のトラフィックを許可するルールを作成する必要があります。このようなルールをすでに作成している場合は、この手順をスキップします。

a) メインメニューで [ポリシー (Policies)] をクリックします。

[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。

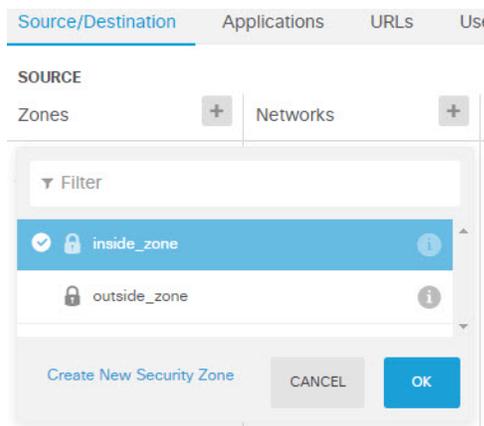
b) [+] をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

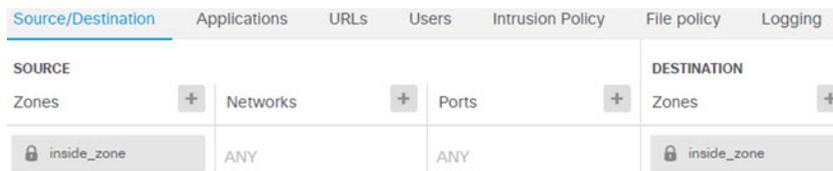
- [順序 (Order)] : デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです)。このルールでは、一意の送信元/宛先条件を使用するため、リストの最後にルールを追加できます。
- [タイトル (Title)] : ルールに Allow_Inside_Inside などの意味のある名前を付けます。
- [アクション (Action)] : [許可 (Allow)] を選択します。

Order	Title	Action
4	Allow_Inside_Inside	Allow

d) [送信元/宛先 (Source/Destination)] タブで、[送信元 (Source)] > [ゾーン (Zones)] の [+] をクリックし、[inside_zone] を選択してからゾーンのダイアログボックスで [OK] をクリックします。



- e) 同じ方法で、**[宛先 (Destination)]** > **[Zones (ゾーン)]** の **[inside_zone]** を選択します。送信元および宛先に同じゾーンを選択するには、セキュリティゾーンに2つ以上のインターフェイスが含まれている必要があります。



- f) (オプション) 侵入およびマルウェアのインスペクションを設定します。
- 内部インターフェイスは信頼できるゾーン内にありますが、一般的に、ユーザはラップトップをネットワークに接続します。そのため、ユーザは、外部ネットワークまたは Wi-Fi ホットスポットからネットワーク内に、知らないうちに脅威を持ち込んでいます。したがって、内部ネットワーク間を移動するトラフィックに侵入やマルウェアの形跡がないかスキャンが必要な場合があります。
- 次の操作の実行を検討します。
- **[侵入ポリシー (Intrusion Policy)]** タブをクリックして侵入ポリシーを有効化し、スライダを使用して **[バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)]** ポリシーを選択します。
 - **[ファイルポリシー (File Policy)]** タブをクリックして、**[すべてのマルウェアをブロックする (Block Malware All)]** ポリシーを選択します。
- g) **[ロギング (Logging)]** タブをクリックして、**[ログアクションの選択 (Select Log Action)]** > **[接続の開始時および終了時 (At Beginning and End of Connection)]** を選択します。
- このルールに一致する接続に関する情報を取得するには、ロギングを有効化する必要があります。ロギングによってダッシュボードにスタティックが追加され、イベントビューアにイベントが表示されます。
- h) **[OK]** をクリックしてルールを保存します。

ステップ 5 新規サブネットに必要なポリシーが定義されていることを確認します。

inside_zone セキュリティゾーンにインターフェイスを追加することによって、inside_zone の既存のポリシーが自動的に新規サブネットに適用されます。ただし、ポリシーのインスペクションには時間がかかるため、ポリシーの追加が必要ないことを確認します。

デバイスの初期設定を完了すると、次のポリシーがすでに適用されています。

- [アクセスコントロール (Access Control)] : Inside_Outside_Rule は、新規サブネットと外部ネットワーク間のすべてのトラフィックを許可します。以前の使用例に従っている場合、ポリシーによって侵入およびマルウェアのインスペクションも提供されます。新規ネットワークと外部ネットワークの間の一部のトラフィックを許可するルールが必要です。このルールがなければ、ユーザはインターネットや他の外部ネットワークにアクセスできません。
- [NAT] : InsideOutsideNATrule は、外部インターフェイスに対するすべてのインターフェイスに適用され、インターフェイス PAT が適用されます。このルールを守っている場合、新規ネットワークから外部に移動するトラフィックの IP アドレスは、外部インターフェイスの IP アドレスの一意のポートに変換されます。すべてのインターフェイスまたは inside_zone インターフェイスに適用されるルールがない場合、外部インターフェイスに移動するときに新しいルールの作成が必要になる場合があります。
- [アイデンティティ (Identity)] : デフォルトのアイデンティティポリシーはありません。ただし、以前の使用例に従っている場合、新規ネットワークの認証に必要なアイデンティティポリシーがある可能性があります。適用されるアイデンティティポリシーがなく、新規ネットワークのユーザベース情報が必要な場合は、新しいポリシーを作成します。

ステップ 6 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスクステータスが [展開済み (Deployed)] になります。

次のタスク

新規サブネットのワークステーションが DHCP を使用して IP アドレスを取得していることと、そのワークステーションが他の内部ネットワークおよび外部ネットワークに到達できることを確認します。監視ダッシュボードおよびイベントビューアを使用して、ネットワークの使用状況を評価します。

その他の例

使用例の章の例に加えて、特定のサービスについて説明している一部の章で設定例が示されています。場合によっては次の例が役立つ可能性があります。

Network Address Translation (NAT)

IPv4 アドレス用の NAT

- 内部 Web サーバへのアクセスの提供 (スタティック自動 NAT) (356 ページ)
- FTP、HTTP、および SMTP の単一アドレス (ポート変換を設定したスタティック自動 NAT) (359 ページ)
- 宛先に応じて異なる変換 (ダイナミック手動 PAT) (366 ページ)
- 宛先アドレスおよびポートに応じて異なる変換 (ダイナミック手動 PAT) (371 ページ)
- DNS 応答修正：外部の DNS サーバ (384 ページ)
- DNS 応答修正：ホスト ネットワーク上の DNS サーバ (388 ページ)
- NAT からのサイト間 VPN トラフィックの除外 (415 ページ)

IPv6 アドレス用の NAT

- NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット (342 ページ)
- NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク (344 ページ)
- NAT66 の例：ネットワーク間のスタティック変換 (350 ページ)
- NAT66 の例：シンプルな IPv6 インターフェイス PAT (352 ページ)
- DNS 64 応答修正 (378 ページ)

リモート アクセス仮想プライベート ネットワーク (RA VPN)

- 外部インターフェイスでリモート アクセス VPN ユーザにインターネットアクセスを提供する方法 (ヘア ピニング) (446 ページ)
- リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバを使用する方法 (453 ページ)

サイト間仮想プライベート ネットワーク (VPN)

- NAT からのサイト間 VPN トラフィックの除外 (415 ページ)
- 外部インターフェイスで外部のサイト間 VPN ユーザにインターネットアクセスを提供する方法 (ヘア ピニング) (422 ページ)

SSL/TLS の復号

- [例：ネットワークからの古い SSL/TLS バージョンのブロック \(227 ページ\)](#)

FlexConfig ポリシー (FlexConfig Policy)

- [グローバル デフォルト インспекションを有効/無効にする方法 \(547 ページ\)](#)
- [FlexConfig の変更を元に戻す方法 \(553 ページ\)](#)
- [一意のトラフィック クラスのインспекションを有効にする方法 \(555 ページ\)](#)



第 3 章

システムのライセンス

ここでは、Firepower Threat Defense デバイスにライセンスを付与する方法について説明します。

- [Firepower システムのスマートライセンス \(95 ページ\)](#)
- [スマートライセンスの管理 \(99 ページ\)](#)

Firepower システムのスマートライセンス

Cisco Smart Licensing によって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー (PAK) ライセンスとは異なり、スマートライセンスは特定のシリアル番号またはライセンスキーに関連付けられません。スマートライセンスを使用すると、ライセンスの使用状況と要件をひと目で確認できます。

また、スマートライセンスでは、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

Cisco Smart Software Manager

Firepower Threat Defense デバイスの1つ以上のライセンスを購入する場合は、Cisco Smart Software Manager (<https://software.cisco.com/#SmartLicensing-Inventory>) で管理します。Cisco Smart Software Manager では、組織のマスターアカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、たとえば、地域、部門、または子会社ごとに、追加の仮想アカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびアプライアンスの管理を行うことができます。

ライセンスとアプライアンスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのアプライアンスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。また、仮想アカウント間でのアプライアンスの譲渡も可能です。

Cisco Smart Software Manager にデバイスを登録するとき、そのマネージャで製品インスタンス登録トークンを作成し、Firepower Device Manager にそのトークンを入力します。登録済みデバイスが、使用されているトークンに基づいて仮想アカウントに関連付けられます。

Cisco Smart Software Manager の詳細については、マネージャのオンラインヘルプを参照してください。

ライセンス認証局との定期通信

Firepower Threat Defense デバイスの登録に製品インスタンス登録トークンを使用すると、デバイスはシスコのライセンス認証局に登録されます。ライセンス認証局は、デバイスとライセンス認証局の間の通信用に ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 ヶ月ごとに更新されます。ID 証明書の期限が切れた場合（通常は、9 ヶ月または 1 年間通信がない状態）、デバイスは登録が解除された状態になり、ライセンスされた機能は使用停止になります。

デバイスは、定期的にライセンス認証局と通信します。Cisco Smart Software Manager に変更を加えた場合は、すぐに変更が有効になるようにデバイス上で認証を更新できます。また、スケジュールどおりにデバイスが通信するのを待つこともできます。通常のライセンス通信は 30 日ごとに行われますが、これには猶予期間があり、デバイスはホームをコールすることなく最大で 90 日間は動作します。90 日が経過する前にライセンス認証局と連絡を取る必要があります。

スマートライセンスのタイプ

次の表に、Firepower Threat Defense デバイスで使用可能なライセンスを示します。

Firepower Threat Defense デバイスを購入すると、自動的に基本ライセンスが含まれます。すべての追加ライセンスはオプションです。



(注) ISA 3000 デバイス用のマルウェアや URL フィルタリングのライセンスを購入することはできません。

表 3: スマートライセンスのタイプ

ライセンス	期間	付与される機能
基本 (Base) (自動的に含まれる)	永久	<p>オプションのターム ライセンスでカバーされないすべての機能。</p> <p>[このトークンに登録した製品でエクスポート制御機能を許可する (Allow export-controlled functionality on the products registered with this token)]かどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。</p>
脅威 (Threat)	ターム ベース	<p>[侵入検知および防御 (Intrusion detection and prevention)]: 侵入ポリシーが侵入とエクスプロイトを検出するためネットワークトラフィックを分析し、またオプションで違反パケットをドロップします。</p> <p>[ファイル制御 (File control)]: ファイルポリシーが特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード (送信) またはダウンロード (受信) をブロックできます。マルウェア ライセンスが必要な AMP for Firepower を使用すると、マルウェアを含むファイルのインスペクションを実行してブロックできます。どのタイプのファイルポリシーを使用する場合でも、脅威ライセンスが必要です。</p> <p>[セキュリティ インテリジェンス フィルタ (Security Intelligence filtering)]: トラフィックがアクセス制御ルールによって分析を受ける前に、選択されたトラフィックをドロップします。ダイナミック フィールドにより、最新の情報に基づいて接続をただちにドロップできます。</p>

ライセンス	期間	付与される機能
マルウェア (Malware)	ターム ベース	マルウェアを確認するポリシーであり、Cisco Advanced Malware Protection (AMP) と一緒に AMP for Firepower (ネットワークベースの高度なマルウェア保護) と Cisco Threat Grid を使用します。 ファイル ポリシーは、ネットワーク上で伝送されるファイルに存在するマルウェアを検出してブロックできます。
URL フィルタリング (URL Filtering)	ターム ベース	カテゴリとレピュテーションに基づく URL フィルタリング。 このライセンスなしでも、個々の URL で URL フィルタリングを実行できます。
RA VPN : <ul style="list-style-type: none"> • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only 	ライセンスタイプに基づきタームベースまたは永久	リモートアクセス VPN の設定。RA VPN を設定するには、基本ライセンスによるエクスポート制御機能を許可する必要があります。デバイスを登録するときに、エクスポート要件を満たすかどうかを選択します。 Firepower Device Manager は、AnyConnect の任意の有効なライセンスを使用できます。使用できる機能はライセンスタイプによって異なります。まだ購入していない場合は、 リモートアクセス VPN のライセンス要件 (432 ページ) を参照してください。 『Cisco AnyConnect Ordering Guide』 (http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf) も参照してください。

期限切れまたは無効なオプションライセンスの影響

オプションのライセンスが期限切れになっても、そのライセンスを必要とする機能を使用し続けることはできます。ただし、ライセンスは非準拠とマークされます。ライセンスを準拠状態に戻すには、ライセンスを購入してアカウントに追加する必要があります。

オプションのライセンスを無効にすると、システムは次のように反応します。

- [マルウェアライセンス (Malware license)]: システムは AMP クラウドへの問い合わせを停止し、AMP レトロスペクティブクラウドから送信されたレトロスペクティブイベントの認証も停止します。既存のアクセス コントロール ポリシーにマルウェア検出を適応するファイル ポリシーが含まれている場合、このアクセス コントロール ポリシーを再展開

することはできません。マルウェアライセンスが無効にされた後、システムが既存のキャッシュファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは **Unavailable** という性質をこれらのファイルに割り当てます。

- [脅威 (Threat)] : システムは侵入またはファイル制御ポリシーを適用しなくなります。セキュリティインテリジェンス ポリシーの場合、システムはこのポリシーを適用せず、フィード更新のダウンロードを停止します。ライセンスを必要とする既存のポリシーを再展開することはできません。
- [URLフィルタリング (URL Filtering)] : URL カテゴリ条件が指定されたアクセスコントロールルールはURLのフィルタリングをただちに停止し、システムはURLデータへの更新をダウンロードしなくなります。既存のアクセスコントロールポリシーに、カテゴリベースまたはレピュテーションベースのURL条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。
- [RA VPN] : リモートアクセスVPN設定は編集できませんが、削除は可能です。ユーザは引き続きRAVPN設定を使用して接続できます。ただし、デバイスの登録を変更してシステムがエクスポートに準拠しなくなると、リモートアクセスVPN設定はただちに停止し、リモートユーザはVPNに接続できなくなります。

スマートライセンスの管理

システムの現在のライセンスステータスを表示するには、[スマートライセンス (SmartLicense)] ページを使用します。システムにはライセンスが必要です。

このページには、90日間の評価ライセンスを使用しているかどうか、またはCisco Smart Software Managerに登録済みかどうかが表示されます。登録すると、Cisco Smart Software Managerへの接続のステータス、および各ライセンスタイプのステータスを確認できます。

使用認証により、スマートライセンスエージェントのステータスが特定されます。

- 承認済み (「接続/接続中」、「十分なライセンス」) : デバイスは、アプライアンスのライセンス権限を承認した License Authority に正常に登録されています。このデバイスはインコンプライアンスの状態です。
- アウトオブコンプライアンス : デバイスで使用可能なライセンス権限がありません。ライセンスされた機能は動作を継続します。ただし、インコンプライアンスにするためには、追加の権限を購入するか、または解放する必要があります。
- 認証期限切れ : デバイスは90日以上ライセンス認証局と通信していません。ライセンスされた機能は動作を継続します。この状態の場合、スマートライセンスエージェントは認証要求を再試行します。再試行に成功すると、エージェントはアウトオブコンプライアンスまたは承認済み状態になり、新たな承認期間が始まります。手動でデバイスの同期を試みます。



- (注) スマートライセンスのステータスの横にある [i] ボタンをクリックすると、バーチャルアカウント、輸出管理機能を確認でき、Cisco Smart Software Manager を開くリンクが表示されます。輸出管理機能により、国家安全保障、外交ポリシー、反テロリズム法令を対象としたソフトウェアが制御されます。

次の手順では、システムライセンスの管理方法の概要について説明します。

手順

ステップ 1 [デバイス (Device)] をクリックし、[スマートライセンス (Smart License)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

ステップ 2 デバイスを登録します。

オプションライセンスを割り当てる前に、Cisco Smart Software Manager に登録する必要があります。評価期間の終了前に登録してください。

[デバイスの登録 \(100 ページ\)](#) を参照してください。

- (注) 登録する際に、使用状況データをシスコに送信するかどうかを選択します。選択内容は、[歯車 (gear)] アイコンの横にある [Cisco Success Network にアクセス (Go To Cisco Success Network)] リンクをクリックすると変更できます。

ステップ 3 オプション機能のライセンスをリクエストして管理します。

ライセンスによって制御される機能を使用するためには、オプションライセンスを登録する必要があります。[オプションライセンスの有効化と無効化 \(101 ページ\)](#) を参照してください。

ステップ 4 システムライセンスを維持します。

次の作業を実行できます。

- [Cisco Smart Software Manager との同期 \(102 ページ\)](#)
- [デバイスの登録解除 \(103 ページ\)](#)

デバイスの登録

Firepower Threat Defense デバイスを購入すると、自動的に基本ライセンスが付いてきます。基本ライセンスは、オプションライセンスではカバーされないすべての機能をカバーしています。これは永久ライセンスです。

システムの初期設定時に、Cisco Smart Software Manager にデバイスを登録するように求められます。登録せずに 90 日間の評価ライセンスを使用する場合、評価期間の終了前にデバイスを登録する必要があります。

デバイスを登録すると、バーチャルアカウントからデバイスにライセンスが割り当てられます。デバイスを登録すると、有効にしているすべてのオプションライセンスも登録されます。

手順

ステップ 1 [デバイス (Device)] をクリックし、[スマートライセンス (Smart License)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

ステップ 2 [Request Register] をクリックして、説明に従います。

- a) リンクをクリックして [Cisco Smart Software Manager](#) を開いて自分のアカウントにログインするか、必要に応じて新しいアカウントを作成します。
- b) 新しいトークンを生成します。

トークンを作成する際に、トークンの有効使用期間を指定します。推奨の有効期間は 30 日です。この期間はトークン自体の有効期限を定義するものであるため、トークンを使用して登録するデバイスには影響しません。使用前にトークンが期限切れになった場合は、簡単に新しいトークンを生成できます。

[このトークンに登録した製品でエクスポート制御機能を許可する (Allow export-controlled functionality on the products registered with this token)] かどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。

- c) トークンをコピーして、[スマートライセンスの登録 (Smart License Registration)] ダイアログボックスの編集ボックスに貼り付けます。
- d) 使用状況データをシスコに送信するかどうかを決定します。

Cisco Success Network ステップの情報を読み、[サンプルデータ (Sample Data)] をクリックして収集された実際のデータへのリンクを表示して、[Cisco Success Network を有効にする (Enable Cisco Success Network)] オプションを選択したままにするかどうかを決定します。接続を有効にしていない場合でも、必要なときにクラウドサービスを有効にできるようにシスコクラウドサービスサーバに登録されます。

- e) [登録の要求 (Request Register)] をクリックします。

オプションライセンスの有効化と無効化

オプションのライセンスを有効化 (登録) または無効化 (リリース) できます。ライセンスによって制御される機能を使用するには、ライセンスを有効にする必要があります。

オプションのタームライセンスの対象となる機能を使用しなくなった場合、ライセンスを無効化できます。ライセンスを無効にすると、Cisco Smart Software Manager アカウントでライセンスがリリースされるため、別のデバイスにそのライセンスを適用できるようになります。

評価モードで動作させる場合は、これらのライセンスの評価バージョンを有効にすることもできます。評価モードでは、デバイスを登録するまでライセンスは Cisco Smart Software Manager

に登録されません。ただし、評価モードではRA VPNライセンスを有効にすることはできません。

始める前に

ライセンスを無効にする前に、そのライセンスが使用中でないことを確認します。ライセンスを必要とするポリシーは書き換えるか削除します。

手順

ステップ 1 [デバイス (Device)] をクリックし、[スマートライセンス (Smart License)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

ステップ 2 必要に応じて、それぞれのオプションライセンスの [有効化/無効化 (Enable/Disable)] コントロールをクリックします。

- [有効化 (Enable)] : Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化 (Disable)] : Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。

ステップ 3 RA VPNライセンスを有効にしている場合、アカウントで使用可能なライセンスタイプを選択します。

AnyConnectの任意のライセンス ([Plus]、[Apex]、[VPNのみ (VPN Only)]) を使用できます。両方のライセンスがあり、どちらも使用する場合は [PlusおよびApex (Plus and Apex)] を選択できます。

Cisco Smart Software Manager との同期

ライセンス情報は、定期的に Cisco Smart Software Manager と同期されます。通常のライセンスに関する通信は 30 日ごとに行われますが、これには猶予期間があり、アップライアンスはホームをコールすることなく最大で 90 日間は動作します。

しかし、Smart Software Manager に変更を加えた場合は、デバイス上で認証を更新し、即座に変更を有効にできます。

同期により、ライセンスの現在のステータスが取得され、認証と ID 証明書が更新されます。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[スマートライセンス (Smart License)] のサマリーで [設定の表示 (View Configuration)] をクリックします。
- ステップ 2** 歯車のドロップダウンリストから [接続の再同期 (Resync Connection)] を選択します。
-

デバイスの登録解除

デバイスを使用しなくなった場合は、Cisco Smart Software Manager からデバイスの登録を解除できます。登録を解除すると、仮想アカウントでデバイスに関連付けられている基本ライセンスとすべてのオプションライセンスが解放されます。オプションライセンスは他のデバイスに割り当てることができます。

デバイスの登録を解除すると、デバイスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[スマートライセンス (Smart License)] のサマリーで [設定の表示 (View Configuration)] をクリックします。
- ステップ 2** 歯車ドロップダウンリストから [Unregister Device] を選択します。
- ステップ 3** 警告を確認し、デバイスの登録を本当に解除する場合は [登録解除 (Unregister)] をクリックします。
-



第 4 章

デバイスのモニタリング

システムには、デバイスとデバイスを通過するトラフィックをモニタするために使用できるダッシュボードとイベントビューアが含まれています。

- [トラフィック統計情報を取得するためにロギングを有効にする \(105 ページ\)](#)
- [トラフィックのモニタリングおよびシステムダッシュボード \(109 ページ\)](#)
- [コマンドラインを使用したその他の統計情報のモニタリング \(112 ページ\)](#)
- [イベントの表示 \(113 ページ\)](#)

トラフィック統計情報を取得するためにロギングを有効にする

モニタリングダッシュボードおよびイベントビューアを使用して、幅広いトラフィック統計をモニタできます。ただし、どの統計情報を収集すべきかシステムに知らせるためにロギングを有効にする必要があります。ロギングでは、システムを通過する接続に対して有用な情報を提供するさまざまな種類のイベントを生成します。

ここでは、イベントおよび提供される情報について、特に接続ロギングに重点を置いて詳しく説明します。

イベントタイプ

システムでは、以下のタイプのイベントが生成されます。監視ダッシュボードで関連する統計を表示するには、これらのイベントを生成する必要があります。

接続イベント

ユーザが生成するトラフィックがシステムを通過する場合、この接続に対してイベントを生成できます。これらのイベントを生成するには、アクセスルールで接続ロギングを有効にします。また、セキュリティインテリジェンスポリシーおよびSSL復号ルールでロギングを有効にすると、接続イベントを生成できます。

接続イベントには接続に関する幅広い種類の情報が含まれ、これには送信元と宛先の IP アドレスおよびポート、使用された URL およびアプリケーション、送信されたバイト数

またはパケット数などがあります。この情報には、実行されたアクション（接続の許可またはブロックなど）、接続に適用されたポリシーも含まれます。

侵入イベント

システムは、ネットワークを通過するパケットを検査し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある、悪意のあるアクティビティについて調べます。システムは潜在的な侵入を識別すると、侵入イベントを生成します。これには、エクスプロイトの日時とタイプ、攻撃とそのターゲットについての状況説明が記録されます。侵入イベントは、アクセス制御ルールのロギング設定に関係なく、ブロックまたはアラートするように設定された侵入ルールに対して生成されます。

ファイル イベント

ファイル イベントは、作成したファイル ポリシーに基づき、ネットワーク トラフィック内でシステムによって検出（オプションとしてブロック）されたファイルを表します。これらのイベントを生成するには、ファイル ポリシーを適用するアクセスルールに対してファイル ロギングを有効にする必要があります。

システムはファイル イベントを生成する場合、基になったアクセス コントロール ルールのロギング設定にかかわらず、関連する接続の終了についても記録します。

マルウェア イベント

システムは、全体的なアクセスコントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。AMP for Firepower は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキストデータを含むマルウェア イベントを生成できます。これらのイベントを生成するには、ファイル ポリシーを適用するアクセスルールに対してファイル ロギングを有効にする必要があります。

ファイルの判定結果は、正常からマルウェア、マルウェアから正常などに変更できます。AMP for Firepower が AMP クラウドにファイルについて照会し、クエリから 1 週間以内に判定結果が変更されたことがクラウドに特定されると、システムはレトロスペクティブマルウェア イベントを生成します。

セキュリティ インテリジェンス イベント

セキュリティ インテリジェンス イベントは、ポリシーによってブラックリストに登録（ブロック）またはモニタされた各接続の、セキュリティ インテリジェンス ポリシーによって生成された接続イベントの一種です。すべてのセキュリティ インテリジェンス イベントには、自動入力された [セキュリティ インテリジェンス カテゴリ (Security Intelligence Category)] フィールドがあります。

これらのイベントのそれぞれについて、対応する「通常」の接続イベントがあります。セキュリティ インテリジェンス ポリシーはアクセスコントロールなどのその他多数のセキュリティ ポリシーより前に評価されるため、セキュリティ インテリジェンスによって接続がブロックされると、その結果のイベントには、以降の評価から収集される情報（ユーザ アイデンティティなど）は含まれません。

設定可能な接続ロギング

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。生成するイベントの数を抑え、パフォーマンスを向上させることが目標である場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワークトラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。

システムは1つの接続をさまざまな理由でロギングすることがあるため、1ヵ所でロギングを無効にしても、一致する接続がロギングされないとは限りません。

接続ロギングは次の場所で設定できます。

- **アクセス制御ルールおよびデフォルトアクション**：接続終了時点のロギングは、接続に関するほとんどの情報を提供します。接続の開始も記録できますが、これらのイベントの情報は不完全です。接続ロギングはデフォルトで無効になっているため、追跡するトラフィックを対象とする各ルール（およびデフォルトのアクション）でこれを有効にする必要があります。
- **セキュリティインテリジェンスポリシー**：ブラックリストに登録された接続ごとにセキュリティインテリジェンス接続イベントを生成するようにロギングを有効にできます。セキュリティインテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティインテリジェンスイベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析できます。
- **SSL 復号ルールとデフォルトのアクション**：接続の最後にロギングを設定できます。ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセスコントロールルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

自動接続ロギング

他のロギング設定に関係なく、次の接続終了イベントは自動的に保存されます。

- システムは、接続がアクセスコントロールポリシーのデフォルトのアクションで処理される限り、侵入イベントに関連付けられている接続を自動的に記録します。一致するトラフィックの侵入イベントを取得するには、デフォルトアクションでロギングを有効にする必要があります。
- システムは、ファイルイベントとマルウェアイベントに関連付けられた接続を自動的にログに記録します。接続イベントのみ：必要に応じてファイルおよびマルウェアイベントの生成を無効にできます。

接続ロギングのためのヒント

ロギング設定および関連する統計情報の評価を検討する際は、次のヒントに注目してください。

- アクセスコントロールルールでトラフィックを許可すると、関連付けられた侵入ポリシーまたはファイルポリシー（またはその両方）を使用して、トラフィックをさらに検査し、トラフィックが最終宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアをブロックできます。ただし、暗号化されたペイロードに対するファイルインスペクションと侵入インスペクションはデフォルトで無効になっていることに注意してください。侵入またはファイルポリシーが接続をブロックする理由を発見した場合、接続ログ設定を問わず、システムは接続終了イベントをただちにログに記録します。ロギングが許可された接続は、ネットワーク内のトラフィックのほとんどの統計情報を提供します。
- 信頼されている接続は、信頼アクセスコントロールルールまたはアクセスコントロールポリシーのデフォルトアクションによって処理される接続です。ただし、信頼されている接続では、ディスクバリエータ、侵入、または禁止されたファイルやマルウェアがインスペクションされません。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。
- トラフィックをブロックするアクセスコントロールルールおよびアクセスコントロールポリシーのデフォルトアクションの場合は、システムは接続開始イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。
- サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システムパフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロックルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

外部の Syslog サーバへのイベントの送信

イベントを格納する容量が限られている、Firepower Device Manager を通してイベントを表示する以外に、外部の syslog サーバにイベントを送信するルールとポリシーを設定することもできます。この機能と、選択した syslog サーバプラットフォームの追加のストレージを使用して、イベントデータを表示および分析できます。

外部の syslog サーバにイベントを送信するには、各ルール、デフォルトのアクション、または接続のログ記録を有効にするポリシーを編集し、ログ設定の syslog サーバオブジェクトを選択します。syslog サーバに侵入イベントを送信するには、侵入ポリシー設定でサーバを設定する必要があります。

詳細については、各ルールとポリシーの種類に応じたヘルプおよび [Syslog サーバの設定（142 ページ）](#) を参照してください。

トラフィックのモニタリングおよびシステム ダッシュボード

システムには、デバイスを通過するトラフィックおよびセキュリティポリシーの結果を分析するために使用できる複数のダッシュボードがあります。ダッシュボード情報は、構成全体の有効性を評価し、ネットワークの問題を特定して解決するために使用します。



- (注) トラフィック関連のダッシュボードで使用されるデータは、接続またはファイルロギングを有効にするアクセス制御ルール、およびロギングを許可するその他のセキュリティポリシーから収集されます。ダッシュボードには、ロギングが有効になっていないルールと一致するトラフィックは反映されません。自分にとって重要な情報をログに記録するルールを設定してください。また、ユーザ情報はユーザ ID を収集するアイデンティティルールを設定している場合にのみ利用できます。最後に、侵入、ファイル、マルウェア、および URL カテゴリの情報を使用できます。ただし、これを使用できるのは、これらの機能に関するライセンスを所有しており、機能を使用するルールを設定している場合のみです。

手順

- ステップ 1** メインメニューの [モニタリング (Monitoring)] をクリックして、[ダッシュボード (Dashboards)] ページを開きます。

ダッシュボードのグラフと表に表示されるデータを制御するために、定義済みの時間範囲（最後の時間や週など）を選択できます。また、特定の開始時刻と終了時刻を指定してカスタムの時間範囲を定義することもできます。

トラフィック関連のダッシュボードには、次のタイプの表示が含まれます。

- 上位 5 つの棒グラフ：これらのグラフは [ネットワークの概要 (Network Overview)] ダッシュボードに表示されます。また、ダッシュボードテーブルで項目をクリックした場合、項目ごとのサマリーのダッシュボードにも表示されます。[トランザクション (Transactions)] または [データの使用状況 (Data Usage)] (送受信バイトの合計) のカウント間で情報を切り替えることができます。すべてのトランザクション、許可トランザクション、または拒否トランザクションを表示するために表示を切り替えることもできます。グラフと関連付けられている表を確認する場合は、[追加表示 (View More)] をクリックします。
- [テーブル (Tables)]：テーブルには、特定のタイプの項目（アプリケーションまたは URL カテゴリなど）およびその項目の合計トランザクション数、許可トランザクション数、ブロックトランザクション数、データ使用量、および送受信バイト数が表示されます。未加工の [値 (Values)] と [パーセンテージ (Percentages)] 間の数字は切り替えることができ、上位 10、100、または 1000 エントリが表示されます。項目がリンクの場合、そのリン

クをクリックして、より詳細な情報が含まれているサマリー ダッシュボードを表示します。

ステップ 2 目次にある [ダッシュボード (Dashboard)] リンクをクリックして、次のデータのダッシュボードを表示します。

- [ネットワークの概要 (Network Overview)] : ネットワークのトラフィックに関するサマリー情報を表示します。これには、一致したアクセスルール (ポリシー) 、トラフィックを開始したユーザ、接続で使用されたアプリケーション、一致した侵入シグネチャ、アクセスされた URL の URL カテゴリ、および最も頻繁に接続される宛先が含まれます。
- [ユーザ (Users)] : ネットワークの上位ユーザが表示されます。ユーザ情報を表示するには、アイデンティティ ポリシーを設定する必要があります。ユーザアイデンティティがない場合は、送信元 IP アドレスが含まれます。以下の特殊なエンティティが表示される場合があります。
 - [認証失敗 (Failed Authentication)] : ユーザは認証を求められましたが、最大許容試行回数内に有効なユーザ名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザのネットワークへのアクセスは妨げられませんが、これらのユーザのネットワークアクセスを制限するためのアクセスルールを記述できます。
 - [ゲスト (Guest)] : ゲストユーザは、これらのユーザをゲストと呼ぶようにアイデンティティルールが設定されている点を除き、認証失敗ユーザと同様です。ゲストユーザは認証を求められましたが、最大試行回数内に認証されることができませんでした。
 - [認証不要 (No Authentication Required)] : ユーザの接続が認証なしに指定されたアイデンティティルールに一致したため、ユーザは認証を求められませんでした。
 - [不明 (Unknown)] : IP アドレスのユーザマッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。
- [アプリケーション (Applications)] : ネットワークで使用されている上位アプリケーション (HTTP など) を示します。この情報は、インスペクションを実行済みの接続にのみ提供されます。接続は、「許可」ルールと一致するか、またはゾーン、アドレス、およびポート以外の基準を使用するブロックルールと一致するかどうかのインスペクションが実行されます。そのため、インスペクションが必要なルールにヒットする前に接続が信頼またはブロックされている場合、アプリケーション情報は使用できません。
- [Web アプリケーション (Web Applications)] : ネットワークで使用されている上位 Web アプリケーション (Google など) を示します。Web アプリケーション情報を収集するための条件は、アプリケーションダッシュボードの場合と同じです。
- [Web カテゴリ (Web Categories)] [URL カテゴリ (URL Categories)] : 参照する Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトのカテゴリ (ジャンルや教育機関など) を示します。この情報を入手するには、トラフィック一致基準として URL カテゴリを使用する少なくとも 1 つのアクセス制御ルールが存在する必要があります。情報は、ルールに一致するトラフィック、またはルールに一致するかどうかを判

断するためにインスペクションを実行する必要があるトラフィックに関してのみ提供されます。最初の Web カテゴリのアクセス コントロールルールよりも前にあるルールと一致する接続に関するカテゴリ（またはレピュテーション）情報は表示されません。

- [アクセスおよび SI ルール (Access And SI Rules)]: ネットワーク トラフィックで一致した上位アクセスルールおよびセキュリティ インテリジェンス ルールに相当するものを示します。
- [ゾーン (Zones)]: デバイスに入ってから出ていくトラフィックの上位セキュリティゾーンのペアを示します。
- [宛先 (Destinations)]: ネットワーク トラフィックの上位の宛先が表示されます。
- [攻撃者 (Attackers)]: 侵入イベントをトリガーする接続の送信元である上位の攻撃者が表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。
- [ターゲット (Targets)]: 攻撃の被害者である、侵入イベントの上位のターゲットが表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。
- [脅威 (Threats)] トリガーされた上位の侵入ルールが表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。
- [ファイルログ (File Logs)]: ネットワーク トラフィックで確認された上位のファイルタイプが表示されます。この情報を表示するには、アクセスルールにファイル ポリシーを設定する必要があります。
- [マルウェア (Malware)]: 上位マルウェアのアクションとディスポジションの組み合わせを示します。ドリルダウンして、関連付けられているファイル タイプの情報を参照できます。この情報を表示するには、アクセスルールにファイル ポリシーを設定する必要があります。
 - 可能なアクション: マルウェアクラウドルックアップ、ブロック、アーカイブブロック (暗号化)、検出、カスタム検出、クラウドルックアップのタイムアウト、マルウェア ホワイトリスト、マルウェア ブロック、アーカイブブロック (深さ超過)、カスタム検出ブロック、TID ブロック、アーカイブブロック (検査失敗)。
 - 可能なディスポジション: マルウェア、不明、クリーン、カスタム検出、使用不可。
- [SSL復号 (SSL Decryption)]: デバイスを経由した暗号化トラフィックとプレーンテキスト トラフィックの内訳、および SSL 復号ルールに従った暗号化トラフィックの復号方法の内訳を示します。
- [システム (System)]: インターフェイスとそのステータス (マウスをインターフェイスに合わせると IP アドレスが表示される)、全体的なシステムの平均スループット (最大 1 時間で 5 分間のバケット、より長い期間で 1 時間のバケット)、およびシステム イベント、CPU 使用率、メモリ使用率、ディスク使用率に関する概要情報の表示を含む、システムの全体図を示します。すべてのインターフェイスではなく特定のインターフェイスを表

示するように、スループットグラフを制限できます。インターフェイス関連の統計情報（スループットなど）には、サブインターフェイスは含まれません。

(注) [システム (System)] ダッシュボードに表示される情報は、全体的なシステムレベルの情報です。デバイスの CLI にログインすると、さまざまなコマンドを使用して詳細情報を確認できます。たとえば、**show cpu** および **show memory** コマンドには、他の詳細を示すパラメータが含まれますが、これらのダッシュボードには **show cpu system** および **show memory system** コマンドからのデータが表示されます。

ステップ 3 目次でこれらのリンクをクリックすることもできます。

- [イベント (Events)] : イベント発生時にイベントが表示する場合に選択します。個々のアクセスルールに関連する接続イベントを表示するには、それぞれのアクセスルールで接続のログギングを有効にする必要があります。また、セキュリティインテリジェンスポリシーおよび SSL 復号ルールでログギングを有効にして、セキュリティインテリジェンスイベントおよびその他の接続イベントデータを参照します。これらのイベントは、ユーザの接続の問題を解決するのに役立ちます。

コマンドラインを使用したその他の統計情報のモニタリング

Firepower Device Manager ダッシュボードには、デバイスを介して移動するトラフィックや一般的なシステム使用状況に関連するさまざまな統計情報が表示されます。ダッシュボードが対応していない領域に関する追加情報は、CLI コンソールを使用するか、またはデバイス CLI にログインすることで得られます ([CLI \(コマンドラインインターフェイス\) へのログイン \(15 ページ\)](#) を参照)。

CLI にはこうした統計情報を提供するためのさまざまな **show** コマンドが含まれます。CLI は一般的なトラブルシューティングにも使用することが可能で、**ping** および **traceroute** といったコマンドが含まれます。ほとんどの **show** コマンドには、統計情報を 0 にリセットする **clear** コマンドがあります。(CLI コンソールから統計情報をクリアすることはできません)

コマンドに関するドキュメントは、『[Cisco Firepower Threat Defense コマンドリファレンス](http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html)』 (http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) にあります。

たとえば、次のコマンドが役に立ちます。

- **show nat** は NAT ルールのヒット数を表示します。
- **show xlate** はアクティブな NAT 変換を表示します。
- **show conn** はデバイスを經由する現在の接続に関する情報を提供します。

- **show dhcpd** はインターフェイスで設定した DHCP サーバに関する情報を提供します。
- **show interface** は各インターフェイスの使用状況の統計情報を提供します。

イベントの表示

ロギングを有効にしたセキュリティポリシーによって生成されるイベントを表示できます。また、イベントは、トリガーされた侵入ポリシーとファイル ポリシーから生成されます。

イベント ビューア テーブルには、リアルタイムに生成されたイベントが示されます。新しいイベントが生成されると、古いイベントはテーブルから削除されます。

始める前に

特定のタイプのイベントが生成されるかどうかは、関連するポリシーに一致する接続に加えて、次の要素によって決まります。

- 接続イベント：アクセスルールは、接続ロギングを有効化する必要があります。また、セキュリティ インテリジェンス ポリシーおよび SSL 復号ルールで接続ロギングを有効にすることもできます。
- 侵入イベント：アクセス ルールは、侵入ポリシーを適用する必要があります。
- ファイルおよびマルウェア イベント：アクセスルールでファイルポリシーを適用し、ファイル ロギングを有効にする必要があります。
- セキュリティ インテリジェンス イベント：セキュリティ インテリジェンス ポリシーを有効にして設定し、ロギングを有効にする必要があります。

手順

ステップ 1 メイン メニューの [モニタリング (Monitoring)] をクリックします。

ステップ 2 コンテンツのテーブルから [イベント (Events)] を選択します。

イベントビューアでは、イベントのタイプに基づいてイベントがタブに分類されます。詳細については、[イベントタイプ \(105 ページ\)](#) を参照してください。

ステップ 3 表示するイベント タイプのタブをクリックします。

イベント リストでは、次の操作を実行できます。

- イベントをより簡単に検索、分析できるようにするために、新しいイベントの追加を停止するには、[一時停止 (Pause)] をクリックします。新しいイベントが表示されるようになるには、[再開 (Resume)] をクリックします。
- 新しいイベントの表示速度を制御するには、別のリフレッシュ レート (5、10、20、60 秒) を選択します。

- 必要なカラムを含むカスタム ビューを作成します。カスタム ビューを作成するには、タブバーの [+] ボタンをクリックするか、[カラムの追加/削除 (Add/Remove Columns)] をクリックします。事前設定されているタブは変更できないため、カラムを追加または削除すると新しいビューが作成されます。詳細については、[カスタムビューの設定 \(114 ページ\)](#) を参照してください。
- カラム幅を変更するには、カラムヘッダーの境界をクリックして、目的の幅までドラッグします。
- イベントに関する詳細情報を表示するには、イベントの上にカーソルを置き、[詳細の表示 (View Details)] をクリックします。イベントの各フィールドの説明については、[イベントフィールドの説明 \(117 ページ\)](#) を参照してください。

ステップ 4 必要な場合は、テーブルにフィルタを適用することで、さまざまなイベント属性に基づいて目的のイベントを見つけることができます。

新規フィルタを作成するには、ドロップダウンリストからアトミック要素を選択してフィルタを手動で入力し、フィルタの値を入力するか、フィルタリングの基準となる値を含むイベントテーブルのセルをクリックしてフィルタを作成します。同じカラムにある複数のセルをクリックして値の間に OR 条件を作成するか、異なるカラムにあるセルをクリックしてカラムの間に AND 条件を作成できます。セルをクリックしてフィルタを作成した場合は、得られたフィルタを編集して、適切に調整することもできます。フィルタの作成ルールの詳細については、[イベントのフィルタリング \(115 ページ\)](#) を参照してください。

フィルタを作成したら、次の操作を実行します。

- フィルタを適用してテーブルを更新し、フィルタと一致するイベントのみが表示されるようにするには、[フィルタ (Filter)] ボタンをクリックします。
- 適用したフィルタをすべてクリアして、フィルタリングされていない状態のテーブルに戻るには、[フィルタ (Filter)] ボックスの [フィルタのリセット (Reset Filters)] をクリックします。
- フィルタのいずれかのアトミック要素をクリアするには、要素の上にカーソルを置き、要素の [X] をクリックします。[フィルタ (Filter)] ボタンをクリックします。

カスタム ビューの設定

独自のカスタムビューを作成して、イベントの表示に必要なカラムが簡単に表示されるようにできます。また、事前定義ビューは編集または削除できませんが、カスタムビューは編集または削除できます。

手順

ステップ 1 [モニタリング (Monitoring)] > [イベント (Events)] を選択します。

ステップ2 次のいずれかを実行します。

- 既存のカスタム（または事前定義された）ビューに基づいて新規ビューを作成するには、そのビューのタブをクリックしてから、ビュータブの左側にある [+] ボタンをクリックします。
- 既存のカスタムビューを編集するには、そのビューのタブをクリックします。

(注) カスタムビューを削除するには、ビューのタブにある [X] ボタンをクリックします。削除すると、元に戻すことはできません。

ステップ3 右側のイベントテーブルの上にある [追加/削除カラム (Add/Remove Columns)] アイコンボタンをクリックし、選択したリストに、ビューに含めるカラムのみが含まれるようになるまで、カラムを選択または選択解除します。

使用可能な（ただし使用されていない）リストと選択されているリストの間で、カラムをクリックしてドラッグします。選択されているリスト内でカラムをクリックしてドラッグし、左から右に向かうテーブル内でのカラムの順番を変更することもできます。カラムについては、[イベントフィールドの説明（117 ページ）](#)を参照してください。

完了したら [OK] をクリックして、カラムの変更を保存します。

(注) 事前定義されたビューを表示しながらカラムの選択を変更すると、新規ビューが作成されます。

ステップ4 必要に応じてカラムのセパレータをクリックしてドラッグし、カラムの幅を変更します。

イベントのフィルタリング

複雑なフィルタを作成してイベントテーブルを制限し、現在関心のあるイベントのみが表示されるようにできます。次の手法を単独または組み合わせて使用して、フィルタを作成できます。

カラムのクリック

フィルタを作成する最も簡単な方法は、フィルタリングの基準となる値を含むイベントテーブルのセルをクリックすることです。セルをクリックすると、その値とフィールドの組み合わせに正しく定式化されているルールを使用して、[フィルタ (Filter)] フィールドが更新されます。ただし、この手法を使用するには、イベントの既存のリストに目的の値が含まれている必要があります。

すべてのカラムをフィルタリングすることはできません。セルのコンテンツをフィルタリングできる場合は、そのセルの上にカーソルを合わせたときに下線が表示されます。

アトミック要素の選択

[フィルタ (Filter)] フィールドをクリックして、ドロップダウンから目的のアトミック要素を選択した後、照合値を入力することでフィルタを作成することもできます。これらの要素には、イベントテーブルのカラムとして表示されないイベントフィールドが含まれます。また、表示するイベントと入力された値との関係を定義するオペレータが含まれます。

す。カラムをクリックすると必ず、「equals(=)」フィルタが表示されますが、要素を選択すると、数値フィールドに「greater than(>)」または「less than(<)」も選択できるようになります。

[フィルタ (Filter)]フィールドに要素を追加する方法に関係なく、フィールドに入力してオペレータまたは値を調整できます。テーブルにフィルタを適用するには、[フィルタ (Filter)]をクリックします。

イベントフィルタの演算子

イベントフィルタには、次の演算子を使用できます。

=	等しい。イベントは指定した値と一致します。ワイルドカードを使用することはできません。
!=	等しくない。イベントは指定した値と一致しません。「等しくない」の式を作成するには、感嘆符 (!) を入力する必要があります。
>	次の値より大きい。イベントに、指定した値よりも大きい値が含まれます。この演算子はポートやIPアドレスなど、数値のみに使用できます。
<	次の値より小さい。イベントに、指定した値よりも小さい値が含まれます。この演算子は、数値のみに使用できます。

複雑なイベントフィルタのルール

複数のアトミック要素を含む複雑なフィルタを作成する場合、次のルールに注意してください。

- 同じタイプの要素には、そのタイプのすべての値の間に OR 関係があります。たとえば、Initiator IP=10.100.10.10 と Initiator IP=10.100.10.11 を含めると、送信元としてこれらのいずれかのアドレスを持つイベントが照合されます。
- 異なるタイプの要素には、AND 関係があります。たとえば、Initiator IP=10.100.10.10 と Destination Port/ICMP Type=80 を含めると、この送信元アドレスと宛先ポートのみを持つイベントが照合されます。10.100.10.10 から異なる宛先ポートへのイベントは表示されません。
- IPv4 アドレスやIPv6 アドレスなどの数値要素は範囲を指定できます。たとえば、Destination Port=50-80 を指定して、この範囲内のポートのすべてのトラフィックを取得できます。ハイフンを使用して、開始と終了の数字を区切ります。すべての数値フィールドに対して、範囲を使用できるわけではありません。たとえば、[送信元 (Source)]要素にIPアドレスを範囲で指定することはできません。
- ワイルドカードまたは正規表現は使用できません。

イベントフィールドの説明

イベントには次の情報が含まれます。これらの情報は、イベントの詳細情報を表示すると確認できます。また、イベントビューア表に列を追加すると、最も関心のある情報を表示できます。

以下に、使用可能なフィールドの完全なリストを示します。すべてのフィールドがどのイベントタイプにも適用されるわけではありません。個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにして接続を記録したかによって異なることに注意してください。

[アクション (Action)]

接続イベントまたはセキュリティインテリジェンスイベントの場合、接続をロギングしたアクセス制御ルールまたはデフォルトアクションに関連付けられたアクション。

[許可 (Allow)]

明示的に許可された接続。

[信頼 (Trust)]

信頼できる接続。最初のパケットが信頼ルールによって検出された TCP 接続のみ、接続終了イベントを生成します。システムは、最後のセッションパケットの1時間後にイベントを生成します。

[ブロック (Block)]

ブロックされている接続。[ブロック (Block)] 動作は、次の条件下で、アクセス許可ルールに関連付けることができます。

- 侵入ポリシーによってエクスプロイトがブロックされた接続。
- ファイルがファイルポリシーによってブロックされている接続。
- セキュリティインテリジェンスによってブラックリストに載せられている接続。
- SSL ポリシーによってブロックされている接続。

[デフォルトアクション (Default Action)]

接続はデフォルトアクションによって処理されました。

ファイルイベントまたはマルウェアイベントの場合は、ファイルが一致したルールのルールアクションに関連付けられたファイルルールアクションと、すべての関連するファイルルールアクションのオプション。

[許可された接続 (Allowed Connection)]

システムがイベントのトラフィックフローを許可したかどうか。

[アプリケーション(Application)]

接続で検出されたアプリケーション。

[アプリケーションのビジネスとの関連性 (Application Business Relevance)]

接続で検出されたアプリケーショントラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネスとの関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

[アプリケーションカテゴリ、アプリケーションタグ (Application Categories, Application Tag)]

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[アプリケーションのリスク (Application Risk)]

接続で検出されたアプリケーショントラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

[ブロックタイプ (Block Type)]

イベントでトラフィックフローが一致したアクセス制御ルールで指定されたブロックのタイプ：block または interactive block。

[クライアントアプリケーション、クライアントバージョン (Client Application, Client Version)]

接続で検出されたクライアントのクライアントアプリケーションとバージョン。

[クライアントのビジネスとの関連性 (Client Business Relevance)]

接続で検出されたクライアントトラフィックに関連するビジネスとの関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

[クライアントカテゴリ、クライアントタグ (Client Application, Client Version)]

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[クライアントリスク (Client Risk)]

接続で検出されたクライアントトラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

[接続 (Connection)]

内部的に生成されたトラフィックフローの固有 ID。

[接続ブロックタイプインジケータ (Connection Blocktype Indicator)]

イベントのトラフィックフローと一致するアクセスコントロールルールで指定されたブロックのタイプ。ブロックまたはインタラクティブブロック。

[接続バイト (Connection Bytes)]

接続の合計バイト数。

[接続時間 (Connection Time)]

接続の開始時刻。

[接続タイムスタンプ (Connection Timestamp)]

接続が検出された時刻。

[拒否された接続 (Denied Connection)]

システムがイベントのトラフィック フローを拒否したかどうか。

[宛先の国または大陸 (Destination Country and Continent)]

受信ホストの国および大陸。

[宛先 IP アドレス (Destination IP)]

侵入、ファイル、またはマルウェア イベントで受信側ホストによって使用された IP アドレス。

[宛先ポート/ICMPコード、宛先ポート、宛先Icode (Destination Port/ICMP Code; Destination Port; Destination Icode)]

セッション レスポンダが使用するポートまたは ICMP コード。

[方向 (Direction)]

ファイルの送信方向。

[傾向 (Disposition)]

ファイルの性質。

[マルウェア (Malware)]

AMP クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイルポリシーで定義されたマルウェアしきい値を超えていることを示します。ローカルマルウェア分析では、ファイルをマルウェアとしてマークすることもできます。

[クリーン (Clean)]

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。

[不明 (Unknown)]

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを正しく分類していませんでした。

[対応不可 (Unavailable)]

システムがAMPクラウドに問い合わせできなかったことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

[該当なし (N/A)]

[ファイル検出 (Detect Files)]または[ファイルブロック (Block Files)]ルールがファイル进行处理し、システムが AMP クラウドに問い合わせなかったことを示します。

[出カインターフェイス、出力セキュリティゾーン (gress Interface, Egress Security Zone)]

接続がデバイスを通り抜けたゾーンとインターフェイス。

[イベント、イベントタイプ (Event, Event Type)]

イベントのタイプ。

[イベント秒、イベントマイクロ秒 (Event Seconds, Event Microseconds)]

イベントが検出された時刻 (秒またはマイクロ秒単位) 。

[ファイルカテゴリ (File Category)]

ファイルタイプの一般的なカテゴリ (Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコードファイル、グラフィック、システムファイルなど) 。

[ファイルイベントタイムスタンプ (File Event Timestamp)]

ファイルまたはマルウェア ファイルが作成された日時。

[ファイル名 (File Name)]

ファイルの名前。

[ファイルルールのアクション (File Rule Action)]

ファイルを検出したファイルポリシールールに関連したアクション、および関連するファイルアクションオプション。

[ファイルSHA-256 (File SHA-256)]

ファイルの SHA-256 ハッシュ値。

[ファイルサイズ (File Size) (KB)]

ファイルのサイズ (KB 単位) 。システムがファイルを完全に受信する前にブロックした場合、ファイルサイズが空白になる場合があります。

[ファイルタイプ (File Type)]

ファイルのタイプ (HTML や MSEXE など) 。

[ファイル/マルウェアポリシー (File/Malware Policy)]

イベントの生成に関連付けられているファイルポリシー。

[ファイルログブロックタイプインジケータ (Filelog Blocktype Indicator)]

イベントでトラフィック フローが一致したファイルルールで指定されたブロックのタイプ : block または interactive block。

[ファイアウォールポリシールール、ファイアウォールルール (Firewall Policy Rule, Firewall Rule)]

接続を処理したアクセス コントロール ルールまたはデフォルト アクション。

[最初のパケット (First Packet)]

セッションの最初のパケットが検出された日時。

[HTTPリファラ (HTTP Referrer)]

接続で検出されたHTTPトラフィックの要求されたURLの参照元を表すHTTP参照元 (別のURLへのリンクを提供したWebサイトや別のURLからのリンクをインポートしたWebサイトなど)。

[HTTPレスポンス (HTTP Response)]

クライアントからの接続経由のHTTP要求に応じて送信されるHTTPステータスコード。

[IDSの分類 (IDS Classification)]

イベントを生成したルールが属している分類。

[入力インターフェイス、入力セキュリティゾーン (Ingress Interface, Ingress Security Zone)]

接続がデバイスに入ったゾーンとインターフェイス。

[イニシエータバイト、イニシエータパケット (Initiator Bytes, Initiator Packets)]

セッションイニシエータが送信した合計バイト数またはパケット数。

[イニシエータの国または大陸 (Initiator Country and Continent)]

セッションを開始したホストの所在地の国と地域の名前。イニシエータのIPアドレスがルーティング可能であるときにのみ使用できます。

[イニシエータ IP (Initiator IP)]

接続イベントまたはセキュリティインテリジェンスイベントでセッションを開始したホストIPアドレス (およびDNS解決が有効になっている場合のホスト名)。

[インライン結果 (Inline Result)]

インラインモードで動作しているときに、侵入イベントをトリガーしたパケットをシステムがドロップした、またはドロップするはずだったか。ブランクは、トリガーとして使用されたルールが [ドロップしてイベントを生成する (Drop and Generate Events)] に設定されていないことを示します

[侵入ポリシー (Intrusion Policy)]

イベントを生成したルールが有効にされた侵入ポリシー。

[IPSブロックタイプインジケータ (IPS Blocktype Indicator)]

イベントのトラフィックフローと一致する侵入ルールのアクション。

[最後のパケット (Last Packet)]

セッションの最後のパケットが検出された日時。

[MPLSラベル (MPLS Label)]

この侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコルラベルスイッチングラベル。

[マルウェアブロックタイプインジケータ (Malware Blocktype Indicator)]

イベントのトラフィックフローと一致するファイルルールで指定されたブロックのタイプ。ブロックまたはインタラクティブブロック。

[メッセージ (Message)]

侵入イベントの場合、イベントの説明テキスト。マルウェアまたはファイルイベントの場合は、マルウェア イベントに関連付けられている追加情報。

[NetBIOSドメイン (NetBIOS Domain)]

セッションで使用された NetBIOS ドメイン。

[元のクライアントの国と大陸 (Original Client Country and Continent)]

セッションを開始した元のクライアントホストの所在地の国と地域の名前。元のクライアントの IP アドレスがルーティング可能であるときにのみ使用できます。

[クライアントのオリジナルIP (Original Client IP)]

HTTP 接続を開始したクライアントの元の IP アドレス。このアドレスは、X-Forwarded-For (XFF) または True-Client-IP HTTP のヘッダーフィールド、またはそれらの同等品から取得されます。

[ポリシー、ポリシーの改訂 (Policy, Policy Revision)]

アクセス コントロール ポリシーとその改訂版。イベントに関連付けられているアクセス (ファイアウォール) ルールを含みます。

[プライオリティ (Priority)]

Cisco Talos Intelligence Group (Talos) により決定されたイベントのプライオリティ (高 (high)、中 (medium)、または低 (low))。

[プロトコル (Protocol)]

接続に使用されるトランスポート プロトコルです。

[理由 (Reason)]

次の表では、接続がロギングされた状況を説明しています。該当しない場合、このフィールドは空になります。これ以外の場合、このフィールドは空です。

理由	説明
[ファイルブロック (File Block)]	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック (File Block)]の理由は必ず[ブロック (Block)]アクションと対として組み合わせられます。

理由	説明
[ファイルモニタ (File Monitor)]	システムが接続において特定のファイルの種類を検出しました。
[ファイル復帰許可 (File Resume Allow)]	ファイル送信がはじめに [ファイルブロック (Block Files)] ルールまたは [マルウェアブロック (Block Malware)] ファイルルールによってブロックされました。ファイルを許可する新しいアクセスコントロールポリシーが展開された後、HTTPセッションが自動的に再開しました。
[ファイル復帰ブロック (File Resume Block)]	ファイル送信がはじめに [ファイル検出 (Detect Files)] ルールまたは [マルウェアクラウドルックアップ (Malware Cloud Lookup)] ファイルルールによって許可されました。ファイルをブロックする新しいアクセスコントロールポリシーが展開された後、HTTPセッションが自動的に停止しました。
[侵入ブロック (Intrusion Block)]	接続で検出されたエクスプロイト (侵入ポリシー違反) をシステムがブロックしたか、ブロックするはずでした。 [侵入ブロック (Intrusion Block)] の理由は、ブロックされたエクスプロイトの場合は [ブロック (Block)]、ブロックされるはずだったエクスプロイトの場合は [許可 (Allow)] のアクションと対として組み合わせられます。
[侵入モニタ (Intrusion Monitor)]	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する (Generate Events)] に設定されている場合に発生します。
[IPブロック (IP Block)]	IPアドレスとセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。 [IPブロック (IP Block)] の理由は必ず [ブロック (Block)] のアクションと対として組み合わせられます。
SSL ブロック (SSL Block)	システムが SSL インスペクション設定に基づいて暗号化接続をブロックしました。 [SSL ブロック (SSL Block)] の理由は必ず [ブロック (Block)] のアクションと対として組み合わせられます。
[URLブロック (URL Block)]	URL とセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。 [URLブロック (URL Block)] の理由は必ず [ブロック (Block)] のアクションと対として組み合わせられます。

[受信時間 (Receive Times)]

イベントが生成された日時。

[参照ホスト (Referenced Host)]

接続のプロトコルが DNS、HTTP、または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

[レスポндаバイト、レスポндаパケツト (Responder Bytes, Responder Packets)]

セッション レスポндаが送信した合計バイト数またはパケツト数。

[レスポндаの国または大陸 (Responder Country and Continent)]

セッションに応答したホストの所在地の国と地域の名前。レスポндаの IP アドレスがルーティング可能であるときにのみ使用できます。

[レスポнда IP (Responder IP)]

接続イベントまたはセキュリティ インテリジェンス イベントのセッション応答側のホスト IP アドレス (および DNS 解決が有効になっている場合のホスト名)。

[SI カテゴリ ID (セキュリティ インテリジェンス カテゴリ) (SI Category ID (Security Intelligence Category))]

ネットワーク名や URL オブジェクト名、フィード カテゴリの名前など、ブラックリスト項目が含まれるオブジェクトの名前。

[シグネチャ (Signature)]

ファイル/マルウェア イベントの署名 ID。

[ソースの国または大陸 (Source Country and Continent)]

送信ホストの国と大陸。送信元 IP アドレスがルーティング可能であるときにのみ使用できます。

[ソース IP (Source IP)]

侵入、ファイル、マルウェア イベントで送信側ホストによって使用された IP アドレス。

[送信元ポート/ICMP タイプ、送信元ポート、送信元ポート Itype (Source Port/ICMP Type; Source Port; Source Port Itype)]

セッション イニシエータが使用するポートまたは ICMP タイプ。

実際の SSL アクション

システムによって接続に適用される実際のアクション。これは期待される動作とは異なることがあります。たとえば、接続が復号化を適用するルールと一致しても、いくつかの理由で復号化できないことがあります。

アクション	説明
[ブロック (Block) /リセットしてブロック (Block With Reset)]	ブロックされた暗号化接続を表します。

アクション	説明
[復号 (再署名) (Decrypt (Resign))]	再署名サーバ証明書を使用して復号された発信接続を表します。
[復号 (キーの交換) (Decrypt (Replace Key))]	置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
[復号 (既知のキー) (Decrypt (Known Key))]	既知の秘密キーを使用して復号化された着信接続を表します。
[デフォルトアクション (Default Action)]	接続がデフォルト アクションによって処理されたことを示します。
[復号しない (Do not Decrypt)]	システムが復号化しなかった接続を表します。

[SSL証明書のフィンガープリント (SSL Certificate Fingerprint)]

証明書の認証に使用する SHA ハッシュ値。

[SSL証明書ステータス (SSL Certificate Status)]

これは、認証ステータスの SSL ルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックが SSL ルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- [自署 (Self Signed)]
- [有効 (Valid)]
- [署名が無効 (Invalid Signature)]
- [発行元が無効 (Invalid issuer)]
- [期限切れ (Expired)]
- [不明 (Unknown)]
- [まだ有効ではない (Not Valid Yet)]
- [失効 (Revoked)]

復号できないトラフィックが SSL ルールと一致する場合、[チェックしていない (Not Checked)]がこのフィールドに表示されます。

[SSL暗号スイート (SSL Cipher Suite)

接続に使用された暗号スイート。

[予期されたSSLアクション (SSL Expected Action)]

接続が一致した SSL ルールで指定されたアクション。

SSL フロー フラグ (SSL Flow Flags)

暗号化された接続の最初の 10 デバッグ レベル フラグ。

[SSLフローメッセージ (SSL Flow Messages)]

HELLO_REQUEST や CLIENT_HELLO など、SSL ハンドシェイク中にクライアントとサーバ間で交換された SSL/TLS メッセージ。TLS 接続で交換されたメッセージの詳細については、<http://tools.ietf.org/html/rfc5246> を参照してください。

[SSLポリシー (SSL Policy)

接続に適用された SSL 復号ポリシーの名前。

[SSLルール (SSL Rule)]

接続に適用された SSL 復号ルールの名前。

[SSLセッションID (SSL Session ID)]

SSL ハンドシェイク時にクライアントとサーバ間でネゴシエートされた 16 進数のセッション ID。

[SSLチケットID (SSL Ticket ID)]

SSL ハンドシェイク中に送信されたセッション チケット情報の 16 進数のハッシュ値。

[SSLURLカテゴリ (SSL URL Category)]

SSL 復号処理中に決定された宛先 Web サーバの URL カテゴリ。

[SSLバージョン (SSL Version)]

接続に使用された SSL/TLS バージョン。

[TCPフラグ (TCP Flags)]

接続で検出された TCP フラグ。

[合計パケット数 (Total Packets)]

接続で送信されたパケットの総数：[イニシエータパケット]+[レスポндаパケット]。

[URL、URLカテゴリ、URLレピュテーション、URLレピュテーションスコア (URL, URL Category, URL Reputation, URL Reputation Score)]

セッション中に監視対象のホストによって要求された URL と、関連付けられたカテゴリ、レピュテーション、およびレピュテーション スコア (利用できる場合)。

システムが SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを識別します。したがって SSL アプリケーションの場合、この URL は証明書に含まれる一般名を表示します。

[ユーザ (User)]

イニシエータの IP アドレスに関連付けられたユーザ。

[VLAN]

イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID。

[Webアプリケーションのビジネスとの関連性 (Web App Business Relevance)]

接続で検出された Web アプリケーショントラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出された Web アプリケーションのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

[Webアプリケーションのカテゴリおよびタグ (Web App Categories、Web App Tag)]

Web アプリケーションの機能を理解するのに役立つ、Web アプリケーションの特性を示す基準。

[Webアプリケーションのリスク (Web App Risk)]

接続で検出された Web アプリケーショントラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出された Web アプリケーションのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

[Webアプリケーション (Web Application)]

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。



第 5 章

オブジェクト

オブジェクトは、ポリシーまたはその他の設定内で使用する基準を定義した再利用可能なコンテナです。たとえば、ネットワーク オブジェクトは、ホストアドレスとサブネットアドレスを定義します。

オブジェクトでは基準を定義することができ、同じ基準を異なるポリシーで簡単に再利用できるようになります。オブジェクトを更新すると、そのオブジェクトを使用するすべてのポリシーが自動的に更新されます。

- [オブジェクトタイプ \(129 ページ\)](#)
- [オブジェクトの管理 \(132 ページ\)](#)

オブジェクトタイプ

次のタイプのオブジェクトを作成できます。ほとんどの場合、ポリシーまたは設定によってオブジェクトを許可する場合、オブジェクトを使用する必要があります。

オブジェクトタイプ	主な用途	説明
AnyConnect クライアントプロファイル	リモート アクセス VPN	AnyConnect クライアントプロファイルは、AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザが AnyConnect クライアントの設定および詳細設定からオプションを変更することを許可するかどうかを定義します。 クライアントプロファイルの設定およびアップロード (434 ページ) を参照してください。

オブジェクトタイプ	主な用途	説明
アプリケーションフィルタ	アクセスコントロールルール	アプリケーションフィルタオブジェクトは、IP接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使うのではなく、ポリシーにこれらのオブジェクトを使用してトラフィックを制御できます。 アプリケーションフィルタオブジェクトの設定 (137ページ) を参照してください。
証明書	アイデンティティポリシー リモートアクセスVPN SSL復号ルール	デジタル証明書は、認証に使用されるデジタルIDを提供します。証明書は、SSL（セキュアソケットレイヤ）接続、TLS（Transport Layer Security）接続、およびDTLS（データグラムTLS）接続（HTTPSやLDAPSなど）に使用されます。 証明書の設定 (154ページ) を参照してください。
位置情報	セキュリティポリシー	地理位置情報オブジェクトは、トラフィックの送信元または宛先であるデバイスをホストする国および大陸を定義します。IPアドレスを使用するのではなく、ポリシーにこれらのオブジェクトを使用してトラフィックを制御できます。 地理位置情報オブジェクトの設定 (141ページ) を参照してください。
アイデンティティレルム	アイデンティティポリシー リモートアクセスVPN	アイデンティティレルムとは、認証サービスの提供に必要なディレクトリサーバとその他の属性のことです。ディレクトリサーバには、ネットワークにアクセスできるユーザおよびユーザグループに関する情報が含まれます。 ADアイデンティティレルムの設定 (143ページ) を参照してください。
IKEポリシー	VPN	インターネットキーエクスチェンジ（IKE）ポリシーオブジェクトは、IPsecピアの認証、IPsec暗号キーのネゴシエーションと配布、およびIPsecセキュリティアソシエーション（SAS）の自動的な確立に使用されるIKEプロポーザルを定義します。IKEv1とIKEv2に対して、異なるオブジェクトがあります。 グローバルIKEポリシーの設定 (403ページ) を参照してください。

オブジェクトタイプ	主な用途	説明
IPsec プロポーザル	VPN	<p>IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルは、IPsec トンネル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組み合わせを定義します。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。</p> <p>IPsec プロポーザルの設定 (408 ページ) を参照してください。</p>
ネットワーク	セキュリティ ポリシーおよびさまざまなデバイス設定	<p>ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト (総称してネットワーク オブジェクトと呼ばれます)。</p> <p>ネットワーク オブジェクトとグループの設定 (133 ページ) を参照してください。</p>
ポート	セキュリティ ポリシー	<p>トラフィックのプロトコル、ポート、または ICMP サービスを定義するポート グループおよびポート オブジェクト (総称してポート オブジェクトと呼ばれます)。</p> <p>ポート オブジェクトとグループの設定 (134 ページ) を参照してください。</p>
秘密キー	Smart CLI および FlexConfig ポリシー	<p>秘密キー オブジェクトは、パスワードや、暗号化および非表示にするその他の認証文字列を定義します。</p> <p>秘密キーオブジェクトの設定 (545 ページ) を参照してください。</p>
セキュリティゾーン	セキュリティ ポリシー	<p>セキュリティゾーンは、インターフェイスのグループです。ゾーンによって、ネットワークがトラフィックの管理や分類に役立つセグメントに分割されます。</p> <p>「セキュリティゾーンの設定 (136 ページ)」を参照してください。</p>
Syslogサーバ	アクセス コントロール ルール 診断ロギング セキュリティ インテリジェンス ポリシー SSL 復号ルール 侵入ポリシー	<p>syslog サーバのオブジェクトはコネクション型メッセージまたは診断システムログ (syslog) メッセージを受信できるサーバを指定します。</p> <p>Syslog サーバの設定 (142 ページ) を参照してください。</p>

オブジェクトタイプ	主な用途	説明
URL	アクセスコントロールルール セキュリティインテリジェンスポリシー	Web リクエストの URL または IP アドレスを定義する URL オブジェクトおよびグループ（総称して URL オブジェクトと呼ばれます）。 URL オブジェクトとグループの設定（139 ページ） を参照してください。

オブジェクトの管理

オブジェクトは、[オブジェクト (Objects)] ページから直接設定することも、ポリシーの編集時に設定することもできます。いずれの方法でも同じく新規または更新されたオブジェクトが作成されるため、その時点で適した方法を使用します。

次の手順では、[オブジェクト (Objects)] ページから直接オブジェクトを作成および管理する方法について説明します。



- (注) ポリシーまたは設定を編集すると、プロパティにオブジェクトが必要な場合、すでに定義されているオブジェクトのリストが表示されるため、適切なオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合は、リストに表示される [新規オブジェクトの作成 (Create New Object)] リンクをクリックします。

手順

ステップ 1 [オブジェクト (Objects)] を選択します。

[オブジェクト (Objects)] ページには、使用可能なオブジェクトタイプが一覧表示される目次があります。オブジェクトタイプを選択すると、既存オブジェクトのリストが表示され、新しいオブジェクトを作成できます。オブジェクトの内容とタイプも確認できます。

ステップ 2 目次からオブジェクトタイプを選択し、次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。オブジェクトの内容はタイプによって異なります。具体的な情報については、各オブジェクトタイプの設定トピックを参照してください。
- グループオブジェクトを作成するには、[グループの追加 (Add Group)] () ボタンをクリックします。グループオブジェクトには複数の項目が含まれます。
- オブジェクトを編集するには、そのオブジェクトの[編集 (edit)] () アイコンをクリックします。定義済みオブジェクトの内容は編集できません。

- オブジェクトを削除するには、そのオブジェクトの [削除 (delete)] () アイコンをクリックします。ポリシーや別のオブジェクトで現在使用されているオブジェクト、または定義済みのオブジェクトは削除できません。

ネットワーク オブジェクトとグループの設定

ホストまたはネットワークのアドレスを定義するには、ネットワークグループとネットワークオブジェクト（ネットワークオブジェクトと総称される）を使用します。これらのオブジェクトは、トラフィックの一致条件を定義するためにセキュリティポリシーで使用するか、サーバその他のリソースのアドレスを定義するために設定で使用できます。

ネットワークオブジェクトは単一のホストまたはネットワークアドレスを定義しますが、ネットワークグループオブジェクトは複数のアドレスを定義できます。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。アドレスプロパティの編集時に、オブジェクトリストに表示される [新しいネットワークの作成 (Create New Network)] リンクをクリックして、ネットワークオブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [ネットワーク (Network)] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加 (Add Group)] ボタン () をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン () をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン () をクリックします。

ステップ 3 オブジェクトの名前を入力し、オプションでオブジェクトの説明を入力してオブジェクトの内容を定義します。

オブジェクトの内容やスタンドアロン IP アドレスからオブジェクト名を簡単に判断できるように、IP アドレスだけの名前を使用しないことをお勧めします。名前に IP アドレスを使用する場合は、host-192.168.1.2 または network-192.168.1.0 など、わかりやすいプレフィックスを付けてください。IP アドレスを名前として使用する場合、システムは縦棒をプレフィックスとして追加します（たとえば、|192.168.1.2）。FDM ではオブジェクトセクタに縦棒が表示されませんが、CLI で **show running-config** コマンドを使用して実行中の設定を調べると、この命名規則を確認できます。

ステップ4 オブジェクトの内容を設定します。

ネットワーク オブジェクト

オブジェクトの [タイプ (Type)] を選択して、コンテンツを設定します。

- [ネットワーク (Network)] : 次のいずれかの形式を使用してネットワーク アドレスを入力します。
 - サブネットマスクを含む IPv4 ネットワーク (10.100.10.0/24、10.100.10.0/255.255.255.0 など)。
 - プレフィックスを含む IPv6 ネットワーク (2001:DB8:0:CD30::/60 など)。
- [ホスト (Host)] : 次のいずれかの形式を使用してホスト IP アドレスを入力します。
 - IPv4 ホストアドレス (10.100.10.10 など)。
 - IPv6 ホストアドレス (2001:DB8::0DB8:800:200C:417A または 2001:DB8:0:0:0DB8:800:200C:417A など)。

ネットワーク グループ

グループに追加するネットワークオブジェクトを選択するには、[+] ボタンをクリックします。新しいオブジェクトを作成することもできます。

ステップ5 [OK] をクリックして変更を保存します。

ポートオブジェクトとグループの設定

トラフィックのプロトコル、ポート、または ICMP サービスを定義するには、ポートグループとポートオブジェクト (まとめてポートオブジェクトと呼ぶ) を使用します。その後、トラフィックの一致基準を定義するためのセキュリティポリシーのオブジェクトを使用して、たとえばアクセスルールを使用して特定の TCP ポートへのトラフィックを許可できます。

ポートオブジェクトは単一のプロトコル、TCP/UDP ポートまたはポート範囲、または ICMP サービスを定義しますが、ポートグループオブジェクトは、複数のサービスを定義できます。

システムには、一般的なサービス向けの複数の事前定義されたオブジェクトが含まれています。これらのオブジェクトはポリシーで使用できます。ただし、システムで定義されたオブジェクトは、編集または削除できません。



- (注) ポートグループオブジェクトを作成する場合、オブジェクトの組み合わせが有効であることを確認してください。たとえば、あるオブジェクトをアクセスルールで送信元と宛先ポートの両方を指定するために使用する場合、そのオブジェクトに複数のプロトコルを組み合わせることはできません。すでに使用されているオブジェクトを編集する場合は注意してください。オブジェクトを使用するポリシーが無効 (かつディセーブル) になる場合があります。

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。オブジェクトリストに表示される [新規ポートの作成 (Create New Port)] リンクをクリックすることで、サービスのプロパティを編集しながらポートオブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、次に目次から [ポート (Ports)] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加 (Add Group)] ボタン  をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン  をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン  をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力し、オブジェクトの内容を定義します。

ポート オブジェクト

[プロトコル (Protocol)] を選択し、次のようにプロトコルを設定します。

- **TCP、UDP** : 単一のポートまたはポート範囲の番号を入力します (たとえば 80 (HTTP の場合) または 1-65535 (すべてのポートをカバー))。
- **ICMP、IPv6 ICMP** : ICMP の [タイプ (Type)] を選択し、オプションで [コード (Code)] を選択します。タイプをすべての ICMP メッセージに適用するには、[任意 (Any)] を選択します。タイプとコードについての詳細は、次のページを参照してください。
 - ICMP : <http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>
 - ICMPv6 : <http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml>
- [その他 (Other)] : 目的のプロトコルを選択します。

ポート グループ

[+] ボタンは、グループに追加するポート オブジェクトを選択するためにクリックします。新しいオブジェクトを作成することもできます。

ステップ 4 [OK] をクリックして変更を保存します。

セキュリティゾーンの設定

セキュリティゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中のみ存在できます。

システムは初期設定時に次のゾーンを作成します。これらのゾーンを編集してインターフェイスを追加または削除したり、使用しなくなったゾーンを削除したりできます。

- **inside_zone** : 内部インターフェイスが含まれます。内部インターフェイスがブリッジグループである場合、このゾーンには内部ブリッジ仮想インターフェイス (BVI) ではなく、すべてのブリッジグループメンバーインターフェイスが含まれます。このゾーンは、内部ネットワークを表します。
- **outside_zone** : 外部インターフェイスが含まれます。このゾーンは、インターネットなどの制御不可能な外部ネットワークを表すことを目的としています。

通常、ネットワーク内で果たす役割によって、インターフェイスをグループ化します。たとえば、インターフェイスに接続するインターフェイスを **outside_zone** セキュリティゾーンに配置し、内部ネットワークに接続するすべてのインターフェイスを **inside_zone** セキュリティゾーンに配置できます。次に、外部ゾーンから来て内部ゾーンへ向かうトラフィックにアクセスコントロールルールを適用できます。

ゾーンを作成する前に、ネットワークに適用するアクセスルールや他のポリシーを検討してください。たとえば、すべての内部インターフェイスを同じゾーンに配置する必要はありません。4つの内部ネットワークがあり、1つだけ他の3つとは異なる処理をしたい場合、1つではなく2つのゾーンを作成できます。パブリック Web サーバへの外部アクセスを許可するインターフェイスがある場合、そのインターフェイスに別のゾーンを使用できます。

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。オブジェクトリストに表示される [新規セキュリティゾーンの作成 (Create New Security Zone)] リンクをクリックすることで、セキュリティゾーンのプロパティを編集しながらセキュリティゾーンを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、次に目次から [セキュリティゾーン (Security Zones)] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [インターフェイス (Interfaces)] リストで、[+]をクリックし、ゾーンに追加するインターフェイスを選択します。

このリストは、現在ゾーンに含まれていないすべての名前付きインターフェイスを表示します。インターフェイスをゾーンに追加するには、インターフェイスを設定して名前を付ける必要があります。

すべての名前付きインターフェイスがすでにゾーンにある場合、リストは空になります。別のゾーンにインターフェイスを移動しようとする場合、最初に現在のゾーンから削除する必要があります。

(注) ゾーンにブリッジグループインターフェイス (BVI) を追加することはできません。代わりに、メンバーインターフェイスを追加します。メンバーを異なるゾーンに配置できます。

ステップ 5 [OK] をクリックして変更を保存します。

アプリケーションフィルタ オブジェクトの設定

アプリケーションフィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

個々のアプリケーションを指定することはできますが、アプリケーションフィルタはポリシーの作成や管理を簡素化します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセスコントロールルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとする、セッションがブロックされます。

アプリケーションフィルタ オブジェクトを使用せず、ポリシーのアプリケーションとアプリケーションフィルタを直接選択できます。ただし、同じアプリケーションまたはフィルタグループに対して複数のポリシーを作成する場合にはオブジェクトが便利です。システムには、事前に定義されたいくつかのアプリケーションフィルタが含まれていて、これらは編集または削除できません。



(注) シスコでは、システムおよび脆弱性データベース (VDB) の更新を通じて、アプリケーションディテクタを頻繁に更新し、追加します。したがって、リスクの高いアプリケーションをブロックするルールは、手動でルールを更新しなくても、新しいアプリケーションに自動的に適用されます。

次の手順では、[オブジェクト (Objects)] ページから直接オブジェクトを作成および編集する方法について説明します。[アプリケーション (Applications)] タブにアプリケーション基準を追加した後、[フィルタとして保存 (Save As Filter)] リンクをクリックして、アクセスコントロールルールを編集しながら、アプリケーションフィルタ オブジェクトも作成できます。

始める前に

フィルタを編集するときに、選択したアプリケーションが VDB の更新によって削除されていた場合は、アプリケーション名の後ろに「(廃止 (Deprecated))」と表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システムソフトウェアのアップグレードがブロックされます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [アプリケーションフィルタ (Application Filters)] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [アプリケーション (Applications)] リストで [追加+ (Add+)] をクリックし、オブジェクトに追加するアプリケーションとフィルタを選択します。

最初のリストには、継続的にスクロールするリストでアプリケーションが表示されます。[フィルタの詳細設定 (Advanced Filter)] をクリックすると、フィルタ オプションが表示され、アプリケーションを容易に選択できます。選択したら、[追加 (Add)] をクリックします。このプロセスを繰り返して、アプリケーションやフィルタを追加できます。

(注) 1つのフィルタ条件内での複数の選択はOR関係にあります。たとえば、リスクが「高 (High)」または (OR) 「非常に高い (Very High)」となります。フィルタ間の関係は「論理積 (AND)」であるため、リスクが「高 (High)」または (OR) 「非常に高い (Very High)」であり、かつ (AND) ビジネスとの関連性が「低 (Low)」または (OR) 「非常に低い (Very Low)」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。

リスク

アプリケーションが組織のセキュリティポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーションプロトコル (Application Protocol)] : HTTP や SSH などのホスト間の通信を表すアプリケーションプロトコル。
- [クライアントプロトコル (Client Protocol)] : Web ブラウザや電子メールクライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Webアプリケーション (Web Application)] : HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も重要な機能を説明する一般分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは [SSL プロトコル (SSL Protocol)] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック (暗号化された、または暗号化されていないトラフィックではなく) のみで検出を行うことができるアプリケーションに [復号されたトラフィック (decrypted traffic)] タグを割り当てます。

アプリケーション リスト (ディスプレイ下部)

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

ステップ 5 [OK] をクリックして変更を保存します。

URL オブジェクトとグループの設定

URL オブジェクトとグループ (URL オブジェクトと総称する) を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。

URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループ オブジェクトは複数の URL またはアドレスを定義できます。

URL オブジェクトを作成する場合は、次の点に注意してください。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバのホスト名のみに基づきます。ホスト名は、:// の区切り記号の後、またはホスト名のドットの後に来る場合、一致とみなされます。たとえば、`ign.com` は `ign.com` および `www.ign.com` と一致しますが、`verisign.com` とは一致しません。
- 1 つ以上の / を含む場合、サーバ名、パス、およびクエリ パラメータを含む文字列の部分一致には URL 文字列全体が使用されます。ただし、サーバは再構成することができ、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部をブロックまたは許可するのに手動の URL フィルタリングは使用しないことをお勧めします。文字列の部分一致も予期しない一致となる可能性があり、URL オブジェクトに含める文字列が意図しないサーバ上のパスやクエリ パラメータ内の文字列とも一致することがあります。
- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com` ではなく `example.com` を使用します。
- アクセス コントロールルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、`www.example.com` ではなく、`example.com` を使用します。

ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、`youtube.com` の証明書のサブジェクト共通名は `*.google.com` です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリングルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。



(注) 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。オブジェクトリストに表示される [新規 URL の作成 (Create New URL)] リンクをクリックすることで、URL のプロパティを編集しながら URL オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、次に目次から [URL] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加 (Add Group)] ボタン (📁) をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 オブジェクトの内容を定義します。

URL オブジェクト

URL または IP アドレスを [URL] ボックスに入力します。URL にはワイルドカードを使用できません。

URL グループ

[+] ボタンは、グループに追加する URL オブジェクトを選択するためにクリックします。新しいオブジェクトを作成することもできます。

ステップ 5 [OK] をクリックして変更を保存します。

地理位置情報オブジェクトの設定

地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。たとえば、地理的な場所を使用して、使用されている可能性のある IP アドレスすべてを把握する必要なしに、特定の国へのアクセスを簡単に制限できます。

通常は、地理位置情報オブジェクトを使用せずに、地理的な場所をポリシーで直接選択できます。とはいえ、同じ国や大陸のグループのために複数のポリシーを作成する場合、オブジェクトが便利です。



(注) 常に最新の地理位置情報データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース (GeoDB) を定期的に更新することを強くお勧めします。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。ネットワークプロパティの編集時に、オブジェクトリストに表示される [新しい地理位置情報の作成 (Create New Geolocation)] リンクをクリックして、地理位置情報オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [地理位置情報 (Geolocation)] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [大陸または国 (Continents/Countries)] リストで [追加+ (Add+)] をクリックして、オブジェクトに追加する大陸や国を選択します。

大陸を選択すると、大陸内のすべての国が選択されます。

ステップ 5 [OK] をクリックして変更を保存します。

Syslog サーバの設定

syslog サーバのオブジェクトはコネクション型メッセージまたは診断システム ログ (syslog) メッセージを受信できるサーバを指定します。syslog サーバにログ収集と分析のための設定がある場合は、オブジェクトを作成してそれらを定義し、関連ポリシーでこのオブジェクトを使用します。

以下のイベント タイプを syslog サーバに送信できます。

- 接続イベント。次のポリシーのタイプで syslog サーバ オブジェクトを構成します：アクセス制御ルールとデフォルトアクション、SSL 復号ルールとデフォルトアクション、セキュリティ インテリジェンス ポリシー。
- 侵入イベント。侵入ポリシーで syslog サーバ オブジェクトを構成します。
- 診断イベント。 [診断ロギングの設定 \(477 ページ\)](#) を参照してください。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。オブジェクトリストに表示される [Syslogサーバの追加 (Add Syslog Server)] リンクをクリックすることで、syslog サーバのプロパティを編集しながら syslog サーバを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、次に目次から [Syslogサーバ (Syslog Server)] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 3 syslog サーバのプロパティを設定します。

- [デバイスインターフェイス (Device Interface)] : syslog サーバにアクセスするインターフェイスを選択します。サーバがブリッジグループのメンバー インターフェイスを介してアクセスできる場合、代わりにブリッジグループインターフェイス (BVI) を選択します。

(注) Snort プロセスでは、侵入イベントにこのインターフェイスを使用しません。Snort では常に仮想管理インターフェイスに侵入 syslog メッセージが送信されます。侵入ポリシーにこの syslog サーバを使用する場合、syslog サーバが管理 IP アドレスからも到達可能であることを確認します。

- [IP アドレス (IP Address)] : syslog サーバの IP アドレスを入力します。
- [ポート (Port)] : サーバが syslog メッセージを受信するために使用する UDP ポートを入力します。デフォルトは 514 です。デフォルトを変更する場合は、1025 ~ 65535 の範囲のポートを使用してください。

ステップ 4 [OK] をクリックして変更を保存します。

AD アイデンティティ レルムの設定

アイデンティティ レルムとは、認証サービスの提供に必要なディレクトリ サーバとその他の属性のことです。ディレクトリ サーバには、ネットワークへのアクセスを許可されているユーザおよびユーザ グループについての情報が含まれます。

Active Directory の場合、レルムは Active Directory ドメインに相当します。

レルムは次のポリシーで使用されます。

- アイデンティティ: レルムは、ユーザ アイデンティティ情報とグループ メンバーシップ情報を提供します。次いでそれらの情報をアクセスコントロールルールで使用できます。システムは、毎日の最終時間 (UTC) に、すべてのユーザとグループに関する更新情報を

ダウンロードします。ディレクトリ サーバに管理インターフェイスから到達できる必要があります。

- リモート アクセス VPN：レルムは、接続が許可されているかどうかを判断する認証サービスを提供します。ディレクトリ サーバに RA VPN 外部インターフェイスから到達できる必要があります。

ディレクトリ管理者に相談して、ディレクトリ サーバのプロパティの設定に必要な値を取得します。



- (注) ディレクトリ サーバが接続済みネットワークに存在しない場合や、デフォルト ルートで使用できない場合には、サーバのスタティック ルートを作成します。スタティック ルートを作成するには、[デバイス (Device)] > [ルーティング (Routing)] > [表示設定 (View Configuration)] の順に選択します。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。レルムプロパティの編集時に、オブジェクトリストに表示される [新しいアイデンティティレルムの作成 (Create New Identity Realm)] リンクをクリックして、アイデンティティレルムを作成することもできます。

始める前に

ディレクトリ サーバ、Firepower Threat Defense デバイス、およびクライアント間で、時刻設定が一致していることを確認します。これらのデバイス間で時刻にずれがあると、ユーザ認証が成功しない場合があります。「一致」とは、別のタイムゾーンを使用できますが、たとえば、10 AM PST = 1 PM EST など、それらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [アイデンティティレルム (Identity Realm)] [アイデンティティソース (Identity Sources)] を選択します。

ステップ 2 次のいずれかを実行します。

- レルムを作成するには、[+] ボタンをクリックします。作成可能なのは 1 つのレルムのみです。
- 既存のレルムを編集するには、そのレルムの編集アイコン (🔗) をクリックします。

作成後にレルムを削除することはできません。レルムの使用を停止するには、レルムを使用する設定済み機能を無効にします。

ステップ 3 基本レルムのプロパティを設定します。

- [名前 (Name)]：ディレクトリ レルムの名前。

- [タイプ (Type)]: ディレクトリ サーバのタイプ。サポートされるタイプは Active Directory のみで、このフィールドを変更することはできません。
- [ディレクトリ ユーザ名 (Directory Username)]、[ディレクトリ パスワード (Directory Password)]: 取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格された特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com (Administrator だけでなく) などの完全修飾名である必要があります。

(注) この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=admin, cn=users, dc=example, dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。
- [ベース DN (Base DN)]: ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリ ツリー。例、cn=users, dc=example, dc=com。ベース DN の検索の詳細については、[ディレクトリ ベースの DN の決定 \(148 ページ\)](#) を参照してください。
- [AD プライマリ ドメイン (AD Primary Domain)]: デバイスが参加する必要がある完全修飾 Active Directory ドメイン名。たとえば、example.com のように指定します。

ステップ 4 ディレクトリ サーバのプロパティを設定します。

- [ホスト名または IP アドレス (Hostname/IP Address)]: ディレクトリ サーバのホスト名または IP アドレス。サーバへの暗号化された接続を使用する場合、IP アドレスではなく完全修飾ドメイン名を入力する必要があります。
- [ポート (Port)]: サーバとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化 (Encryption)]: ユーザおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法 ([STARTTLS] または [LDAPS]) を選択します。デフォルトでは [なし (None)] になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。
 - [STARTTLS] では、暗号化方式をネゴシエートし、ディレクトリ サーバでサポートされる最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモート アクセス VPN にレルムを使用する場合はサポートされません。
 - [LDAPS] では、LDAP over SSL が必要です。ポート 636 を使用します。
- [信頼できる CA 証明書 (Trusted CA Certificate)]: 暗号化方式を選択する場合、認証局 (CA) の証明書をアップロードして、システムとディレクトリ サーバの間で信頼できる接続を有効化します。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス (Hostname/IP Address)] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

ステップ 5 [テスト (Test)] ボタンをクリックして、システムがサーバに接続できることを確認します。

システムは別個のプロセスおよびインターフェイスを使用してサーバにアクセスします。このため、アイデンティティ ポリシーでは接続に成功してリモートアクセス VPN では失敗するなど、ある使用方法では接続が成功しても、別の方法では失敗したことを示すエラーが表示される場合があります。サーバに到達できない場合は、正しい IP アドレスとホスト名を指定していること、DNS サーバに当該ホスト名のエン트리などが設定されていることを確認します。サーバにスタティックルートを設定する必要があるかもしれません。詳細については、[ディレクトリ サーバ接続のトラブルシューティング \(146 ページ\)](#) を参照してください。

ステップ 6 [OK] をクリック

ディレクトリ サーバ接続のトラブルシューティング

システムは、機能に応じて異なるプロセスを使用して、ディレクトリサーバと通信します。そのため、アイデンティティ ポリシー用の接続は機能しますが、リモートアクセス VPN 用の接続は失敗します。

これらのプロセスでは、さまざまなインターフェイスを使用してディレクトリサーバと通信します。次のインターフェイスからの接続を確認する必要があります。

- 管理インターフェイス (アイデンティティ ポリシーの場合)
- データ インターフェイス (リモート アクセス VPN (外部インターフェイス) の場合)

アイデンティティ レalmを設定する場合、[テスト (Test)] ボタンを使用して接続が機能することを確認します。障害メッセージによって、接続上の問題がある機能が示されます。次に、認証属性およびルーティング/インターフェイス設定に基づいて、発生する可能性がある一般的な問題を示します。

Directory ユーザの認証問題。

ユーザ名またはパスワードが原因でシステムがディレクトリサーバにログインできない問題の場合、名前とパスワードが正しく、ディレクトリサーバで有効なことを確認します。Active Directory では、昇格された特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com (Administrator だけでなく) などの完全修飾名である必要があります。

また、システムはユーザ名とパスワードの情報から ldap-login-dn と ldap-login-password も生成します。たとえば、Administrator@example.com は cn=admin, cn=users, dc=example, dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

ディレクトリサーバにはデータ インターフェイスを介してアクセスできます。

ディレクトリサーバがデータ インターフェイス (GigabitEthernet インターフェイスなど) に直接接続されているネットワークまたは直接接続されたネットワークからルーティング

可能なネットワーク上にある場合、仮想管理インターフェイスとディレクトリサーバの間にルートがあることを確認する必要があります。

- **data-interfaces** を管理ゲートウェイとして使用すると、ルーティングが成功します。
- 管理インターフェイス上に明示的なゲートウェイがある場合、そのゲートウェイルータにディレクトリサーバへのルートが存在している必要があります。
- 仮想管理インターフェイスによって使用される物理インターフェイスである [診断 (diagnostic)] インターフェイスで IP アドレスを設定する必要はありません。ただし、アドレスを設定する場合、ディレクトリサーバに対するトラフィックを診断インターフェイスにリダイレクトするスタティックルート (デフォルトルートなど) も設定しないでください。
- 直接接続されたネットワークとディレクトリサーバをホストするネットワークの間にルータがある場合、ディレクトリサーバのスタティックルートを設定します ([デバイス (Device)] > [ルーティング (Routing)])。
- データインターフェイスの IP アドレスとサブネットマスクが正しいことを確認します。

ディレクトリサーバには物理的な管理インターフェイスを介してアクセスできます。

ディレクトリサーバが物理的な管理インターフェイス (Management0/0 など) に直接接続されているネットワークまたはそのネットワークからルーティング可能なネットワーク上にある場合、次の手順を実行する必要があります。

- 管理インターフェイスの IPv4 アドレス (論理名 **diagnostic**) を [デバイス (Device)] > [インターフェイス (Interfaces)] で設定します。IP アドレスは仮想管理アドレスと同じサブネット上にある必要があります ([デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)])。
- ディレクトリサーバと管理インターフェイスの間にルータがある場合、[診断 (diagnostic)] インターフェイスの [デバイス (Device)] > [ルーティング (Routing)] で、ディレクトリサーバ用のルートを設定します。
- 診断インターフェイスおよび管理インターフェイスの IP アドレスとサブネットマスクが正しいことを確認します。

ディレクトリサーバは外部ネットワークにあります。

ディレクトリサーバが外部 (アップリンク) インターフェイスの反対側のネットワークにある場合、サイト間 VPN 接続を設定する必要がある場合があります。詳細な手順については、[リモートアクセス VPN を使用して外部ネットワークのディレクトリサーバを使用する方法 \(453 ページ\)](#) を参照してください。

ユーザ数の制限

Firepower Device Manager はディレクトリサーバから最大 2000 人のユーザに関する情報をダウンロードできます。

ディレクトリ サーバに 2000 以上のユーザアカウントが含まれる場合、アクセスルールでユーザを選択するとき、またはユーザベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

この制限は、グループに関連付けられた名前にも適用されます。グループに 2000 を超えるメンバーが含まれている場合は、ダウンロードした 2000 個の名前だけをグループメンバーシップと照合できます。

2000 人以上のユーザがいる場合、Firepower Device Manager ではなく Firepower Management Center (リモートマネージャ) の使用を検討してください。Firepower Management Center では、はるかに多くのユーザをサポートします。

サポートされるディレクトリ サーバ

Windows サーバ 2008 および 2012 で Microsoft Active Directory (AD) を使用できます。

サーバの設定に関して次の点に注意してください。

- ユーザグループまたはグループ内のユーザに対してユーザ制御を実行する場合、ディレクトリ サーバでユーザグループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、システムはユーザグループ制御を実行できません。
- ディレクトリ サーバは、次の表に示すフィールド名を使用して、システムがそのフィールドのサーバからユーザメタデータを取得できるようにする必要があります。

メタデータ	Active Directory フィールド
LDAP ユーザ名	samaccountname
名	givenname
姓	sn
メールアドレス	メールアドレス userprincipalname (mail に値が設定されていない場合)
部署	部署 distinguishedname (department に値が設定されていない場合)
電話番号	telephonenumber

ディレクトリ ベースの DN の決定

ディレクトリの各プロパティを設定する際、ユーザおよびグループに共通のベース識別名 (DN) を指定する必要があります。ベースはディレクトリサーバ内で定義され、ネットワークごとに異なります。アイデンティティポリシーが正しく機能するには、適切なベースを入力する必要

があります。ベースが誤っていると、ユーザ名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。



ヒント 正しいベースを取得するには、ディレクトリ サーバを担当する管理者に確認してください。

Active Directory の場合は、ドメイン管理者として Active Directory サーバにログインし、コマンドプロンプトで **dsquery** コマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べる既知のユーザ名（一部または全部）を指定します。たとえば次のコマンドでは、部分名「John*」を使用して、「John」で始まるすべてのユーザに対する情報を返します。

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

dsquery group コマンドを入力し、ベース識別名を調べたい既知のグループ名を指定します。たとえば次のコマンドでは、グループ名「Employees」を使用して識別名を返します。

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

グループのベース DN は「DC=csc-lab,DC=example,DC=com」となります。

ADSI Edit プログラムを使用して、Active Directory 構造を参照することもできます（[スタート (Start)] > [ファイル名を指定して実行 (Run)] > [adsiedit.msc]）。ADSI Edit で、組織単位 (OU)、グループ、ユーザなど任意のオブジェクトを右クリックし、[プロパティ (Properties)] を選択すると、識別名が表示されます。DC 値の文字列を、ベースとしてコピーします。

正しいベースであることを確認するには、次の手順を実行します。

1. ディレクトリ プロパティの [テスト接続 (Test Connection)] ボタンをクリックし、接続を確認します。問題があった場合には修正して、ディレクトリ プロパティを保存します。
2. 変更をデバイスに適用します。
3. アクセスルールを作成して、[ユーザ (Users)] タブを選択し、ディレクトリから既知のユーザおよびグループ名の追加を試みます。ディレクトリを含むレルム内の一致ユーザ名およびグループ名を入力すると、入力中にオートコンプリートによる候補が表示されます。ドロップダウンリストに候補が表示される場合は、システムがディレクトリに適切に照会できたことを意味します。入力した文字列がユーザ名またはグループ名として表示されることが確かであるにもかかわらず、候補が表示されない場合は、対応する検索ベースを修正する必要があります。



第 6 章

証明書

デジタル証明書は、認証に使用されるデジタル ID を提供します。証明書は、SSL（セキュアソケットレイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。次のトピックでは、証明書の作成と管理の方法について説明します。

- [証明書について（151 ページ）](#)
- [証明書の設定（154 ページ）](#)

証明書について

デジタル証明書は、認証に使用されるデジタル ID を保持しています。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、ユーザまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれています。証明書は、SSL（セキュアソケットレイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。

次のタイプの証明書を作成できます。

- **内部証明書**：内部アイデンティティ証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。
- **内部証明書認証局（CA）証明書**：内部 CA 証明書は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。
- **信頼できる認証局（CA）証明書**：信頼できる CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

認証局 (CA) は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザーのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。CA は、信頼できるサードパーティ (VeriSign など) の場合もあれば、組織内に設置したプライベート CA (インハウス CA) の場合もあります。CA は、証明書要求の管理とデジタル証明書の発行を行います。詳細については、[公開キー暗号化 \(152 ページ\)](#) を参照してください。

公開キー暗号化

RSA 暗号化システムなどの公開キー暗号化では、各ユーザーは、公開キーと秘密キーの両方を含むキーペアを使用します。これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号できます。

簡単に言えば、データが秘密キーで暗号化されたとき、署名が形成されます。署名はデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信された署名が、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは外部で取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。

デジタル証明書および公開キー暗号化の詳細については、[openssl.org](#)、[Wikipedia](#)、またはその他のソースを参照してください。SSL/TLS 暗号化をしっかりと理解することで、デバイスへのセキュアな接続を確立できます。

各機能で使用される証明書タイプ

各機能に適したタイプの証明書を作成する必要があります。次の機能は、証明書が必要です。

アイデンティティ ポリシー (キャプティブ ポータル) : 内部証明書

(オプション) キャプティブ ポータルはアイデンティティ ポリシーで使用されます。この証明書は、ユーザーが自身を特定し、自分のユーザー名にデバイスの IP アドレスを関連付けることを目的としてデバイスを認証するときに承認する必要があります。証明書を提示しないと、デバイスは自動生成された証明書を使用します。

アイデンティティ レalm (アイデンティティ ポリシーおよびリモート アクセス VPN) : 信頼できる CA 証明書

(オプション) ディレクトリ サーバに暗号化接続を使用する場合、ディレクトリ サーバの認証を行うためにこの証明書を承認する必要があります。ユーザーは、アイデンティティ ポリシーおよびリモート アクセス VPN ポリシーから求められたときに認証する必要があります。ディレクトリ サーバに暗号化を使用しない場合、証明書は必要ありません。

リモート アクセス VPN：内部証明書

(必須) 内部証明書は、AnyConnect クライアントがデバイスへの接続を行うときにデバイス ID を確立する外部インターフェイスに使用します。クライアントはこの証明書を承認する必要があります。

SSL 復号ポリシー：内部、内部 CA、および信用できる CA 証明書

(必須) SSL 復号ポリシーは、以下の目的のため証明書を使用します。

- 内部証明書は既知のキー復号ルールに使用されます。
- 内部 CA 証明書は、クライアントと FTD デバイス間にセッションを作成するときに、再署名の復号ルールに使用されます。
- 信頼できる CA 証明書は、FTD デバイスとサーバ間にセッションを作成するときに、再署名の復号ルールに間接的に使用されます。その他の証明書とは異なり、これらの証明書は SSL 復号ポリシーで直接設定しません。これらは単にシステムにアップロードする必要があります。システムには多数の信用できる CA 証明書が含まれるため、追加の証明書をアップロードする必要はないことがあります。

例：OpenSSL を使用した内部証明書の生成

次の例では、OpenSSL コマンドを使用して内部サーバの証明書を生成します。OpenSSL は [openssl.org](https://www.openssl.org) から取得できます。具体的な情報については、OpenSSL のマニュアルを参照してください。この例で使用するコマンドは変更される場合があります、この他にも利用できるオプションがある可能性もあります。

この手順は、FTD にアップロードする証明書の取得方法について、1つの考え方を示すものです。



(注) 次に示す OpenSSL コマンドは一例にすぎません。セキュリティ要件に合わせてパラメータを調整してください。

手順

ステップ 1 キーを生成します。

```
openssl genrsa -out server.key 4096
```

ステップ 2 証明書署名要求 (CSR) を生成します。

```
openssl req -new -key server.key -out server.csr
```

ステップ 3 キーと CSR を持つ自己署名証明書を生成します。

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Firepower Device Manager は暗号化キーをサポートしないため、自己署名証明書を生成するときはリターンキーを押してチャレンジパスワードをスキップしてください。

ステップ 4 内部証明書のオブジェクトを Firepower Device Manager で作成するときは、正しいフィールドにファイルをアップロードします。

ファイルの内容をコピーして貼り付けることもできます。サンプルコマンドは、次のファイルを作成します。

- `server.crt` : [サーバ証明書 (Server Certificate)] フィールドにコンテンツをアップロードするか、貼り付けます。
- `server.key` : [証明書キー (Certificate Key)] フィールドにコンテンツをアップロードするか、貼り付けます。キーの生成時にパスワードを入力すると、次のコマンドを使用してそれを復号できます。出力は `stdout` に送信され、コピーできます。

```
openssl rsa -in server.key -check
```

証明書の設定

FTDPEM または DER 形式の X509 証明書をサポートします。OpenSSL を使用して必要に応じて証明書を生成、信頼できる認証局から取得、または自己署名証明書を作成します。

証明書の詳細については、[証明書について \(151 ページ\)](#) を参照してください。

各機能にどのタイプが使用されているかについては、[各機能で使用される証明書タイプ \(152 ページ\)](#) を参照してください。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。オブジェクトリストに表示されている [新規証明書の作成 (Create New Certificate)] リンクをクリックし、証明書プロパティを編集しながら、証明書オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [証明書 (Certificates)] を選択します。

システムには、そのまま、または置き換えて使用できる次の事前定義された証明書が付属します。

- `DefaultInternalCertificate`
- `NGFW-Default-InternalCA`

システムには、サードパーティ証明機関からの多数の信頼された CA の証明書も含まれています。これらは再署名の復号アクションのために SSL 復号化ポリシーが使用します。

ステップ 2 次のいずれかを実行します。

- 新しい証明書オブジェクトを作成するには、[+] メニューから証明書のタイプに適したコマンドを使用します。
- 証明書を表示または編集するには、証明書の [編集 (edit)] アイコン (🔗) または [表示 (view)] アイコン (👁️) をクリックします。
- 証明書を削除するには、その証明書のごみ箱アイコン (🗑️) をクリックします。

証明書の作成と編集の詳細については、次のトピックを参照してください。

- [内部および内部 CA 証明書のアップロード \(155 ページ\)](#)
- [自己署名内部および内部 CA 証明書の生成 \(157 ページ\)](#)
- [信頼できる CA 証明書のアップロード \(158 ページ\)](#)

内部および内部 CA 証明書のアップロード

内部アイデンティティ証明書は、特定のシステムまたはホストの証明書です。

内部 CA 証明書は、他の証明書の署名に使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。

この証明書は、OpenSSL ツールキットを使用して自分で生成するか、認証局から取得できます。その後、次の手順を使用してアップロードします。キー生成の例については、[例 : OpenSSL を使用した内部証明書の生成 \(153 ページ\)](#) を参照してください。

自己署名内部アイデンティティ証明書および内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。自己署名証明書の作成の詳細については、[自己署名内部および内部 CA 証明書の生成 \(157 ページ\)](#) を参照してください。

これらの証明書を使用する機能の詳細については、[各機能で使用される証明書タイプ \(152 ページ\)](#) を参照してください。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [証明書 (Certificates)] を選択します。

ステップ 2 次のいずれかを実行します。

- **[+] > [内部証明書の追加 (Add Internal Certificate)]** をクリックし、次に **[証明書とキーのアップロード (Upload Certificate and Key)]** をクリックします。
- **[+] > [内部CA証明書の追加 (Add Internal CA Certificate)]** をクリックし、次に **[証明書とキーのアップロード (Upload Certificate and Key)]** をクリックします。
- 証明書を編集または表示するには、情報アイコン (i) をクリックします。ダイアログボックスには、証明書の件名、発行者、および有効な時間範囲が表示されます。**[証明書の置換 (Replace Certificate)]** をクリックして、新しい証明書とキーをアップロードします。ダイアログボックスで証明書とキーを貼り付けることもできます。

ステップ 3 証明書の名前を入力します。

名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 4 [証明書のアップロード (Upload Certificate)] (編集する場合は、[証明書の置換 (Replace Certificate)]) をクリックし、証明書ファイル (例: *.cert) を選択します。許可されるファイル拡張子は、.pem、.cert、.cer、.crt、および .der です。または、証明書に貼り付けます。

証明書は PEM または DER 形式の X509 証明書である必要があります。

貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UZETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ210
(...5 lines removed...)
shGJDRerYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOqoHBp
HMUwmhiGZ1zJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfwxCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
v1k3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

ステップ 5 [キーのアップロード (Upload Key)] (または編集時に、[キーの交換 (Replace Key)]) をクリックし、証明書ファイル (例: *.key) を選択します。ファイル拡張子は .key である必要があります。または、証明書のキーに貼り付けます。

キーは暗号化できません。

次に例を示します。

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC1Su1BknrMjzw/5FZ9YgdMLDUGJlbYgkN7mVrkjyLQx2TYsem
r8iTikB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPslA8e60r5mImeDrtw+
Cc005cSfnlTAw5CgcGkcxTCaGIzmXmkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVdgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdlqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuhV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2ST1Z3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfsOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrG+3zau6oKXiuv6db8Rn+71
MU0x09tvtbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

ステップ 6 [OK] をクリックします。

自己署名内部および内部 CA 証明書の生成

内部アイデンティティ証明書は、特定のシステムまたはホストの証明書です。

内部 CA 証明書は、他の証明書の署名に使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。

ユーザは、自己署名内部アイデンティティと内部 CA 証明書を生成できます。つまり、証明書はデバイス自体によって署名されます。自己署名内部 CA 証明書を設定すると、CA がデバイス上で有効になります。システムは、証明書とキーの両方を生成します。

また、これらの証明書は、OpenSSL を使用して作成することも、信頼できる CA から取得してアップロードすることもできます。詳細については、[内部および内部 CA 証明書のアップロード \(155 ページ\)](#) を参照してください。

これらの証明書を使用する機能の詳細については、[各機能で使用される証明書タイプ \(152 ページ\)](#) を参照してください。



(注) 新しい自己署名証明書は5年の有効期間で生成されます。期限が切れる前に必ず証明書を交換してください。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [証明書 (Certificates)] を選択します。

ステップ 2 次のいずれかを実行します。

- [+] > [内部証明書の追加 (Add Internal Certificate)] をクリックし、次に [自己署名証明書 (Self-Signed Certificate)] をクリックする。
- [+] > [内部CA証明書の追加 (Add Internal CA Certificate)] をクリックし、次に [自己署名証明書 (Self-Signed Certificate)] をクリックする。

(注) 証明書を編集または表示するには、情報アイコン (i) をクリックします。ダイアログボックスには、証明書の件名、発行者、および有効な時間範囲が表示されます。[証明書の置換 (Replace Certificate)] をクリックして、新しい証明書とキーをアップロードします。証明書を交換する際は、次の手順で説明されている自己署名の特性を設定し直すことはできません。代わりに、[内部および内部 CA 証明書のアップロード \(155 ページ\)](#) の説明に従って、新しい証明書を貼り付けるかアップロードする必要があります。残りの手順は、新しい自己署名証明書のみにも適用されます。

ステップ 3 証明書の名前を入力します。

名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 4 証明書の件名および発行者の情報については、次の少なくとも 1 つを設定します。

- **Country (C)** : 証明書に含める 2 文字の ISO 3166 国コード。たとえば、米国の国コードは US です。ドロップダウン リストから国コードを選択します。
- **State or Province (ST)** : 証明書に含める都道府県または州。
- **Locality or City (L)** : 都市の名前など、証明書に含める地域。
- **Organization (O)** : 証明書に含める組織または会社の名前。
- **Organizational Unit (Department) (OU)** : 証明書に含める組織単位の名前 (部門名など)。
- **Common Name (CN)** : 証明書に含める X.500 共通名。これは、デバイスの名前、Web サイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモートアクセス VPN で使用する内部証明書に CN を含める必要があります。

ステップ 5 [保存 (Save)] をクリックします。

信頼できる CA 証明書のアップロード

信頼できる認証局 (CA) の証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

これらの証明書を使用する機能の詳細については、[各機能で使用される証明書タイプ \(152 ページ\)](#) を参照してください。

外部の認証局から信頼できる CA 証明書を取得するか、自身の内部 CA を使用して (OpenSSL ツールを使用するなど) CA 証明書を作成します。その後、次の手順を使用して証明書をアップロードします。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [証明書 (Certificates)] を選択します。

ステップ 2 次のいずれかを実行します。

- **[+] > [信頼済みCAの証明書の追加 (Add Trusted CA Certificate)]** をクリックします。
- 証明書を編集するには、その証明書の編集アイコン (🔗) をクリックします。

ステップ 3 証明書の名前を入力します。

名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 4 [証明書のアップロード (Upload Certificate)] (または、編集時は [証明書の置換 (Replace Certificate)]) をクリックして、信頼できる CA 証明書ファイル (*.pem など) を選択します。許可されるファイル拡張子は、.pem、.cert、.cer、.crt、および .der です。または、信頼できる CA 証明書に貼り付けます。

証明書内のサーバ名は、サーバのホスト名または IP アドレスと一致している必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

証明書は PEM または DER 形式の X509 証明書である必要があります。

貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTA1VTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAx
OTIuMTY4LjEueUMTEUMBIGAlUEAwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxZzAN
BgNVBACMBmF1c3RpbjEUMBIGAlUECgwLMTkyLjE2OC4xLjEwExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIIICiJANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEA5NceYwtP
ES6Ve+S9z7WLGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6H0gKlOwXbRvOdkstzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN200jv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

ステップ 5 [OK] をクリックします。



第 Ⅰ 部

基本

- インターフェイス (163 ページ)
- ルーティング (191 ページ)



第 7 章

インターフェイス

ここでは、FTD デバイスでのインターフェイスの設定方法について説明します。

- [FTD インターフェイスについて \(163 ページ\)](#)
- [インターフェイスに関する注意事項と制限事項 \(167 ページ\)](#)
- [物理インターフェイスの設定 \(170 ページ\)](#)
- [ブリッジグループの設定 \(174 ページ\)](#)
- [VLAN サブインターフェイスと 802.1Q トランキングの設定 \(179 ページ\)](#)
- [高度なインターフェイス オプションの設定 \(183 ページ\)](#)
- [Firepower Threat Defense Virtual へのインターフェイスの追加 \(186 ページ\)](#)
- [モニタリング インターフェイス \(188 ページ\)](#)
- [インターフェイスの例 \(189 ページ\)](#)

FTD インターフェイスについて

FTD には、データ インターフェイスや管理/診断インターフェイスが組み込まれています。

インターフェイス接続（物理的または仮想）のためにケーブルを接続するとき、インターフェイスを設定する必要があります。最小限の作業として、トラフィックを通過させることができるようにインターフェイスを指定して有効化します。インターフェイスがブリッジグループのメンバーである場合、これで十分です。ブリッジグループのメンバーでない場合、インターフェイスに IP アドレスを割り当てる必要があります。単一の物理インターフェイスではなく、VLAN サブインターフェイスを特定のポートで作成する場合、通常、物理インターフェイスではなくサブインターフェイス上で IP アドレスを設定します。VLAN サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。これは、スイッチのトランクポートに接続する場合に役立ちます。

インターフェイスリストに、利用可能なインターフェイスとそれぞれの名前、アドレス、状態が示されます。インターフェイスのステータスは、インターフェイスのリストで直接オン/オフを変更できます。このリストは、設定に基づいたインターフェイス特性を示します。また、ブリッジグループインターフェイスの開く/閉じる矢印を使用すると、メンバーインターフェイスが表示されます。これはリストにも個別に表示されます。これらのインターフェイスが仮想インターフェイスおよびネットワーク アダプタにどのようにマッピングされるかについて

は、[Firepower Threat Defense の物理インターフェイスへの VMware ネットワーク アダプタとインターフェイスのマッピング方法 \(24 ページ\)](#) を参照してください。

次のトピックでは、Firepower Device Manager、および他のインターフェイス管理概念を通じたインターフェイス設定に関する制限事項について説明します。

インターフェイスモード

インターフェイスごとに、次のいずれかのモードを設定できます。

ルーテッド (Routed)

各レイヤ3 ルーテッド インターフェイスに、固有のサブネット上の IP アドレスが必要です。通常、これらのインターフェイスをスイッチ、別のルータ上のポート、または ISP/WAN ゲートウェイに接続します。

BridgeGroupMember

ブリッジグループは、FTD がルーティングではなくブリッジするインターフェイスのグループです。すべてのインターフェイスが同じネットワーク上にあります。ブリッジグループはブリッジネットワークに IP アドレスを持つブリッジ仮想インターフェイス (BVI) によって表されます。

BVI に名前を付けると、ルーテッド インターフェイスと BVI の間のルーティングを実行できます。この場合、BVI はメンバー インターフェイスとルーテッド インターフェイス間のゲートウェイとして機能します。BVI に名前を指定しない場合、ブリッジグループメンバーのインターフェイス上のトラフィックはブリッジグループを離れることができません。通常、インターネットにメンバーインターフェイスをルーティングするため、インターフェイスに名前を付けます。

ブリッジグループのルーテッドモードでの使い方の 1 つは、外部スイッチの代わりに Firepower Threat Defense デバイスで追加のインターフェイスを使用することです。ブリッジグループのメンバー インターフェイスにエンドポイントを直接接続できます。また、BVI と同じネットワークにより多くのエンドポイントを追加するために、スイッチを接続できます。

管理/診断インターフェイス

管理ラベル付けされた物理ポート（または、Firepower Threat Defense Virtual の場合は Management0/0 仮想インターフェイス）には、2 つの別個のインターフェイスが実際に関連付けられています。

- 管理仮想インターフェイス：この IP アドレスは、システムの通信に使用されます。これはシステムがスマートライセンスに使用し、データベースの更新情報を取得するためのアドレスです。これに対して管理セッションを開くことができます (Firepower Device Manager および CLI)。[システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で定義されている管理アドレスを設定する必要があります。

- 診断物理インターフェイス：物理管理ポートは、実際には診断という名前が付けられています。外部 syslog サーバに syslog メッセージを送信するためにこのインターフェイスを使用できます。診断物理インターフェイスの IP アドレスの設定は任意です。syslog で使用する場合にのみ、インターフェイスを設定します。このインターフェイスは、**[デバイス (Device)] > [インターフェイス (Interfaces)]** ページに表示され、そこで設定できます。診断物理インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。

(ハードウェア デバイス) 管理/診断を設定する際、物理ポートをネットワークに接続しないことをお勧めします。代わりに、管理 IP アドレスのみを設定し、インターネットからの更新情報を得るためのゲートウェイとして、データ インターフェイスを使用するように設定します。次に、HTTPS/SSH トラフィック (デフォルトで HTTPS は有効) への内部インターフェイスを開き、内部 IP アドレスを使用して Firepower Device Manager を開きます ([管理アクセス リストの設定 \(475 ページ\)](#) を参照)。

Firepower Threat Defense Virtual の推奨設定は、Management0/0 を内部インターフェイスと同じネットワークに接続し、内部インターフェイスをゲートウェイとして使用することです。診断用に別のアドレスを設定しないでください。

個別の管理ネットワークの設定に関する推奨事項

(ハードウェア デバイス) 分離した管理ネットワークを使用する場合は、物理管理/診断インターフェイスをスイッチまたはルータに有線で接続します。

Firepower Threat Defense Virtual では、Management0/0 を任意のデータ インターフェイスから個別のネットワークに接続します。デフォルトの IP アドレスを使用している場合、管理 IP アドレスまたは内部インターフェイス IP アドレスは同一サブネット上にあるため、いずれかを変更する必要があります。

その後、次の設定を行います。

- **[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)]** を選択して、接続されたネットワークで IPv4 または IPv6 アドレス (または両方) を設定します。必要に応じて、ネットワーク上の他のエンドポイントに IPv4 アドレスを指定するように DHCP サーバを設定できます。管理ネットワーク上にインターネットへのルートを持つルータがある場合、それをゲートウェイとして使用します。なければ、データ インターフェイスをゲートウェイとして使用します。
- インターフェイスを介して syslog サーバに syslog メッセージを送信しようとする場合にのみ、診断インターフェイスのアドレスを設定します (**[デバイス (Device)] > [インターフェイス (Interface)]**)。そうでない場合は、診断用のアドレスは設定しないでください。必要ありません。設定する IP アドレスは、管理 IP アドレスと同じサブネット上に存在する必要があります。DHCP サーバプールに設定することはできません。たとえば、デフォルト設定では 192.168.45.45 を管理アドレスとして使用し、192.168.45.46-192.168.45.254 を DHCP プールとして使用しているため、192.168.45.1 から 192.168.45.44 のアドレスを使用して診断アドレスを設定できます。

別の管理ネットワークのための管理/診断インターフェイス設定に関する制限事項

物理管理インターフェイスを配線する場合、または Firepower Threat Defense Virtual の場合は、Management0/0 を分離したネットワークに接続し、次の制限に従ってください。

- 管理ネットワークで DHCP サーバを設定する場合、管理インターフェイス ([デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)]) で設定します。診断 (物理) インターフェイスで DHCP サーバを設定することはできません。
- 管理ネットワークに別の DHCP サーバがある場合、それを無効にしないと管理インターフェイス上でその DHCP サーバが実行されます。一般に、特定のサブネットで複数の DHCP サーバを設定することはできません。
- 管理および診断の両方にアドレスを設定する場合、それらが同じサブネット上にあることを確認します。
- (ハードウェア デバイスのみ) 診断の IP アドレスを設定する場合であっても、データ インターフェイスを管理ゲートウェイとして使用できます。しかし、診断インターフェイスはデータ インターフェイスをゲートウェイとして使用することはありません。診断インターフェイスから他のネットワークへのパスが必要な場合、管理ネットワーク上の別のルータが、診断 IP アドレスから送信されるトラフィックをルーティングする必要があります。必要に応じて、診断インターフェイスにスタティック ルートを設定します ([デバイス (Device)] > [ルーティング (Routing)] を選択)。

セキュリティ ゾーン

各インターフェイスは単一のセキュリティゾーンに割り当てることができます。ゾーンに基づいてセキュリティポリシーを適用されます。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。

ブリッジグループでは、メンバー インターフェイスをゾーンに追加できますが、ブリッジ仮想インターフェイス (BVI) を追加することはできません。

ゾーンには診断/管理インターフェイスを含めません。ゾーンは、データ インターフェイスにのみ適用されます。

セキュリティ ゾーンは [オブジェクト (Objects)] ページで作成できます。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル: グローバルアドレスは、パブリック ネットワークで使用可能なパブリックアドレスです。ブリッジグループの場合、各メンバーインターフェイスではなくブリッジ

仮想インターフェイス (BVI) 上でグローバルアドレスを設定します。次のいずれかをグローバルアドレスとして指定することはできません。

- 内部で予約済みの IPv6 アドレス : fd00:: - 未指定のアドレス (::/128 など)
 - ループバック アドレス (::1/128)
 - マルチキャストアドレス (ff00:: - リンクローカル アドレス (fe80::
- リンクローカル : リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベートアドレスです。ルータは、リンクローカルアドレスを使用してパケットを転送するのではなく、特定の物理ネットワークセグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決およびネイバー探索などのネットワーク検出機能に使用できます。ブリッジグループでは、BVI で IPv6 を有効にすると、自動的に各ブリッジグループのメンバー インターフェイスのリンクローカルアドレスが設定されます。リンクローカルアドレスがセグメントでのみ使用可能であり、インターフェイス MAC アドレスに接続されているため、各インターフェイスは独自のアドレスを持つ必要があります。

最低限、IPv6 が動作するようにリンクローカルアドレスを設定する必要があります。グローバルアドレスを設定すると、リンクローカルアドレスがインターフェイスに自動的に設定されるため、リンクローカルアドレスを個別に設定する必要はありません。グローバルアドレスを設定しない場合は、リンクローカルアドレスを自動的にするか、手動で設定する必要があります。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーションフェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロスケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX を有効にするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。ギガビットイーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

インターフェイスに関する注意事項と制限事項

ここでは、インターフェイスに関する制限事項について説明します。

インターフェイス設定の制限事項

Firepower Device Manager を使用してデバイスを設定する場合、インターフェイス設定に関するいくつかの制限があります。次の機能のいずれかが必要である場合、デバイスを設定するために Firepower Management Center を使用する必要があります。

- ルーテッド ファイアウォール モードのみがサポートされます。トランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- パッシブ インターフェイスまたは ERSPAN インターフェイスを設定することはできません。
- インターフェイスをインライン（インラインセット内）またはインラインタップ（IPS オンリー処理用）に設定することはできません。IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティ ポリシーのみをサポートします。対照的に、ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、TCP の標準化などのファイアウォール機能の対象となります。また、任意で、セキュリティ ポリシーに従ってファイアウォールモードのトラフィックに IPS 機能を設定することもできます。
- EtherChannel や冗長インターフェイスは設定できません。
- 追加できるブリッジグループは1つだけです。
- IPv4 の PPPoE を設定することはできません。インターネット インターフェイスが DSL、ケーブル モデム、または ISP へのその他の接続に接続されていて、ISP が PPPoE を使用して IP アドレスを提供している場合、これらの構成を設定するには、Firepower Management Center を使用する必要があります。
- ASA 5512-X、5515-X、5525-X、5545-X および 5555-X と Firepower 2100 シリーズでは、オプションのネットワーク インターフェイス モジュールをインストールできます。モジュールはブートストラップ中（つまり、初期インストールまたは再イメージ化、ローカル/リモート管理間の切り替え時）にのみ検出されます。Firepower Device Manager はこれらのインターフェイスの速度とデュプレックスに正しいデフォルトを設定します。利用可能なインターフェイスの合計数を変更することなく、オプションのモジュールを、インターフェイスの速度やデュプレックスのオプションが変わるモジュールと交換する場合、交換されたインターフェイスの正しい速度やデュプレックスの値をシステムが認識できるように、デバイスを再起動します。デバイスとの SSH セッションまたはコンソールセッションで、**reboot** コマンドを入力します。次に、Firepower Device Manager で、機能の変更を含む各物理インターフェイスを編集し、有効な速度とデュプレックスのオプションを選択します。システムは元の設定を自動的に修正しないためです。すぐに変更を展開して、システムが正しく動作していることを確認します。



(注) モジュールをインターフェイスの総数が変更されたモジュールと交換した場合や、他のオブジェクトによって参照されたインターフェイスを削除した場合は、予期しない問題が発生することがあります。このような変更が必要な場合は、まずセキュリティゾーンのメンバーシップ、VPN 接続など、削除するインターフェイスへのすべての参照を削除してください。また、変更を行う前にバックアップを実行することもお勧めします。

- [Firepower Threat Defense Virtual へのインターフェイスの追加 \(186 ページ\)](#) で説明しているように、Firepower Threat Defense Virtual デバイスでは、デバイスを再初期化せずに、インターフェイスを追加または削除することはできません。ただし、インターフェイスを異なる速度/デュプレックス能力を持っているインターフェイスと単純に交換する場合は、システムで新しい速度/デュプレックス値が認識されるようにデバイスを再起動してください。CLI コンソールから、**reboot** コマンドを入力します。次に、Firepower Device Manager で、能力の変更を含む各インターフェイスを編集し、有効な速度とデュプレックスのオプションを選択します。システムは元の設定を自動的に修正しないためです。すぐに変更を展開して、システムの正しい動作を確認します。

デバイス モデルによる VLAN サブインターフェイスの最大数

デバイス モデルにより、設定できる VLAN サブインターフェイスの最大数が制限されます。データ インターフェイスでのみサブインターフェイスを設定することができ、管理インターフェイスでは設定できないことに注意してください。

次の表で、各デバイス モデルの制限について説明します。

モデル	VLAN サブインターフェイスの最大数
Firepower 2100	1024
Firepower Threat Defense Virtual	50
ASA 5506-X	30
ASA 5506W-X	
ASA 5506H-X	
ASA 5508-X	50
ASA 5512-X	100
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200

モデル	VLAN サブインターフェイスの最大数
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	25

物理インターフェイスの設定

少なくとも、使用する物理インターフェイスは有効にする必要があります。通常は名前も付けて、IPアドレッシングを設定します。VLANサブインターフェイスを設定する予定の場合、またはインターフェイスをブリッジグループに追加する予定の場合は、IPアドレッシングを設定しません。

接続されたネットワークでの送信を一時的に防ぐために、インターフェイスを無効にできます。インターフェイスの設定を削除する必要はありません。

手順

- ステップ 1** [デバイス (Device)] をクリックしてから、[インターフェイス (Interface)] サマリーにあるリンクをクリックします。
インターフェイスリストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。
- ステップ 2** 編集する物理インターフェイスの [編集 (edit)] アイコン () をクリックします。
- ステップ 3** 次の設定を行います。

Ethernet1/2
Edit Physical Interface

Interface Name: inside Mode: Routed Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address IPv6 Address Advanced

Type: Static

IP Address and Subnet Mask: 10.99.10.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask: 10.99.10.2 / 24
e.g. 192.168.5.16

CANCEL OK

- a) [インターフェイス名 (Interface Name)] を設定します。

インターフェイスの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

- b) [ステータス (Status)] スライダを [有効 (enabled)] 設定 () に設定します。

この物理インターフェイスのサブインターフェイスを設定する予定の場合、すでに設定している可能性が高いです。[保存 (Save)] をクリックして、[VLAN サブインターフェイスと 802.1Q トランッキングの設定 \(179 ページ\)](#) に進みます。保存しない場合は、次に進みません。

(注) サブインターフェイスを設定している場合でも、インターフェイスに名前を付けて、IPアドレスを指定できます。これは一般的な設定ではありませんが、必要だとわかっている場合は設定できます。

c) (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 4 [IPv4アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [ダイナミック (Dynamic)] (DHCP) : ネットワーク上の DHCP サーバからアドレスを取得する必要がある場合は、このオプションを選択します。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)] : DHCP サーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1~255 の間です。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)] : デフォルトルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトであるこのオプションを選択します。
- [スタティック (Static)] : 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。[DHCP サーバの設定 \(479 ページ\)](#) を参照してください。

ステップ 5 (オプション) [IPv6アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

- [状態 (State)] : グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効 (Enabled)] を選択します。リンクローカルアドレスはインターフェイスの MAC アドレス (*Modified EUI-64* 形式) に基づいて生成されます。

(注) IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定 (Address Auto Configuration)]: アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバルプレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカルアドレスは Modified EUI-64 インターフェイス ID に基づいています。

RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、FTD デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制 (Suppress RA)] を選択します。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]: ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、[IPv6 アドレス指定 \(166 ページ\)](#) を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル (Link - Local)] オプションを選択します。リンクローカルアドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループ インターフェイスには設定できません。

(注) リンクローカルアドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feec:6a82。Modified EUI-64 形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカルアドレスによりパケットがドロップされることがあります。

- [RA を抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Firepower Threat Defense デバイスはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ (ICMPv6 Type 133) に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定できます。

FTD デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス (外部インターフェイスなど) では、これらのメッセージを抑制できます。

ステップ 6 (任意) 詳細オプションの設定 (184 ページ)。

詳細設定には、ほとんどのネットワークで最適となるデフォルトが用意されています。ネットワーク問題を解決する場合に限り、これらを編集します。

ステップ7 [OK] をクリックします。

次のタスク

- インターフェイスを適切なセキュリティゾーンに追加します。[セキュリティゾーンの設定 \(136 ページ\)](#) を参照してください。

ブリッジグループの設定

ブリッジグループは1つ以上のインターフェイスをグループ化する仮想インターフェイスです。インターフェイスをグループ化する主な理由は、スイッチドインターフェイスのグループを作成することにあります。そのため、ブリッジグループに含まれているインターフェイスにワークステーションやその他のエンドポイントデバイスを直接接続できます。それらは別の物理スイッチを介して接続する必要はありませんが、スイッチをブリッジグループメンバーに接続することもできます。

グループメンバーにはIPアドレスはありません。代わりに、すべてのメンバーインターフェイスがブリッジ仮想インターフェイス (BVI) のIPアドレスを共有します。BVIでIPv6を有効にすると、メンバーインターフェイスには一意のリンクローカルアドレスが自動的に割り当てられます。

メンバーインターフェイスは個別に有効または無効にします。そのため、未使用のインターフェイスはブリッジグループから削除することなく無効化できます。ブリッジグループ自体は常に有効になっています。

通常は、メンバーインターフェイス経由で接続されているエンドポイントのIPアドレスを提供するブリッジグループインターフェイス (BVI) にDHCPサーバを設定します。ただし、必要に応じて、メンバーインターフェイスに接続されているエンドポイントにスタティックアドレスを設定できます。ブリッジグループ内のすべてのエンドポイントには、ブリッジグループのIPアドレスと同じサブネットのIPアドレスが必要です。

注意事項と制約事項

- ブリッジグループを1つ追加できます。
- Firepower 2100 シリーズまたは Firepower Threat Defense Virtual デバイスにブリッジグループを設定することはできません。
- すべての ASA 5506-X モデル、新バージョンの 6.2+ システム、または再イメージ化された 6.2+ システムの場合、デバイスは、**inside** という名前のブリッジグループ BVI1 が事前に設定されています。このブリッジグループには、**outside** インターフェイスを除くすべてのデータインターフェイスが含まれています。そのため、デバイスにはインターネットやその他のアップストリームネットワークへの接続に使用される1つのポートが事前に設定されています。また、その他のポートはすべて有効になっていて、エンドポイントへの直接接続に使用できます。ISA 3000 モデルは、このデフォルトの構成も付属します。新しい

サブネットで内部インターフェイスを使用する場合は、まず必要なインターフェイスを BVII から削除する必要があります。

始める前に

ブリッジグループのメンバーになるインターフェイスを設定します。具体的には、各メンバーインターフェイスは、次の要件を満たしている必要があります。

- インターフェイスには名前が必要です。
- 静的に、または DHCP を介してインターフェイス用に定義された IPv4 または IPv6 アドレスは設定できません。現在使用しているインターフェイスからアドレスを削除する必要がある場合、そのインターフェイスのその他の設定（アドレスを持つインターフェイスに依存するスタティックルート、DHCP サーバ、NAT ルールなど）も削除する必要がある場合があります。
- インターフェイスをブリッジグループに追加する前に、セキュリティゾーン（ゾーン内にある場合）からそのインターフェイスを削除し、そのインターフェイスのすべての NAT ルールを削除する必要があります。

手順

ステップ 1 [デバイス (Device)] をクリックして、[インターフェイス (Interfaces)] サマリーのリンクをクリックします。

インターフェイスリストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。ブリッジグループがすでに存在している場合、それはフォルダです。開く/閉じる矢印をクリックして、メンバーインターフェイスを表示します。メンバーインターフェイスは、リストにも個別に表示されます。

ステップ 2 次のいずれかを実行します。

- BVII ブリッジグループの編集アイコン (🔗) をクリックします。
- 歯車のドロップダウンリストから [ブリッジグループインターフェイスの追加 (Add Bridge Group Interface)] を選択して、新しいグループを作成します。

(注) ブリッジグループは 1 つ設定できます。ブリッジグループをすでに定義している場合は、新しいグループ作成するのではなく、そのグループを編集する必要があります。新しいブリッジグループを作成する必要がある場合は、まず既存のブリッジグループを削除する必要があります。
- 不要になったブリッジグループの [削除 (delete)] アイコン (🗑️) をクリックします。ブリッジグループを削除すると、そのメンバーは標準のルーテッドインターフェイスになり、NAT ルールまたはセキュリティゾーンのメンバーシップはすべて維持されます。インターフェイスを編集して、IP アドレスを付与できます。新しいブリッジグループにそ

これらのインターフェイスを追加する場合は、まず NAT ルールを削除し、インターフェイスをセキュリティゾーンから削除する必要があります。

ステップ 3 以下を設定します。

- a) (任意) [インターフェイス名 (Interface Name)] を設定します。

ブリッジグループの名前 (最大 48 文字) を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。この BVI を他の名前付きインターフェイスとの間におけるルーティングに参加させる場合は、名前を設定します。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所 (セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む) に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

- b) (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

- c) [ブリッジグループメンバー (Bridge Group Members)] のリストを編集します。

1 つのブリッジグループに最大 64 個のインターフェイスまたはサブインターフェイスを追加できます。

- インターフェイスの追加: プラスアイコン (+) をクリックし、1 つまたは複数のインターフェイスをクリックして、[OK] をクリックします。

- インターフェイスの削除：インターフェイスにカーソルを合わせ、右側に表示される [x] をクリックします。

ステップ 4 [IPv4アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [スタティック (Static)]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。ブリッジグループの IP アドレスとサブネットマスクを入力します。接続されているエンドポイントはすべて、このネットワーク上に存在することになります。ブリッジグループが事前設定されたモデルでは、デフォルトの BVII 「inside」 ネットワークは 192.168.1.1/24 (例：255.255.255.0) です。このアドレスがネットワーク上ですでに使用されていないことを確認します。

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレスプールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。DHCP サーバの設定 (479 ページ) を参照してください。

- [ダイナミック (Dynamic)] (DHCP)：ネットワーク上の DHCP サーバからアドレスを取得する必要がある場合は、このオプションを選択します。これはブリッジグループの一般的なオプションではありませんが、必要に応じて設定できます。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)]：DHCP サーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1~255 の間です。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)]：デフォルトルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

ステップ 5 (オプション) [IPv6アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

- [状態 (State)]：グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効 (Enabled)] を選択します。リンクローカルアドレスはインターフェイスの MAC アドレス (Modified EUI-64 形式) に基づいて生成されます。

(注) IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレ

フィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6アドレッシングの詳細については、[IPv6アドレス指定（166ページ）](#)を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカルアドレスでは、ローカルネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループインターフェイスには設定できません。

(注) リンクローカルアドレスは、FE8、FE9、FEA、またはFEBで始まっている必要があります。例、fe80::20d:88ff:feec:6a82。Modified EUI-64形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスでModified EUI-64形式の使用が強制される場合、手動で割り当てたリンクローカルアドレスによりパケットがドロップされることがあります。

- [RAを抑制（Suppress RA）]：ルータアドバタイズメントを抑制するかどうかを指定します。ネイバーデバイスがデフォルトのルータアドレスをダイナミックに把握できるように、Firepower Threat Defense デバイスはルータアドバタイズメントに参加できます。デフォルトでは、ルータアドバタイズメントメッセージ（ICMPv6 Type 134）は、設定済みの各IPv6インターフェイスに定期的に送信されます。

ルータアドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータアドバタイズメントメッセージを待つことなくただちに自動設定できます。

FTD デバイスでIPv6プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを抑制できます。

ステップ6（オプション）[詳細オプションの設定（184ページ）](#)。

ブリッジグループメンバーインターフェイスに対して最も詳細なオプションを設定しますが、一部はブリッジグループインターフェイスでも使用できます。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ7 [OK] をクリックします。

次のタスク

- 使用する予定のすべてのメンバーインターフェイスが有効になっていることを確認します。
- ブリッジグループのDHCPサーバを設定します。[DHCPサーバの設定（479ページ）](#)を参照してください。
- メンバーインターフェイスを適切なセキュリティゾーンに追加します。[セキュリティゾーンの設定（136ページ）](#)を参照してください。

- アイデンティティ、NAT、アクセスなどのポリシーにより、ブリッジグループとメンバーインターフェイスに必要なサービスが提供されることを確認します。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが1つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはデバイスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

物理インターフェイスをスイッチのトランクポートに接続する場合は、サブインターフェイスを作成します。スイッチ トランク ポートで表示できる各 VLAN のサブインターフェイスを作成します。物理インターフェイスをスイッチのアクセスポートに接続する場合は、サブインターフェイスを作成しても意味がありません。

注意事項と制約事項

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。サブインターフェイスでトラフィックを通過させるには物理的インターフェイスを有効にする必要があるため、インターフェイスに名前を付けないことでトラフィックを通過させないようにします。物理インターフェイスにタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます。
- 必要に応じて詳細設定を変更することはできますが、ブリッジグループメンバーインターフェイスの IP アドレスを設定することはできません。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- FTD はダイナミック トランキング プロトコル (DTP) をサポートしないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスと同じバーンドイン MAC アドレスを使用するので、FTD で定義されたサブインターフェイスに一意の MAC アドレスを割り当てる必要がある場合があります。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interface)] サマリーにあるリンクをクリックします。

インターフェイスリストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。

ステップ 2 次のいずれかを実行します。

- 歯車のドロップダウンリストから [サブインターフェイスの追加 (Add Subinterface)] を選択し、サブインターフェイスを新規作成します。
- 編集するサブインターフェイスの編集アイコン (🔗) をクリックします。

サブインターフェイスが不要になった場合は、このサブインターフェイスの [削除 (delete)] アイコン (🗑️) をクリックして削除します。

ステップ 3 [ステータス (Status)] スライダを [有効 (enabled)] 設定 (🔘) に設定します。

ステップ 4 親インターフェイス、名前、および説明を設定します。

a) [親インターフェイス (Parent Interface)] を選択します。

親インターフェイスは、サブインターフェイスの追加先となる物理インターフェイスです。いったん作成したサブインターフェイスの親インターフェイスは変更できません。

b) [サブインターフェイス名 (Subinterface Name)] (最大 48 文字) を設定します。

英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所 (セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む) に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

c) (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

d) [VLAN ID] を設定します。

このサブインターフェイス上のパケットにタグを付けるために使用する VLAN ID を 1 ~ 4094 の範囲で入力します。

e) [サブインターフェイス ID (Subinterface ID)] を設定します。

サブインターフェイス ID を 1 ~ 4294967295 の範囲の整数で入力します。この ID は、インターフェイス ID に追加されます。たとえば、Ethernet1/1.100 のようになります。便宜上 VLAN ID を一致させることもできますが、必須ではありません。いったん作成したサブインターフェイスの ID は変更できません。

ステップ 5 [IPv4アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [ダイナミック (Dynamic)] (DHCP) : ネットワーク上の DHCP サーバからアドレスを取得する必要がある場合は、このオプションを選択します。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)] : DHCP サーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1~255 の間です。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)] : デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトであるこのオプションを選択します。
- [スタティック (Static)] : 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネットマスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。DHCP サーバの設定 (479 ページ) を参照してください。

ステップ 6 (オプション) [IPv6アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

- [状態 (State)] : グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効 (Enabled)] を選択します。リンクローカルアドレスはインターフェイスの MAC アドレス (Modified EUI-64 形式) に基づいて生成されます。

(注) IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定 (Address Auto Configuration)] : アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバルプレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部には

アクセスできません。リンクローカルアドレスは Modified EUI-64 インターフェイス ID に基づいています。

RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、FTD デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制 (Suppress RA)] を選択します。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)] : ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、[IPv6 アドレス指定 \(166 ページ\)](#) を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル (Link - Local)] オプションを選択します。リンクローカルアドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループ インターフェイスには設定できません。

(注) リンクローカルアドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feec:6a82。Modified EUI-64 形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカルアドレスによりパケットがドロップされることがあります。

- [RA を抑制 (Suppress RA)] : ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Firepower Threat Defense デバイスはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ 要請メッセージ (ICMPv6 Type 133) に応答して送信されます。ルータ 要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定できます。

FTD デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス (外部インターフェイスなど) では、これらのメッセージを抑制できます。

ステップ 7 (オプション) [詳細オプションの設定 \(184 ページ\)](#)。

詳細設定には、ほとんどのネットワークで最適となるデフォルトが用意されています。ネットワーク問題を解決する場合に限り、これらを編集します。

ステップ 8 [OK] をクリックします。

次のタスク

- サブインターフェイスを適切なセキュリティゾーンに追加します。[セキュリティゾーンの設定 \(136 ページ\)](#) を参照してください。

高度なインターフェイス オプションの設定

[詳細 (Advanced)] オプションには、MTU、ハードウェア設定、管理専用、MAC アドレス、およびその他の設定が含まれています。

MTU について

MTU は、Firepower Threat Defense デバイスが特定のイーサネット インターフェイスで送信可能な最大フレーム ペイロード サイズを指定します。MTU の値は、イーサネット ヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば MTU を 1500 に設定した場合、想定されるフレーム サイズはヘッダーを含めて 1518 バイト、VLAN を使用する場合は 1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

パス MTU ディスカバリ

Firepower Threat Defense デバイスは、Path MTU Discovery (RFC 1191 の定義に従う) をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

MTU およびフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットをフラグメント化することはできません。したがって、フラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

UDP または ICMP の場合、アプリケーションではフラグメント化を避けるために MTU を考慮する必要があります。



(注) Firepower Threat Defense デバイスはメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

MTU とジャンボ フレーム

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- トラフィックパスの MTU の一致：すべての FTD インターフェイスとトラフィックパス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボフレームへの対応：ジャンボフレームとは、標準的な最大値 1522 バイト（レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む）より大きく、9216 バイトまでのイーサネットパケットのことです。ジャンボフレームに対応するために、9198 バイトまでの MTU を設定できます。Firepower Threat Defense Virtual の最大値は 9184 です。



(注) MTU を増やすとジャンボフレームに割り当てられるメモリが増加し、他の機能（アクセスルールなど）の最大使用量が制限される場合があります。ASA 5500-X シリーズデバイスまたは Firepower Threat Defense Virtual で、MTU をデフォルトの 1500 以上に増やす場合、システムを再起動する必要があります。ジャンボフレームのサポートが常に有効な場合、Firepower モデルを再起動する必要はありません。

詳細オプションの設定

高度なインターフェイスオプションには、ほとんどのネットワークに適合するデフォルト設定が用意されています。ネットワークの問題を解決している場合にのみ、これを設定します。

次の手順では、インターフェイスが定義済みであることを前提としています。インターフェイスを最初に編集または作成するときに、これらの設定を編集することもできます。

制限事項

- ブリッジグループの場合は、このほとんどのオプションはメンバーインターフェイスに対して設定します。DAD 試行回数を除き、これらのオプションはブリッジ仮想インターフェイス（BVI）では使用できません。
- Firepower 2100 デバイス上の管理インターフェイスに、MTU、デュプレックス、または速度を設定することはできません。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interface)] サマリーにあるリンクをクリックします。

インターフェイスリストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。

ステップ 2 編集するインターフェイスの編集アイコン (🔗) をクリックします。

ステップ 3 [詳細オプション (Advanced Options)] をクリックします。

ステップ 4 データ インターフェイスを管理専用に指定する場合は、[管理専用 (Management Only)] を選択します。

管理専用インターフェイスはトラフィックの通過を許可しないため、データインターフェイスを管理専用に設定する意味はあまりありません。管理/診断インターフェイスは、常に管理専用であるため、この設定を変更することはできません。

ステップ 5 [MTU] (最大伝送ユニット) を任意の値に設定します。

デフォルトの MTU は 1500 バイトです。64 ~ 9198 (Firepower Threat Defense Virtual の場合は 9184) の値を指定できます。ジャンボフレームが頻繁にやり取りされるネットワークでは、大きな値に設定します。

(注) ASA 5500-X シリーズデバイス、ISA 3000 シリーズデバイス、または Firepower Threat Defense Virtual で MTU を 1500 より大きい値に設定する場合は、デバイスを再起動する必要があります。CLI にログインして **reboot** コマンドを使用します。ジャンボフレームのサポートが常に有効な場合、Firepower モデルを再起動する必要はありません。

ステップ 6 (物理インターフェイスのみ) 速度およびデュプレックスの設定を変更します。

デフォルトでは、インターフェイスは接続相手のインターフェイスに対し、互いに最適なデュプレックスおよび速度をネゴシエートしますが、必要に応じて、特定のデュプレックスおよび速度を強制的に適用することもできます。記載されているオプションは、インターフェイスでサポートされるもののみです。ネットワーク モジュールのインターフェイスにこれらのオプションを設定する前に、[インターフェイス設定の制限事項 \(168 ページ\)](#) をお読みください。

- [二重 (Duplex)] : [自動 (Auto)]、[ハーフ (Half)]、[フル (Full)]、または [デフォルト (Default)] を選択します。[自動 (Auto)] は、インターフェイスによってサポートされる場合のみデフォルトとなります。たとえば、Firepower 2100 シリーズデバイスの SFP インターフェイスでは [Auto] を選択できません。

Firepower Device Manager が設定を試行できないことを示すために [Default] を選択します。既存の設定は、すべてそのまま変更されません。

- [速度 (Speed)] : [自動 (Auto)] を選択してインターフェイスに速度をネゴシエートさせるか (これがデフォルトです)、または特定の速度 : [10]、[100]、[1000]、[10000] Mbps を選択します。 次の特別オプションも選択できます。
 - [ネゴシエートなし (No Negotiate)] : ファイバインターフェイスの場合は、速度を 1000 Mbps に設定し、リンク パラメータをネゴシエートしません。これは、これらのインターフェイスのデフォルトの設定です。
 - [デフォルト (Default)] : Firepower Device Manager が設定を試行できないことを示します。いずれかが既存の設定のまま変更されていません。

インターフェイスのタイプによって、選択可能なオプションが制限されます。たとえば、Firepower 2100 シリーズデバイスの SFP+ インターフェイスは 1000 (1 Gbps) および 10000

(10 Gbps) のみをサポートし、SFP インターフェイスは 1000 (1 Gbps) のみをサポートしますが、GigabitEthernet ポートは 10000 (10 Gbps) をサポートしません。その他のデバイス上の SPF インターフェイスでは [ネゴシエートなし (No Negotiate)] が必須場合があります。インターフェイスのサポート対象については、ハードウェアのマニュアルを参照してください。

ステップ 7 [IPv6設定 (IPv6 Configuration)] を変更します。

- [Enable DHCP for IPv6 address configuration] : IPv6 ルータのアドバタイズメントパケットに、管理アクセス設定フラグを設定するかどうか。このフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。
- [Enable DHCP for IPv6 non-address configuration] : IPv6 ルータのアドバタイズメントパケットに、その他のアクセス設定フラグを設定するかどうか。このフラグは、DHCPv6 から DNS サーバアドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。
- [DADの試行 (DAD Attempts)] : インターネット上で重複アドレス検出 (DAD) を実行する頻度 (0 ~ 600)。デフォルトは 1 です。ステートレス自動設定プロセスでは、DAD はアドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を検証します。重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバルアドレスであれば、そのアドレスは使用されません。インターフェイスは、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。重複アドレス検出 (DAD) プロセスを無効にするには、この値を 0 に設定します。

ステップ 8 [OK] をクリックします。

Firepower Threat Defense Virtual へのインターフェイスの追加

FTDv を展開する際は、仮想マシンにインターフェイスを割り当てます。次に、FDM 内から、ハードウェア デバイスを設定する場合と同じ方法で、それらのインターフェイスを設定します。

ただし、仮想マシンにさらに仮想インターフェイスを追加して、FDM にそれらを自動的に認識させることはできません。FTDv と同等の物理インターフェイスを追加する必要がある場合は、基本的に初めからやり直す必要があります。新しい仮想マシンを導入することもできれば、次の手順を使用することもできます。



注意 仮想マシンにインターフェイスを追加する場合は、完全に FTDv 設定を消去する必要があります。設定でそのまま残しておく唯一の部分は、管理アドレスとゲートウェイ設定です。

始める前に

FDM で次の手順を実行します。

- FTDv 設定を調べ、新しい仮想マシンで複製する設定値を書き留めておきます。
- [デバイス (Devices)] > [スマートライセンス (Smart License)] > [設定の表示 (View Configuration)] の順に選択し、すべての機能ライセンスを無効にします。

手順

ステップ 1 FTDv の電源を切ります。

ステップ 2 仮想マシン ソフトウェアを使用して、FTDv にインターフェイスを追加します。

VMware の場合、仮想アプライアンスはデフォルトで e1000 (1 Gbit/s) インターフェイスを使用します。また、vmxnet3 または ixgbe (10 Gbit/s) インターフェイスを使用することもできます。

ステップ 3 FTDv の電源を入れます。

ステップ 4 FTDv コンソールを開いて、ローカルマネージャを削除し、その後、ローカルマネージャを有効にします。

ローカルマネージャを削除してから、それを有効にすると、デバイス設定がリセットされ、システムに新しいインターフェイスを認識させることができます。管理インターフェイス設定はリセットされません。次の SSH セッションはコマンドを表示します。

```
> show managers
Managed locally.

> configure manager delete

If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled

> show managers
No managers configured.

> configure manager local
>
```

ステップ 5 Firepower Device Manager へのブラウザセッションを開き、デバイスのセットアップ ウィザードを完了して、デバイスを設定します。[初期設定の完了 \(27 ページ\)](#) を参照してください。

モニタリング インターフェイス

次の領域に、インターフェイスに関する一部の基本情報を表示できます。

- **[デバイス (Device)]**。インターフェイスの現在の状態をモニタするには、ポート グラフィックを使用します。ポートにマウス ポインタを合わせると、その IP アドレス、有効ステータス、リンク ステータスが表示されます。IP アドレスは DHCP を使用して静的に割り当てたり取得したりできます。

インターフェイス ポートは、次のカラー コーディングを使用します。

- 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
 - グレー：インターフェイスは無効です。
 - オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。
- **[モニタリング (Monitoring)] > [システム (System)]**。[スループット (Throughput)] ダッシュボードには、システムを介して移動するトラフィックに関する情報が表示されます。すべてのインターフェイスに関する情報を表示できます。または、調査する特定のインターフェイスを選択できます。
 - **[モニタリング (Monitoring)] > [ゾーン (Zones)]**。これらのダッシュボードにはインターフェイスを設定するセキュリティゾーンに基づく統計情報が表示されます。詳細について、この情報を掘り下げることができます。

CLI でのインターフェイスのモニタリング

CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用し、インターフェイス関連の動作と統計情報に関する詳細情報を取得することもできます。

- **show interface** はインターフェイスの統計情報と設定情報を表示します。このコマンドには多数のキーワードがあり、必要な情報を取得するために使用できます。使用可能なオプションを表示するには、「?」をキーワードとして使用します。
- **show ipv6 interface** はインターフェイスに関する IPv6 設定情報を表示します。
- **show bridge-group** はブリッジ仮想インターフェイス (BVI) に関する情報を表示し、メンバー情報と IP アドレスが含まれます。
- **show conn** は現在インターフェイスを通じて確立されている接続に関する情報を表示します。
- **show traffic** は各インターフェイスを介したトラフィック フローに関する統計情報を表示します。

- **show ipv6 traffic** はデバイスを介した IPv6 トラフィック フローに関する統計情報を表示します。
- **show dhcpd** はインターフェイスの DHCP 使用状況に関する統計とその他の情報を表示し、特にインターフェイスで設定されている DHCP サーバに関する情報が含まれます。

インターフェイスの例

使用例の章には、次のインターフェイス関連の例が含まれています。

- [Firepower Device Manager でデバイスを設定する方法 \(51 ページ\)](#)
- [サブネットを追加する方法 \(85 ページ\)](#)



第 8 章

ルーティング

システムはルーティングテーブルを使用して、システムに入力されるパケットの出力インターフェイスを決定します。ここでは、ルーティングの基本とデバイスでのルーティングの設定方法について説明します。

- [ルーティングの概要 \(191 ページ\)](#)
- [スタティック ルート \(197 ページ\)](#)
- [ルーティングのモニタリング \(200 ページ\)](#)

ルーティングの概要

ここでは、FTDデバイス内でルーティングがどのように動作するのかを説明します。ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも1つの中間ノードがあります。ルーティングには、最適なルーティングパスの決定と、ネットワーク経由のパケットの転送という2つの基本的なアクティビティが含まれます。

ルート タイプ

ルートには、スタティックまたはダイナミックの2つの主要な種類があります。

スタティックルートは、明示的に定義するものです。これらは通常は優先度の高い安定したルートで、ルートの宛先へのトラフィックを常に正しいインターフェイスに送信するために使用されます。たとえば、その他のルートでカバーされていないすべてのトラフィックをカバーする、デフォルトのスタティックルート（つまり IPv4 では 0.0.0.0/0、IPv6 では ::/0）を作成する場合などです。別の例では、常に使用する内部syslogサーバへのスタティックルートがあります。

ダイナミックルートは、OSPF、BGP、EIGRP、IS-IS、またはRIPなどのルーティングプロトコルの動作を通じて学習されるものです。ルートを直接定義することはありません。その代わりにルーティングプロトコルを設定すると、システムはネイバルータと通信してルーティングアップデートを送信し、次にルーティングアップデートを受信します。

ダイナミックルーティングプロトコルはルーティングテーブルを調整し、着信ルーティング更新メッセージを分析することで、ネットワーク状況の変化に対応します。ネットワークが変化したことをメッセージが示している場合は、システムはルートを再計算し、新しいルーティングアップデートメッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティングテーブルを変更します。

スタティックルーティングは単純であり、基本的なルーティングの目的を果たします。ネットワークトラフィックが比較的予想しやすい環境や、ネットワーク設計が比較的単純な環境での使用に適しています。ただし、編集しない限りスタティックルートは変更できないため、ネットワークの変化に対応することはできません。

小規模ネットワークがある場合を除き、通常はスタティックルートを1つまたは複数のダイナミックルーティングプロトコルと組み合わせます。明示ルートに一致しないトラフィックのデフォルトルートとして、少なくとも1つのスタティックルートを定義します。



(注) スマート CLI を使用して次のルーティングプロトコルを設定することができます : OSPF。FlexConfig を使用して、ASA ソフトウェアでサポートされるその他のルーティングプロトコルを設定します。

ルーティングテーブルとルート選択

NAT 変換 (xlates) およびルールで出力インターフェイスを決定しない場合、システムはルーティングテーブルを使用してパケットのパスを決定します。

ルーティングテーブルのルートには、指定ルートに相対的な優先順位を定める「アドミニストレーティブディスタンス」というメトリックが含まれています。パケットが複数のルートエントリと一致する場合、最短距離のルートエントリが使用されます。直接接続されたネットワーク (インターフェイス上で定義されたネットワーク) の距離は0のため、これが常に優先されます。スタティックルートのデフォルトの距離は1ですが、1～254の距離で作成できます。

特定の宛先が指定されたルートは、デフォルトルート (宛先が0.0.0.0/0または::/0のルート) よりも優先されます。

ルーティングテーブルへの入力方法

FTD のルーティングテーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミックルーティングプロトコルで検出されたルートを入力できます。FTD は、ルーティングテーブルに含まれるスタティックルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティングテーブルに追加されると、ルーティングテーブルに残るルートは次のように決定されます。

- 2つのルートのネットワークプレフィックス長（ネットワークマスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが2つのうちどちらを使用するかを決定します。

たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

- RIP : 192.168.32.0/24
- OSPF : 192.168.32.0/19

OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティングテーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決めます。

- FTD が、1つのルーティングプロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティングテーブルに入力されます。

メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コストパスに対してロード バランシングが行われます。

- FTD が、ある宛先へのルーティングプロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティングテーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティングプロトコルによって検出されるルート、またはルーティングプロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブ ディスタンスが同じ場合、デフォルトのアドミニストレーティブ ディスタンスが小さい方のルートがルーティングテーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブ ディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、Firepower Threat Defense デバイスが最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への2つのルートについて常にベストパスを判定できるわけではありません。

各ルーティングプロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。次の表に、Firepower Threat Defense デバイスがサポートするルーティングプロトコルのデフォルトのアドミニストレーティブ ディスタンス値を示します。

表 4: サポートされるルーティングプロトコルのデフォルトアドミニストレーティブディスタンス

ルートの送信元	デフォルトアドミニストレーティブディスタンス
接続中のインターフェイス	0
スタティックルート	1
EIGRP 集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカル BGP	200
不明	255

アドミニストレーティブディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、Firepower Threat Defense デバイスが OSPF ルーティングプロセス（デフォルトのアドミニストレーティブディスタンスが 110）と RIP ルーティングプロセス（デフォルトのアドミニストレーティブディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティングプロセスの方が優先度が高いため、Firepower Threat Defense デバイスは OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティングテーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、Firepower Threat Defense デバイスは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された Firepower Threat Defense デバイスのルーティングテーブルにだけ影響します。アドミニストレーティブディスタンスがルーティングアップデートでアドバタイズされることはありません。

アドミニストレーティブディスタンスは、ルーティングプロセスに影響を与えません。ルーティングプロセスは、ルーティングプロセスで検出されたか、またはルーティングプロセスに再配布されたルートだけをアドバタイズします。たとえば、RIP ルーティングプロセスは、のルーティングテーブルで OSPF ルーティングプロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミック ルートとフローティングスタティック ルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされているためにインストールできなかった場合、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティングテーブルメンテナンスプロセスが、登録されたバックアップルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先ルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティング スタティック ルートを作成できます。フローティング スタティック ルートとは、単に、Firepower Threat Defense デバイス で動作しているダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブディスタンスが設定されているスタティックルートです。ダイナミックルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエン트리と一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエン트리と一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエン트리と一致し、パケットはネットワークプレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティングテーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます (24 ビットと 19 ビット)。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。



- (注) ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ実践として、データトラフィックを管理トラフィックから分離しなければならない場合があります。この分離を実現するために、FTDは管理専用トラフィックとデータトラフィックに個別のルーティングテーブルを使用します。個別のルーティングテーブルは、データと管理用に別のデフォルトルートを作成できることを意味します。

デバイス間トラフィックでは、常にデータルーティングテーブルが使用されます。

デバイス間トラフィックでは、そのタイプに応じて、デフォルトで管理ルーティングテーブルまたはデータルーティングテーブルのいずれかが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デバイス間トラフィックの管理テーブルには、HTTP、SCP、TFTP、などを使用してリモートファイルを開く機能が含まれています。

データテーブルのデバイス間トラフィックには、ping、DNS、DHCPなどの他のすべての機能が含まれています。

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。FTDは、正しいルーティングテーブルをチェックし、そのインターフェイスのルートがないか調べます。たとえば、管理専用インターフェイスにpingを送信する必要がある場合は、ping機能でそのインターフェイスを指定します。そうではなく、データルーティングテーブルにデフォルトルートがある場合は、デフォルトルートに一致し、管理ルーティングテーブルにフォールバックすることは決してありません。

管理ルーティングテーブルは、データインターフェイスルーティングテーブルとは分離したダイナミックルーティングをサポートします。ダイナミックルーティングプロセスは管理専用インターフェイスまたはデータインターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。

管理専用インターフェイスには、すべてのManagement x/x（「diagnostic」と名付けられた）インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。



- (注) このルーティングテーブルは、FMCとの通信に使用する特別なFTD管理論理インターフェイスには影響しません。そのインターフェイスには独自のルーティングテーブルが備わっています。一方、診断論理インターフェイスは、この項で説明している管理専用ルーティングテーブルを使用します。



- (注) このルーティングテーブルは、ライセンスサーバとの通信またはデータベースの更新に使用する特別な FTD 管理仮想インターフェイスには影響を及ぼしません。このインターフェイスには独自のルーティングテーブルが備わっています。一方、診断物理インターフェイスは、この項で説明している管理専用ルーティングテーブルを使用します。

等コスト マルチパス (ECMP) ルーティング

Firepower Threat Defense デバイスは、等コスト マルチパス (ECMP) ルーティングをサポートしています。

インターフェイスごとに最大 3 の等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロード バランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレス、着信トラフィック、プロトコル、送信元ポートおよび宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMPは複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを実験することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

スタティック ルート

スタティックルートを作成して、ネットワークの基本的なルーティングを提供することができます。

スタティック ルートとデフォルト ルートについて

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティックルーティングとダイナミックルーティングのどちらかを使用して、ホストまたはネットワークへのルートを実験する必要があります。通常は、少なくとも1つのスタティックルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルトルート (通常、ネクスト ホップ ルータ) を設定する必要があります。

デフォルトルート

最も単純なオプションは、すべてのトラフィックをアップストリームルータに送信するようにデフォルトスタティックルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルトルートは、既知のルートもスタティックルートも指定されていないIPパケットすべてを、FTDデバイスが送信するゲートウェイのIPアドレスを特定するルートです。デフォルトスタティックルートとは、つまり宛先のIPアドレスとして0.0.0.0/0 (IPv4) または::/0 (IPv6) が指定されたスタティックルートのことです。

デフォルトルートを常に定義する必要があります。

FTDはデータトラフィックと管理トラフィックに別々のルーティングテーブルを使用するため、必要に応じて、データトラフィック用のデフォルトルートと管理トラフィック用の別のデフォルトルートを設定できます。デバイス間トラフィックでは、タイプに応じてデフォルトで管理またはデータルーティングテーブルが使用されます（[管理トラフィック用ルーティングテーブル \(196ページ\)](#) を参照）。ただし、ルートが見つからない場合は、他のルーティングテーブルにフォールバックします。デフォルトルートは常にトラフィックに一致するため、他のルーティングテーブルへのフォールバックが妨げられます。この場合、インターフェイスがデフォルトのルーティングテーブルになれば、出力トラフィックに使用するインターフェイスを指定する必要があります。

スタティックルート

次の場合は、スタティックルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。
- ネットワークが小規模でスタティックルートを容易に管理できる。
- ルーティングプロトコルが関係するトラフィックまたはCPUのオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルトルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルトルートは、FTDデバイスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミックルーティングプロトコルをサポートしていない機能を使用している。

スタティックルーティングのガイドライン

ブリッジグループ

- ルーテッドモードでは、BVIをゲートウェイとして指定する必要があります。メンバーインターフェイスを指定することはできません。
- ブリッジグループメンバーインターフェイスを通じて直接には接続されていないネットワークに向かうFirepower Threat Defenseデバイスで発信されるトラフィックの場合（syslog

またはSNMPなど)、Firepower Threat Defense デバイスがどのブリッジグループメンバー インターフェイスからトラフィックを送信するかを認識するように、デフォルトルートまたはスタティックルートを設定する必要があります。1つのデフォルトルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。

スタティック ルートの設定

システムのインターフェイスに直接接続されているネットワークに向かわないパケットの送信先をシステムに伝えるため、スタティック ルートを定義します。

少なくとも1つのスタティック ルート、ネットワーク 0.0.0.0/0 のデフォルト ルートが必要になります。このルートは、既存の NAT xlates (変換) またはスタティック NAT ルール、またはその他のスタティックルートでは出力インターフェイスを判別できないパケットの送信先を定義します。

デフォルト ゲートウェイを使用してもすべてのネットワークに到達できない場合、他のスタティック ルートが必要になる可能性があります。たとえば、デフォルト ルートは通常、外部インターフェイスの上流に位置するルータです。デバイスに直接接続されていない追加の内部ネットワークがあり、それらにデフォルトゲートウェイを介してアクセスできない場合、これらそれぞれの内部ネットワークに対してスタティック ルートが必要です。

システムのインターフェイスに直接接続されたネットワークのスタティックルートを定義することはできません。システムは自動でこれらのルートを作成します。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[ルーティング (Routing)] サマリーにあるリンクをクリックします。

ステップ 2 [ルーティングの選択 (Select Routing)] ページで、次のいずれかを実行します。

- 新しいルートを追加するには、[+] をクリックします。
- 編集するルートの編集アイコン (✎) をクリックします。

ルートが不要になったら、ルートの [ごみ箱 (trash can)] アイコンをクリックして削除します。

ステップ 3 ルート プロパティの設定

[名前 (Name)]

ルートの表示名。

説明

ルートの目的の説明 (オプション) 。

インターフェイス

トラフィックの送信を行うインターフェイスを選択します。ゲートウェイアドレスは、このインターフェイスを介してアクセス可能である必要があります。

ブリッジグループの場合、メンバー インターフェイスではなくブリッジグループ インターフェイス (BVI) のルートを設定します。

プロトコル

[IPv4] または [IPv6] アドレスのどちらのルートであるかを選択します。

ネットワーク

このルートのゲートウェイを使用する必要がある、宛先ネットワークまたはホストを特定するネットワーク オブジェクトを選択します。

デフォルト ルートを定義するには、事前定義された `any-ipv4` または `any-ipv6set` ネットワーク オブジェクトを使用するか、または `0.0.0.0/0` (IPv4) または `::/0` (IPv6) ネットワークのオブジェクトを作成します。

ゲートウェイ

ゲートウェイの IP アドレスを特定するホスト ネットワーク オブジェクトを選択します。トラフィックはこのアドレスに送信されます。複数のインターフェイス上のルートには同じゲートウェイを使用できません。

メトリック (Metric)

1~254 間のルートのアドミニストレーティブ ディスタンス。スタティック ルートのデフォルト値は1です。インターフェイスとゲートウェイの間に追加ルータがある場合、アドミニストレーティブ ディスタンスとしてホップ数を入力します。

アドミニストレーティブ ディスタンスは、ルートと比較するために使用されるパラメータです。番号が低いほど、ルートに高い優先順位が与えられます。接続されたルート (デバイスのインターフェイスに直接接続されているネットワーク) は、スタティックルートよりも常に優先されます。

ステップ 4 [OK] をクリックします。

ルーティングのモニタリング

ルーティングをモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。

- **show route** はデータ インターフェイスのルーティング テーブルを表示します。直接接続されたネットワークのルートが含まれます。
- **show ipv6 route** はデータ インターフェイスの IPv6 ルーティング テーブルを表示します。直接接続されたネットワークのルートが含まれます。
- **show network** は仮想管理インターフェイスの設定を表示します。管理ゲートウェイが含まれます。仮想インターフェイスを介したルーティングは、データ インターフェイスを管理ゲートウェイに指定しなければ、データ インターフェイス ルーティング テーブルによって処理されません。

- **show network-static-routes** は、**configure network static-routes** コマンドを使用して仮想管理インターフェイスに対して設定されたスタティックルートを表示します。通常、ほとんどの場合、管理ゲートウェイは管理ルーティングに対して十分機能するため、スタティックルートは存在しません。これらのルートは、データ インターフェイス上のトラフィックには使用できません。このコマンドは、CLI コンソールでは使用できません。



第 II 部

セキュリティポリシー

- [SSL 復号 \(205 ページ\)](#)
- [アイデンティティポリシー \(231 ページ\)](#)
- [セキュリティインテリジェンス \(245 ページ\)](#)
- [アクセス制御 \(251 ページ\)](#)
- [侵入ポリシー \(279 ページ\)](#)
- [ネットワークアドレス変換 \(NAT\) \(293 ページ\)](#)



第 9 章

SSL 復号

HTTPS など一部のプロトコルは、セキュア ソケット レイヤ (SSL) またはその後継バージョンである Transport Layer Security (TLS) を使用して、セキュアな転送のためにトラフィックを暗号化します。システムでは暗号化された接続を検査できないため、アクセス判断のために上位層のトラフィック特性を考慮したアクセスルールを適用する場合は、暗号化された接続を復号する必要があります。

- [SSL 復号について \(205 ページ\)](#)
- [SSL 復号のためのライセンス要件 \(209 ページ\)](#)
- [SSL 復号のガイドライン \(209 ページ\)](#)
- [SSL 復号ポリシーの実装および管理方法 \(210 ページ\)](#)
- [SSL 復号ポリシーの設定 \(212 ページ\)](#)
- [例：ネットワークからの古い SSL/TLS バージョンのブロック \(227 ページ\)](#)
- [SSL 復号のモニタリングとトラブルシューティング \(229 ページ\)](#)

SSL 復号について

通常、接続は、許可されるかブロックされるかを決定するアクセス コントロール ポリシーを経由します。ただし、SSL 復号ポリシーを有効にする場合、暗号化された接続は最初に SSL 復号ポリシー経由で送信され、復号化するかブロックする必要があるかが判断されます。ブロックされていない接続は、復号化されているかどうかにかかわらず、許可/ブロックの最終的な決定のためアクセス コントロール ポリシーを経由します。



- (注) アイデンティティ ポリシーでアクティブな認証ルールを実装するためには、SSL 復号ポリシーを有効にする必要があります。SSL 復号を有効にしてアイデンティティ ポリシーを有効にするのが、SSL 復号は実装しない場合、デフォルトのアクションに [復号しない (Do Not Decrypt)] を選択し、追加の SSL 復号ルールは作成しないでください。アイデンティティ ポリシーでは、必要なルールを自動的に生成します。

ここでは、暗号化トラフィック フロー管理と復号化についてさらに詳しく説明します。

SSL 復号を実装する理由

HTTPS 接続などの暗号化されたトラフィックは検査することができません。

銀行や他の金融機関への接続など、多くの接続は合法的に暗号化されます。多くの Web サイトでは、プライバシーや機密性の高いデータを保護するために暗号化を使用します。たとえば、Firepower Device Manager への接続は暗号化されます。

ただし、暗号化された接続の中ではユーザが望ましくないトラフィックを隠すこともできます。

SSL 復号を実装することによって、接続を復号して脅威またはその他の望ましくないトラフィックが含まれていないかを確認するために検査し、再度暗号化してから接続の続行を許可できます。（復号されたトラフィックは、アクセス制御ポリシーを通過し、暗号化された特性ではなく、復号された接続の検査特性に基づいたルールに一致します。）これは、機密情報を保護するために、アクセス制御ポリシーを適用する必要性とユーザの必要性との間でバランスをとります。

ネットワークを利用させたくない種類の暗号化されたトラフィックをブロックする SSL 復号ルールを構成することもできます。

トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

暗号化されたトラフィックに適用できるアクション

SSL 復号ルールを設定する場合は、次のトピックで説明しているアクションを適用できます。これらのアクションは、明示的なルールと一致しないすべてのトラフィックに適用されるデフォルトのアクションにも使用できます。



- (注) SSL 復号ポリシーを経由するすべてのトラフィックは、アクセスコントロールポリシーを経由する必要があります。SSL 復号ポリシーにドロップするトラフィックを除き、許可またはドロップの最終的な決定はアクセスコントロールポリシーに委ねられます。

再署名の復号

トラフィックを復号し再署名する場合、システムは中間者として機能します。

たとえば、ユーザがブラウザで <https://www.cisco.com> と入力します。トラフィックが FTD デバイスに達すると、デバイスはルールで指定された CA 証明書を使用するユーザとネゴシエーションを行い、ユーザと FTD デバイス間に SSL トンネルを構築します。同時に、デバイスは <https://www.cisco.com> に接続し、サーバと FTD デバイス間に SSL トンネルを作成します。

このため、ユーザには、www.cisco.com からの証明書ではなく、SSL 復号ルールで設定された CA 証明書が表示されます。ユーザは、接続を完了するために証明書を信頼する必要があります。FTD デバイスは、ユーザと宛先サーバ間のトラフィックで両方向に復号/再暗号化を実行します。



- (注) サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザに出されます。これを防ぐには、クライアントの信頼できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。

再署名の復号アクションでルールを設定する場合、設定されているルールの条件に加え、参照される内部 CA 証明書の署名アルゴリズムの種類に基づいてルールがトラフィックと一致します。SSL 復号ポリシーに 1 つの再署名証明書を選択できるため、これによって再署名ルールのトラフィック一致を制限できます。

たとえば、楕円曲線 (EC) アルゴリズムで暗号化された発信トラフィックは、再署名証明書が EC ベースの CA 証明書の場合にのみ、再署名の復号ルールと一致します。同様に、RSA アルゴリズムで暗号化されたトラフィックは、グローバル再署名証明書が RSA の場合にのみ、再署名の復号ルールと一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されたその他すべてのルール条件が一致していても、このルールとは一致しません。

既知のキーの復号

宛先サーバを所有している場合、既知のキーで復号化を実装できます。この場合、ユーザが <https://www.cisco.com> への接続を開くと、証明書を提示しているのが FTD デバイスであっても、www.cisco.com の実際の証明書がユーザに表示されます。



ドメインおよび証明書の所有者は、所属組織でなければなりません。[cisco.com](https://www.cisco.com) を例として取り上げると、エンドユーザにシスコの証明書が表示されるのは、組織が実際にドメイン [cisco.com](https://www.cisco.com) の所有者であり (つまり、所属企業が Cisco Systems であること)、パブリック CA によって署名された [cisco.com](https://www.cisco.com) 証明書の所有権を持っている場合のみです。復号できるのは、所属組織が所有するサイトの既存のキーを使用する場合のみです。

既知のキーを使用して復号する主な目的は、HTTPS サーバへのトラフィックを復号して、社内サーバを外部の攻撃から保護することです。外部 HTTPS サイトへのクライアント側のトラ

フィックを検査する場合は、サーバを所有していないので、再署名の復号を使用する必要があります。



- (注) 既知のキーの復号を使用するには、サーバの証明書およびキーを内部アイデンティティ証明書としてアップロードし、SSL復号ポリシー設定で既知のキーの証明書一覧に追加する必要があります。その後は、宛先アドレスとしてサーバのアドレスを使用して既知のキーの復号化のルールを作成できます。SSL復号ポリシーに証明書を追加する方法については、[既知のキーと復号の再署名の証明書の設定 \(224 ページ\)](#) を参照してください。

復号禁止

特定の種類のトラフィックで復号をバイパスする場合、トラフィックの処理は行われません。暗号化されたトラフィックはアクセスコントロールポリシーに渡され、一致するアクセス制御ルールに基づいて許可またはドロップされます。

ブロック

単にSSL復号ルールと一致する暗号化されたトラフィックをブロックできます。SSL復号ポリシーのブロックでは、アクセスコントロールポリシーに接続が達することを防ぎます。

HTTPS 接続をブロックすると、ユーザにはシステムのデフォルトのブロック応答ページが表示されません。代わりに、ブラウザのセキュアな接続の障害時のデフォルトページが表示されます。エラーメッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

自動的に生成された SSL 復号ルール

SSL復号ポリシーを有効にしてもしなくても、システムはアクティブな認証を実装する各アイデンティティポリシールールに対して再署名の復号ルールを自動的に生成します。これは、HTTPS 接続でアクティブな認証を有効にするために必要です。

SSL復号ポリシーを有効にすると、アイデンティティポリシーのアクティブな認証ルールの見出しの下にこれらのルールが表示されます。これらのルールは、SSL復号ポリシーの上部にグループ化されます。ルールは読み取り専用です。アイデンティティポリシーを変更することによってのみ変更できます。

復号できないトラフィックの処理

接続が復号できなくなる特性は複数あります。接続に次の特性のいずれかがある場合、接続で一致するルールがあっても接続にはデフォルトのアクションが適用されます。([復号しない (Do Not Decrypt)]ではなく) デフォルトアクションとしてブロックを選択する場合、正当なトラフィックの過剰なドロップなどの問題があることがあります。

- 圧縮されたセッション：データ圧縮が接続に適用されています。

- SSLv2 セッション：サポートされている最下位の SSL バージョンは SSLv3 です。
- 不明な暗号スイート：システムで接続の暗号スイートが認識されません。
- サポート外の暗号スイート：システムで、検出された暗号スイートに基づく復号化がサポートされません。
- キャッシュされないセッション：SSL セッションにおいてセッションの再利用が可能になっていて、クライアントとサーバがセッション ID でセッションを再確立したときに、システムがそのセッション ID をキャッシュに入れなかったことを意味します。
- ハンドシェイクエラー：SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。
- 復号エラー：復号処理中にエラーが発生しました。

SSL 復号のためのライセンス要件

SSL 復号ポリシーを使用するのに特別なライセンスは必要ありません。

ただし、URL カテゴリおよびレピュテーションを一致基準として使用するルールを作成するには、[URL フィルタリング](#) ライセンスが必要です。ライセンスの設定については、[オプションライセンスの有効化と無効化 \(101 ページ\)](#) を参照してください。

SSL 復号のガイドライン

SSL 復号ポリシーを設定してモニタする場合は、次の点に注意してください。

- SSL 復号ポリシーは、次のようなアクセス制御ルールがトラフィックを信頼またはブロックするように設定されている場合に、それらのルールに一致する接続に関してバイパスされます。
 - セキュリティゾーン、ネットワーク、地理位置情報、およびポートだけをトラフィック照合基準として使用する。
 - 検査を必要とする他のルール（アプリケーションまたは URL に基づいて接続を照合するルールなど）に先立つか、侵入またはファイル検査を適用するルールを許可する。
- URL カテゴリのマッチングを使用するときは、サイトのログインページがサイトそのものと異なるカテゴリにある場合に注意してください。たとえば、Gmail は「Web ベースの電子メール」カテゴリにあり、ログインページは「インターネット ポータル」カテゴリにあります。これらのサイトへの接続を復号するには、両方のカテゴリをルールに含める必要があります。
- 脆弱性データベース（VDB）の更新によってアプリケーションが削除（廃止）される場合は、削除されたアプリケーションを使用する SSL 復号ルールまたはアプリケーションフィ

ルタに変更を加える必要があります。これらのルールを修正するまで、変更を展開することはできません。また、問題を修正前にシステム ソフトウェア アップデートをインストールすることはできません。[アプリケーションフィルタ (Application Filters)] オブジェクトページ、またはルールの[アプリケーション (Application)] タブでは、これらのアプリケーション名の後に「(廃止) (Deprecated)」と表示されます。

SSL 復号ポリシーの実装および管理方法

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーンテキストトラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL 復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。

他のセキュリティポリシーの場合とは異なり、SSL 復号ポリシーは、監視して積極的に保守する必要があります。これは、証明書の期限が切れたり、宛先サーバで変更されたりするためです。さらに、クライアントソフトウェアの変更により特定の接続を復号する能力が変わる場合もあります。これは、再署名の復号アクションを中間者攻撃と区別できないためです。

次の手順では、SSL 復号ポリシーの実装と保守のエンドツーエンドプロセスを説明します。

手順

ステップ 1 再署名の復号ルールを実装する場合は、必要な内部 CA 証明書を作成します。

内部認証局 (CA) 証明書を使用する必要があります。次の選択肢があります。ユーザは証明書を信頼する必要があるため、すでに信頼されると設定されているクライアントブラウザに証明書をアップロードするか、またはアップロードする証明書がブラウザの信頼ストアに追加されるようにします。

- デバイス自体によって署名される自己署名内部 CA 証明書を作成します。 [自己署名内部および内部 CA 証明書の生成 \(157 ページ\)](#) を参照してください。
- 外部の信頼できる CA または組織内部の CA によって署名される内部 CA 証明書およびキーをアップロードします。 [内部および内部 CA 証明書のアップロード \(155 ページ\)](#) を参照してください。

ステップ 2 既知のキーの復号ルールを実装する場合は、各内部サーバから証明書とキーを収集します。

サーバから証明書とキーを取得するため、既知のキーの復号は自分で制御しているサーバでのみ使用できます。これらの証明書とキーを内部証明書 (内部 CA 証明書ではない) としてアップロードします。 [内部および内部 CA 証明書のアップロード \(155 ページ\)](#) を参照してください。

ステップ 3 [SSL 復号ポリシーの有効化 \(213 ページ\)](#)。

ポリシーを有効にする際に、いくつかの基本的な設定も構成します。

ステップ 4 [SSL 復号のデフォルトアクションの設定 \(214 ページ\)](#)。

不確かな場合は、デフォルトアクションとして[復号しない (Do not decrypt)]を選択します。この場合でも、アクセスコントロールポリシーは、デフォルトのSSL復号ルールに一致するトラフィックを適切であればドロップできます。

ステップ 5 [SSL 復号ルールの設定 \(215 ページ\)](#)。

復号するトラフィック、および適用する復号のタイプを識別します。

ステップ 6 既知のキーでの復号を設定する場合は、これらの証明書を含めるようにSSL復号ポリシー設定を編集します。[既知のキーと復号の再署名の証明書の設定 \(224 ページ\)](#)を参照してください。

ステップ 7 必要に応じて、再署名の復号ルールに使用するCA証明書をダウンロードして、クライアントワークステーションのブラウザにアップロードします。

証明書のダウンロードおよびクライアントへの配布については、[再署名の復号ルールのCA証明書のダウンロード \(225 ページ\)](#)を参照してください。

ステップ 8 定期的に、再署名証明書および既知のキーの証明書を更新します。

- 再署名証明書：期限切れになる前にこの証明書を更新します。Firepower Device Managerを使用して証明書を生成する場合は、5年間有効です。証明書の有効期間を確認するには、**[オブジェクト (Objects)] > [証明書 (Certificates)]**を選択し、リスト内で証明書を見つけて**[アクション (Actions)]**列の**[情報] (information) アイコン (i)**をクリックします。情報ダイアログボックスに、有効期間およびその他の特性が表示されます。このページから代替証明書をアップロードすることもできます。
- 既知のキーの証明書：既知のキーによる復号ルールの場合、宛先サーバの現在の証明書とキーがアップロードされていることを確認する必要があります。サポートされるサーバで証明書およびキーが変更されるたびに、新しい証明書およびキーを(内部証明書として)アップロードし、新しい証明書を使用するようにSSL復号設定を更新する必要があります。

ステップ 9 外部サーバで不足している信頼できるCA証明書をアップロードします。

システムには、サードパーティによって発行された、広範な信頼できるCAルート証明書および信頼できるCA中間証明書が含まれています。これらは、再署名の復号ルールについてFTDと宛先サーバの間で接続をネゴシエートするときに必要です。

信頼できるルートCAの信頼チェーン内にあるすべての証明書を、信頼できるCA証明書のリストにアップロードしますが、これにはルートCA証明書およびすべての中間CA証明書が含まれます。これを行わないと、中間CAから発行された信頼できる証明書の検出が困難になります。**[オブジェクト (Objects)] > [証明書 (Certificates)]**ページで証明書をアップロードします。[信頼できるCA証明書のアップロード \(158 ページ\)](#)を参照してください。

SSL 復号ポリシーの設定

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーンテキストトラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL 復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。



- (注) VPN トンネルは SSL 復号ポリシーが評価される前に復号されるので、トンネル自体にはポリシーは適用されません。ただし、トンネル内で暗号化された接続は SSL 復号ポリシーによる評価の対象となります。

以下の手順で、SSL 復号ポリシーを設定する方法を説明します。SSL 復号を作成および管理するエンドツーエンドプロセスの説明については、[SSL 復号ポリシーの実装および管理方法 \(210 ページ\)](#) を参照してください。

始める前に

SSL 復号ルール テーブルには、2 つのセクションが含まれています。

- [アイデンティティポリシーアクティブ認証ルール (Identity Policy Active Authentication Rules)] : アイデンティティポリシーを有効にしてアクティブ認証を使用するルールを作成すると、システムがこれらのポリシーの動作に必要な SSL 復号ルールを自動的に作成します。これらのルールは、常に自分で作成した SSL 復号ルールの前に評価されます。アイデンティティポリシーに変更することによって、間接的にのみこれらのルール変更できます。
- [SSLネイティブルール (SSL Native Rules)] : これらは自分で構成したルールです。このセクションにのみルールを追加できます。

手順

ステップ 1 [ポリシー (Policies)] > [SSL復号 (SSL Decryption)] の順に選択します。

ポリシーをまだ有効化していない場合は、[SSL復号の有効化 (Enable SSL Decryption)] をクリックし、「[SSL 復号ポリシーの有効化 \(213 ページ\)](#)」の説明に従ってポリシーを設定します。

ステップ 2 ポリシーのデフォルト アクションを設定します。

最も安全な選択肢は、[復号しない (Do Not Decrypt)] です。詳細については、[SSL 復号のデフォルトアクションの設定 \(214 ページ\)](#) を参照してください。

ステップ3 SSL 復号ポリシーを管理します。

SSL 復号を設定した後、このページにすべてのルールが順番に一覧表示されます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- ポリシーを無効にするには、[SSL復号ポリシー (SSL Decryption Policy)] トグルをクリックします。[SSL複合を有効化 (Enable SSL Decryption)] をクリックすると再度有効にできます。
- ポリシーで使用する証明書のリストを含むポリシー設定を編集するには、[SSL復号設定 (SSL Decryption Settings)] ボタン (⚙️) をクリックします。また、クライアントに配布できるように、再署名の復号ルールで使用する証明書をダウンロードできます。次のトピックを参照してください。
 - [既知のキーと復号の再署名の証明書の設定 \(224 ページ\)](#)
 - [再署名の復号ルールの CA 証明書のダウンロード \(225 ページ\)](#)
- ルールを設定するには、次の手順を実行します。
 - 新しいルールを作成するには、[+] ボタンをクリックします。 [SSL 復号ルールの設定 \(215 ページ\)](#) を参照してください。
 - 既存のルールを編集する場合は、([操作 (Actions)] 列の) 対象のルールの編集アイコン (🔗) をクリックします。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。
 - 不要になったルールを削除する場合は、([操作 (Actions)] 列の) 対象のルールの [削除 (delete)] アイコン (🗑️) をクリックします。
- ルールを移動するには、編集して [順序 (Order)] ドロップダウン リストから新しい場所を選択します。

SSL 復号ポリシーの有効化

SSL 復号ルールを設定する前に、ポリシーを有効にして、いくつかの基本的な設定を構成する必要があります。以下の手順で、ポリシーを直接有効にする方法を説明します。アイデンティティ ポリシーを有効にするときにこのポリシーを有効にすることもできます。アイデンティティ ポリシーでは、SSL 復号ポリシーを有効にする必要があります。

始める前に

SSL 復号ポリシーを持たないリリースからアップグレードし、アクティブな認証ルールを使用してアイデンティティ ポリシーを設定した場合、SSL 復号ポリシーはすでに有効になっています。

す。必ず使用する再署名の復号証明書を選択し、必要に応じて事前定義されたルールを有効にします。

手順

ステップ 1 [ポリシー (Policies)] > [SSL復号 (SSL Decryption)] の順に選択します。

ステップ 2 [SSL復号の有効化 (Enable SSL Decryption)] をクリックしてポリシー設定を構成します。

- このポリシーを初めて有効にする場合は、[SSL復号設定 (SSL Decryption Configuration)] ダイアログ ボックスが開きます。次の手順に進みます。
- 以前にこのポリシーを設定した後で無効にした場合は、前の設定とルールを使用してポリシーが再度有効になります。[SSL復号設定 (SSL Decryption Settings)] ボタン (⚙️) をクリックし、[既知のキーと復号の再署名の証明書の設定 \(224 ページ\)](#) で説明されているように設定できます。

ステップ 3 [再署名証明書の復号 (Decrypt Re-Sign Certificate)] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成 (Create Internal CA)] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン (📄) をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。[再署名の復号ルールのCA証明書のダウンロード \(225 ページ\)](#) も参照してください。

ステップ 4 初期 SSL 復号ルールを選択します。

システムには以下の事前定義ルールが含まれており、役立つ場合があります。

- [Sensitive_Data] : このルールでは、金融サービスまたは健康と医療の URL カテゴリ (銀行、医療機関、ヘルスケア サービスなど) 内の Web サイトに一致するトラフィックは復号しません。このルールを実装するには、URL ライセンスを有効にする必要があります。

ステップ 5 [有効 (Enable)] をクリックします。

SSL 復号のデフォルトアクションの設定

暗号化された接続が特定の SSL 復号ルールに一致しない場合、SSL 復号ポリシーのデフォルトアクションに基づいて処理されます。

手順

ステップ 1 [ポリシー (Policies)] > [SSL復号 (SSL Decryption)] の順に選択します。

ステップ 2 [デフォルトアクション (Default Action)] フィールドの任意の場所をクリックします。

ステップ 3 一致するトラフィックに適用するアクションを選択します。

- [復号しない (Do Not Decrypt)] : 暗号化された接続を許可します。次にアクセス制御ポリシーは、暗号化された接続を評価し、アクセス制御ルールに基づいてドロップまたは許可します。
- [ブロック (Block)] : 接続をすぐに切断します。接続はアクセス制御ポリシーに渡されません。

ステップ 4 (オプション) デフォルトアクションのロギングを設定します。

デフォルトアクションに一致するトラフィックのロギングをダッシュボードのデータまたはイベントビューアに記載されるようにするには、トラフィックのロギングを有効にする必要があります。次のオプションから選択します。

- [接続終了時 (At End of Connection)] : 接続の終了時にイベントを生成します。
 - [接続イベントの送信先 (Send Connection Events To)] : 外部の syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバオブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成 (Create New Syslog Server)] をクリックして作成します (syslog サーバへのロギングを無効にするには、サーバリストから [任意 (Any)] を選択します)。

デバイスのイベントストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

- [ロギングなし (No Logging)] : イベントを生成しません。

ステップ 5 [保存 (Save)] をクリックします。

SSL 復号ルールの設定

SSL 復号ルールを使用して、暗号化された接続を処理する方法を決定します。SSL 復号ポリシーに設定されたルールは、上から下への順に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

[SSLネイティブルール (SSL Native Rules)] セクションでのみルールを作成し、編集できます。



- (注) SSL 復号ポリシーが接続を評価する前に、VPN 接続（サイト間とリモートアクセスの両方）のトラフィックが復号されます。したがって、SSL 復号ルールが VPN 接続に適用されるのではなく、これらのルールを作成するときに VPN 接続を考慮する必要はありません。ただし、VPN トンネル内で暗号化された接続を使用する場合は評価されます。たとえば、RA VPN トンネル自体は（すでに復号されているので）評価されなくても、RA VPN 接続経由の内部サーバへの HTTPS 接続は、SSL 復号ルールによって評価されます。

始める前に

既知のキーの復号ルールを作成する場合は、宛先サーバのための証明書とキーを（内部証明書として）アップロードし、証明書を使用するために SSL 復号ポリシーの設定も編集します。既知のキーのルールは通常、ルールの宛先ネットワークの条件で宛先サーバを指定します。詳細については、[既知のキーと復号の再署名の証明書の設定（224 ページ）](#) を参照してください。

手順

ステップ 1 [ポリシー (Policies)] > [SSL 復号 (SSL Decryption)] の順に選択します。

（アクティブ認証アイデンティティ ルール用に自動的に生成されたもの以外に）任意の SSL 復号ルールを構成していない場合、[事前定義済みルールを追加 (Add Pre-Defined Rules)] をクリックして、事前定義済みのルールを追加できます。ルールを選択するように要求されません。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (🔍) をクリックします。

不要になったルールを削除するには、ルールの [削除 (delete)] アイコン (🗑️) をクリックします。

ステップ 3 [順序 (Order)] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

[SSL ネイティブルール (SSL Native Rules)] セクションにのみルールを挿入できます。アイデンティティ ポリシー アクティブ認証ルールはアイデンティティ ポリシーから自動的に生成され、読み取り専用です。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル (Title)] にルールの名前を入力します。

この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます：+
._-

ステップ 5 一致するトラフィックに適用するアクションを選択します。

各オプションの詳細については、次を参照してください。

- [再署名の復号 \(206 ページ\)](#)
- [既知のキーの復号 \(207 ページ\)](#)
- [復号禁止 \(208 ページ\)](#)
- [ブロック \(208 ページ\)](#)

ステップ 6 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/送信先 (Source/Destination)]: トラフィックが通過するセキュリティゾーン (インターフェイス)、IP アドレスまたは IP アドレスの国/大陸 (地理的ロケーション)、トラフィックで使用されている TCP ポート。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。 [SSL 復号ルールの送信元/送信先基準 \(218 ページ\)](#) を参照してください。
- [アプリケーション (Application)]: アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトは任意の暗号化されたアプリケーションです。 [SSL 復号ルールのアプリケーション基準 \(220 ページ\)](#) を参照してください。
- [URL]: Web 要求の URL カテゴリ。デフォルトでは URL カテゴリおよびレピュテーションはマッチングの目的では考慮されません。「[SSL 復号ルールの URL 基準 \(221 ページ\)](#)」を参照してください。
- [ユーザ (Users)]: ユーザまたはユーザ グループ。アイデンティティ ポリシーは、ユーザとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティポリシーを設定する必要があります。 [SSL 復号ルールのユーザ基準 \(222 ページ\)](#) を参照してください。
- [拡張 (Advanced)]: SSL/TLS バージョンや証明書のステータスなどの接続に使用する証明書に由来する特性。 [SSL 復号ルールの詳細条件 \(223 ページ\)](#) を参照してください。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成 (Create New Object)] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

条件を SSL 復号ルールに追加する際は、以下のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、URL カテゴリに基づいて復号するために単一のルールを使用できます。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはア

アプリケーションフィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。

- URL カテゴリのマッチングには、URL フィルタリング機能のライセンスが必要です。

ステップ7 (オプション) ルールのロギングを設定します。

ルールと一致するトラフィックをダッシュボードデータまたはイベントビューアに含めるには、ロギングを有効にする必要があります。次のオプションから選択します。

- [接続終了時 (At End of Connection)]: 接続の終了時にイベントを生成します。
 - [接続イベントの送信先 (Send Connection Events To)]: 外部の syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバオブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成 (Create New Syslog Server)]をクリックして作成します (syslog サーバへのロギングを無効化するには、サーバのリストから [任意 (Any)]を選択します)。

デバイスのイベントストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。
- [ロギングなし (No Logging)]: イベントを生成しません。

ステップ8 [OK] をクリックします。

SSL 復号ルールの送信元/送信先基準

SSL 復号ルールの [送信元/送信先 (Source/Destination)] 基準で、トラフィックが通過するセキュリティゾーン (インターフェイス)、IP アドレスまたは IP アドレスの国/大陸 (地理的ロケーション)、トラフィックで使用されている TCP ポートを定義します。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。TCP は、SSL 復号ルールに一致する唯一のプロトコルです。

条件を変更するには、その条件内の [+] ボタンをクリックして、目的のオブジェクトまたは要素を選択し、[OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成 (Create New Object)] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティゾーンオブジェクト。1つの基準を定義する、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン (Destination Zones)] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン (Source Zones)] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通して出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、外部ホストから内部ホストへのすべてのトラフィックが復号されたことを確認したい場合、[送信元ゾーン (Source Zones)] で外部ゾーンを選択し、[送信先ゾーン (Destination Zones)] で内部ゾーンを選択します。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク (Source Networks)] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク (Destination Networks)] を設定します。
- 送信元 (Source) ネットワーク条件と宛先 (Destination) ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク (Network)] : 制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。



(注) 既知のキーの復号ルールの場合、証明書とアップロードしたキーを使用する送信先サーバの IP アドレスを持つオブジェクトを選択します。

- [地理位置情報 (Geolocation)] : 位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポートオブジェクト。SSL 復号ルールに対してのみ TCP プロトコルとポートを指定できます。

- TCP ポートからのトラフィックを一致させるには、[送信元ポート (Source Ports)] を設定します。
- TCP ポートへのトラフィックを一致させるには、[送信先ポート/プロトコル (Destination Ports/Protocols)] を設定します。
- 特定の TCP ポートから特定の TCP ポートへ発信されるトラフィックを一致させるには、両方のポートを設定します。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

SSL 復号ルール of アプリケーション基準

SSL 復号ルール of アプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタ処理が定義されます。デフォルトは、SSL プロトコル タグを持つアプリケーションです。暗号化されていないアプリケーションは SSL 復号ルールと一致できません。

ルールで個別のアプリケーションを指定できますが、アプリケーションフィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高くビジネスとの関連性が低いすべてのアプリケーションを復号またはブロックする SSL 復号ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとする、セッションが復号またはブロックされます。

また、シスコは、システムおよび脆弱性データベース (VDB) の更新を通じて頻繁にアプリケーションディテクタを更新し追加します。これにより、リスクの高いアプリケーションのルールが新しいアプリケーションに自動的に適用される可能性があり、手動でルールを更新する必要がなくなります。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーションフィルタオブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタリストを変更するには、条件内の [+] ボタンをクリックし、別のタブに表示される目的のアプリケーションまたはアプリケーションフィルタオブジェクトを選択してから、ポップアップ表示されるダイアログボックスで [OK] をクリックします。いずれかのタブで [詳細フィルタ (Advanced Filte)] をクリックするか、またはフィルタ条件を選択して特定のアプリケーションを検索します。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x] をクリックします。[フィルタとして保存 (Save As Filter)] リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーションフィルタオブジェクトとして保存します。

アプリケーション基準と、高度なフィルタを設定してアプリケーションを選択する方法の詳細については、[アプリケーションフィルタオブジェクトの設定 \(137 ページ\)](#) を参照してください。

SSL 復号ルールでアプリケーション基準を使用する場合は、次のヒントを考慮してください。

- このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS ClientHello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。
- システムは、サーバ証明書の交換後にのみアプリケーションを識別できます。SSL ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。システムによる識別が完了すると、アプリケーション条件に一致する残りのセッショントラフィックに SSL ルールのアクションが適用されます。
- 選択したアプリケーションが VDB の更新によって削除されていた場合は、アプリケーション名の後ろに「(廃止 (Deprecated))」と表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システムソフトウェアのアップグレードがブロックされます。

SSL 復号ルールの URL 基準

SSL 復号ルールの URL の基準は、Web 要求の URL が属するカテゴリを定義します。また、復号、ブロック、または復号せずに許可するサイトの相対的なレピュテーションも指定できます。デフォルトでは、URL カテゴリに基づき接続と一致しません。

たとえば、すべての暗号化されたギャンブルサイトをブロックしたり、リスクの高いすべてのソーシャル ネットワーキングサイトを復号できます。該当するカテゴリとレピュテーションの URL をユーザが参照しようとする、セッションがブロックされるか、または復号されません。URL カテゴリの照合の詳細については、[カテゴリ別とレピュテーション別の URL のフィルタリング \(254 ページ\)](#) を参照してください。

[カテゴリ (Categories)] タブ

[+] をクリックし、目的のカテゴリを選択して、[OK] をクリックします。ポリシーからカテゴリやオブジェクトを削除するには、該当する [x] をクリックします。

デフォルトでは、レピュテーションに関係なく、選択した各カテゴリ内のすべての URL にルールが適用されます。レピュテーションに基づいてルールを制限するには、各カテゴリの下矢印をクリックして、[任意 (Any)] チェックボックスを選択解除し、[レピュテーション (Reputation)] スライダを使用してレピュテーションレベルを選択します。レピュテーションスライダの左側に復号なしで許可されるサイトが示され、右側に復号またはブロックされるサイトが示されます。レピュテーションがどのように使用されるかは、ルールアクションによって異なります。

- ルールで接続が復号またはブロックされる場合は、レピュテーションレベルを選択すると、そのレベルよりも重大度が高いすべてのレピュテーションも選択されます。たとえば、[\[疑わしいサイト \(Suspicious sites\) \]](#) (レベル2) を復号またはブロックする

ようにルールを設定した場合、**[高リスク (High risk)]** (レベル 1) サイトも自動的に復号またはブロックします。

- ルールで復号なし (復号しない) で接続が許可される場合は、レピュテーションレベルを選択すると、そのレベルよりも重大度が低いすべてのレピュテーションも選択されます。たとえば、**[無害なサイト (Benign sites)]** (レベル 4) を復号しないルールを設定した場合、**[既知 (Well known)]** (レベル 5) サイトも自動的に復号されません。

SSL 復号ルールのユーザ基準

SSL 復号ルールのユーザ基準は、IP 接続のユーザまたはユーザグループを定義します。ルールにユーザまたはユーザグループの基準を含めるように、アイデンティティポリシーと関連ディレクトリサーバを設定する必要があります。

アイデンティティポリシーは、特定の接続に関してユーザアイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストのIPアドレスに識別されたユーザが関連付けられます。したがって、送信元IPアドレスがユーザにマッピングされているトラフィックは、そのユーザからのものとみなされます。IPパケット自体にはユーザアイデンティティ情報は含まれていないため、このIPアドレスとユーザ間のマッピングが使用可能な中での最良近似となります。

1つのルールに最大50のユーザまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザを選択するより有意義です。たとえば、外部ネットワークからエンジニアリンググループへのトラフィックを復号するルールを作成し、そのグループからの発信トラフィックを復号しない別のルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリサーバのエンジニアリンググループに追加するだけです。

ユーザリストを変更するには、条件内の[+]ボタンをクリックし、次の手法のいずれかを使用して、目的のユーザまたはユーザグループを選択します。ポリシーからユーザまたはグループを削除するには、対応する[x]をクリックします。

- **[ユーザおよびグループ (Users and Groups)]** タブ：目的のユーザまたはユーザグループを選択します。グループは、ディレクトリサーバにグループが設定されている場合のみ使用可能です。グループを選択すると、ルールはサブグループを含むグループのすべてのメンバーに適用されます。サブグループを別の方法で処理する場合は、サブグループ用の個別のアクセスルールを作成し、それをアクセスコントロールポリシー内で親グループのルールの上に配置する必要があります。
- **[特別なエンティティ (Special Entities)]**：次から選択します。
 - **[認証失敗 (Failed Authentication)]**：ユーザは認証を求められましたが、最大許容試行回数内に有効なユーザ名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザのネットワークへのアクセスは妨げられませんが、これらのユーザのネットワークアクセスを制限するためのアクセスルールを記述できます。
 - **[ゲスト (Guest)]**：ゲストユーザは、これらのユーザをゲストと呼ぶようにアイデンティティルールが設定されている点を除き、認証失敗ユーザと同様です。ゲストユー

ザは認証を求められましたが、最大試行回数内に認証されることができませんでした。

- [認証不要 (No Authentication Required)] : ユーザの接続が認証なしに指定されたアイデンティティルールに一致したため、ユーザは認証を求められませんでした。
- [不明 (Unknown)] : IPアドレスのユーザマッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。

SSL 復号ルールの詳細条件

詳細のトラフィックの一致条件は、接続に使用する証明書に由来する特徴に関連します。次のオプションのいずれかまたはすべてを設定できます。

証明書のプロパティ

トラフィックは、選択したプロパティのいずれかに一致する場合、ルールの証明書プロパティのオプションに一致します。次の設定を行えます。

証明書のステータス

証明書が [有効 (Valid)] か [無効 (Invalid)] か。証明書のステータスを気にしない場合は、[任意 (Any)] (デフォルト) を選択します。

証明書は、次の条件のすべてが満たされている場合に有効とみなされ、それ以外の場合は無効とみなされます。

- ポリシーが証明書を発行した CA を信用できる。
- 証明書の署名を証明書の内容に対して正しく検証できる。
- 発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
- ポリシーの信頼できる CA のいずれも証明書を失効させていません。
- 現在の日付が証明書の [有効期間の開始 (Valid From)] と [有効期間の終了 (Valid To)] の期間内にある。

自己署名

サーバ証明書に同じサブジェクトおよび発行元識別名が含まれているかどうか。次のいずれかを選択します。

- [自己署名 (Self-Signing)] : サーバ証明書は自己署名されています。
- [CA 署名 (CA-Signing)] : サーバ証明書は認証局によって署名されています。つまり、発行元とサブジェクトは同じではありません。
- [任意 (Any)] : 証明書が自己署名されているかどうかを一致条件として考慮しません。

サポートされるバージョン

一致する SSL/TLS バージョン。ルールは、選択したいいずれかのバージョンを使用するトラフィックにのみ適用されます。デフォルトは全バージョンです。[SSLv3.0]、[TLSv1.0]、[TLSv1.1]、[TLSv1.2] から選択します。

たとえば、TLSv1.2 の接続のみを許可する場合は、TLSv1.2 以外のバージョンにブロックルールを作成できます。

記載されていない SSL v2.0 などのバージョンを使用するトラフィックは、SSL 復号ポリシーのデフォルトのアクションによって処理されます。

既知のキーと復号の再署名の証明書の設定

再署名によってまたは既知のキーを使用して復号を実装する場合は、SSL 復号ルールが使用できる証明書を特定する必要があります。すべての証明書が有効で、期限が切れていないことを確認します。

特に既知のキーを復号する場合は、復号する接続の各宛先サーバの現在の証明書とキーがシステムにあることを確認する必要があります。既知のキーの復号ルールでは、復号の宛先サーバからの実際の証明書とキーを使用します。したがって、常に FTD デバイスに現在の証明書とキーがあることを確認する必要があります。そうでない場合復号は失敗します。

既知のキーのルールで宛先サーバの証明書またはキーを変更するたびに新しい内部証明書とキーをアップロードします。それらを内部証明書（内部 CA 証明書ではありません）としてアップロードします。次の手順の間に証明書をアップロードするか、**[オブジェクト (Objects)] > [証明書 (Certificates)]** ページに進み、そこにアップロードします。

手順

ステップ 1 **[ポリシー (Policies)] > [SSL復号 (SSL Decryption)]** の順に選択します。

ステップ 2 **[SSL復号設定 (SSL Decryption Settings)]** ボタン (⚙️) をクリックします。

ステップ 3 **[再署名証明書の復号 (Decrypt Re-Sign Certificate)]** で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、**[内部CAを作成 (Create Internal CA)]** をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン (↓) をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。[再署名の復号ルールのCA証明書のダウンロード \(225 ページ\)](#) も参照してください。

ステップ 4 既知のキーを使用して復号するルールごとに、宛先サーバの内部証明書とキーをアップロードします。

a) **[既知のキーの証明書の復号 (Decrypt Known-Key Certificates)]** で **[+]** をクリックします。

- b) 内部IDの証明書を選択するか、[新しい内部証明書の作成 (Create New Internal Certificate)] をクリックし、ここでそれをアップロードします。
- c) [OK] をクリックします。

ステップ5 [保存 (Save)] をクリックします。

再署名の復号ルールの CA 証明書のダウンロード

トラフィックを復号する場合、ユーザは、TLS/SSLを使用するアプリケーションで信頼できるルート認証局として定義された暗号化プロセスで使用される、内部 CA 証明書を持っている必要があります。通常、証明書を生成した場合や、証明書をインポートした場合であっても、これらのアプリケーションで証明書がすでに信頼されているものとして定義されることはありません。大部分の Web ブラウザはデフォルトで、ユーザが HTTPS 要求を送信すると、Web サイトのセキュリティ証明書に問題があることを知らせる警告メッセージがクライアントアプリケーションから表示されます。通常、このエラーメッセージでは、Web サイトのセキュリティ証明書が信頼された認証局から発行されたものではないこと、または Web サイトが不明な認証局で証明されたものであることが示されますが、警告によって処理中に中間者攻撃の可能性があることが示唆される場合もあります。クライアントアプリケーションによっては、この警告メッセージがユーザに示されず、ユーザは承認されない証明書を受け入れることができません。

以下のいくつかの方法で、ユーザに必要な証明書を提供できます。

ルート証明書を受け入れるようにユーザに通知する

組織内のユーザに、企業の新しいポリシーについて通知し、組織が提供したルート証明書を、信頼できる認証局として受け入れるように指示できます。ユーザは証明書を受け入れ、信頼されたルート認証局のストレージエリアにそれを保存して、次にサイトにアクセスしたときにプロンプトが再度表示されないようにする必要があります。



- (注) ユーザは、代替証明書を作成した CA 証明書を受け入れて、信頼する必要があります。そうではなく、単に代替サーバ証明書を信頼した場合は、異なる HTTPS サイトを訪問するたびに、警告が表示される状況が続きます。

クライアント デバイスにルート証明書を追加する

ネットワーク上のすべてのクライアントデバイスに、信頼できるルート認証局としてルート証明書を追加できます。そうすれば、クライアントアプリケーションは自動的にルート証明書を持つトランザクションを受け入れるようになります。

証明書を電子メールで送信するか、共有サイトに置くことで、ユーザが証明書を入手できるようにします。または、会社のワークステーションイメージに証明書を組み込み、アプリケーションの更新機能を使用して、ユーザに証明書を自動的に配布することもできます。

次に、内部 CA 証明書をダウンロードして、Windows クライアントにインストールする方法を説明します。

手順

ステップ 1 Firepower Device Manager から証明書をダウンロードします。

- a) [ポリシー (Policies)] > [SSL復号 (SSL Decryption)] の順に選択します。
- b) [SSL復号設定 (SSL Decryption Settings)] ボタン (⚙️) をクリックします。
- c) [ダウンロード (Download)] ボタン (↓) をクリックします。
- d) ダウンロード場所を選択して、必要に応じてファイル名を変更し (拡張子そのまま)、[保存 (Save)] をクリックします。

これで、[SSL復号設定 (SSL Decryption Settings)] ダイアログ ボックスからキャンセルできます。

ステップ 2 クライアントシステムの Web ブラウザにある信頼されたルート認証局のストレージエリアに証明書をインストールするか、クライアント自体が証明書をインストールできるようにします。

プロセスは、オペレーティング システムとブラウザの種類によって異なります。たとえば、Windows 上で実行されている Internet Explorer および Chrome の場合は次のプロセスを使用できます。(Firefox の場合は、[ツール (Tools)] > [オプション (Options)] > [詳細 (Advanced)] ページでインストールします。)

- a) [スタート (Start)] メニューから、[コントロールパネル (Control Panel)] > [インターネット オプション (Internet Options)] を選択します。
- b) [コンテンツ (Content)] タブを選択します。
- c) [証明書 (Certificates)] ボタンをクリックして、[証明書 (Certificates)] ダイアログ ボックスを開きます。
- d) [信頼されたルート証明機関 (Trusted Root Certification Authorities)] タブを選択します。
- e) [インポート (Import)] をクリックし、ウィザードに従ってダウンロードされたファイル (<uuid>_internalCA.crt) を見つけて選択し、信頼できるルート認証局のストアに追加します。
- f) [終了 (Finish)] をクリックします。

メッセージは、インポートが成功したことを示しているはずですが、ユーザがよく知られたサードパーティの認証局から証明書を取得するのではなく自己署名証明書を生成した場合は、途中で Windows が証明書を検証できなかったことを警告するダイアログ ボックスが表示される場合があります。

[証明書 (Certificates)] ダイアログ ボックスと [インターネットオプション (Internet Options)] ダイアログ ボックスを閉じることができます。

例：ネットワークからの古いSSL/TLSバージョンのブロック

組織によっては、政府の規制や会社のポリシーで、古いバージョンのSSLまたはTLSを使用できないように義務付けている場合があります。SSL復号ポリシーを使用して、禁止するSSL/TLSバージョンを使用しているトラフィックをブロックできます。禁止されたトラフィックが即座に捕捉されるように、SSL復号ポリシーの先頭にこのルールを配置することを検討してください。

次に、すべてのSSL 3.0 および TLS 1.0 接続をブロックする例を示します。

始める前に

この手順では、SSL復号ポリシーがすでに有効になっていると仮定します（[SSL復号ポリシーの有効化（213 ページ）](#)を参照）。

手順

- ステップ 1** [ポリシー (Policies)] > [SSL復号 (SSL Decryption)] の順に選択します。
- ステップ 2** [+] ボタンをクリックして、新しいルールを作成します。
- ステップ 3** [順序 (Order)] で、[1] を選択してルールをポリシーの先頭に配置するか、またはネットワークに最も適した数を選択します。
デフォルトでは、ルールはポリシーの最後に追加されます。
- ステップ 4** [タイトル (Title)] に、ルールの名前（たとえば、Block_SSL3.0_and_TLS1.0）を入力します。
- ステップ 5** [アクション (Action)] で、[ブロック (Block)] を選択します。これで、ルールに一致するすべてのトラフィックがただちにドロップされます。
- ステップ 6** [送信元/宛先 (Source/Destination)]、[アプリケーション (Applications)]、[URLs]、[ユーザ (Users)] の各タブについては、すべてのオプションをデフォルト値のままにします。
- ステップ 7** [詳細 (Advanced)] タブをクリックし、[サポートされているバージョン (Supported Versions)] の下の [SSL3.0] と [TLS1.0] を選択したままにします。ただし、[TLS1.1] と [TLS1.2] はオフにします。
ポリシーは次のようになります。

Add SSL Decryption Rule

Order	Title	Action
1	Block_SSL3.0_and_TLS1.0	Block

Source / Destination Applications URLs Users **Advanced** Logging

CERTIFICATES

Certificate Status: Any Self Signed: Any

SUPPORTED VERSION

Version	Selected
SSL 3.0	<input checked="" type="checkbox"/>
TLS 1.0	<input checked="" type="checkbox"/>
TLS 1.1	<input type="checkbox"/>
TLS 1.2	<input type="checkbox"/>

ステップ 8 (任意) ブロックされた接続をダッシュボードやイベントに反映させるには、[ロギング (Logging)] タブをクリックし、[接続終了 (At End of Connection)] を選択します。外部 syslog サーバを選択することもできます (使用している場合)。

ステップ 9 [OK] をクリックします。

これでポリシーを展開できます。展開すると、システムを通過するすべての SSL 3.0 または TLS 1.0 接続がドロップされます。

(注) SSL 2.0 接続は、ポリシーのデフォルトアクションによって処理されます。これらもドロップされるようにするには、デフォルトアクションを [ブロック (Block)] に変更します。

次のタスク

このルールを実装する場合は、次の推奨事項をお勧めします。

- どのタイプの復号ルールでも、[詳細 (Advanced)] タブのデフォルト設定のままにします。その場合はすべての SSL/TLS オプションが選択されます。すべてのバージョンに適用することで、ハンドシェイク プロセスが簡素化されます。ただし、最初のブロックルールでは、SSL 3.0 および TLS 1.0 接続が引き続き妨げられます。
- 通常は、ポリシーのデフォルトアクションとして [復号しない (Do Not Decrypt)] を使用することをお勧めします。しかし、SSL 2.0 接続は常にデフォルトアクションによって処理されるため、代わりに [ブロック (Block)] を使用することもできます。ただし、すべての復号可能なトラフィックのデフォルトアクションとして [復号しない (Do Not Decrypt)] を適用する場合は、ポリシーの最後に [復号しない (Do Not Decrypt)] ルールを作成し、トラフィック一致基準のすべてのデフォルト値を受け入れます。このルールならば、テーブル内の以前のルールに一致しない、すべてのサポート対象の TLS 接続に一致し、それらの TLS バージョンにおけるデフォルトとして機能します。

SSL 復号のモニタリングとトラブルシューティング

ここでは、SSL 復号ポリシーのモニタリングおよびトラブルシューティング方法について説明します。

SSL 復号のモニタリング

ダッシュボードに復号についての情報を表示でき、ログ収集を有効化したルール（またはデフォルトのアクション）に一致するトラフィックのイベントを表示できます。

SSL 復号のダッシュボード

全体的な復号の統計情報を評価するには、**[モニタリング (Monitoring)] > [SSL 復号 (SSL Decryption)]** ダッシュボードを表示します。ダッシュボードには次の情報が表示されます。

- 暗号化されたトラフィックとプレーンテキストトラフィックの割合。
- SSL ルールに従って、暗号化されたトラフィックがどの程度復号されたか。

イベン

ダッシュボードに加えて、イベントビューア (**[モニタリング (Monitoring)] > [イベント (Events)]**) には、暗号化されたトラフィックの SSL 情報が含まれています。イベントの評価についていくつかのヒントを次に示します。

- 一致するトラフィックをブロックする SSL ルール（またはデフォルトのアクション）と一致したためにドロップされた接続の場合、**[アクション (Action)]** は「ブロック」、**[理由 (Reason)]** は「SSL ブロック」であることが必要です。
- **[実際の SSL アクション (SSL Actual Action)]** フィールドは、システムが接続に適用した実際のアクションを示します。これは、一致するルールに定義されたアクションを示す **[予期された SSL アクション (SSL Expected Action)]** とは異なります。たとえば、接続が復号を適用するルールと一致しても、いくつかの理由で復号できないことがあります。

復号再署名がブラウザでは機能するがアプリでは機能しない Web サイトの処理 (SSL または認証局ピンング)

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL（または認証局）ピンング」と呼ばれる手法が使用されます。SSL ピンング手法では、元のサーバ証明書のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが再署名された証明書を Firepower Threat Defense から受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Web サイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Web ブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上

のブラウザでも接続できるというのが主な症状です。たとえば、Facebook の iOS または Android アプリケーションを使用すると接続に失敗しますが、Safari または Chrome で `https://www.facebook.com` を指定すると接続に成功します。

SSL ピンングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

- アプリケーションのユーザをサポートします。この場合は、サイトへのトラフィックを復号できません。[SSL 復号 (SSL Decryption)] ルールの [アプリケーション (Application)] タブで、サイトのアプリケーションの [復号しない (Do Not Decrypt)] ルールを作成し、そのルールが、接続に適用される [再署名の復号 (Decrypt Re-sign)] ルールの前に適用されることを確認します。
- ユーザにブラウザだけを使用させます。サイトへのトラフィックを復号する必要がある場合は、ネットワーク経由での接続にサイトのアプリケーションを使用できないため、ブラウザのみを使用しなければならないことをユーザに通知する必要があります。

詳細

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実に SSL ピンングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用して SSL ピンングを識別できます。

アプリケーションは、次の 2 つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ 1 のアプリケーション (Facebook など) は、サーバから SH、CERT、SHD メッセージを受け取るとすぐに SSL ALERT メッセージを送信します。アラートは、通常、SSL ピンングを示す「Unknown CA (48)」アラートです。アラートメッセージの後に TCP リセットが送信されます。イベントの詳細情報で次のような症状が見られます。
 - SSL フロー フラグには ALERT_SEEN が含まれます。
 - SSL フロー フラグには APP_DATA_C2S または APP_DATA_S2C は含まれません。
 - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE です。
- グループ 2 のアプリケーション (Dropbox など) はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってから TCP リセットを送信します。イベントで次のような症状が見られます。
 - SSL フロー フラグには ALERT_SEEN、APP_DATA_C2S または APP_DATA_S2C は含まれません。
 - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED です。



第 10 章

アイデンティティポリシー

アイデンティティポリシーを使用して、接続からユーザアイデンティティ情報を収集できます。その後、ダッシュボードにユーザアイデンティティに基づく使用状況を表示し、ユーザまたはユーザグループに基づくアクセスコントロールを設定できます。

- [アイデンティティポリシーの概要 \(231 ページ\)](#)
- [アイデンティティポリシーの設定 \(232 ページ\)](#)
- [トランスペアレントユーザ認証の有効化 \(239 ページ\)](#)
- [アイデンティティポリシーのモニタリング \(243 ページ\)](#)
- [アイデンティティポリシーの例 \(243 ページ\)](#)

アイデンティティポリシーの概要

接続に関連付けられているユーザを検出するためにアイデンティティポリシーを使用できます。ユーザを識別することで、脅威、エンドポイント、およびネットワークインテリジェンスをユーザID情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。

たとえば、侵入イベントのターゲットとされたホストを誰が所有し、誰が内部攻撃やポートスキャンを開始したかを確認できます。また、高帯域幅のユーザや、望ましくない Web サイトまたはアプリケーションにアクセスしているユーザを確認することもできます。

ユーザの検出は、分析用のデータを収集するだけではありません。ユーザアイデンティティに基づいてリソースへのアクセスを選択的に許可またはブロックできるユーザ名やユーザグループ名に基づくアクセスルールを作成することもできます。

アクティブ認証によるユーザIDの確立

認証は、ユーザのアイデンティティを確認する動作です。

アクティブ認証を使用すると、HTTP トラフィックフローがユーザIDのマッピングがないシステムの IP アドレスから送られてきたときに、ネットワークに設定されたディレクトリを使用して、トラフィックフローを開始したユーザを認証するかどうかを決定できます。ユーザが

正常に認証された場合、IPアドレスは認証されたユーザの識別情報を保持していると見なされます。

認証が失敗しても、ユーザのネットワーク アクセスは妨げられません。アクセスルールは最終的に、これらのユーザにどのアクセスを提供するか決定します。

不明なユーザの対処

アイデンティティポリシーのディレクトリサーバを設定すると、システムはディレクトリサーバからユーザおよびグループメンバーシップ情報をダウンロードします。この情報は、24時間ごとに夜中に更新されるか、またはディレクトリ設定を編集して保存するたびに（変更がなくても）更新されます。

アクティブな認証アイデンティティルールによって求められた認証に成功したにも関わらず、ユーザ名がダウンロードしたユーザID情報の中に存在しない場合、不明なユーザとしてマークされます。ID関連のダッシュボードにそのユーザのIDは表示されず、ユーザー一致グループルールにも検出されません。

ただし、不明なユーザに対するアクセスコントロールルールが適用されます。たとえば、不明なユーザの接続をブロックすると、これらのユーザは、たとえ認証に成功（ディレクトリサーバがユーザとパスワードが有効であると認識したことを意味する）してもブロックされます。

そのため、ユーザの追加や削除、グループメンバーシップの変更などをディレクトリサーバに加えた場合、システムがディレクトリから更新情報をダウンロードするまで、これらの変更はポリシーの適用に反映されません。

真夜中の日次更新まで待たず、すぐに更新を適用させる必要がある場合は、ディレクトリのレルム情報を編集します（[オブジェクト（Objects）]>[アイデンティティレルム（Identity Realm）]に移動し、レルムを編集する）。[保存（Save）]をクリックして、変更を展開します。システムはただちに更新情報をダウンロードします。



- (注) 新規に追加したユーザ、または削除したユーザの情報がシステムに反映されているかどうかを確認するには、[ポリシー（Policies）]>[アクセスコントロール（Access Control）]を選択して、[ルールの追加(+)(Add Rule (+))]ボタンをクリックします。[ユーザ（Users）]タブに表示されたユーザのリストを確認してください。新規ユーザを検出できないか、または削除されたユーザが検出される場合、システムには古い情報があります。

アイデンティティポリシーの設定

アイデンティティポリシーを使用して、接続からユーザアイデンティティ情報を収集できます。その後で、ダッシュボードにユーザアイデンティティに基づく使用状況を表示し、ユーザまたはユーザグループに基づくアクセスコントロールを設定できます。

次に、アイデンティティ ポリシーでユーザ アイデンティティを取得するために必要な要素を設定する方法の概要を示します。

手順

ステップ 1 [ポリシー (Policies)] > [アイデンティティ (Identity)] を選択します。

アイデンティティ ポリシーをまだ定義していない場合には、[アイデンティティポリシーを有効にする (Enable Identity Policy)] をクリックして、[アイデンティティ ポリシーの設定 \(233 ページ\)](#) の説明のとおり設定します。

ステップ 2 アイデンティティ ポリシーを管理します。

アイデンティティ設定を行うと、このページにすべてのルールが順番にリストアップされます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- アイデンティティ ポリシーを有効または無効にするには、[アイデンティティポリシー (Identity Policy)] トグルをクリックします。
- アイデンティティポリシー設定を変更するには、[アイデンティティポリシー設定 (Identity Policy Configuration)] ボタン (⚙️) をクリックします。
- ルールを移動するには、編集して [順序 (Order)] ドロップダウン リストから新しい場所を選択します。
- ルールを設定するには、次の手順を実行します。
 - 新しいルールを作成するには、[+] ボタンをクリックします。
 - 既存のルールを編集する場合は、([操作 (Actions)] 列の) 対象のルールの編集アイコン (🔗) をクリックします。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。
 - 不要になったルールを削除する場合は、([操作 (Actions)] 列の) 対象のルールの [削除 (delete)] アイコン (🗑️) をクリックします。

アイデンティティ ルールの作成と変更の詳細については、[アイデンティティ ルールの設定 \(235 ページ\)](#) を参照してください。

アイデンティティ ポリシーの設定

アイデンティティ ポリシーを機能させるには、ネットワークのユーザ アカウントを含むディレクトリ レalm とサーバを設定する必要があります。また、ユーザがデバイスを経由する Web 要求を作成したときに、ユーザをアクティブに認証するために使用されるキャプティブ ポータルを設定する必要があります。

始める前に

ディレクトリ サーバ、Firepower Threat Defense デバイスおよびクライアント間で、時刻設定が一致していることを確認します。これらのデバイス間で時刻にずれがあると、ユーザ認証が成功しない場合があります。「一致」とは、別のタイムゾーンを使用できますが、たとえば、10 AM PST=1 PM EST など、それらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

ステップ 1 [ポリシー (Policies)] > [アイデンティティ (Identity)] を選択します。

ステップ 2 次のいずれかを実行します。

- アイデンティティ ポリシーが未設定の場合は、[アイデンティティポリシーを有効にする (Enable Identity Policy)] をクリックして、アイデンティティ ポリシーを設定します。
- [アイデンティティポリシー設定 (Identity Policy Configuration)] ボタン () をクリックします。

ステップ 3 [レルムサーバ (Realm Server)] を選択します。

レルムサーバが未設定の場合は、ドロップダウンリストから [新しいアイデンティティレルムの設定 (Configure New Identity Realm)] をクリックします。詳細については、[AD アイデンティティレルムの設定 \(143 ページ\)](#) を参照してください。

ステップ 4 [アクティブ認証 (Active Authentication)] オプションを設定します。

アイデンティティルールがユーザのアクティブ認証を必要とする場合、ユーザは接続されているインターフェイス上のキャプティブ ポータル ポートにリダイレクトされ、その後、認証が求められます。

サーバ証明書

アクティブ認証時にユーザに表示する内部証明書を選択します。必要な証明書をまだ作成していない場合は、ドロップダウンリストの一番下にある [新規内部証明書の作成 (Create New Internal Certificate)] をクリックします。

ブラウザが信頼している証明書をアップロードしない場合、ユーザは証明書を許可する必要があります。

ポート

キャプティブ ポータル ポート。デフォルトは、885 (TCP) です。別のポートを設定する場合は、1025 ~ 65535 の範囲にする必要があります。

(注) HTTP Basic、HTTP 応答ページ、および NTLM 認証方式では、ユーザはインターフェイスの IP アドレスを使用してキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名 `firewall-hostname.AD-domain-name` を使用してリダイレクトされます。HTTP ネゴシエートを使用する場合、アクティブ認証を必要としているすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要があります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。

ステップ 5 [再署名証明書の復号 (Decrypt Re-Sign Certificate)] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成 (Create Internal CA)] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン  をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールの CA 証明書のダウンロード ([225 ページ](#)) も参照してください。

(注) SSL 復号ポリシーをまだ構成していない場合にのみ SSL 復号の設定が求められます。ID ポリシーを有効にした後、これらの設定を変更するには、SSL 復号ポリシー設定を編集します。

ステップ 6 [保存 (Save)] をクリックします。

アイデンティティルールの設定

アイデンティティルールは、一致するトラフィックに対してユーザ識別情報を収集する必要があるかどうかを定義します。一致するトラフィックのユーザ識別情報を取得しない場合は、「認証なし」を設定します。

ルール設定に関係なく、アクティブ認証は HTTP トラフィックに対してのみ実行されることに注意してください。したがって、HTTP 以外のトラフィックをアクティブ認証から除外するルールを作成する必要はありません。すべての HTTP トラフィックに対してユーザ識別情報を取得する場合は、アクティブ認証ルールをすべての送信元および宛先に適用するだけで済みます。



(注) また、認証に失敗してもネットワークアクセスには影響しません。アイデンティティポリシーは、ユーザ識別情報のみを収集します。認証に失敗したユーザがネットワークにアクセスできないようにするには、アクセスルールを使用する必要があります。

手順

ステップ1 [ポリシー (Policies)] > [アイデンティティ (Identity)] を選択します。

ステップ2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (🔍) をクリックします。

不要になったルールを削除するには、ルールの [削除 (delete)] アイコン (🗑️) をクリックします。

ステップ3 [順序 (Order)] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

ルールは最初に一致したのから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ4 [ユーザ認証 (User Authentication)]

パッシブおよびアクティブ認証ルールのユーザアカウントが含まれる AD アイデンティティレルムを選択する必要があります。

- [アクティブ認証 (Active Auth)] : アクティブ認証を使用して、ユーザアイデンティティを判断します。アクティブ認証は HTTP トラフィックのみに適用されます。他のタイプのトラフィックが、アクティブ認証を要求または許可するアイデンティティポリシーに適合した場合、アクティブ認証は試行されません。
- [認証なし (No Auth)] : ユーザ識別情報を取得しません。このトラフィックに、アイデンティティベースのアクセスルールは適用されません。これらのユーザは、[認証不要 (No Authentication Required)] とマークが付けられます。

ステップ5 (アクティブ認証のみ) ディレクトリサーバでサポートする認証方法 ([タイプ (Type)]) を選択します。

- [HTTP基本 (HTTP Basic)] : 暗号化されていない HTTP 基本認証 (BA) 接続を使用して、ユーザを認証します。ユーザはブラウザのデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。これがデフォルトです。
- [NTLM] : NTLAN マネージャ (NTLM) 接続を使用して、ユーザを認証します。この選択は AD レルムを選択するときのみ使用できます。Windows ドメインのログインを使ってトランスペアレント認証が行われるよう、IE と Firefox ブラウザを設定することはできますが、ユーザはブラウザのデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします (トランスペアレントユーザ認証の有効化 (239ページ) を参照してください)。
- [HTTPネゴシエート (HTTP Negotiate)] : ユーザ エージェント (トラフィックフローを開始するためにユーザが使用しているアプリケーション) 方式と Active Directory サーバ方

式の間でデバイスがネゴシエーションできるようになります。ネゴシエーションの結果は、NTLM、ベーシックの順に、共通にサポートされ、使用されている最も強力な方式になります。ユーザはブラウザのデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。

- [HTTP応答ページ (HTTP Response Page)]: システムが提供する Web ページを使用して、ユーザに認証を求めるプロンプトを表示します。これは、HTTP 基本認証の 1 つの形式です。

(注) HTTP Basic、HTTP 応答ページ、および NTLM 認証方式では、ユーザはインターフェイスの IP アドレスを使用してキャプティブ ポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してリダイレクトされます。HTTP ネゴシエートを使用する場合、アクティブ認証を必要としているすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要があります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。

ステップ 6 (アクティブ認証のみ) アクティブ認証に失敗したユーザをゲストユーザとしてラベル付けするかどうかを決めるには、[ゲストとしてフォールバック (Fall Back as Guest)] > [オン/オフ (On/Off)] を選択します。

ユーザは、正常に認証する 3 つの機会が得られます。失敗した場合、このオプションの選択により、ユーザがどのようにマーク付けされるかが決まります。これらの値に基づき、アクセスルールを書き込みできます。

- [ゲストとしてフォールバック (Fall Back as Guest)] > [オン (On)]: ユーザは [ゲスト (Guest)] としてマークされます。
- [ゲストとしてフォールバック (Fall Back as Guest)] > [オフ (Off)]: ユーザは [失敗した認証 (Failed Authentication)] としてマークされます。

ステップ 7 [送信元/宛先 (Source/Destination)] タブで、トラフィック一致基準を定義します。

アクティブ認証は、HTTP トラフィックに対してのみ試されることに注意してください。したがって、HTTP 以外のトラフィックに対して「認証なし」のルールを設定は不要で、HTTP 以外のトラフィックに対してアクティブ認証ルールを作成するポイントもありません。

アイデンティティ ルールの送信元/宛先基準は、トラフィックが通過するセキュリティ ゾーン (インターフェイス)、IP アドレス、または IP アドレスの国または大陸 (地理的位置)、またはトラフィックで使用されるプロトコルおよびポートを定義します。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成 (Create New Object)] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次のトラフィック一致基準を設定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティゾーンオブジェクト。1つの基準を定義する、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン (Destination Zones)] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン (Source Zones)] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの1つから発生し、宛先ゾーンの1つを通して出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、内部ネットワークから発信されるすべてのトラフィックからユーザ識別情報を収集する場合、内部ゾーンを [送信元ゾーン (Source Zones)] として選択し、宛先ゾーンを空のままにします。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク (Source Networks)] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク (Destination Networks)] を設定します。
- 送信元 (Source) ネットワーク条件と宛先 (Destination) ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク (Network)] : 制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。
- [地理位置情報 (Geolocation)] : 位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

(注) 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース (GeoDB) を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、これにポートを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート (Source Ports)] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート/プロトコル (Destination Ports/Protocols)] を設定します。
- 特定の TCP/UDP ポートから発生し、特定の TCP/UDP ポートに向かうトラフィックを照合するには、両方設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポート プロトコル、TCP、または UDP を共有するポートのみを追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

ステップ 8 [OK] をクリックします。

トランスペアレント ユーザ認証の有効化

アクティブ認証を有効にするためにアイデンティティ ポリシーを設定する場合、ユーザ ID を取得するために次の認証方式を使用できます。

HTTP Basic

HTTP 基本認証では、ユーザは常に自分のディレクトリ ユーザ名とパスワードを認証するように要求されます。パスワードはクリアテキストで送信されます。そのため、基本認証はセキュアな認証形式とは見なされません。

基本認証は、デフォルトの認証メカニズムです。

HTTP 応答ページ

これは、HTTP 基本認証の一種であり、ユーザのログイン ブラウザ ページに表示されません。

NTLM、HTTP ネゴシエート (Active Directory のための統合 Windows 認証)

統合 Windows 認証は、実際にはユーザがドメインにログインしてワークステーションを使用するために利用されます。ブラウザは、アクティブ認証中の Firepower Threat Defense キャプティブ ポータルを含め、サーバへのアクセス時にこのドメイン ログインの使用を試みます。パスワードは送信されません。認証が成功すると、ユーザは何らかの認証チャレンジが実行されたことを意識せずに、トランスペアレント認証が行われます。

ブラウザがドメインログイン クレデンシャルを使用して認証要求を満たせない場合、ユーザは、ユーザ名とパスワードの入力を要求されますが、これは基本認証と同じユーザエクスペリエンスです。したがって、統合 Windows 認証を設定した場合、同じドメイン内のネットワークまたはサーバにアクセスするときに、ユーザがクレデンシャルを入力する必要性を減らすことができます。

なお、HTTP ネゴシエートは、アクティブ ディレクトリ サーバとユーザ エージェントの両方がサポートする、最も強力な方式を選択することに注意してください。ネゴシエーションが認証方式として HTTP 基本認証を選択した場合、トランスペアレント認証は行われません。強度の順序は、NTLM、次に基本認証です。トランスペアレント認証を可能にするには、ネゴシエーションが NTLM を選択する必要があります。

トランスペアレント認証を有効にするには、統合 Windows 認証をサポートするようにクライアント ブラウザを設定する必要があります。以下に、統合 Windows 認証をサポートする、広く使用されている一部のブラウザに関して、一般的な要件と基本設定について説明します。ソフトウェア リリースごとに技術が変更される場合があるため、詳細情報についてはブラウザ（または他のユーザ エージェント）のヘルプを参照してください。



ヒント Chrome および Safari など、すべてのブラウザが統合 Windows 認証をサポートするとは限りません（このガイドのリリース時に使用可能だったバージョンに基づきます）。ユーザはユーザ名とパスワードの入力を要求されます。使用しているバージョンでサポートが使用可能かどうかを確認するには、ブラウザのマニュアルを参照してください。

トランスペアレント認証の要件

トランスペアレント認証を実装するには、ブラウザまたはユーザ エージェントを設定する必要があります。これは、個別に実行することも、そのための設定を作成し、ソフトウェア配布ツールを使用してその設定をクライアント ワークステーションにプッシュすることもできます。この作業をユーザが自分で実行する場合は、ネットワークで機能する具体的な設定パラメータを提供する必要があります。

ブラウザまたはユーザ エージェントに関係なく、次の一般的な設定を実装する必要があります。

- ユーザがネットワークへの接続に使用する Firepower Threat Defense インターフェイスを [信頼済みサイト (Trusted Sites)] リストに追加します。IP アドレスか、使用可能な場合は完全修飾ドメイン名（たとえば、inside.example.com）を使用できます。また、ワイルドカードまたはアドレスの一部を使用して、汎用化された信頼済みサイトを作成できます。たとえば、一般的には *.example.com または単に example.com を使用してすべて内部サイトを網羅し、ネットワーク内のすべてのサイトを信頼できます（自身のドメイン名を使用）。インターフェイスの特定アドレスを追加する場合は、信頼済みサイトに複数のアドレスを追加して、ネットワークへのすべてのユーザ アクセス ポイントに対処することが必要な場合があります。
- 統合 Windows 認証は、プロキシサーバ経由で機能しません。したがって、プロキシを使用しないか、またはプロキシを通過しないアドレスに Firepower Threat Defense インターフェイスを追加する必要があります。プロキシを使用する必要がある場合、ユーザは NTLM を使用する場合でも認証を要求されます。



ヒント トランスペアレント認証の設定は必須ではありませんが、エンドユーザにとって便利です。トランスペアレント認証を設定しなかった場合、ユーザはすべての認証方式に対するログインチャレンジを提示されます。

トランスペアレント認証用の Internet Explorer の設定

NTLM トランスペアレント認証を有効にするよう Internet Explorer を設定するには、次の手順を実行します。

手順

- ステップ 1** [ツール (Tools)]>[インターネットオプション (Internet Options)]を選択します。
- ステップ 2** [セキュリティ (Security)]タブを選択し、[ローカルイントラネット (Local Intranet)]ゾーンを選択した後、次の手順を実行します。
- [サイト (Sites)]ボタンをクリックして、信頼できるサイトのリストを開きます。
 - 少なくとも次のオプションの 1 つが選択されていることを確認します。
 - [イントラネットネットワークを自動的に検出する (Automatically detect intranet network)] このオプションを選択すると、他のすべてのオプションが無効になります。
 - [プロキシをバイパスするすべてのサイトを含める (Include all sites that bypass the proxy)]
 - [詳細 (Advanced)]をクリックして[ローカルイントラネットサイト (Local Intranet Sites)]ダイアログボックスを開き、次に信頼する URL を [サイトの追加 (Add Site)]ボックスに貼り付けて [追加 (Add)]をクリックします。

複数の URL が存在する場合は、このステップを繰り返します。ワイルドカードを使用して、**http://*.example.com** のように URL の一部を指定するか、または単に ***.example.com** と指定します。

このダイアログボックスを閉じて、[インターネットオプション (Internet Options)]ダイアログボックスに戻ります。
 - [ローカルイントラネット (Local Intranet)]が選択されたままの状態、[カスタムレベル (Custom Level)]をクリックして[セキュリティ設定 (Security Settings)]ダイアログボックスを開きます。[ユーザ認証 (User Authentication)]>[ログオン (Logon)]設定を探して、[自動ログオンをイントラネットゾーンのみで有効にする (Automatic logon only in Intranet zone)]を選択します。[OK] をクリックします。
- ステップ 3** [インターネットオプション (Internet Options)]ダイアログボックスで [接続 (Connections)]タブをクリックし、次に [LAN 設定 (LAN Settings)]をクリックします。
- [LAN でプロキシサーバを使用する (Use a proxy server for your LAN)]が選択されている場合、Firepower Threat Defense インターフェイスがプロキシをバイパスすることを確認する必要があります。必要に応じて、次のいずれかを実行します。

- [ローカルアドレスにはプロキシサーバを使用しない (Bypass proxy server for local addresses)] を選択します。
- [詳細 (Advanced)] をクリックして、アドレスを [次で始まるアドレスにはプロキシサーバを使用しない (Do not use proxy server for addresses beginning with)] ボックスに入力します。たとえば、***.example.com** のようにワイルドカードを使用できます。

トランスペアレント認証用の Firefox の設定

NTLM トランスペアレント認証を有効にするよう Firefox を設定するには、次の手順を実行します。

手順

ステップ 1 [about:config] を開きます。フィルタバーを使用して、修正する必要がある設定を検索します。

ステップ 2 NTLM をサポートするには、次の設定を修正します (network.automatic でフィルタリング)。

- [network.automatic-ntlm-auth.trusted-uris] : 設定をダブルクリックし、URL を入力して [OK] をクリックします。カンマで区切って複数の URL を入力できます。プロトコルを含めるかどうかは任意です。次に例を示します。

```
http://host.example.com, http://hostname, myhost.example.com
```

URL の一部を使用することもできます。Firefox は、ランダムに部分文字列と照合するのではなく、文字列の末尾と照合します。したがって、ドメイン名のみ指定することにより、内部ネットワーク全体を包含することができます。次に例を示します。

```
example.com
```

- [network.automatic-ntlm-auth.allow-proxies] : 値が、デフォルトの [true] であることを確認します。値が [false] になっている場合は、ダブルクリックして変更します。

ステップ 3 HTTP プロキシ設定を確認します。これは、[ツール (Tools)] > [オプション (Options)] を選択し、次に [オプション (Options)] ダイアログボックスで [ネットワーク (Network)] タブをクリックすると見つかります。[接続 (Connection)] グループで、[設定 (Settings)] ボタンをクリックします。

- [プロキシなし (No Proxy)] が選択されている場合は、何も設定する必要がありません。
- [システムのプロキシ設定を使用 (Use System Proxy Settings)] が選択されている場合、[about:config] 内の [network.proxy.no_proxies_on] プロパティを修正して、[network.automatic-ntlm-auth.trusted-uris] に含めた信頼済み URI を追加する必要があります。
- [手動プロキシ設定 (Manual Proxy Configuration)] が選択されている場合、これらの信頼済み URI を包含するように [プロキシなし (No Proxy For)] リストを更新します。

- 他のオプションの1つが選択されている場合、これらの設定で使用するプロパティから同一の信頼済み URI が除外されていることを確認します。

アイデンティティ ポリシーのモニタリング

認証を必要とするアイデンティティ ポリシーが正常に動作している場合は、**[モニタリング (Monitoring)] > [ユーザ (Users)]** ダッシュボードやユーザ情報を含むその他のダッシュボードにユーザ情報が表示されます。

さらに、**[モニタリング (Monitoring)] > [イベント (Events)]** に表示されるイベントにもユーザ情報が含まれています。

ユーザ情報が表示されない場合は、ディレクトリ サーバが正常に機能していることを確認します。接続を確認するには、ディレクトリ サーバの設定ダイアログボックスの**[テスト (Test)]** ボタンを使用します。

ディレクトリ サーバが機能し、使用可能である場合、アクティブ認証を必要とするアイデンティティ ルールのトラフィック一致条件が、ユーザを照合するように書かれていることを確認します。たとえば、送信元ゾーンに、ユーザトラフィックがデバイスに入力するために経由するインターフェイスが含まれていることを確認します。アクティブ認証アイデンティティ ルールは HTTP トラフィックのみを照合するため、ユーザはデバイスを通じてそのタイプのトラフィックを送信している必要があります。

アイデンティティ ポリシーの例

使用例の章には、アイデンティティ ポリシーの実装例が含まれています。[ネットワーク トラフィックを調べる方法 \(56 ページ\)](#) を参照してください。



第 11 章

セキュリティ インテリジェンス

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。ここでは、セキュリティ インテリジェンスの実装方法について説明します。

- [セキュリティ インテリジェンスについて \(245 ページ\)](#)
- [セキュリティ インテリジェンスのためのライセンス要件 \(247 ページ\)](#)
- [セキュリティ インテリジェンスの設定 \(247 ページ\)](#)
- [セキュリティ インテリジェンスのモニタリング \(249 ページ\)](#)
- [セキュリティ インテリジェンスの例 \(249 ページ\)](#)

セキュリティ インテリジェンスについて

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。システムは、ブラックリストに登録されたこのトラフィックをアクセス コントロール ポリシーで評価する前にドロップすることにより、使用されるシステム リソースの量を減らします。

次に基づいてトラフィックをブラックリストに登録できます。

- **Cisco Talos Intelligence Group (Talos) フィード** : Talos定期的に更新されるセキュリティ インテリジェンスフィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。システムはフィードの更新を定期的にダウンロードするため、設定を再導入する必要なく新しい脅威インテリジェンスを利用できます。



(注) Talos フィードはデフォルトで1時間ごとに更新されます。[デバイス (Device)] > [更新 (Updates)] ページからは、更新頻度を変更するだけでなく、オンデマンドでフィードを更新することもできます。

- ネットワークおよび URL オブジェクト：ブロック対象の IP アドレスまたは URL が既知の場合は、それらのオブジェクトを作成し、それらをブラックリスト（またはホワイトリストとも呼ばれる例外リスト）に追加できます。

IP アドレス（ネットワーク）と URL で別のブラックリストを作成します。

ブラックリストの例外の作成

各ブラックリストには関連付けられた例外リストを作成でき、これはホワイトリストとも呼ばれます。例外リストの唯一の目的は、ブラックリストに表示される IP アドレスまたは URL を除外することです。つまり、使用する必要があり、安全であることがわかっているアドレスや URL が、ブラックリストに設定されているフィードにある場合、ブラックリストから完全にカテゴリを削除せずに、そのネットワーク/URL を除外できます。

除外された、またはホワイトリストに登録されたトラフィックは、以後アクセスコントロールポリシーによって評価されます。接続が許可またはドロップされたかどうかの最終決定は、接続に一致するアクセス制御ルールに基づきます。また、アクセスルールは接続に侵入やマルウェア検査を適用するかどうかも判断します。

セキュリティ インテリジェンス フィード カテゴリ

次の表では、Cisco Talos Intelligence Group (Talos) フィードで使用可能なカテゴリについて説明します。これらのカテゴリは、ネットワークと URL のブラックリストの両方に使用できます。

表 5: Talos フィードのカテゴリ

カテゴリ	説明
attackers	アウトバウンドの悪意のあるアクティビティで知られている、アクティブなスキャナとブラックリストに登録されたホスト。
bogon	bogon ネットワークと未割り当て IP アドレス。
bots	バイナリ マルウェア ドロッパーをホストするサイト。
CnC	ボットネットの指示管理サーバをホストするサイト。
dga	指示管理サーバでランデブーポイントとして動作する多数のドメイン名の生成に使用されるマルウェア アルゴリズム。
exploitkit	クライアントでのソフトウェアの脆弱性を識別するために設計されたソフトウェア キット。
malware	マルウェア バイナリまたはエクスプロイト キットをホストするサイト。
open_proxy	匿名での Web ブラウジングを許可するオープン プロキシ。

カテゴリ	説明
open_relay	スパムに使用されることが知られているオープン メール リレー。
phishing	フィッシング詐欺のページをホストするサイト。
response	悪意のある、または不審なアクティビティに積極的に参加している IP アドレスおよび URL。
spam	スパムの送信で知られているメール ホスト。
suspicious	疑わしく、既知のマルウェアのような特性を持っていると思われるファイル。
tor_exit_node	Tor の出口ノード。

セキュリティ インテリジェンスのためのライセンス要件

セキュリティ インテリジェンスを使用するには、**脅威**ライセンスを有効にする必要があります。[オプション ライセンスの有効化と無効化 \(101 ページ\)](#) を参照してください。

セキュリティ インテリジェンスの設定

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティ インテリジェンスを使用するには、**脅威**ライセンスを有効にする必要があります。

手順

- ステップ 1** [ポリシー (Policies)] > [セキュリティ インテリジェンス (Security Intelligence)] の順に選択します。
- ステップ 2** ポリシーが有効になっていない場合は、[セキュリティ インテリジェンスの有効化 (Enable Security Intelligence)] ボタンをクリックします。
[セキュリティ インテリジェンス (Security Intelligence)] をクリックして [オフ (Off)] にすることで、いつでもポリシーを無効にできます。設定は維持されるため、ポリシーを再度有効にするときに再設定する必要はありません。
- ステップ 3** セキュリティ インテリジェンスを設定します。
ネットワーク (IP アドレス) と URL には別々のブラック リストがあります。

- a) [ネットワーク (Network)] または [URL] タブをクリックして、構成するブラックリストを表示します。
- b) [ブラックリスト (Blacklist)] で、[+] をクリックして接続をすぐにドロップするオブジェクトまたはフィールドを選択します。

オブジェクトセレクトは、種類によってオブジェクトおよびフィールドを別々のタブに整理します。希望するオブジェクトがまだ存在しない場合、リストの下部にある [新しいオブジェクトの作成 (Create New Object)] リンクをクリックして作成します。Cisco Talos Intelligence Group (Talos) フィールドの説明については、フィールドの横にある [i] ボタンをクリックしてください。セキュリティインテリジェンスフィールドカテゴリ (246 ページ) も参照してください。

(注) セキュリティインテリジェンスは、/0 ネットマスクを使用して、IP アドレスブロックを無視します。これには、any-ipv4 と any-ipv6 のネットワーク オブジェクトが含まれます。ネットワークのブラックリストにこれらのオブジェクトを選択しないでください。

- c) [ブロックしない (Do Not Block)] リストで、[+] をクリックしてブラックリストの例外をすべて選択します。

このリストを構成する唯一の理由は、ブラックリストにある IP アドレスまたは URL を例外にすることです。適用除外された接続は、その後アクセス制御ポリシーによって評価され、いずれにしても破棄される可能性があります。

- d) 他のブラックリストを構成するには上記の手順を繰り返します。

ステップ 4 (オプション) [ログ設定の編集 (Edit Logging Settings)] ボタン (⚙️) をクリックしてログを設定します。

ロギングを有効にした場合は、ブラックリストのエントリに一致するものが記録されます。ロギングを有効にして、除外された接続がアクセス制御ルールに一致した場合、ログメッセージは取得しますが例外エントリに一致するものは記録されません。

次を設定します。

- [接続イベントロギング (Connection Events Logging)] : クリックしてロギングを有効または無効に切り替えます。
- [Syslog] : 外部の syslog サーバにイベントのコピーを送信するには、このオプションを選択して、syslog サーバを定義するサーバオブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しいSyslogサーバの追加 (Add Syslog Server)] をクリックして作成します。

デバイスのイベントストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

セキュリティインテリジェンスのモニタリング

セキュリティインテリジェンスポリシーのログ記録を有効にすると、システムはブラックリストに追加された接続ごとにセキュリティインテリジェンスイベントを生成します。これらの接続に一致する接続イベントがあります。

ブラックリストに追加されたドロップされた接続の統計情報は、[モニタリング (Monitoring)] ページの、使用可能なさまざまなダッシュボードに表示されます。

[モニタリング (Monitoring)] > [アクセスおよびSIルール (Access and SI Rules)] ダッシュボードに、トラフィックと一致する、上位のアクセスルールとセキュリティインテリジェンスに相当するルールが表示されます。

さらに、[モニタリング (Monitoring)] > [イベント (Events)]、次に [セキュリティインテリジェンス (Security Intelligence)] を選択して、セキュリティインテリジェンスイベントと、関連する接続イベントを [接続 (Connection)] タブに表示できます。

- イベントの [SIカテゴリID (SI Category ID)] フィールドは、ネットワークまたは URL オブジェクトあるいはフィードなど、ブラックリストに一致するオブジェクトを示します。
- 接続イベントの [理由 (Reason)] フィールドは、イベントに表示されたアクションが適用された理由について説明します。たとえば、ブロックアクションは、IP ブロックまたは URL ブロックなどの理由と組み合わせられて、接続がブラックリストに追加され、セキュリティインテリジェンスによってドロップされたことを示します。

セキュリティインテリジェンスの例

使用例の章には、セキュリティインテリジェンスポリシーの実装例が含まれています。 [脅威をブロックする方法 \(65 ページ\)](#) を参照してください。



第 12 章

アクセス制御

ここでは、アクセス コントロールルールについて説明します。これらのルールにより、デバイスを通過するトラフィックが制御されるとともに、侵入インスペクションなどの高度なサービスがトラフィックに適用されます。

- [アクセス コントロールの概要 \(251 ページ\)](#)
- [アクセス制御のためのライセンス要件 \(261 ページ\)](#)
- [アクセス コントロール ポリシーに関する注意事項と制限事項 \(261 ページ\)](#)
- [アクセス コントロール ポリシーを設定する \(263 ページ\)](#)
- [アクセス コントロール ポリシーのモニタリング \(276 ページ\)](#)
- [アクセス制御の例 \(278 ページ\)](#)

アクセス コントロールの概要

次に、アクセス コントロール ポリシーを説明します。

アクセス コントロールルールとデフォルト アクション

ネットワーク リソースへのアクセスを許可またはブロックするには、アクセス コントロール ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。

アクセスの制御は次に基づいて行われます。

- 送信元と宛先の IP アドレス、プロトコル、ポート、インターフェイスなど従来のネットワーク特性 (セキュリティ ゾーンの形式で)。
- 使用されているアプリケーション。アクセスコントロールは特定のアプリケーションに基づいて行うことも、アプリケーションのカテゴリ、特定の特性がタグ付けされたアプリケーション、アプリケーションのタイプ (クライアント、サーバ、Web)、またはアプリケーションのリスクやビジネスとの関連性の格付けを対象とするルールを作成できます。

- 汎用的なURLのカテゴリが含まれる Web 要求の宛先 URL。ターゲットサイトのパブリックレピュテーションに基づいて、カテゴリの一致を絞り込むことができます。
- 要求を作成したユーザ、またはユーザが所属するユーザグループ。

ユーザが許可する暗号化トラフィックの場合、IPS インスペクションを適用して脅威をチェックし、攻撃だと思われるトラフィックをブロックできます。また、禁止されたファイルやマルウェアをチェックするためにファイルポリシーも使用できます。

アクセスルールに一致しないすべてのトラフィックは、アクセスコントロールの[デフォルトアクション (Default Action)] によって処理されます。デフォルトでトラフィックを許可する場合は、侵入インスペクションをトラフィックに適用できます。ただし、デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。

アプリケーションフィルタリング

アクセスコントロールルールを使用すると、接続で使用されるアプリケーションに基づいてトラフィックをフィルタリングできます。このシステムはさまざまなアプリケーションを認識できるため、すべての Web アプリケーションをブロックせずに 1 つの Web アプリケーションをブロックする方法を探す必要はありません。

人気のあるアプリケーションでは、アプリケーションのさまざまな要素にフィルタ処理を行います。たとえば、Facebook をブロックせずに、Facebook Games をブロックするルールを作成できます。

一般的なアプリケーション特性に基づいて、リスクまたはビジネスとの関連性、タイプ、タグを選択することでアプリケーショングループ全体をブロックまたは許可するルールを作成できます。ただし、アプリケーションフィルタでカテゴリを選択するときは、目的のアプリケーション以外を含まないように一致するアプリケーションのリストをよく確認してください。可能なグループ処理の詳細については、[アプリケーション基準 \(268 ページ\)](#) を参照してください。

暗号化および復号トラフィックのアプリケーション制御

アプリケーションが暗号化を使用する場合、システムはアプリケーションを識別できない場合があります。

システムは StartTLS (SMTPS、POPS、FTPS、TelnetS、IMAPS など) で暗号化されたアプリケーショントラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

アプリケーションフィルタのダイアログボックスを使用し、次のタグを選択することでアプリケーションに復号が必要かどうかを決定してから、アプリケーションのリストを確認します。

- [SSL プロトコル (SSL Protocol)] : SSL プロトコルとしてタグ付けされたトラフィックを解釈する必要はありません。システムはこのトラフィックを認識し、アクセスコントロー

ル操作を適用できます。リストされたアプリケーションのアクセスコントロールルールは、想定される接続に一致する必要があります。

- [復号されたトラフィック (Decrypted Traffic)] : 最初にトラフィックを復号する場合のみ、システムがこのトラフィックを特定できます。このトラフィックにSSL復号ルールを設定します。

アプリケーションフィルタリングのベストプラクティス

アプリケーションフィルタリングのアクセス制御ルールを設計する際は、次の推奨事項を覚えておいてください。

- アドバタイズメントトラフィックなどの Web サーバによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。
- アプリケーションと URL の基準を同じルールで組み合わせることは避けてください (特に暗号化されたトラフィックの場合)。
- [復号トラフィック (Decrypted Traffic)] のタグが付けられたトラフィックにルールを作成する場合、一致するトラフィックを復号する SSL 復号ルールがあることを確認します。これらのアプリケーションは、復号された接続でのみ識別できます。
- システムは、Skype の複数のタイプのアプリケーショントラフィックを検出できます。Skype トラフィックを制御するには、個々のアプリケーションを選択する代わりに、[アプリケーションフィルタ (Application Filters)] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。
- Zoho メールへのアクセスを制御するには、Zoho アプリケーションと Zoho Mail アプリケーションの両方を選択します。

URL フィルタリング

アクセス制御ルールを使用して、HTTP または HTTPS 接続に使用される URL に基づいてトラフィックをフィルタ処理できます。HTTPS は暗号化されるので、HTTP の URL フィルタリングは HTTPS の URL フィルタリングよりも簡単なものであることに注意してください。

次の手法を使用して、URL フィルタリングを実装できます。

- カテゴリおよびレピュテーションベースの URL フィルタリング : URL フィルタリングライセンスにより、URL の一般的な分類 (カテゴリ) とリスクレベル (レピュテーション) に基づいて、Web サイトへのアクセスを制御できます。これは、不要なサイトをブロックするのに最も簡単で効果的な方法です。
- 手動 URL フィルタリング : 任意のライセンスで、個々の URL および URL のグループを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。手動フィルタリングの主な目的はカテゴリベースのブロックルールに例外を作成することですが、他の目的にも手動ルールを使用できます。

ここでは、URL フィルタリングについてさらに詳しく説明します。

カテゴリ別とレピュテーション別の URL のフィルタリング

URL フィルタリング ライセンスを使用することにより、要求された URL のカテゴリおよびレピュテーションに基づいて Web サイトへのアクセスを制御できます。

- **カテゴリ**：URL の一般的な分類。たとえば `ebay.com` はオークションカテゴリ、`monster.com` は求職カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- **レピュテーション**：この URL が、組織のセキュリティポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションは、高リスク（レベル 1）からウェルノウン（レベル 5）の範囲です。

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセスコントロールを使用して、乱用薬物カテゴリの高リスク URL をブロックできます。

カテゴリ データおよびレピュテーションデータを使用することで、ポリシーの作成と管理も簡素化されます。脅威を示すサイトや、望ましくないコンテンツを提供するサイトが現れては消えるペースが早すぎて、新しいポリシーを更新して適用するのが間に合わないこともあります。シスコが URL データベースで新しいサイト、変更された分類、変更されたレピュテーションについて更新すると、ルールは自動的に新しい情報に調整されます。新しいサイトを考慮するようにルールを編集する必要はありません。

定期的な URL データベースの更新を有効にすると、システムは最新の情報を使用して URL フィルタリングを行うことができます。また、Cisco Collective Security Intelligence (CSI) との通信を有効にすると、不明なカテゴリとレピュテーションについて URL の最新の脅威インテリジェンスを取得することもできます。詳細については、[URL フィルタリングの設定 \(485 ページ\)](#) を参照してください。



- (注) イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのルールを作成する必要があります。

カテゴリとレピュテーションでの URL の検索

次のサイトを使用して、特定の URL のカテゴリとレピュテーションをチェックできます。この情報は、カテゴリおよびレピュテーションベースの URL フィルタリングルールの動作をチェックするために役立ちます。

<https://www.brightcloud.com/tools/url-ip-lookup.php>

手動 URL フィルタリング

個別の URL または URL のグループを手動でフィルタリングすることにより、カテゴリおよびレピュテーションベースの URL フィルタリングを補完または選択的にオーバーライドできます。特殊なライセンスなしでこのタイプの URL フィルタリングを実行できます。

たとえば、アクセス制御を使用して、組織にとって不適切なカテゴリの Web サイトをブロックできます。ただし、カテゴリに適切な Web サイトが含まれ、アクセスを提供したい場合、そのサイトに対して手動の許可ルールを作成し、カテゴリのブロックルールの前に配置できます。

手動で URL フィルタリングを設定するには、対象の URL を含む URL オブジェクトを作成します。この URL を解釈する方法は、次のルールに基づきます。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバのホスト名のみに基づきます。ホスト名は、:// の区切り記号の後、またはホスト名のドットの後に来る場合、一致とみなされます。たとえば、`ign.com` は `ign.com` および `www.ign.com` と一致しますが、`verisign.com` とは一致しません。
- 1 つ以上の / を含める場合、サーバ名、パス、およびクエリ パラメータを含む文字列の部分一致には URL 文字列全体が使用されます。ただし、サーバは再構成することができ、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部をブロックまたは許可するのに手動の URL フィルタリングは使用しないことをお勧めします。文字列の部分一致も予期しない一致となる可能性があり、URL オブジェクトに含める文字列が意図しないサーバ上のパスやクエリ パラメータ内の文字列とも一致することがあります。
- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com` ではなく `example.com` を使用します。
- アクセス コントロールルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、`www.example.com` ではなく、`example.com` を使用します。

ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、`youtube.com` の証明書のサブジェクト共通名は `*.google.com` です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリングルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。



(注) 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

HTTPS トラフィックのフィルタリング

HTTPS トラフィックは暗号化されているために、HTTPS トラフィックに対して直接 URL フィルタリングを実行しても、HTTP トラフィックに対して行う場合ほどシンプルではありません。そのため、SSL 復号ポリシーを使用してフィルタリング対象のすべての HTTPS トラフィックを復号することを検討する必要があります。この方法では、URL フィルタリングアクセスコントロールポリシーは復号されたトラフィックで機能し、通常の HTTP トラフィックの場合と同じ結果が得られます。

ただし、一部の HTTPS トラフィックが復号せずにアクセスコントロールポリシーに渡されるようにする場合は、HTTPS トラフィックと一致するルールは HTTP トラフィックの場合と異なることを理解する必要があります。暗号化されたトラフィックをフィルタリングするには、システムは SSL ハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。URL の Web サイトのホスト名とサブジェクト共通名の間には、ほとんど、またはまったく関係がないことがあります。

HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。HTTPS の URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、`www.example.com` ではなく、`example.com` を使用します。また、サイトによって使用される証明書の内容を確認し、サブジェクト共通名で使用されるドメインが正しいこと、この名前が他のルールと競合しないことを確認してください（たとえば、ブロックするサイトの名前が許可する名前と重複する可能性があります）。たとえば、`youtube.com` の証明書のサブジェクト共通名は `*.google.com` です（当然、これは随時変更される可能性があります）。



(注) 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

暗号化プロトコルによるトラフィックの制御

システムは、URL フィルタリングの実行時に暗号化プロトコル（HTTP と HTTPS）を無視します。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングでは、次の Web サイトへのトラフィックが同様に処理されます。

- `http://example.com`
- `https://example.com`

両方ではなく、HTTP トラフィックのみまたは HTTPS トラフィックのみと一致するルールを設定するには、宛先の条件で TCP ポートを指定するか、アプリケーション条件をルールに追加します。たとえば、それぞれ、TCP ポートまたはアプリケーション条件と URL 条件を含む 2 つのアクセス制御ルールを作成することにより、サイトへの HTTPS アクセスを許可しながら、HTTP アクセスを禁止できます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

アクション：許可

TCP ポートまたはアプリケーション：HTTPS (TCP ポート 443)

URL：example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

アクション：ブロック

TCP ポートまたはアプリケーション：HTTP (TCP ポート 80)

URL：example.com

URL フィルタリングとアプリケーション フィルタリングの比較

URL フィルタリングとアプリケーション フィルタリングには類似点があります。しかし、それらは非常に異なる目的で使用する必要があります。

- URL フィルタリングは、Web サーバ全体へのアクセスをブロックまたは許可するのに適しています。たとえば、ネットワーク上であらゆるタイプのギャンブルを許可しないようにする場合は、ギャンブルカテゴリをブロックする URL フィルタリングルールを作成できます。このルールでは、ユーザはカテゴリ内の Web サーバ上のどのページにもアクセスできません。
- アプリケーション フィルタリングは、ホスティング サイトに関係なく特定のアプリケーションをブロックするため、またはそうしないと許容される Web サイトの特定の機能をブロックするために便利です。たとえば、Facebook のすべてをブロックすることなく Facebook のゲーム アプリケーションだけをブロックできます。

アプリケーション基準と URL の基準を組み合わせると予期しない結果につながることもあるため、URL とアプリケーションの基準では別のルールを作成するのが良いポリシーです。1 つのルールでアプリケーション基準と URL の基準を組み合わせる必要がある場合は、アプリケーションと URL のルールがより一般的なアプリケーションのみまたは URL のみのルールの例外として機能する場合を除き、単純なアプリケーションのみまたは URL のみのルールの後に配置する必要があります。URL フィルタリングブロックルールはアプリケーション フィルタリングよりも広範になるため、アプリケーションのみのルールの上に配置する必要があります。

アプリケーション基準と URL の基準を組み合わせる場合、より慎重にネットワークをモニタし、不要なサイトやアプリケーションへのアクセスを許可しないようにする必要があります。

効果的な URL フィルタリングのベスト プラクティス

URL フィルタリングのアクセス制御ルールを設計するときは、次の推奨事項を覚えておいてください。

- カテゴリとレピュテーションブロックは可能な限り使用します。これにより、新しいサイトはカテゴリに追加されるとともに、自動的にブロックされ、そのレピュテーションに基づくブロックは、サイトの評判が上がる（または下がる）と調整されます。
- URL カテゴリのマッチングを使用するときは、サイトのログイン ページがサイトそのものと異なるカテゴリにある場合に注意してください。たとえば、Gmail は [Web ベースの電子メール (Web-based Email)] カテゴリにあり、ログイン ページは [インターネットポ

タル (Internet Portals)] カテゴリにあります。それらのカテゴリに関して異なるアクションを実行する異なるルールがある場合、意図しない結果が生じる可能性があります。

- URL オブジェクトを使用して、Web サイト全体を対象とし、カテゴリ ブロック ルールの例外を作成します。つまり、本来はカテゴリルールでブロックされる特定のサイトを許可します。
- (URL オブジェクトを使用して) Web サーバを手動でブロックする場合は、セキュリティ インテリジェンス ポリシーでこれを行うとより効果的です。セキュリティ インテリジェンス ポリシーはアクセス制御ルールが評価される前に接続をドロップするので、より速くより効率的にブロックできます。
- HTTPS 接続の最も効果的なフィルタリングのために、記述しているアクセス制御ルールの対象のトラフィックを復号する SSL 復号ルールを実装します。復号された HTTPS 接続はアクセス制御ポリシーの HTTP 接続としてフィルタ処理されるので、HTTPS フィルタリングの制限はすべて回避されます。
- URL のブロック ルールはアプリケーション フィルタリング ルールの前に配置します。URL フィルタリングは Web サーバ全体をブロックするのに対し、アプリケーション フィルタリングは Web サーバに関係なく、特定のアプリケーションの使用を対象とするためです。

Web サイトのブロック時にユーザに表示される内容

URL フィルタリングルールで Web サイトをブロックした場合、ユーザに表示される内容は、サイトが暗号化されているかどうかに基づいて異なります。

- HTTP 接続：タイムアウトまたはリセットされた接続の場合、通常のブラウザ ページの代わりにシステムのデフォルトのブロック応答ページが表示されます。このページには、故意に接続がブロックされたことが明確に示されます。
- HTTPS (暗号化) 接続：システムのデフォルトのブロック応答ページは表示されません。代わりに、ブラウザのセキュアな接続の障害時のデフォルト ページが表示されます。エラーメッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

さらに、Web サイトは、明示的な URL フィルタリングルールではないその他のアクセス コントロールルールまたはデフォルトのアクションによってブロックされている場合があります。たとえば、ネットワーク全体または地理位置情報をブロックしている場合、ネットワーク上またはその地理的な位置にある Web サイトもブロックされます。これらのルールによってブロックされたユーザには、以下の制限で説明するとおり、応答ページが表示されることもあれば、表示されないこともあります。

URL フィルタリングを実装している場合、サイトが意図的にブロックされているときに表示されることがある内容と、どのタイプのサイトをブロックしているかについてエンドユーザに説明することを検討してください。そうでないと、エンドユーザがブロックされた接続のトラブルシューティングにかなりの時間を費やしてしまう場合があります。

HTTP 応答ページの制限

システムが Web トラフィックをブロックする場合に、常に、HTTP 応答ページが表示されるわけではありません。

- Web トラフィックがプロモートされたアクセス コントロール ルール（単純なネットワーク条件のみの早期に適用されたブロッキングルール）の結果としてブロックされている場合、システムは応答ページを表示しません。
- システムが要求された URL を特定する前に、Web トラフィックがブロックされている場合、システムは応答ページを表示しません。
- アクセス コントロール ルールによってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。

侵入、ファイル、マルウェアのインスペクション

侵入ポリシーとファイルポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイルポリシーは、システムのファイルコントロールと AMP for Firepower の機能を制御します。

他のトラフィック処理はすべて、侵入、禁止されたファイル、およびマルウェアについて、ネットワーク トラフィックが調べられる前に実行されます。侵入ポリシーまたはファイルポリシーをアクセスコントロールルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックを [許可 (allow)] するのみの侵入ポリシーおよびファイルポリシーを設定できます。トラフィックを [信頼 (trust)] または [ブロック (block)] するように設定されたルールではインスペクションは実行されません。さらに、アクセスコントロールポリシーのデフォルトのアクションが [許可 (allow)] の場合は、侵入ポリシーを設定できますが、ファイルポリシーは設定できません。

アクセスコントロールルールによって処理される単一接続の場合、ファイルインスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイルポリシーによってブロックされたファイルを検査しません。ファイルインスペクション内では、タイプによる単純なブロッキングの方が、マルウェアインスペクションおよびブロッキングよりも優先されます。ファイルがセッションで検出されてブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。



- (注) デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセスコントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。暗号化されていないトラフィックのみのインスペクションが実行されます。

アクセス制御ルールの順序のベストプラクティス

ルールは最初に一致したのから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。次の推奨事項を考慮してください。

- 固有のルールは一般的なルールの前に来る必要があります（特に特定のルールが一般的なルールの例外である場合）。
- レイヤ3/4基準（IPアドレス、セキュリティゾーン、ポート番号など）にのみ基づいてトラフィックをドロップするルールはできるだけ早く来る必要があります。レイヤ3/4基準は迅速かつ検査なしで評価することができるので、アプリケーションやURL基準などの検査を必要とするルールの前に来ることをお勧めします。もちろん、これらのルールの例外はこれらより上位に配置されなければなりません。
- 可能な限り、固有のドロップルールはポリシーの最上位近くに配置します。これにより、望ましくないトラフィックへの可能な限り早期の決定が保証されます。
- アプリケーションとURLの基準の両方を含むルールは、より一般的なアプリケーションのみまたはURLのみのルールの例外として機能している場合を除き、単純なアプリケーションのみまたはURLのみのルールの後に来る必要があります。アプリケーションとURLの基準を組み合わせることで、予期しない結果が生じることがある（特に暗号化されたトラフィックの場合）ため、可能な限り、URLとアプリケーションのフィルタリング用に個別のルールを作成することをお勧めします。

NAT とアクセスルール

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

その他のセキュリティポリシーがアクセス制御に影響する仕組み

その他のセキュリティポリシーは、アクセス制御ルールが機能し接続と一致する方法に影響を与えます。アクセスルールを設定するときは、次の点に注意してください。

- [SSL復号] ポリシー：SSL 復号ルールはアクセス制御の前に評価されます。したがって、暗号化された接続が、復号化のいくつかのタイプを適用する SSL 復号ルールと一致する場合、それはアクセス コントロール ポリシーによって評価されるプレーン テキスト（復号化）接続です。アクセス ルールは、暗号化されたバージョンの接続を参照しません。また、トラフィックをドロップする SSL 復号ルールと一致するすべての接続はアクセス コントロールポリシーによって参照されることがありません。最後に、復号しないルールと一致する暗号化された接続は、その暗号化された状態で評価されます。
- [アイデンティティ] ポリシー：送信元 IP アドレスのユーザ マッピングがある場合にのみ接続はユーザ（およびユーザ グループ）と一致します。ユーザまたはグループ メンバーシップを重視するアクセス ルールは、ユーザ アイデンティティがアイデンティティ ポリシーによって正常に収集された接続のみと一致できます。
- [セキュリティインテリジェンス] ポリシー：アクセス コントロール ポリシーではブラックリストに登録されてドロップされた接続が参照されることはありません。
- [VPN]（サイト間またはリモートアクセス）：VPN トラフィックは常にアクセス コントロールポリシーに対して評価され、一致するルールに基づいて接続は許可またはドロップされます。ただし、VPN トンネル自体はアクセス コントロール ポリシーが評価される前に復号化されます。アクセス コントロール ポリシーは、トンネル自体ではなく VPN トンネル内に組み込まれている接続を評価します。

アクセス制御のためのライセンス要件

アクセス制御ポリシーを使用するのに特別なライセンスは必要ありません。

ただし、アクセス制御ポリシー内の特定の機能には、次のライセンスが必要です。ライセンスの設定については、[オプションライセンスの有効化と無効化（101 ページ）](#)を参照してください。

- [URLフィルタリング] ライセンス：URL カテゴリおよびレピュテーションを一致基準として使用するルールを作成するため。
- [脅威] ライセンス：アクセス ルールまたはデフォルト アクションに侵入ポリシーを設定するため。ファイル ポリシーを使用する場合もこのライセンスが必要です。
- [マルウェア] ライセンス：マルウェア制御のためのアクセス ルールにファイル ポリシーを設定するため。

アクセスコントロールポリシーに関する注意事項と制限事項

アクセス制御のためのいくつかの追加の制限事項を次に示します。ルールから期待どおりの結果を得ているかどうかを評価してこれらを検討してください。

- **Firepower Device Manager** はディレクトリ サーバから最大 2000 人のユーザに関する情報をダウンロードできます。ディレクトリ サーバに 2000 以上のユーザアカウントが含まれる場合、アクセスルールでユーザを選択するとき、またはユーザベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

2000 までの制限は、グループに関連付けられた名前にも適用されます。グループに 2000 を超えるメンバーが含まれている場合は、ダウンロードした 2000 個の名前だけをグループメンバーシップと照合できます。
- 脆弱性データベース (VDB) の更新によってアプリケーションが削除 (廃止) される場合は、削除されたアプリケーションを使用するアクセス制御ルールまたはアプリケーションフィルタに変更を加える必要があります。これらのルールを修正するまで、変更を展開することはできません。また、問題を修正する前にシステム ソフトウェア アップデートをインストールすることはできません。[アプリケーションフィルタ (Application Filters)] オブジェクトページ、またはルールの [アプリケーション (Application)] タブでは、これらのアプリケーション名の後に「(廃止) (Deprecated)」と表示されます。
- 実際に使用されているルールを編集する場合、その変更は、**Snort** によって検査されなくなった、確立されている接続には適用されません。新しいルールは、将来の接続に対する照合に使用されます。また、**Snort** によって接続がアクティブに検査されている場合、**Snort** は、変更された一致またはアクション基準を既存の接続に適用できます。現在のすべての接続に変更を確実に適用する必要がある場合は、デバイス CLI にログインし、**clear conn** コマンドを使用して、確立されている接続を終了させることができます。これは、その後に接続の送信元が接続を再確立を試み、そのために新しいルールに対して適切に照合されることを前提としています。
- 接続のアプリケーションまたは URL を識別するためにシステムは 3 ~ 5 パケットを使用します。したがって、正しいアクセス制御ルールでも特定の接続ではすぐに一致しない可能性があります。ただし、アプリケーション/URL が判明すると、接続は一致するルールに基づいて処理されます。暗号化された接続の場合、これは SSL ハンドシェイクでのサーバ証明書の交換後に発生します。
- システムは、アプリケーションが識別される接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。
- 可能な場合は常に、一致基準を空のままにします (特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合)。たとえば、すべてのインターフェイスを含むゾーンを作成するのではなく、セキュリティゾーンの条件を空白のままにするだけで、すべてのインターフェイスのトラフィックについて照合の効率を高めることができます。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。
- メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによってほとんどの URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合でも、一部のデバイスでは、親 URL のデータのみが保存される場合があります。これらのデバイスによって処理される Web トラフィックの場合、システムはクラウドルックアップ

プを実行して、ローカルデータベースにないサイトのカテゴリとレピュテーションを判断できます。低メモリ デバイスには、5506-X、5506H-X、5506W-X、5508-X、5512-X、5515-X、5516-X、5525-X などの ASA モデルが含まれます。

アクセスコントロール ポリシーを設定する

ネットワーク リソースへのアクセスを制御するには、アクセスコントロール ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。トラフィックに一致するルールがない場合、ページ下部に表示されるデフォルトアクションが適用されます。

アクセスコントロール ポリシーを設定するには、**[ポリシー (Policies)] > [アクセスコントロール (Access Control)]** を選択します。

アクセスコントロール表には、すべてのルールが順番に表示されます。各ルールで以下を実行します。

- 左側の列にあるルール番号の隣の **[>]** ボタンをクリックし、ルール図を開きます。この図は、ルールがトラフィックをどのように制御するかを視覚的に示します。ボタンを再度クリックして図を閉じます。
- ほとんどのセルはインライン編集が可能です。たとえば、アクションをクリックして別のものを選択したり、送信元ネットワークオブジェクトをクリックして送信元の条件を追加または変更したりできます。
- ルールを移動するには、**[移動 (move)]** アイコン (📁) が表示されるまでルールにカーソルを合わせ、次にルールをクリックして新しいロケーションにドラッグし、ドロップします。また、ルールを編集して**[順序 (Order)]** リストで新しいロケーションを選択することで、ルールを移動することもできます。希望する処理の順番にルールを配置することが重要です。具体的なルール（特に、より一般的なルールに対する例外を定義するルール）は上部近くに配置します。
- 右側の列には、ルールのアクションボタンが含まれます。セルにマウスを当てるとボタンが表示されます。ルールを編集 (🔍) または削除 (🗑️) できます。

次に、ポリシーの設定方法について説明します。

デフォルトアクションの設定

接続が特定のアクセスルールに一致しない場合、アクセスコントロールポリシーのデフォルトアクションによって処理されます。

手順

ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] を選択します。

ステップ 2 [デフォルトアクション (Default Action)] フィールドの任意の場所をクリックします。

ステップ 3 一致するトラフィックに適用するアクションを選択します。

- [信頼性 (Trust)] : いかなる種類の追加インスペクションもなしでトラフィックを許可します。
- [許可 (Allow)] : 侵入ポリシーの対象となるトラフィックを許可します。
- [ブロック (Block)] : トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 4 アクションが [許可 (Allow)] の場合、侵入ポリシーを選択します。

ポリシーオプションの説明については、[侵入ポリシーの設定 \(272 ページ\)](#) を参照してください。

ステップ 5 (オプション) デフォルトアクションのロギングを設定します。

デフォルトアクションに一致するトラフィックのロギングをダッシュボードのデータまたはイベントビューアに記載されるようにするには、トラフィックのロギングを有効にする必要があります。[ロギングの設定 \(275 ページ\)](#) を参照してください。

ステップ 6 [OK] をクリックします。

アクセスコントロール ルールの設定

アクセスコントロールルールを使用して、ネットワークリソースへのアクセスを制御します。アクセスコントロールポリシーのルールは、上から下に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

手順

ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン  をクリックします。

不要になったルールを削除するには、ルールの [削除 (delete)] アイコン  をクリックします。

ステップ 3 [順序 (Order)] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル (Title)] にルールの名前を入力します。

この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます： +
_ -

ステップ 5 一致するトラフィックに適用するアクションを選択します。

- [信頼 (Trust)] : どのような種類のインスペクションも行わずにトラフィックを許可します。
- [許可 (Allow)] : ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可します。
- [ブロック (Block)] : トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 6 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/宛先 (Source/Destination)] : トラフィックが通過するセキュリティゾーン (インターフェイス) 、 IP アドレス、または IP アドレスの国または大陸 (地理的位置) 、またはトラフィックで使用されるプロトコルおよびポート。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。 [送信元/宛先基準 \(266 ページ\)](#) を参照してください。
- [アプリケーション (Application)] : アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトはすべてのアプリケーションです。 [アプリケーション基準 \(268 ページ\)](#) を参照してください。
- [URL] : Web リクエストの URL または URL カテゴリ。デフォルトはすべての URL です。 [URL 基準 \(270 ページ\)](#) を参照してください。
- [ユーザ (Users)] : ユーザまたはユーザ グループ。アイデンティティ ポリシーは、ユーザとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティ ポリシーを設定する必要があります。 [ユーザ基準 \(271 ページ\)](#) を参照してください。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成 (Create New Object)] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

条件をアクセスコントロールルールに追加する場合は、次のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、特定のホストまたはネットワークの URL フィルタリングを行う単一のルールを使用できます。

- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはアプリケーションフィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。
- 一部の機能では、適切なライセンスを有効にする必要があります。

ステップ 7 (オプション) [許可 (Allow)] アクションを使用するポリシーの場合、暗号化されていないトラフィックについてさらにインスペクションを設定できます。次のいずれかのリンクをクリックします。

- [侵入ポリシー (Intrusion Policy)] : トラフィックで侵入およびエクスプロイトを検査する場合は、**[侵入ポリシー (Intrusion Policy)] > [オン (On)]** を選択し、侵入検査ポリシーを選択します。「[侵入ポリシーの設定 \(272 ページ\)](#)」を参照してください。
- [ファイルポリシー (File Policy)] : マルウェアを含むファイルやブロックすべきファイルのトラフィックのインスペクションを実行するファイルポリシーを選択します。[ファイルポリシーの設定 \(273 ページ\)](#) を参照してください。

ステップ 8 (オプション) ルールのロギングを設定します。

デフォルトでは、ルールに一致するトラフィックに対して接続イベントは生成されませんが、ファイルポリシーを選択した場合、ファイルイベントはデフォルトで生成されます。この動作は変更できます。ダッシュボードデータまたはイベントビューアに含まれるポリシーに一致するトラフィックのロギングを有効にする必要があります。[ロギングの設定 \(275 ページ\)](#) を参照してください。

マッチングアクセスルールのログ構成に関係なくドロップまたはアラートするように設定されている侵入ルールについては、常に侵入イベントが生成されます。

ステップ 9 [OK] をクリックします。

送信元/宛先基準

アクセスルールの送信元/宛先基準によって、トラフィックが通過するセキュリティゾーン（インターフェイス）、IP アドレスや IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポートが定義されます。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

条件を変更するには、その条件内の [+] ボタンをクリックして、目的のオブジェクトまたは要素を選択し、[OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成 (Create New Object)] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティゾーンオブジェクト。1つの基準を定義する、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン (Destination Zones)] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン (Source Zones)] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの1つから発生し、宛先ゾーンの1つを通して出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、ホスト内部に向かうすべてのトラフィックが侵入検査を受けるようにする場合は、内部ゾーンを [送信先ゾーン (Destination Zones)] として選択し、送信元ゾーンは空白のままにします。侵入フィルタリングをルールに含めるには、ルールのアクションを [許可 (Allow)] にし、ルールで侵入ポリシーを選択する必要があります。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク (Source Networks)] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク (Destination Networks)] を設定します。
- 送信元 (Source) ネットワーク条件と宛先 (Destination) ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク (Network)] : 制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。
- [地理位置情報 (Geolocation)] : 位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、そこで使用される可能性があるすべての IP アドレスを知らなくても、特定の国へのアクセスを簡単に制限できます。



- (注) 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース (GeoDB) を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポートオブジェクト。TCP/UDP では、ポートを含めることができます。ICMP では、コードとタイプを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート (Source Ports)] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート (Destination Ports)]/[宛先プロトコル (Destination Protocols)] を設定します。宛先ポートだけを条件に追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。ICMP およびその他の非 TCP/UDP 仕様は、宛先ポートでのみ許可されます。送信元ポートでは許可されません。
- 特定の TCP/UDP ポートから送信されるトラフィックと特定の TCP/UDP ポートに向かうトラフィックの両方を照合するには、両方を設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポートプロトコル、TCP、または UDP を共有するポートのみを追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックをターゲットにできます。

アプリケーション基準

アクセスルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタが規定されます。デフォルトは任意のアプリケーションです。

ルールで個別のアプリケーションを指定できますが、アプリケーションフィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセスコントロールルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとする、セッションがブロックされます。

また、シスコは、システムおよび脆弱性データベース (VDB) の更新を通じて頻繁にアプリケーションディテクタを更新し追加します。そのため、ルールを手動で更新せずに、高リスクアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーションフィルタオブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタリストを変更するには、条件内の [+] ボタンをクリックし、別のタブに表示される目的のアプリケーションまたはアプリケーションフィルタオブジェクトを

選択してから、ポップアップ表示されるダイアログボックスで [OK] をクリックします。いずれかのタブで [詳細フィルタ (Advanced Filter)] をクリックするか、またはフィルタ条件を選択して特定のアプリケーションを検索します。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x] をクリックします。[フィルタとして保存 (Save As Filter)] リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーションフィルタ オブジェクトとして保存します。



- (注) 選択したアプリケーションが VDB の更新によって削除されていた場合は、アプリケーション名の後ろに「(廃止 (Deprecated))」と表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システムソフトウェアのアップグレードがブロックされます。

次の [詳細フィルタ (Advanced Filter)] 基準を使用すると、ルールに一致するアプリケーションまたはフィルタを特定できます。これらはアプリケーションフィルタ オブジェクトで使用されるものと同じ要素です。



- (注) 1つのフィルタ条件内での複数の選択はOR関係にあります。たとえば、リスクが「高 (High)」または (OR) 「非常に高い (Very High)」となります。フィルタ間の関係は「論理積 (AND)」であるため、リスクが「高 (High)」または (OR) 「非常に高い (Very High)」であり、かつ (AND) ビジネスとの関連性が「低 (Low)」または (OR) 「非常に低い (Very Low)」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。

リスク

アプリケーションが組織のセキュリティポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーションプロトコル (Application Protocol)] : HTTP や SSH などのホスト間の通信を表すアプリケーションプロトコル。
- [クライアントプロトコル (Client Protocol)] : Web ブラウザや電子メールクライアントなどのホスト上で動作しているソフトウェアを表すクライアント。

- [Webアプリケーション (Web Application)] : HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も重要な機能を説明する一般分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは[SSLプロトコル (SSL Protocol)]とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化された、または暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに[復号されたトラフィック (decrypted traffic)]タグを割り当てます。

アプリケーションリスト (ディスプレイ下部)

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

URL 基準

アクセスルールの URL 基準は、Web 要求で使用される URL または要求された URL が属するカテゴリを定義します。カテゴリが一致する場合は、許可またはブロックするためのサイトの相対レピュテーションも指定できます。デフォルトでは、すべての URL が許可されます。

URL のカテゴリおよびレピュテーションにより、アクセスコントロールルールの URL 条件をすぐに作成できます。たとえば、すべての暗号化されたギャンブルサイトをブロックしたり、リスクの高いすべてのソーシャルネットワーキングサイトを復号できます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとする、セッションがブロックされます。

カテゴリ データおよびレピュテーションデータを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、脅威インテリジェンスは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して、要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と現れては消える可能性があります。

URL リストを変更するには、条件内の [+] ボタンをクリックし、次の手法のいずれかを使用して、目的のカテゴリまたは URL を選択します。ポリシーからカテゴリまたはオブジェクトを削除するには、対応する [x] をクリックします。

[URL] タブ

[+] をクリックし、URL オブジェクトまたはグループを選択して、[OK] をクリックします。必要なオブジェクトが存在しない場合は、[URLの新規作成 (Create New URL)] をクリックします。



(注) 特定のサイトをターゲットにするようにURLオブジェクトを設定する前に、手動URLフィルタリングに関する情報を注意深く読みます。

[カテゴリ (Categories)] タブ

[+] をクリックし、目的のカテゴリを選択して、[OK] をクリックします。

デフォルトでは、レピュテーションに関係なく、選択した各カテゴリ内のすべてのURLにルールが適用されます。レピュテーションに基づいてルールを制限するには、各カテゴリの下矢印をクリックして、[任意 (Any)] チェックボックスを選択解除し、[レピュテーション (Reputation)] スライダを使用してレピュテーションレベルを選択します。レピュテーションスライダの左側は許可されるサイトを、右側はブロックされるサイトを示しています。レピュテーションがどのように使用されるかは、ルールアクションによって異なります。

- ルールによって Web アクセスをブロックまたは監視する場合は、レピュテーションレベルを選択することで、そのレベルより深刻なすべてのレピュテーションも選択されます。たとえば、[疑わしいサイト (Suspicious sites)] (レベル2) をブロックまたはモニタするルールを設定した場合、[高リスク (High risk)] (レベル1) サイトも自動的にブロックまたはモニタされます。
- ルールが Web アクセスを許可する場合は、レピュテーションレベルを選択すると、そのレベルより深刻でないすべてのレピュテーションも選択されます。たとえば、[無害なサイト (Benign sites)] (レベル4) を許可するルールを設定した場合、[既知 (Well known)] (レベル5) サイトも自動的に許可されます。

ユーザ基準

アクセスルールのユーザ基準は、IP 接続のユーザまたはユーザグループを定義します。アクセスルールにユーザまたはユーザグループの基準を含めるには、アイデンティティポリシーと関連付けられたディレクトリサーバを設定する必要があります。

アイデンティティポリシーは、特定の接続に関してユーザアイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストのIPアドレスに識別されたユーザが関連付けられます。したがって、送信元IPアドレスがユーザにマッピングされているトラフィックは、そのユーザからのものとみなされます。IPパケット自体にはユーザアイデンティティ情報は含まれていないため、このIPアドレスとユーザ間のマッピングが使用可能な中での最良近似となります。

1つのルールに最大50のユーザまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザを選択するより有意義です。たとえば、エンジニアリンググループに開発

ネットワークへのアクセスを許可するルールを作成し、それに続くルールとして、そのネットワークへの他のすべてのアクセスを拒否するルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバのエンジニアリング グループに追加するだけです。

ユーザリストを変更するには、条件の中にある [+] ボタンをクリックし、次のいずれかの方法で必要なアイデンティティを選択します。ポリシーからアイデンティティを削除するには、該当する [x] をクリックします。

- [ユーザおよびグループ (Users and Groups)] タブ : 目的のユーザまたはユーザ グループを選択します。グループは、ディレクトリ サーバにグループが設定されている場合のみ使用可能です。グループを選択すると、ルールはサブグループを含むグループのすべてのメンバーに適用されます。サブグループを別の方法で処理する場合は、サブグループ用の個別のアクセスルールを作成し、それをアクセス コントロール ポリシー内で親グループのルールの上に配置する必要があります。
- [特別なエンティティ (Special Entities)] : 次から選択します。
 - [認証失敗 (Failed Authentication)] : ユーザは認証を求められましたが、最大許容試行回数内に有効なユーザ名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザのネットワークへのアクセスは妨げられませんが、これらのユーザのネットワーク アクセスを制限するためのアクセスルールを記述できます。
 - [ゲスト (Guest)] : ゲストユーザは、これらのユーザをゲストと呼ぶようにアイデンティティルールが設定されている点を除き、認証失敗ユーザと同様です。ゲストユーザは認証を求められましたが、最大試行回数内に認証されることができませんでした。
 - [認証不要 (No Authentication Required)] : ユーザの接続が認証なしに指定されたアイデンティティルールに一致したため、ユーザは認証を求められませんでした。
 - [不明 (Unknown)] : IP アドレスのユーザマッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。

侵入ポリシーの設定

Firepower システムには複数の侵入ポリシーが付属しています。これらのポリシーは Cisco Talos Intelligence Group (Talos) によって設計されており、侵入ルール、プリプロセッサ ルール状態、詳細設定が設定されています。これらのポリシーは変更できません。ただし、[侵入ルールのアクションの変更 \(289ページ\)](#) で説明しているように、特定のルールに対して実行するアクションを変更することは可能です。

トラフィックを許可するアクセス コントロール ルールでは、次の侵入ポリシーのいずれかを選択して、トラフィックの侵入やエクスプロイトのインスペクションを実行できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。

侵入検査を有効化するには、[侵入ポリシー (Intrusion Policy)] > [オン (On)] を選択し、必要なポリシーを選択します。ポリシーは、安全性の低いものから高いものへの順で表示されています。

- [セキュリティよりも接続性を優先 (Connectivity over Security)] : このポリシーは、ネットワークインフラストラクチャのセキュリティよりも接続性（すべてのリソースにアクセスできること）が優先される組織のために作成されています。侵入ポリシーは、[接続性を上回るセキュリティ (Security over Connectivity)] ポリシーで有効にされるルールよりはるかに少ないルールが有効化されます。トラフィックをブロックする最も重要なルールのみが有効にされます。このポリシーは、侵入からの保護を適用する必要があるが、ネットワークのセキュリティにかなり自信がある場合に選択します。
- [バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] : このポリシーは、全体的なネットワークパフォーマンスとネットワークインフラストラクチャのセキュリティのバランスを取るよう設計されています。このポリシーは大部分のネットワークに適しています。このポリシーは、侵入防御を適用したい大部分の状況で選択できます。
- [接続性よりもセキュリティを優先 (Security over Connectivity)] : このポリシーは、ユーザの利便性よりもネットワークインフラストラクチャのセキュリティが優先される組織のために作成されています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。このポリシーは、セキュリティが特に重要であるか、トラフィックのリスクが高い場合に選択します。
- [最大検出 (Maximum Detection)] : このポリシーは、[接続性よりもセキュリティを優先 (Security over Connectivity)] ポリシーよりもさらに、ネットワークインフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、 익스プロイトキット、古い脆弱性や一般的な脆弱性、および既知の流行中の 익스プロイトを含め、多数の脅威カテゴリのルールを有効にします。このポリシーを選択する場合、正当なトラフィックが過剰にドロップされていないか慎重に評価してください。

ファイルポリシーの設定

Advanced Malware Protection for Firepower (AMP for Firepower) を使用して悪意のあるソフトウェア、つまり、マルウェアを検出するファイルポリシーを使用します。ファイル制御を実行するファイルポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

AMP for Firepower は、ネットワークトラフィックで検出された潜在的なマルウェアの性質を取得し、ローカルマルウェアファイル分析と事前分類の更新を取得するために AMP クラウドを使用します。AMP クラウドにアクセスし、マルウェアルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドに問い合わせます。可能な性質を次に示します。

- マルウェア (Malware) : AMPクラウドはファイルをマルウェアクラウドとして分類しました。ファイル内のいずれかのファイルがマルウェアである場合、アーカイブファイル (たとえば zip ファイル) はマルウェアとしてマークされます。
- クリーン (Clean) : AMPクラウドはファイルがマルウェアが含まれないクリーンな状態であると分類しました。その中のすべてのファイルがクリーンであれば、アーカイブファイルはクリーンであるとマークされます。
- 不明 (Unknown) : AMPクラウドがまだファイルの性質を指定していません。その中のすべてのファイルが不明であれば、アーカイブファイルは不明であるとマークされます。
- 利用不可 (Unavailable) : システムは、ファイルの性質を判断するために AMPクラウドに問い合わせできませんでした。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。複数の「利用不可」イベントが連続して発生している場合、管理アドレスのインターネット接続が正常に機能していることを確認します。

使用可能なファイルポリシー

次のいずれかのファイルポリシーを選択できます。

- [なし (None)] は、送信したファイルでマルウェアの評価を行わず、特定のファイルをブロックしません。このオプションは、ファイル送信が信頼されている、またはファイル送信の可能性が低い (または不可能である)、あるいはアプリケーションを信頼している、または URL フィルタリングがネットワークを適切に保護しているルールに対して選択します。
- [マルウェアをすべてブロック (Block Malware All)] は、AMPクラウドに問い合わせネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [クラウドをすべてルックアップ (Cloud Lookup All)] は、AMPクラウドに問い合わせネットワークを通過するファイルの傾向を取得して記録したうえでその伝送を許可します。
- [オフラインドキュメントとアップロードされたPDFをブロック、その他のマルウェアをブロック (Block Office Document and PDF Upload, Block Malware Others)] は、ユーザによる Microsoft Office のドキュメントと PDF のアップロードをブロックします。AMPクラウドに問い合わせネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [オフラインドキュメントのアップロードをブロック、その他のマルウェアをブロック (Block Office Documents Upload, Block Malware Others)] は、ユーザによる Microsoft Office のドキュメントのアップロードをブロックします。AMPクラウドに問い合わせネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。

ロギングの設定

アクセスルールのロギング設定は、接続イベントがルールに一致するトラフィックに対して発行されるかどうかを決定します。イベントビューアでルールに関連するイベントを確認するには、ロギングを有効にする必要があります。また、一致するトラフィックがシステムをモニターするために使用できるさまざまなダッシュボードに反映されるようにするためにも、ロギングを有効にする必要があります。

組織のセキュリティおよびコンプライアンスの要件に従って接続をロギングしてください。生成するイベントの数を抑え、パフォーマンスを向上させることが目標である場合は、分析のために重要な接続のロギングのみを有効にします。一方、プロファイリングの目的でネットワークトラフィックの広範な表示が必要な場合は、その他の接続のロギングを有効化します。



注意

サービス妨害 (DoS) 攻撃の間にブロックされた TCP 接続をロギングすると、システムパフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロックルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイスを対象としているかどうかを検討します。

次のロギング オプションを設定できます。

ログアクションの選択

次のいずれかのアクションを選択できます。

- [接続の開始時と終了時にログを記録する (Log at Beginning and End of Connection)] : 接続の開始時と終了時にイベントを発行します。接続終了イベントには接続開始イベントに含まれるすべての情報と、接続中に拾うことができるすべての情報が含まれているため、許可しようとしているトラフィックではこのオプションを選択しないことをお勧めします。両方のイベントのロギングは、システムパフォーマンスに影響する可能性があります。ただし、これはブロックされているトラフィックに許可されている唯一のオプションです。
- [接続終了時にログを記録する (Log at End of Connection)] : 接続の終了時に接続ログの記録を許可する場合は、このオプションを選択します。これは許可されている、または信頼されているトラフィックに推奨されます。
- [接続のロギングなし (No Logging at Connection)] : ルールのロギングを無効にするには、このオプションを選択します。これがデフォルトです。



- (注) アクセスコントロールルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。侵入がブロックされた接続では、接続ログ内の接続のアクションは [ブロック (Block)]、理由は [侵入ブロック (Intrusion Block)] ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ファイル イベント

禁止されたファイルまたはマルウェア イベントのログギングを有効にするには、[ファイルのログギング (Log Files)] を選択します。このオプションを設定するには、ルールでファイル ポリシーを選択する必要があります。ルールにファイル ポリシーを選択している場合、このオプションはデフォルトで有効になっています。シスコは、このオプションを有効のままにすることを推奨します。

システムが禁止されたファイルを検出すると、次のタイプのイベントの1つを自動的にログギングします。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

ファイルがブロックされた接続の場合、接続ログにおける接続のアクションは[ブロック (Block)] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、[ファイルモニタ (File Monitor)]（ファイルタイプまたはマルウェアが検出された）、あるいは[マルウェアブロック (Malware Block)] または [ファイルブロック (File Block)]（ファイルがブロックされた）です。

接続イベントの送信先

外部 syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバオブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成 (Create New Syslog Server)] をクリックして作成します（syslog サーバへのログギングを無効にするには、サーバリストから [任意 (Any)] を選択します）。

デバイスのイベントストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

アクセスコントロールポリシーのモニタリング

以下のトピックでは、アクセス制御ポリシーのモニタ方法について説明します。

ダッシュボードでのアクセス制御統計情報のモニタリング

[モニタリング (Monitoring)] ダッシュボードの大半のデータは、アクセスコントロールポリシーに直接関連しています。「[トラフィックのモニタリングおよびシステム ダッシュボード \(109 ページ\)](#)」を参照してください。

- [モニタリング (Monitoring)] > [アクセスおよびSIルール (Access And SI Rules)] には最もヒットしたアクセスルールと関連する統計情報が表示されます。

- 一般的な統計情報は、[ネットワーク概要 (Network Overview)]、[送信先 (Destinations)] および [ゾーン (Zones)] ダッシュボードで確認できます。
- URL フィルタリングの結果は [Webカテゴリ (Web Categories)]、[URLカテゴリ (URL Categories)] および [送信先 (Destinations)] ダッシュボードで確認できます。[Webカテゴリ (Web Categories)]、[URLカテゴリ (URL Categories)] ダッシュボードに情報を表示するには、少なくとも1つのURL フィルタリングポリシーが必要です。
- アプリケーションフィルタリングの結果は、[アプリケーション (Applications)] および [Webアプリケーション (Web Applications)] ダッシュボードで確認できます。
- [ユーザ (Users)] ダッシュボードでは、ユーザベースの統計情報を確認できます。ユーザ情報を収集するには、アイデンティティポリシーを実装する必要があります。
- [攻撃者 (Attackers)] および [ターゲット (Targets)] ダッシュボードでは、侵入ポリシーの統計情報を確認できます。これらのダッシュボードで情報を表示するには、少なくとも1つのアクセスコントロールルールに侵入ポリシーを適用する必要があります。
- ファイルポリシーおよびマルウェアフィルタリング統計情報は、[ファイルログ (File Logs)] および [マルウェア (Malware)] ダッシュボードで確認できます。このダッシュボードに情報を表示するには、ファイルポリシーを1つ以上のアクセス制御ルールに適用する必要があります。
- [モニタリング (Monitoring)] > [イベント (Events)] には、アクセスコントロールルールに関連する接続とデータのイベントも表示されます。

CLIでのアクセスコントロールポリシーのモニタリング

CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用し、アクセス制御ポリシーと統計情報に関する詳細情報を取得することもできます。

- **show access-control-config** はアクセス制御ルールに関する概要情報とルールごとのヒット数を表示します。
- **show access-list** はアクセス制御ルールから生成されたアクセス制御リスト (ACL) を表示します。ACL は初期フィルタを提供し、できる限り迅速な決定を実現しようとするため、ドロップされる接続を調査する (および、そのために不必要にリソースを消費する) 必要はありませんこの情報には、ヒット数が含まれます。
- **show snort statistics** は主要なインスペクタである Snort インスペクションエンジンに関する情報を表示します。Snort は、アプリケーションフィルタリング、URL フィルタリング、侵入からの保護、ファイルおよびマルウェアフィルタリングを実装します。
- **show conn** は現在インターフェイスを通じて確立されている接続に関する情報を表示します。
- **show traffic** は各インターフェイスを介したトラフィックフローに関する統計情報を表示します。

- **show ipv6 traffic** はデバイスを介した IPv6 トラフィック フローに関する統計情報を表示します。

アクセス制御の例

使用例の章には、アクセス制御ルールのいくつかの実装例が含まれています。次の例を参照してください。

- [ネットワーク トラフィックを調べる方法 \(56 ページ\)](#)。この例では、全体的な接続およびユーザ情報を収集するための基本的な考え方が示されています。
- [脅威をブロックする方法 \(65 ページ\)](#)。この例では、侵入ポリシーを適用する方法が示されています。
- [マルウェアをブロックする方法 \(72 ページ\)](#)。この例では、ファイル ポリシーを適用する方法が示されています。
- [アクセプタブルユース ポリシー \(URL フィルタリング\) の実装方法 \(76 ページ\)](#)。この例では、URL フィルタリングを実行する方法が示されています。
- [アプリケーションの使用を制御する方法 \(81 ページ\)](#)。この例では、アプリケーション フィルタリングを実行する方法が示されています。
- [サブネットを追加する方法 \(85 ページ\)](#)。この例では、トラフィック フローを許可するために必要なアクセスルールを含め、新しいサブネットをネットワーク全体に統合する方法が示されています。



第 13 章

侵入ポリシー

次のトピックでは、侵入ポリシーと密接に関連付けられているネットワーク分析ポリシー（NAP）について説明します。侵入ポリシーには、脅威についてトラフィックをチェックし、攻撃が判明したトラフィックをブロックするルールが含まれます。ネットワーク分析ポリシーは、トラフィックを正規化してプロトコルの異常を識別することによってさらに検査するためにトラフィックの準備を行う、トラフィックの前処理を制御します。

前処理と侵入検査を非常に密接に関連しているため、1つのパケットを調べるネットワーク分析と侵入ポリシーはお互いを補完する必要があります。

- [侵入ポリシーとネットワーク分析ポリシーについて \(279 ページ\)](#)
- [侵入ポリシーのためのライセンス要件 \(287 ページ\)](#)
- [侵入ポリシーの管理 \(288 ページ\)](#)
- [侵入ポリシーのモニタリング \(291 ページ\)](#)
- [侵入ポリシーの例 \(291 ページ\)](#)

侵入ポリシーとネットワーク分析ポリシーについて

ネットワーク分析ポリシーと侵入ポリシーは、共同で侵入の脅威を検出し、防ぎます。

- ネットワーク分析ポリシー（NAP）では、トラフィックの復号化および前処理の方法について、特に侵入の試行を示す可能性がある異常なトラフィックをさらに評価できるよう、制御します。
- 侵入ポリシーでは、侵入ルールと呼ばれる侵入やプリプロセッサのルールを使用し、パターンに基づいて攻撃がないかデコードされたパケットを調べます。ルールでは、脅威となるトラフィックを防いで（ドロップして）イベントを生成したり、単に検出（警告）してイベントの生成のみを行うことができます。

システムがトラフィックを分析するとき、ネットワーク分析の復号化および前処理のフェーズは、侵入防御のフェーズより前に、個別に発生します。ネットワーク分析ポリシーと侵入ポリシーは、共同で広範かつ深いパケット検査を提供します。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワークトラフィックの検知、通知および防御に役立ちます。

システム定義のネットワーク分析および侵入ポリシー

システムには、相互に補完して動作する、同じ名前のネットワーク分析と侵入ポリシーのいくつかのペアが含まれています。たとえば「バランスのとれたセキュリティと接続性」という名前の NAP と侵入ポリシーの両方があり、一緒に使用されることを意図しています。システムによって提供されるポリシーは Cisco Talos Intelligence Group (Talos) によって設定されます。これらのポリシーに対して Talos は侵入とプリプロセッサルールの状態を設定し、プリプロセッサの最初の設定とその他の高度な設定を行います。

新たな脆弱性が既知になった時点で、Talos は侵入ルールの更新をリリースします。これらのルール更新により、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやプリプロセッサルールの新規作成または更新、既存ルールのステータスの変更、デフォルトのポリシー設定の変更が実施されます。ルールの更新はまた、システム提供のポリシーからルールを削除、新しいルールのカテゴリを提供、デフォルトの変数セットを変更できます。

手動で、ルールデータベースを更新したり、定期的な更新スケジュールを設定できます。有効にするには更新を展開する必要があります。システムデータベースの更新についての詳細は、[システム データベースの更新 \(491 ページ\)](#) を参照してください。

次にシステム提供のポリシーについて示します。

[バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。これらを一緒に使用すると、ほとんどの種類のネットワークおよび展開に適した出発点として機能します。[バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] ネットワーク分析ポリシーがデフォルトとして使用されます。

[セキュリティよりも接続性を優先 (Connectivity Over Security)] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続性、すべてのリソースを取得する機能が、ネットワークインフラストラクチャのセキュリティよりも優先されるネットワーク向けに作られています。この侵入ポリシーは、[接続性よりもセキュリティを優先 (Security over Connectivity)] ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

[接続性よりもセキュリティを優先 (Security over Connectivity)] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性よりも優先されるネットワーク向けに作られています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

[最大検出 (Maximum Detection)] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティが、運用に対する影響が大きい、[接続性よりもセキュリティを優先 (Security Over Connectivity)] ポリ

シーで考慮されるセキュリティよりもさらに重視されるネットワーク向けに作られています。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイトキット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

侵入ルールおよびプリプロセッサルール

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワークトラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データパケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

システムには、Cisco Talos Intelligence Group (Talos) によって作成された次のタイプのルールが含まれています。

- 侵入ルール。共有オブジェクトルールおよび標準のテキストルールに細分されます。
- プリプロセッサルール。プリプロセッサと、ネットワーク分析ポリシーのパケットデコーダ検出オプションが関連付けられたルールです。デフォルトではほとんどのプリプロセッサルールは無効です。

ここでは、侵入ルールについてより詳細に説明します。

侵入ルール属性

[ポリシー (Policies)] > [侵入 (Intrusion)] を選択するときに、脅威を特定するために利用できるすべての侵入ルールのリストを参照してください。上記の表で、侵入ポリシーの名前をクリックすると、各ポリシーのルールを表示できます。

各ポリシーのルールのリストには、アラートまたはドロップに設定されているルールと、明示的に無効にしたルールだけが示されます。デフォルトで無効になっているルールは表示されません。30,000以上のルールがありますが、すべての可能なルールのサブセットのみが表示されます。しかし、最小の有効なルールセットですら、リスト全体をスクロールするには時間がかかります。ルールは、スクロールしていくと明らかになります。

次に、各ルールを定義する属性を示します。

> (シグニチャの説明)

左の列の[>]ボタンをクリックして、署名の説明を開きます。説明は、トラフィックとルールを照合するために、Snort インспекション エンジンによって使用されます。コードの説明はこのドキュメントの範囲外ですが、『Firepower Management Center Configuration Guide』で詳しく説明しています。<http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html> からご使用のソフトウェアのバージョン用のブックを選択してください。侵入ルールの編集についての情報を探します。

署名には、特定の項目の変数が含まれています。詳細については、[デフォルトの侵入変数セット \(282 ページ\)](#) を参照してください。

GID

ジェネレータ識別子 (ID)。この数は、ルールを評価し、イベントを生成する、システムコンポーネントを示します。1は標準テキスト侵入ルール、3は共有オブジェクト侵入ルールを示します (これらのルールタイプの違いは **Firepower Device Manager ユーザ** にとって意味はありません)。これらは、侵入ポリシーを設定するときに対象となる主なルールです。その他のGIDの詳細については、[ジェネレータ識別子 \(283 ページ\)](#) を参照してください。

SID

Snort 識別子 (ID)。署名 ID とも呼ばれます。1000000 より小さい Snort ID は Cisco Talos Intelligence Group (Talos) によって作成されたものです。

操作 (Action)

選択した侵入ポリシーでのこのルールの状態。各ルールに対し、このポリシー内のルールのデフォルトアクションに「(デフォルト)」が追加されます。ルールをデフォルトの設定に戻すには、このアクションを選択します。指定できるアクションは、次のとおりです。

- **アラート** : このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
- **[ドロップ (Drop)]** : このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
- **[無効 (Disabled)]** : このルールではトラフィックは一致しません。イベントは生成されません。

ステータス (Status)

ルールに対するデフォルトのアクションを変更すると、この列に「上書き済み」と表示されます。それ以外の場合は、この列は空です。

メッセージ (Messages)

これはルールの名前で、ルールによってトリガーされたイベントにも表示されます。メッセージは通常、署名が一致した脅威を識別します。それぞれの脅威の詳細についてインターネットで検索できます。

デフォルトの侵入変数セット

侵入ルールの署名には、特定の項目の変数が含まれます。変数のデフォルト値を次に示します。`$HOME_NET` と `$EXTERNAL_NET` が最もよく使用される変数です。プロトコルはポート番号とは別々に指定されるため、ポート変数は数字のみです。

- `$AIM_SERVERS` = ネットワークまたはホストのアドレス 20 個 : 64.12.24.0/23、64.12.28.0/23、64.12.31.136、64.12.46.140、64.12.161.0/24、64.12.163.0/24、64.12.186.85、64.12.200.0/24、205.188.1.132、205.188.3.0/24、205.188.5.0/24、205.188.7.0/24、205.188.9.0/24、205.188.11.228、205.188.11.253、205.188.11.254、205.188.153.0/24、205.188.179.0/24、205.188.210.203、205.188.248.0/24。

- `$DNS_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。
- `$EXTERNAL_NET = 任意の IP アドレス`。
- `$FILE_DATA_PORTS = $HTTP_PORTS, 143, 110`。
- `$FTP_PORTS = 21, 2100, 3535`。
- `$GTP_PORTS = 3386, 2123, 2152`。
- `$HOME_NET = 任意の IP アドレス`。
- `$HTTP_PORTS = 次の番号の 144 個のポート : 36, 80 ~ 90, 311, 383, 443, 555, 591, 593, 631, 666, 801, 808, 818, 901, 972, 1158, 1212, 1220, 1414, 1422, 1533, 1741, 1830, 1942, 2231, 2301, 2381, 2578, 2809, 2980, 3029, 3037, 3057, 3128, 3443, 3507, 3702, 4000, 4343, 4848, 5000, 5117, 5222, 5250, 5450, 5600, 5814, 6080, 6173, 6767, 6988, 7000, 7001, 7005, 7071, 7080, 7144, 7145, 7510, 7770, 7777 ~ 7779, 8000, 8001, 8008, 8014, 8015, 8020, 8028, 8040, 8060, 8080 ~ 8082, 8085, 8088, 8118, 8123, 8161, 8180 ~ 8182, 8222, 8243, 8280, 8300, 8333, 8344, 8400, 8443, 8500, 8509, 8787, 8800, 8888, 8899, 8983, 9000, 9002, 9060, 9080, 9090, 9091, 9111, 9290, 9443, 9447, 9710, 9788, 9999, 10000, 11371, 12601, 13014, 15489, 19980, 23472, 29991, 33300, 34412, 34443, 34444, 40007, 41080, 44449, 50000, 50002, 51423, 53331, 55252, 55555, 56712`。
- `$HTTP_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。
- `$ORACLE_PORTS = 任意`。
- `$SHELLCODE_PORTS = 180`。
- `$SIP_PORTS = 5060, 5061, 5600`。
- `$SIP_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。
- `$SMTP_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。
- `$SNMP_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。
- `$SQL_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。
- `$SSH_PORTS = 22`。
- `$SSH_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。
- `$TELNET_SERVERS = $HOME_NET` (任意の IP アドレスを示します)。

ジェネレータ識別子

ジェネレータ識別子 (GID) は、侵入ルールを評価し、イベントを生成するサブシステムを識別します。標準のテキスト侵入ルールのジェネレータ ID は 1、共有オブジェクト侵入ルールのジェネレータ ID は 3 です。また、各種プリプロセッサに対して複数のルールセットがあります。次の表で、GID について説明します。

表 6: ジェネレータ ID

ID	コンポーネント
1	標準テキストルール。
2	タグ付きパケット。 (タグ付きセッションからパケットを生成するタグジェネレータのルール。)
3	共有オブジェクトルール。
102	HTTP デコーダ。
105	バック オフィス探知機。
106	RPC デコーダ。
116	パケット デコーダ。
119、120	HTTP インスペクト プリプロセッサ (GID 120 ルールは、サーバ固有の HTTP トラフィックに関連しています)。
122	ポートスキャン デテクタ。
123	IP 最適化。
124	SMTP デコーダ。 (SMTP 動詞に対するエクスプロイト。)
125	FTP デコーダ。
126	Telnet デコーダ。
128	SSH プリプロセッサ。
129	ストリーム プリプロセッサ。
131	DNS プリプロセッサ。
133	DCE/RPC プリプロセッサ。
134	ルール遅延、パケット遅延。 (これらのルールのイベントは、ルール遅延中断 (SID 1) または侵入ルールのグループの再有効化 (SID 2) のとき、またはパケット遅延のしきい値を超えた (SID 3) ためにシステムがパケットの検査を中止したときに生成されます)。
135	レートベースの攻撃デテクタ。 (ネットワーク上のホストへの過剰な接続。)

ID	コンポーネント
137	SSL プリプロセッサ。
138、139	機密データ プリプロセッサ。
140	SIP プリプロセッサ。
141	IMAP プリプロセッサ。
142	POP プリプロセッサ。
143	GTP プリプロセッサ。
144	Modbus プリプロセッサ。
145	DNP3 プリプロセッサ。

ネットワーク分析ポリシー

ネットワーク分析ポリシーはトラフィック前処理を制御します。プリプロセッサは、トラフィックを正規化し、プロトコル異常を識別することにより、トラフィックがさらに検査されるように準備します。ネットワーク分析関連の前処理は、セキュリティインテリジェンスのブラックリストの登録と SSL 復号後、アクセス制御と侵入やファイル検査の前に発生します。

デフォルトでは、システムは [バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] ネットワーク分析ポリシーを使用して、アクセス制御ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、システムはアクセス制御ルールで選択した侵入ポリシーに基づいて、異なるネットワーク分析ポリシーを適用します。

システムは、最適な処理が行われるように、侵入やネットワーク分析ポリシーに一致するように試みます。ただし、ネットワーク分析ポリシー (NAP) ルールはアクセス制御ルールで使用されるのと同じトラフィック一致基準を持っていないので、推奨されるガイドラインに従わないと、一致しないポリシーが取得される可能性があります。

システムによる NAP ルールを使用したネットワーク分析ポリシーの選択方法

ネットワーク分析ポリシーを直接割り当てることはできません。代わりに、システムは、アクセス制御ルールで割り当てた侵入ポリシーに基づいて NAP ルールを自動的に生成します。

NAP ルールは、セキュリティゾーンとネットワーク仕様のみに基づいています。したがって、侵入ポリシーを含むアクセス制御ルールごとに、同じ送信元/送信先のセキュリティゾーンとネットワークに、同じ名前のネットワーク分析ポリシーを適用する NAP ルールが作成されません。ポート、URL、ユーザ、およびアプリケーションの基準は無視されます。

これは重要な違いです。ポート、アプリケーション、URL などのレイヤ 4 または 7 基準に基づいて異なる侵入ポリシーを適用できますが、それより高い層の基準はネットワーク分析ポリシーの選択に影響を与えません。

システムは、アクセス制御ルールと同じ順序でNAPルールを順序付けします。システムでは、最初に一致した NAP ルールを使用して、適用するネットワーク分析ポリシーを決定します。

したがって、同じ送信元/送信先ゾーンとネットワーク オブジェクトの組み合わせのトラフィックを許可する制御ルールが複数あるが、別のトラフィック一致基準では異なる場合、システムは重複する複数のNAPルールを生成し、2番目とその後の重複するルールは、トラフィックに一致しなくなります。これらの「重複する」ルールに別の侵入ポリシーを適用する場合、少なくともトラフィックの一部は、侵入およびネットワーク分析ポリシーに一致しなくなります。

たとえば、次のルールについて考えてみます。

1. アクセス ルール 1

アクション：許可

[送信元ゾーン (Source zone)] : inside_zone

[送信元ネットワーク (Source network)] : any

[送信先ゾーン (Destination zone)] : outside_zone

[送信先ネットワーク (Destination Network)] : any

[URLカテゴリ (URL category)] : ソーシャル ネットワーク

[侵入ポリシー (Intrusion policy)] : 接続性よりもセキュリティを優先

2. アクセス ルール 2

アクション：許可

[送信元ゾーン (Source zone)] : inside_zone

[送信元ネットワーク (Source network)] : any

[送信先ゾーン (Destination zone)] : outside_zone

[送信先ネットワーク (Destination Network)] : any

[侵入ポリシー (Intrusion policy)] : バランスのとれたセキュリティと接続性

この場合、2つの NAP ルールがあります。

1. NAP ルール 1

[送信元ゾーン (Source zone)] : inside_zone

[送信元ネットワーク (Source network)] : any

[送信先ゾーン (Destination zone)] : outside_zone

[送信先ネットワーク (Destination Network)] : any

[ネットワーク分析ポリシー (Network analysis policy)] : 接続性よりもセキュリティを優先

2. NAP ルール 2

[送信元ゾーン (Source zone)] : inside_zone

[送信元ネットワーク (Source network)] : any

[送信先ゾーン (Destination zone)] : outside_zone

[送信先ネットワーク (Destination Network)] : any

[ネットワーク分析ポリシー (Network analysis policy)] : バランスのとれたセキュリティと接続性

両方の NAP ルールには同じ一致基準があるために、システムは [接続性よりもセキュリティを優先 (Security over Connectivity)] ネットワーク分析ポリシーを、アクセス制御ルール 1 または 2 のいずれかに一致するトラフィックに適用します。ただし、アクセス制御ルール 2 に一致するほとんどのトラフィックは、バランスのとれた侵入ポリシーを使用します。したがって、アクセス制御ルール 2 に一致するトラフィックは、NAP および侵入ポリシーに一致しません。



- (注) アクセス制御ポリシーで 1 つの侵入ポリシーを使用する場合、システムはデフォルトのポリシーと同じ名前のネットワーク分析ポリシーを設定するだけで、NAP ルールは生成しません。それ以外の場合は、デフォルトのネットワーク分析ポリシーとしてバランスのとれたポリシーを設定します。他の NAP ルールが適用されない場合はデフォルトのポリシーが適用されます。これは侵入ポリシーを割り当てていないゾーンとネットワークの組み合わせでは一般的です。

NAP の処理を最適化する侵入のポリシーを適用するためのベスト プラクティス

適したネットワーク分析ポリシーを得るために侵入ポリシーの割り当て方法を決定する際は、次の推奨事項を考慮してください。

- 同じ侵入ポリシーを常に使用する場合、同じ名前のネットワーク分析ポリシーをデフォルトとして設定し、常に適した侵入ポリシーおよびネットワーク分析ポリシーを取得します。
- 特定のトラフィックに対して異なる侵入ポリシーを使用する必要がある場合は、送信元/送信先のセキュリティゾーンとネットワークオブジェクトの同じ組み合わせに対し常に同じ侵入ポリシーを使用します。これにより NAP ルールは、すべての関連付けられているアクセス制御ルールに対し同じ名前のネットワーク分析ポリシーを割り当てることが保証されます。

たとえば、`network_one` の `inside_zone` から `outside_zone` への一部のトラフィックに対し、[接続性よりもセキュリティを優先 (Security over Connectivity)] ポリシーを使用する必要があると決定した場合、同じ送信元/送信先ゾーンとネットワーク仕様を持つアクセス制御ルールごとに、[接続性よりもセキュリティを優先 (Security over Connectivity)] ポリシーを割り当てます。

侵入ポリシーのためのライセンス要件

アクセス制御ルールの侵入ポリシーを適用するには、[脅威 (Threat)] ライセンスを有効にする必要があります。ライセンスの設定については、[オプションライセンスの有効化と無効化 \(101 ページ\)](#) を参照してください。

ネットワーク分析ポリシーには追加ライセンスは必要ありません。

侵入ポリシーの管理

Firepower Device Manager では、あらかじめ定義された侵入ポリシーのいずれかを適用できます。これらの各ポリシーには同じ侵入ルール（署名とも呼ばれます）の一覧が含まれていますが、各ルールに対して実行する操作は異なります。たとえば、あるルールは1つのポリシーでアクティブになる可能性があります、別のポリシーでは無効化されます。

適用されている特定のルールであまりにも誤検出が多く、そのルールでブロックして欲しくないトラフィックがブロックされている場合、安全性の低い侵入ポリシーに切り替えることなく、ルールを無効にできます。または、トラフィックをドロップせずに、一致すると警告するように変更することもできます。

ただし、ルールが侵入ポリシーでデフォルトで無効な場合は、一致したトラフィックをドロップまたは警告するように変更することはできません。有効なポリシーまたは以前無効にしたポリシーでのみ、アクションを変更できます。

侵入に関連するダッシュボードおよびイベントビューアを使用して（両方、[モニタリング (Monitoring)] ページ）、侵入ルールがトラフィックに与えている影響を評価します。警告や削除に設定された侵入ルールに一致したトラフィックに対してのみ、侵入イベントや侵入データが表示されることに注意してください。無効になっているルールは評価されません。

ここでは、侵入ポリシーおよびルールの調整について詳しく説明します。

アクセス制御ルールでの侵入ポリシーの適用

侵入ポリシーをネットワークトラフィックに適用するには、トラフィックを許可するアクセス制御ルール内でポリシーを選択します。侵入ポリシーを直接指定しません。

保護するネットワークの相対的なリスクに基づいた可変の侵入保護を提供する別の侵入のポリシーを割り当てることができます。たとえば、内部ネットワークと外部ネットワーク間のトラフィックには、より厳しい [接続性よりもセキュリティを優先 (Security over Connectivity)] ポリシーを使用する場合があります。一方で、内部ネットワーク間のトラフィックに対しては、より緩やかな [セキュリティよりも接続性を優先 (Connectivity over Security)] ポリシーを適用する場合があります。

また、すべてのネットワークに対して同じポリシーを使用することで、構成を簡略化することもできます。たとえば、[バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] ポリシーは、接続に過度に影響を与えずに良好な保護を提供するための設計です。

異なるネットワークに対して異なるポリシーを使用する場合は、同じ送信元/送信先のセキュリティゾーンを使用するすべてのルールに同じポリシーを適用し、ネットワークオブジェクトが条件に一致する場合に最良の結果を得ることになります。詳細については、「[NAPの処理を最適化する侵入のポリシーを適用するためのベストプラクティス \(287ページ\)](#)」を参照してください。

手順

ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] を選択します。

ステップ 2 トラフィックを許可する、新しいルールを作成するか、既存のルールを編集します。

既定のアクションを許可する場合は、既定のアクションで侵入ポリシーを指定することもできます。

ステップ 3 [侵入ポリシー (Intrusion Policy)] タブをクリックします。

ステップ 4 [侵入ポリシー (Intrusion Policy)] > [オン (On)] を選択し、トラフィックの照合に使用する侵入検査ポリシーを選択します。

侵入ルールアクションの変更

事前定義された各侵入ポリシーには同じルールがあります。違いは、各ルールで取られるアクションがポリシーごとに異なる場合があることです。

指定されたポリシーの中で、ルールの既定のアクションは、それが有効な場合のみ、つまりアラートまたはドロップに設定されていれば変更できます。既定のアクションを変更すると、誤検出が多すぎるルールを無効できます。またはルールが一致するトラフィックをアラートまたはドロップするかどうかを変更できます。



(注) デフォルトのアクションを変更した場合、次回侵入ルールデータベースが更新された際に、システムがルールのデフォルトを選択したアクションに再設定します。その時点で、選択が新しいデフォルトとなり、ステータスにはアクションが上書き済みとして表示されなくなります。

手順

ステップ 1 [ポリシー (Policies)] > [侵入 (Intrusion)] の順に選択します。

ステップ 2 変更するルールアクションの侵入ポリシーのタブをクリックします。

事前定義されているポリシーは次のとおりです。

- セキュリティよりも接続性を優先
- バランスのとれたセキュリティと接続性
- 接続性よりもセキュリティを優先
- 最大検出

ステップ 3 変更するアクションのルールを検索します。

ルールは上書き済みが一番上に並べ替えられ、また上書きされたルールのグループ内でアクション順に並べ替えられます。それ以外の場合、ルールは、GID、次に SID で並べ替えられます。

各ポリシーのルールのリストには、アラートまたはドロップに設定されているルールと、明示的に無効にしたルールのみが示されます。デフォルトで無効になっているルールは表示されません。

変更するルールを検索するには検索ボックスを使用します。理想的には、連携して問題に取り組んでいる場合にイベントやシスコテクニカルサポートから Snort 識別子 (SID) とジェネレータ識別子 (GID) を取得できます。

各ルールの要素の詳細については、[侵入ルール属性 \(281 ページ\)](#) を参照してください。

このリストを検索するには、次の手順を実行します。

- a) [検索 (Search)] ボックス内でクリックして、[検索属性 (search attributes)] ダイアログボックスを開きます。
- b) ジェネレータ ID ([GID])、Snort ID ([SID])、またはルール[アクション (Action)] の組み合わせを入力し、[検索 (Search)] をクリックします。

たとえば [アクション=ドロップ (Action = Drop)] を選択して、一致する接続をドロップするポリシーのすべてのルールを表示できます。検索ボックスの横にあるテキストは、条件に一致するルールの数が表示されます (たとえば「9416 中 8937 ルールが見つかりました」)。

検索条件をクリアするには、検索ボックスの条件の [x] をクリックします。

ステップ 4 ルールの [アクション (Action)] の列をクリックして、必要なアクションを選択します。

- [アラート (Alert)] : このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
- [ドロップ (Drop)] : このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
- [無効 (Disabled)] : このルールではトラフィックは一致しません。イベントは生成されません。

ルールのデフォルトのアクションは、アクションに加えて「(デフォルト)」と表示されます。デフォルトを変更すると、状態の列にそのルールに対して「上書き済み」と表示されます。

侵入イベントの Syslog の設定

侵入ポリシーの外部 syslog サーバを設定して Syslog サーバに侵入イベントを送信できます。サーバに送信される侵入イベントを取得するために侵入ポリシーで Syslog サーバを設定する必

必要があります。アクセスルールで syslog サーバを設定し、侵入イベントではなく、接続イベントのみ syslog サーバに送信します。

手順

- ステップ 1 [ポリシー (Policies)] > [侵入 (Intrusion)] の順に選択します。
- ステップ 2 [ログ設定の編集 (Edit Logging Settings)] ボタン (⚙️) をクリックして syslog を設定します。
- ステップ 3 [接続イベント送信先 (Send Connection Events To)] フィールドをクリックして、syslog サーバを定義するサーバオブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成 (Create New Syslog Server)] をクリックして作成します。
- ステップ 4 [OK] をクリックします。

侵入ポリシーのモニタリング

侵入ポリシー統計情報は、[モニタリング (Monitoring)] ページの [攻撃者 (Attackers)] および [ターゲット (Targets)] ダッシュボードで確認できます。これらのダッシュボードで情報を表示するには、少なくとも 1 つのアクセス コントロール ルールに侵入ポリシーを適用する必要があります。「[トラフィックのモニタリングおよびシステムダッシュボード \(109 ページ\)](#)」を参照してください。

侵入イベントを表示するには、[モニタリング (Monitoring)] > [イベント (Events)] を選択して、[侵入 (Intrusion)] タブをクリックします。イベントの上にマウスを置き、[詳細の表示 (View Details)] へのリンクをクリックして、詳細情報を表示できます。詳細ページから、[IPS ルールの表示 (View IPS Rule)] をクリックして、関連する侵入ポリシーのルールへ移動し、そこでルールアクションを変更できます。ルールによりブロックされる適切な接続が多すぎる場合に、アクションをドロップから警告に変更することにより、誤検出の影響を軽減できます。逆に、ルールに対する攻撃トラフィックが多い場合は、アラートルールをドロップルールに変更できます。

侵入ポリシーの例

使用例の章には、次の侵入ポリシーの実装例が含まれています。

- [脅威をブロックする方法 \(65 ページ\)](#)



第 14 章

ネットワーク アドレス変換 (NAT)

ここでは、ネットワーク アドレス変換 (NAT) とその設定方法について説明します。

- [NAT を使用する理由 \(293 ページ\)](#)
- [NAT の基本 \(294 ページ\)](#)
- [NAT のガイドライン \(302 ページ\)](#)
- [NAT の設定 \(307 ページ\)](#)
- [IPv6 ネットワークの変換 \(341 ページ\)](#)
- [NAT のモニタリング \(356 ページ\)](#)
- [NAT の例 \(356 ページ\)](#)

NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

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

NAT の他の機能は、次のとおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。

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



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

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするとき内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけでなく、デバイスに接続されている任意のネットワークに変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピングアドレス/ホスト/ネットワーク/インターフェイス：マッピングアドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするとき内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。



(注) アドレスの変換中、デバイス インターフェイスに設定された IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、双方向に接続を開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。

- 送信元および宛先の NAT : 任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

NAT タイプ

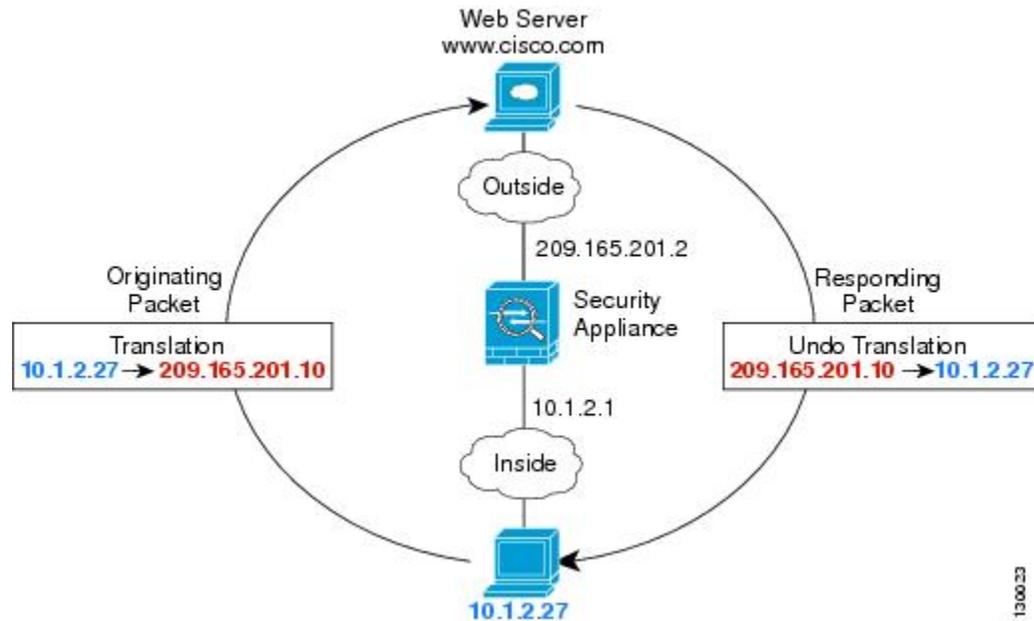
NAT は、次の方法を使用して実装できます。

- **ダイナミック NAT** : 実際の IP アドレスのグループが、(通常は、より小さい) マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。[ダイナミック NAT \(308 ページ\)](#) を参照してください。
- **ダイナミック ポートアドレス変換 (PAT)** : 実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。[ダイナミック PAT \(314 ページ\)](#) を参照してください。
- **スタティック NAT** : 実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。[スタティック NAT \(320 ページ\)](#) を参照してください。
- **アイデンティティ NAT** : 実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。[アイデンティティ NAT \(330 ページ\)](#) を参照してください。

ルーテッド モードの NAT

次の図は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。

図 4: NAT の例 : ルーテッド モード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピングアドレス 209.165.201.10 に変換されます。
2. サーバが応答すると、マッピングアドレス 209.165.201.10 に応答を送信し、Firepower Threat Defense デバイス がそのパケットを受信します。これは、Firepower Threat Defense デバイスがプロキシ ARP を実行してパケットを要求するためです。
3. Firepower Threat Defense デバイス はその後、パケットをホストに送信する前に、マッピングアドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

自動 NAT および 手動 NAT

自動 NAT および 手動 NAT という 2 種類の方法でアドレス変換を実装できます。

手動 NAT の追加機能を必要としない場合は、自動 NAT を使用することをお勧めします。自動 NAT の設定が容易で、Voice over IP (VoIP) などのアプリケーションでは信頼性が高い場合があります (VoIP では、ルールで使用されているオブジェクトのいずれにも属さない間接アドレスの変換が失敗することがあります)。

自動 NAT

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、自動 NAT ルールと見なされます。これは、ネットワーク オブジェクトに NAT を設定するための迅速かつ簡単な方法です。しかし、グループオブジェクトに対してこれらのルールを作成することはできません。

これらのルールはオブジェクト自体の一部として設定されますが、オブジェクトマネージャを通してオブジェクト定義内の NAT 設定を確認することはできません。

パケットがインターフェイスに入ると、送信元 IP アドレスと宛先 IP アドレスの両方が自動 NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元アドレスと宛先アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないため、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、手動 NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

手動 NAT

手動 NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。



(注) スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポートアドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

自動 NAT と手動 NAT の比較

自動 NAT と手動 NAT の主な違いは、次のとおりです。

- 実アドレスの定義方法。
 - 自動 NAT : NAT ルールがネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは、元の（実）アドレスとして機能します。
 - 手動 NAT : 実際のアドレスとマッピングアドレスの両方のネットワークオブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT 設定のパラメータとなります。実際のアドレスのネットワーク オブジェクトグループを使用できることは、手動 NAT がよりスケーラブルであることを意味します。
- 送信元および宛先 NAT の実装方法。

- 自動 NAT : 各ルールは、パケットの送信元または宛先のいずれかに適用できます。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような 2 つのルールを 1 つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
- 手動 NAT : 1 つのルールで送信元と宛先の両方を変換します。1 つのパケットは 1 つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは 1 つの手動 NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるため、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、送信元 A/宛先 A のペアには、送信元 A/宛先 B のペアとは異なる変換を適用できます。
- NAT ルールの順序。
 - 自動 NAT : NAT テーブルで自動的に順序付けされます。
 - 手動 NAT : NAT テーブルで手動で順序付けします (自動 NAT ルールの前または後)。

NAT ルールの順序

自動 NAT および手動 NAT ルールは、3 つのセクションに分かれた単一のテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 7: NAT ルール テーブル

テーブルのセクション	ルールタイプ	セクション内のルールの順序
セクション 1	手動 NAT	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、手動 NAT ルールはセクション 1 に追加されます。

テーブルのセクション	ルールタイプ	セクション内のルールの順序
セクション 2	自動 NAT	<p>セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。</p> <ol style="list-style-type: none"> 1. スタティック ルール 2. ダイナミック ルール <p>各ルールタイプでは、次の順序ガイドラインが使用されます。</p> <ol style="list-style-type: none"> 1. 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 2. 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 3. 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。
セクション 3	手動 NAT	<p>まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。</p>

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24 (スタティック)
- 192.168.1.0/24 (ダイナミック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.1/32 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)

この結果、使用される順序は次のとおりです。

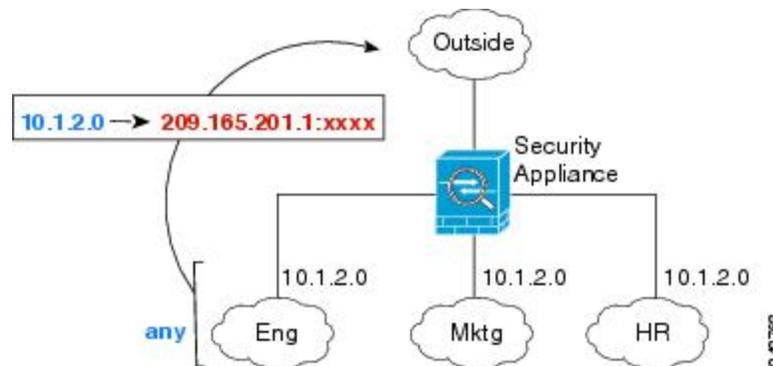
- 192.168.1.1/32 (スタティック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.0/24 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 192.168.1.0/24 (ダイナミック)

NAT インターフェイス

ブリッジグループメンバーインターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用される NAT ルールを設定したり、特定の実際のインターフェイスとマッピングインターフェイスを識別したりできます。実際のアドレスには任意のインターフェイスを指定できます。マッピングインターフェイスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベートアドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバルプールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピングアドレスには `outside` インターフェイスを指定します。

図 5: 任意のインターフェイスの指定



ただし、「任意」のインターフェイスの概念は、ブリッジグループメンバーインターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジグループメンバーインターフェイスが除外されます。そのため、ブリッジグループメンバーに NAT を適用するには、メンバーインターフェイスを指定する必要があります。この結果、1つのインターフェイスのみが異なる同様のルールが多数作成されることとなります。ブリッジ仮想インターフェイス (BVI) 自体に NAT を設定することはできず、メンバーインターフェイスにのみ NAT を設定できます。

NAT のルーティング設定

FTD デバイスは、変換された（マッピング）アドレスに送信されるパケットの宛先である必要があります。

パケットを送信する際の出カインターフェイスの決定に、指定した場合はその宛先インターフェイスが使用され、指定していない場合はルーティング テーブル ルックアップが使用されます。アイデンティティ NAT の場合は、宛先インターフェイスを指定している場合でも、ルート ルックアップの使用を選択できます。

必要となるルーティング設定のタイプは、マッピングアドレスのタイプによって異なります。以下の各トピックでは、その詳細について説明します。

マッピング インターフェイスと同じネットワーク上のアドレス

宛先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用する場合、Firepower Threat Defense デバイスはプロキシ ARP を使用してマッピングアドレスの ARP 要求に応答し、マッピングアドレス宛てのトラフィックを代行受信します。この方法では、Firepower Threat Defense デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるため、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

一意のネットワーク上のアドレス

宛先（マッピング）インターフェイスのネットワーク上で使用可能な数より多くのアドレスが必要な場合は、別のサブネット上でアドレスを指定できます。アップストリーム ルータには、Firepower Threat Defense デバイスを指しているマッピングアドレスのスタティック ルートが必要です。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP を無効にすることができます。必要に応じて標準スタティック NAT のプロキシ ARP を無効にできます。その場合は、アップストリーム ルータに適切なルートがあることを確認する必要があります。

アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。たとえば、「任意」の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP を有効のままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（「任意」のアドレスと一致する）NAT ルールと一致します。このとき、実際には Firepower Threat Defense デバイス 向けのパケットでない場合でも、Firepower Threat Defense デバイスはこのアドレスの ARP をプロキシします（この問題は、手動 NAT ルールが

設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます。実際のホストの ARP 応答の前に Firepower Threat Defense デバイスの ARP 応答を受信した場合、トラフィックは誤って Firepower Threat Defense デバイス に送信されます。

NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

インターフェイスのガイドライン

NAT は標準のルーテッド物理インターフェイスまたはルーテッドサブインターフェイスでサポートされます。

ただし、ブリッジグループメンバーインターフェイス（ブリッジ仮想インターフェイス、BVI の一部であるインターフェイス）での NAT の設定には次の制限があります。

- ブリッジグループのメンバーに NAT を設定するには、メンバーインターフェイスを指定します。NAT をブリッジグループインターフェイス（BVI）自体に設定することはできません。
- ブリッジグループメンバーインターフェイス間で NAT を行う場合、送信元インターフェイスと宛先インターフェイスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。
- インターフェイスに接続されている IP アドレスがないため、宛先インターフェイスがブリッジグループのメンバーインターフェイスである場合、インターフェイス PAT を設定することはできません。
- 送信元インターフェイスと宛先インターフェイスが同じブリッジグループのメンバーである場合、IPv4 ネットワークと IPv6 ネットワーク（NAT64/46）同士を変換することはできません。スタティック NAT/PAT 44/66、ダイナミック NAT44/66、およびダイナミック PAT44 のみが許可されている方法であり、ダイナミック PAT66 はサポートされません。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 標準のルーテッドモードのインターフェイスの場合は、IPv4 と IPv6 との間でも変換できます。
- 同じブリッジグループのメンバーであるインターフェイスでは、IPv4 と IPv6 の間の変換はできません。2つの IPv6 ネットワーク間または2つの IPv4 ネットワーク間でのみ変換できます。この制限は、ブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。

- 同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT (NAT66) は使用できません。この制限は、ブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブモード (EPSV) または拡張ポートモード (EPRT) を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

IPv6 NAT のベスト プラクティス

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます (ルーテッドモードのみ)。次のベスト プラクティスを推奨します。

- NAT66 (IPv6-to-IPv6) : スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。
- NAT46 (IPv4-to-IPv6) : スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。IPv6 サブネットに変換する場合 (/96 以下)、結果のマッピングアドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます (混合表記で表示)。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。
- NAT64 (IPv6-to-IPv4) : IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

インスペクション対象プロトコルに対する NAT サポート

セカンダリ接続を開くアプリケーション層プロトコルの一部、またはパケットに IP アドレスを埋め込んだアプリケーション層プロトコルの一部は、次のサービスを提供するためにインスペクションが実行されます。

- ピンホールの作成 : 一部のアプリケーションプロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、

これらのセカンダリポートのピンホールが開くため、ユーザはそれらを許可するアクセスコントロールルールを作成する必要はありません。

- NATの書き換え：プロトコルの一部としてのパケットデータ内のセカンダリ接続用のFTP埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクションエンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケットデータを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制：一部のインスペクションでは、インスペクション対象プロトコルにある程度の RFC への準拠が強制されます。

次の表に、NAT の書き換えと NAT の制限事項を適用するインスペクション対象プロトコルを示します。これらのプロトコルを含む NAT ルールの作成時は、これらの制限事項に留意してください。ここに記載されていないインスペクション対象プロトコルは NAT の書き換えを適用しません。これらのインスペクションには、GTP、HTTP、IMAP、POP、SMTP、SSH、および SSL が含まれます。



- (注) NAT の書き換えは、リストされているポートでのみサポートされます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 8: NAT のサポート対象アプリケーションインスペクション

アプリケーション	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし。	あり
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	なし
ESMTP	TCP/25	NAT64 なし。	なし
FTP	TCP/21	制限なし。	あり
H.323 H.225 (コールシグナリング) H.323 RAS	TCP/1720 UDP/1718 RAS の場合、 UDP/1718 ~ 1719	NAT64 なし。	あり

アプリケーション	インスペクション対象 プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
ICMP ICMP エラー	ICMP (デバイス インターフェイスに送信される ICMP トラフィックのインスペクションは実行されません)	制限なし。	なし
IP オプション	RSVP	NAT64 なし。	なし
NetBIOS Name Server over IP	UDP/137、138 (送信元ポート)	NAT64 なし。	なし
RSH	TCP/514	PAT なし。 NAT64 なし。	あり
RTSP	TCP/554 (HTTP クローキングは処理しません)	NAT64 なし。	あり
SIP	TCP/5060 UDP/5060	拡張 PAT なし NAT64 または NAT46 なし	あり
Skinny (SCCP)	TCP/2000	NAT64、NAT46、または NAT66 なし	あり
SQL*Net (バージョン 1、2)	TCP/1521	NAT64 なし。	あり
Sun RPC	TCP/111 UDP/111	NAT64 なし。	あり
TFTP	UDP/69	NAT64 なし。 ペイロード IP アドレスは変換されません。	あり
XDMCP	UDP/177	NAT64 なし。	あり

NAT のその他のガイドライン

- ブリッジグループのメンバーであるインターフェイスの場合は、メンバー インターフェイス用の NAT ルールを記述します。ブリッジ仮想インターフェイス (BVI) 自体に対する NAT ルールは記述できません。

- (自動 NAT のみ)。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- インターフェイスで VPN が定義されている場合、そのインターフェイスの着信 ESP トラフィックには NAT ルールは適用されません。システムは、確立済みの VPN トンネルに対してのみ ESP トラフィックを許可し、既存のトンネルに関連付けられていないトラフィックはドロップされます。この制約は、ESP および UDP のポート 500 と 4500 に適用されません。
- ダイナミック PAT を適用するデバイスの背後のデバイス (VPN UDP ポート 500 と 4500 は実際に使用されるポートではない) でサイト間 VPN を定義した場合、PAT デバイスの背後にあるデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンドはセキュリティアソシエーション (SA) を開始できません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションが使用されるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。



(注) ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピングアドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- 1 つのオブジェクトグループに IPv4 と IPv6 の両方のアドレスを含めることはできません。オブジェクトグループには、1 つのタイプのアドレスのみを含める必要があります。
- (手動 NAT のみ) NAT ルールで送信元アドレスとして **any** を使用する場合、「any」トラフィックの定義 (IPv4 と IPv6) はルールによって異なります。Firepower Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Firepower Threat Defense デバイスは、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマップされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングインターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、次のアドレスを含めることはできません。

- マッピングインターフェイスの IP アドレス。ルールに「any」インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッドモードのみ）の場合は、インターフェイスアドレスの代わりにインターフェイス名を指定します。
- フェールオーバー インターフェイスの IP アドレス。
- (ダイナミック NAT) VPN が有効な場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT ルールの送信元アドレスとリモートアクセス VPN アドレス プールの重複アドレスは使用できません。
- ルールで宛先インターフェイスを指定すると、ルーティングテーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。
- NAT はトラフィックを介してのみ適用されます。システムによって生成されたトラフィックは NAT の対象にはなりません。

NAT の設定

ネットワークアドレス変換は非常に複雑な場合があります。変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。次の手順では、基本的なアプローチを示します。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 必要なルールを決定します。

ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールを作成できます。概要については、「[NAT タイプ \(295 ページ\)](#)」を参照してください。

ステップ 3 手動 NAT または自動 NAT として実装するルールを決定します。

これらの 2 つの実装オプションの比較については、[自動 NAT および手動 NAT \(296 ページ\)](#)を参照してください。

ステップ 4 次の項で説明するルールを作成します。

- [ダイナミック NAT \(308 ページ\)](#)
- [ダイナミック PAT \(314 ページ\)](#)
- [スタティック NAT \(320 ページ\)](#)
- [アイデンティティ NAT \(330 ページ\)](#)

ステップ 5 NAT ポリシーとルールを管理します。

ポリシーとそのルールを管理するには、次のことを行います。

- ルールを編集するには、ルールの編集アイコン (✎) をクリックします。
- ルールを削除するには、ルールの [削除 (delete)] アイコン (🗑️) をクリックします。

ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

ダイナミック NAT について

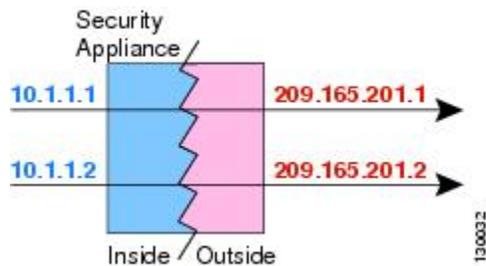
ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。



- (注) 変換が継続している間、アクセスルールで許可されていれば、リモートホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスルールのセキュリティに依存できます。

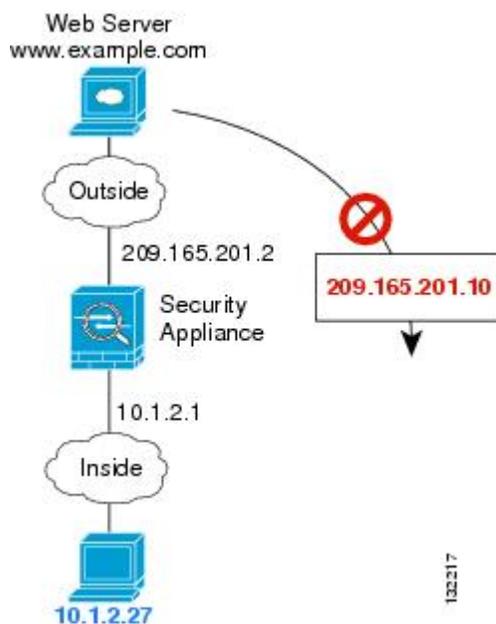
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 6: ダイナミック NAT



次の図に、マッピングアドレスへの接続開始を試みているリモートホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。

図 7: マッピングアドレスへの接続開始を試みているリモートホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

PAT では、1つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

- マッピングプールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディアアプリケーションなどのように、1つのポート上にデータストリームを持ち、別のポート上に制御パスを持ち、オープンスタンダードではないアプリケーションでも機能しません。

ダイナミック自動 NAT の設定

ダイナミック自動 NAT ルールを使用して、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス (Original Address)] : ネットワーク オブジェクト (グループではなく) にする必要があります。ホストまたはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)] : ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (✎) をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [自動 NAT (Auto NAT)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)]: (ブリッジグループメンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)]は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)]はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。
- [元のアドレス (Original Address)]: 変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス (Translated Address)]: マッピングアドレスを含むネットワーク オブジェクトまたはグループ。

ステップ 5 (オプション) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)]: DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(377 ページ\)](#) を参照してください。
- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT)] (宛先インターフェイス) : その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。

ステップ 6 [OK] をクリックします。

ダイナミック手動 NAT の設定

自動 NAT では要件を満たせない場合は、ダイナミック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス (Original Source Address)] : ネットワーク オブジェクトまたはグループを指定できます。ホストまたはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元アドレス (Translated Source Address)] : ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先アドレス (Original Destination Address)] および [変換済み宛先アドレス (Translated Destination Address)] のネットワーク オブジェクトを作成できます。

ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクトマネージャで、[元の宛先ポート (Original Destination Port)] と [変換済み宛先ポート (Translated Destination Port)] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (🔧) をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : ルールの追加先。ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上下に挿入できます。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

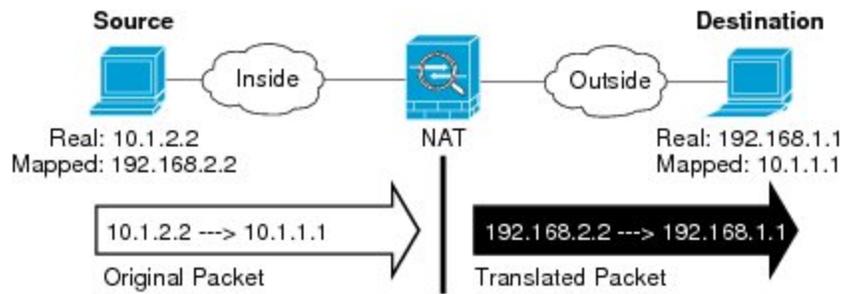
ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)]

はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

ステップ 5 元の packets アドレス (IPv4 または IPv6)、つまり、元の packets に表示される packets アドレスを特定します。

元の packets と変換済み packets の例については、次の図を参照してください。



- [Original Source][Address] : 変換するアドレスを含むネットワーク オブジェクト、またはネットワーク グループ。
- [Original Destination][Address] : (オプション)。宛先アドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[インターフェイス (Interface)] [送信元インターフェイス IP (Source Interface IP)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

ステップ 6 変換済み packets アドレス (つまり、IPv4 または IPv6) を特定します。 packets アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス (Translated Source Address)] : マッピングアドレスを含むネットワーク オブジェクトまたはグループ。
- [変換済み宛先アドレス (Translated Destination Address)] : (オプション) 変換済み packets で使用されていた宛先アドレスを含むネットワーク オブジェクトまたはグループ。 [元の宛先アドレス (Original Destination Address)] のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます (つまり、変換は不要です)。

ステップ 7 (オプション) サービス変換の宛先サービス ポートを特定します。 [元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート (Original Source Port)] フィールドと [変換済み送信元ポート (Translated Source Port)] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 (オプション) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(377 ページ\)](#) を参照してください。
- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT)] (宛先インターフェイス) : その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。

ステップ 9 [OK] をクリックします。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

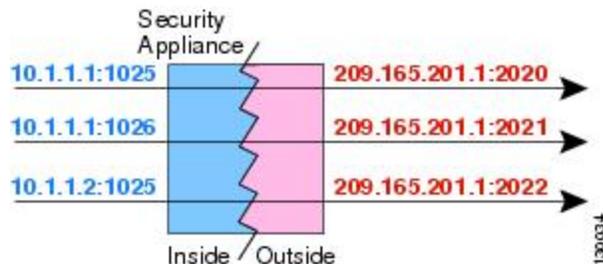
ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピングアドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピングポートは実際のポート番号と同じポート範囲 (0 ~ 511、512 ~ 1023、および 1024 ~ 65535) から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図は、ダイナミック PAT の一般的なシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピングアドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 8: ダイナミック PAT



変換が継続している間、アクセスルールで許可されていれば、宛先ネットワーク上のリモートホストは変換済みホストへの接続を開始できます。実際のポートアドレスおよびマッピングポートアドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も有効期限切れになります。



- (注) インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイス、特に「any」インターフェイスに同じプールを使用すると、プールがすぐに枯渇し、新しい変換に使用できるポートがなくなります。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1つのマッピングアドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、Firepower Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用できます。ただし、インターフェイス上の IPv6 アドレスに対しインターフェイス PAT を使用することはできません。

同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT (NAT66) は使用できません。この制限は、ブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。詳細については、[インスペクション対象プロトコルに対する NAT サポート \(303 ページ\)](#) を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。

ダイナミック自動 PAT の設定

ダイナミック自動 PAT ルールを使用して、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。単一のアドレス（宛先インターフェイスのアドレスや別のアドレス）に変換できます。

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス (Original Address)] : ネットワーク オブジェクト（グループではなく）にする必要があります。ホストまたはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)] : PAT アドレスを指定するオプションは次のとおりです。
 - [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
 - [単一の PAT アドレス (Single PAT address)] : 単一のホストを含むネットワーク オブジェクトを作成します。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (🔧) をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [自動 NAT (Auto NAT)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループ メンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、この

インターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループ メンバー インターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

- [元のアドレス (Original Address)]: 変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス (Translated Address)]: 次のいずれかになります。
 - (インターフェイス PAT) 宛先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス (Interface)] を選択します。特定の宛先インターフェイスを選択することもできます。ブリッジグループ メンバー インターフェイスは選択できません。IPv6 にインターフェイス PAT を使用することはできません。
 - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。

ステップ 5 (オプション) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT)] (宛先インターフェイス) : その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 6 [OK] をクリックします。

ダイナミック手動 PAT の設定

自動 PAT がお客様のニーズを満たしていない場合は、ダイナミック手動 PAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック PAT は、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。単一のアドレス (宛先インターフェイスのアドレスや別のアドレス) に変換できます。

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス (Original Source Address)]: ネットワーク オブジェクトまたはグループを指定できます。ホストまたはサブネットを含めることができます。すべての元の

送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。

- [変換済み送信元アドレス (Translated Source Address)] : PAT アドレスを指定するオプションは次のとおりです。
 - [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
 - [単一の PAT アドレス (Single PAT address)] : 単一のホストを含むネットワーク オブジェクトを作成します。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス (Original Destination Address)] と [変換済み宛先アドレス (Translated Destination Address)] のネットワーク オブジェクトも作成できます。

ダイナミック PAT の場合、宛先でポート変換を実行することもできます。オブジェクトマネージャで、[元の宛先ポート (Original Destination Port)] と [変換済み宛先ポート (Translated Destination Port)] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン  をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : ルールの追加先。ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上に挿入できます。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

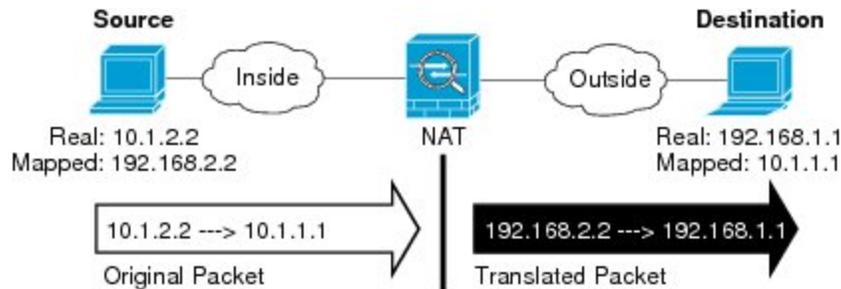
ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループ メンバー インターフェイスに必須)。この NAT ルール

が適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

ステップ 5 元の packets アドレス (IPv4 または IPv6)、つまり、元の packets に表示される packets アドレスを特定します。

元の packets と変換済み packets の例については、次の図を参照してください。



- [Original Source][Address] : 変換するアドレスを含むネットワーク オブジェクト、またはネットワーク グループ。
- [Original Destination][Address] : (オプション)。宛先アドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[インターフェイス (Interface)] [送信元インターフェイス IP (Source Interface IP)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

ステップ 6 変換済み packets アドレス (つまり、IPv4 または IPv6) を特定します。packets アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス (Translated Source Address)] : 次のいずれかになります。
 - (インターフェイス PAT) 宛先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス (Interface)] を選択します。特定の宛先インターフェイスを選択することもできます。ブリッジグループメンバー インターフェイスは選択できません。IPv6 にインターフェイス PAT を使用することはできません。
 - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。

- [変換済み宛先アドレス (Translated Destination Address)]: (オプション) 変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)]を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

ステップ 7 (オプション) サービス変換の宛先サービスポートを特定します。[元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート (Original Source Port)]フィールドと [変換済み送信元ポート (Translated Source Port)]フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 (オプション) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT)] (宛先インターフェイス) : その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 9 [OK] をクリックします。

スタティック NAT

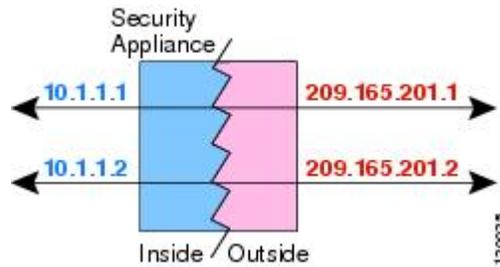
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じであるため、スタティック NAT では、双方向の接続 (ホストへの接続とホストから接続の両方) を開始できます (接続を許可するアクセス ルールが存在する場合)。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するため、双方向の開始はサポートされません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブであるため、実際のホストとリモート ホストの両方が接続を開始できます。

図 9:スタティック NAT



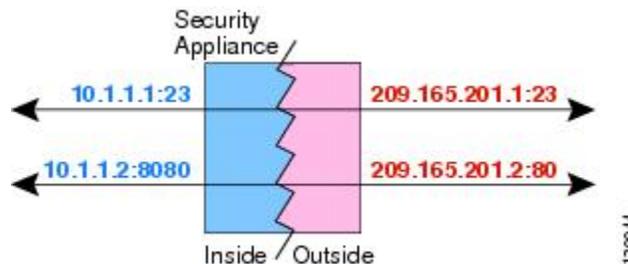
ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルおよびポートとマッピングされたプロトコルおよびポートを指定できます。

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IP アドレスは別の値にマッピングされています。この変換は常にアクティブであるため、変換されたホストとリモートホストの両方が接続を開始できます。

図 10:ポート変換を設定したスタティック NAT の一般的なシナリオ



ポート変換ルールを設定したスタティック NAT は、指定されたポートの宛先 IP アドレスのみにアクセスを制限します。NAT ルール対象外の別のポートで宛先 IP アドレスにアクセスしようとする、接続がブロックされます。さらに、手動 NAT の場合、NAT ルールの送信元 IP アドレスと一致しないトラフィックが宛先 IP アドレスと一致する場合、宛先ポートに関係なくドロップされます。したがって、宛先 IP アドレスに対して許可される他のすべてのトラフィックに追加ルールを追加する必要があります。たとえば、ポートを指定せずに IP アドレスにスタティック NAT ルールを設定し、ポート変換ルールの後ろにそれを配置できます。



(注) セカンダリチャネルのアプリケーションインスペクションが必要なアプリケーション (FTP、VoIP など) を使用する場合は、NAT が自動的にセカンダリポートを変換します。

次に、ポート変換を設定したスタティック NAT のその他の使用例の一部を示します。

アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する3つの個別のサーバ（FTP、HTTP、SMTPなど）がある場合は、それらのサービスにアクセスするための単一の IP アドレスを外部ユーザに提供できます。その後、アイデンティティ ポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバの正しい IP アドレスにマッピングできます。サーバは標準のポート（それぞれ 21、80、および 25）を使用しているため、ポートを変更する必要はありません。

標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

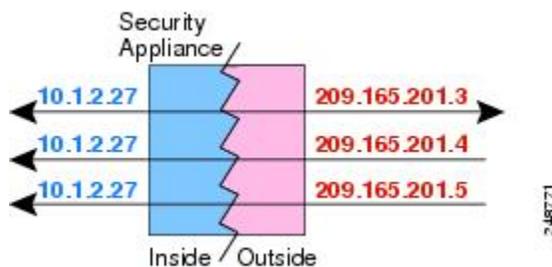
スタティック NAT は、実際のアドレスをインターフェイスアドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

1対多のスタティック NAT

通常、スタティック NAT は 1対1 のマッピングで設定します。しかし、場合によっては、1つの実際のアドレスを複数のマッピングアドレスに設定することがあります（1対多）。1対多のスタティック NAT を設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピングアドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピングアドレスへのトラフィックを開始でき、1つの実際のアドレスには変換されません。

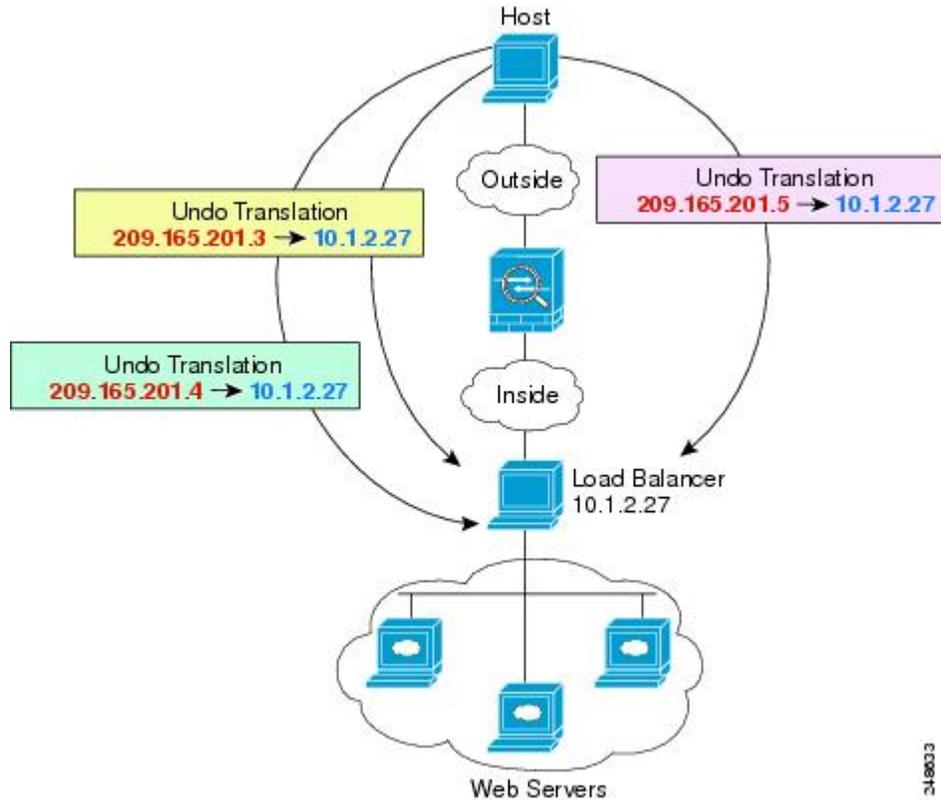
次の図に、一般的な 1対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 11: 1対多のスタティック NAT



たとえば、10.1.2.27 にロードバランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 12:1 対多のスタティック NAT の例



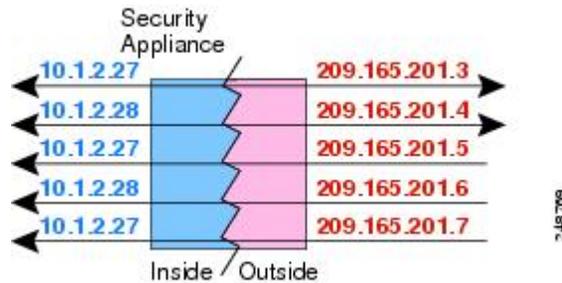
他のマッピングシナリオ（非推奨）

NATには、1対1、1対多だけではなく、少対多、多対少、多対1など任意の種類スタティックマッピングシナリオを使用できるという柔軟性があります。1対1マッピングまたは1対多マッピングだけを使用することをお勧めします。これらの他のマッピングオプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は1対多と同じです。ただし、設定が複雑になり、実際のマッピングがひと目で明らかにならない可能性があるため、必要とする実際の各アドレスに対して1対多の設定を作成することをお勧めします。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピングアドレスに順番にマッピングされます（Aは1、Bは2、Cは3）。すべての実際のアドレスがマッピングされたら、次のマッピングアドレスが最初の実際のアドレスにマッピングされ、すべてのマッピングアドレスがマッピングされるまで続行されます（Aは4、Bは5、Cは6）。この結果、実際の各アドレスに対して複数のマッピングアドレスが存在することになります。1対多の設定のように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピングアドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 13: 少対多のスタティック NAT



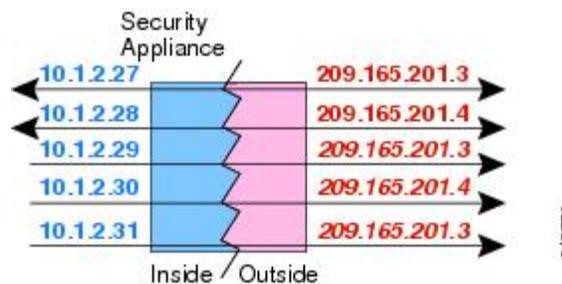
多対少または多対1コンフィギュレーションでは、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングプールの中でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の5つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。



- (注) 多対少または多対1の NAT は PAT ではありません。2つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 14: 多対少のスタティック NAT



このようにスタティックルールを使用するのではなく、双方向の開始を必要とするトラフィックに1対1のルールを作成し、残りのアドレスにダイナミックルールを作成することをお勧めします。

スタティック自動 NAT の設定

スタティック自動 NAT ルールを使用して、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

始める前に

[オブジェクト (Objects)] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス (Original Address)] : ネットワーク オブジェクト (グループではなく) する必要があります。ホストまたはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)] : 変換済みアドレスを指定するには、次のオプションがあります。
 - [宛先インターフェイス (destination interface)] : 宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
 - [アドレス (Address)] : ホスト、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (🔧) をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [自動 NAT (Auto NAT)] を選択します。
- [タイプ (Type)] : [スタティック (Static)] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)]

はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

- [元のアドレス (Original Address)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス (Translated Address)] : 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティック インターフェイス NAT) 宛先インターフェイスの IP アドレスを使用するには、[インターフェイス (Interface)] を選択します。また、特定の宛先インターフェイスを選択する必要があります。この宛先インターフェイスをブリッジグループメンバーインターフェイスにすることはできません。IPv6 にインターフェイス PAT は使用できません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- (オプション) [元のポート (Original Port)]、[Translated Port (変換済みポート)] : TCP または UDP ポートを変換する必要がある場合、元のポートと変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコル用でなければなりません。そのオブジェクトがまだ存在しない場合、[新規オブジェクトの作成 (Create New Object)] をクリックします。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

ステップ 5 (オプション) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(377 ページ\)](#) を参照してください。このオプションはポート変換を行う場合は使用できません。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に回答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の

場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

ステップ 6 [OK] をクリックします。

スタティック手動 NAT の設定

自動 NAT がニーズを満たさない場合、スタティック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック NAT は、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス (Original Source Address)] : ネットワーク オブジェクトまたはグループを指定できます。ホストまたはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元アドレス (Translated Source Address)] : 変換済みアドレスを指定するには、次のオプションがあります。
 - [宛先インターフェイス (destination interface)] : 宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
 - [アドレス (Address)] : ホスト、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先アドレス (Original Destination Address)] および [変換済み宛先アドレス (Translated Destination Address)] のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。オブジェクトマネージャでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (✎) をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

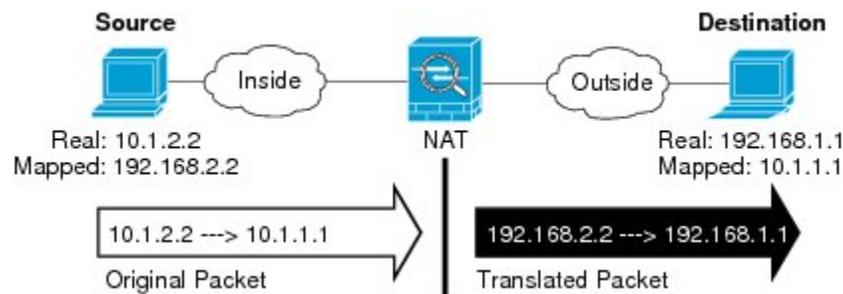
- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : ルールの追加先。ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上に挿入できます。
- [タイプ (Type)] : [スタティック (Static)] を選択します。この設定は送信元アドレスのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

ステップ 5 元のパケットアドレス (IPv4 または IPv6)、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。



- [Original Source][Address] : 変換するアドレスを含むネットワーク オブジェクト、またはネットワーク グループ。
- [Original Destination][Address] : (オプション)。宛先アドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[インターフェイス (Interface)][送信元インターフェイスIP (Source Interface IP)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

ステップ 6 変換済みパケットアドレス (つまり、IPv4 または IPv6) を特定します。パケットアドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス (Translated Source Address)] : 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティック インターフェイス NAT) 宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス (Interface)] を選択します。また、ブリッジグループメンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
- [変換済み宛先アドレス (Translated Destination Address)] : (オプション) 変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

ステップ7 (オプション) サービス変換の送信元サービスポートまたは宛先サービスポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービスオブジェクトのプロトコルとマッピングサービスオブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイデンティティ NAT では、実際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。

- [元の送信元ポート (Original Source Port)]、[変換済み送信元ポート (Translated Source Port)] : 送信元アドレスのポート変換を定義します。
- [元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)] : 宛先アドレスのポート変換を定義します。

ステップ8 (オプション) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(377 ページ\)](#) を参照してください。このオプションはポート変換を行う場合は使用できません。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

ステップ9 [OK] をクリックします。

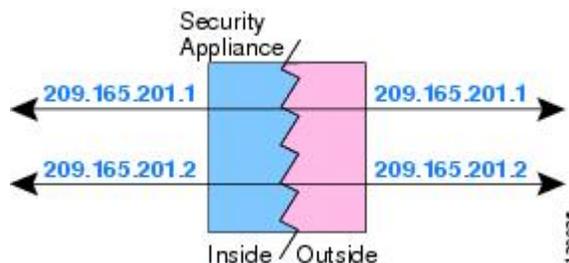
アイデンティティ NAT

IP アドレスを自身に変換する必要がある NAT コンフィギュレーションを設定できます。たとえば、NAT を各ネットワークに適するものの、1つのネットワークを NAT から除外するとい

う広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換できます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 15: アイデンティティ NAT



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ自動 NAT の設定

スタティック アイデンティティ自動 NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス (Original Address)]: ネットワーク オブジェクト (グループではなく) にする必要があります。ホストまたはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)]: 元の送信元オブジェクトとコンテンツがまったく同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (✎) をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [自動 NAT (Auto NAT)] を選択します。
- [タイプ (Type)] : [スタティック (Static)] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。
- [元のアドレス (Original Address)] : 変換するアドレスを含むネットワークオブジェクト。
- [変換済みアドレス (Translated Address)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

アイデンティティ NAT には、[元のポート (Original Port)] オプションと [変換済みポート (Translated Port)] オプションを設定しないでください。

ステップ 5 (オプション) [詳細オプション (Advanced Options)] リンクをクリックして、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルートルックアップの実行 (Perform Route Lookup for Destination Interface)] : 元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 6 [OK] をクリックします。

アイデンティティ手動 NAT の設定

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック アイデンティティ NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス (Original Source Address)] : ネットワーク オブジェクトまたはグループを指定できます。ホストまたはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元アドレス (Translated Source Address)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス (Original Destination Address)] と [変換済み宛先アドレス (Translated Destination Address)] のネットワーク オブジェクトも作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。オブジェクトマネージャでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。アイデンティティ NAT には同じオブジェクトを使用できます。

手順

ステップ 1 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集 (edit)] アイコン (✎) をクリックします。

(不要になったルールを削除するには、ルールの [ごみ箱 (trash can)] アイコンをクリックします)。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。

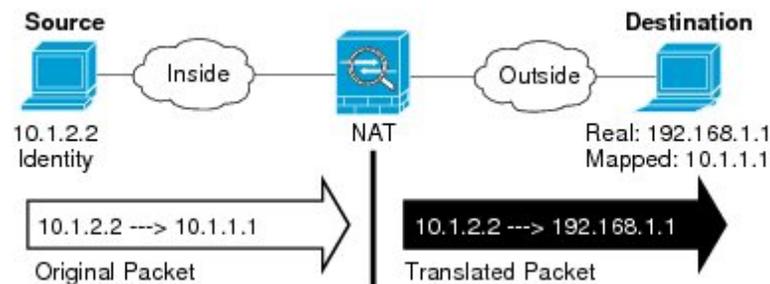
- [ルール作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : ルールの追加先。ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上下に挿入できます。
- [タイプ (Type)] : [スタティック (Static)] を選択します。この設定は送信元アドレスのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

ステップ 5 元の packets アドレス (IPv4 または IPv6)、つまり、元の packets に表示される packets アドレスを特定します。

元の packets と変換済みの packets の例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



- [元の送信元アドレス (Original Source Address)] : 変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address)] : (任意) 宛先アドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[インターフェイス (Interface)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケットアドレス（つまり、IPv4 または IPv6）を特定します。パケットアドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス (Translated Source Address)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。
- [変換済み宛先アドレス (Translated Destination Address)] : (オプション) 変換済みパケットで使用されていた宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先アドレス (Original Destination Address)] のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

ステップ 7 (オプション) サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート (Original Source Port)]、[変換済み送信元ポート (Translated Source Port)] : 送信元アドレスのポート変換を定義します。
- [元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)] : 宛先アドレスのポート変換を定義します。

ステップ 8 (オプション) [詳細オプション (Advanced Options)] リンクをクリックして、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に回答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルートルックアップの実行 (Perform Route Lookup for Destination Interface)] : 元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代

わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 9 [OK] をクリックします。

Firepower Threat Defense の NAT ルール プロパティ

ネットワークアドレス変換 (NAT) ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常は、NAT ルールを使用してプライベート アドレスをパブリックにルーティングできるアドレスに変換します。1つのアドレスから別のアドレスに変換するか、ポートアドレス変換 (PAT) を使用して多数のアドレスを1つに変換し、ポート番号を使用して送信元アドレスを識別できます。

NAT ルールの基本的なプロパティは、次のとおりです。プロパティは、指示されていることを除き、自動 NAT ルールと手動 NAT ルールで同じです。

[役職 (Title)]

ルールの名前を入力します。名前にスペースを含めることはできません。

[ルールの作成対象 (Create Rule For)]

変換ルールを [自動 NAT (Auto NAT)]にするか、[手動 NAT (Manual NAT)]にするか。自動 NAT は手動 NAT よりシンプルですが、手動 NAT を使用すると、宛先アドレスに基づいて送信元アドレスの個別の変換を作成できます。

[ステータス (Status)]

ルールをアクティブにするか無効にするか。

[配置 (Placement)] (手動 NAT のみ)

ルールの追加先。ルールはカテゴリ内 (自動 NAT のルールの前後) 、または選択するルールの上に挿入できます。

[タイプ (Type)]

変換ルールを [ダイナミック (Dynamic)]にするか、[スタティック (Static)]にするかを指定します。ダイナミック変換では、アドレスプールからマッピングアドレスが自動的に選択されるか、または、PAT の実装時にはアドレス/ポートの組み合わせが自動的に選択されます。マッピングアドレス/ポートを明確に定義する必要がある場合は、スタティック変換を使用します。

次に、残りの NAT ルール プロパティを説明します。

自動 NAT のパケット変換プロパティ

[パケット変換 (Packet Translation)] オプションを使用して、送信元アドレスと変換済みマッピングアドレスを定義します。次のプロパティは、自動 NAT にのみ適用されます。

[送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)]

(ブリッジグループ メンバー インターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)]は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)]はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループ メンバー インターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

[元のアドレス (Original Address)] (常に必須)

変換している送信元アドレスを含むネットワーク オブジェクト。グループではなくネットワーク オブジェクトにする必要があり、ホスト、またはサブネットを含めることができます。

[変換済みアドレス (Translated Address)] (通常は必須)

変換先のマッピングアドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミック NAT (Dynamic NAT)]: マッピングアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにできますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。
- [ダイナミック PAT (Dynamic PAT)]: 次のいずれかを実行します。
 - (インターフェイス PAT)。宛先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス (Interface)]を選択します。特定の宛先インターフェイスを選択することもできます。ブリッジグループ メンバー インターフェイスは選択できません。IPv6にインターフェイス PATを使用することはできません。
 - 宛先インターフェイスアドレス以外の単一アドレスを使用するには、この目的のために作成したホスト ネットワーク オブジェクトを選択します。
- [スタティック NAT (Static NAT)]: 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホストまたはサブネットを含めることができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティック インターフェイス NAT) 宛先インターフェイスの IP アドレスを使用するには、[インターフェイス (Interface)]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。この宛先インターフェイスをブリッジグループ メンバー インターフェイスにすることはできません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6にインターフェイス PATを使用することはできません。

- [アイデンティティ NAT (Identity NAT)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

[元のポート (Original Port)]、[変換済みポート (Translated Port)] (スタティック NAT のみ)。

TCP または UDP ポートを変換する必要がある場合、元のポートおよび変換済みポートを定義するポートオブジェクトを選択します。オブジェクトは同じプロトコル向けにする必要があります。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

手動 NAT のパケット変換プロパティ

[パケット変換 (Packet Translation)] オプションを使用して、送信元アドレスと変換済みマッピングアドレスを定義します。次のプロパティは、手動 NAT にのみ適用されます。指示されている場合を除き、すべてオプションです。

[送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)]

(ブリッジグループメンバーインターフェイスに必須)。この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

[元の送信元アドレス (Original Source Address)] (常に必須)

変換しているアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることが可能で、ホスト、またはサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、ルールに [すべて (Any)] を指定します。

[変換済み送信元アドレス (Translated Source Address)] (通常は必須)

変換先のマッピングアドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミック NAT (Dynamic NAT)] : マッピングアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにできますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。
- [ダイナミック PAT (Dynamic PAT)] : 次のいずれかを実行します。
 - (インターフェイス PAT)。宛先インターフェイスの IP アドレスを使用するには、[インターフェイス (Interface)] を選択します。また、特定の宛先インターフェイスを選択する必要もあります。この宛先インターフェイスをブリッジグループメンバーインターフェイスにすることはできません。IPv6 にインターフェイス PAT を使用することはできません。

- 宛先インターフェイスアドレス以外の単一アドレスを使用するには、この目的のために作成したホスト ネットワーク オブジェクトを選択します。
- [スタティック NAT (Static NAT)]: 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホストまたはサブネットを含めることができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティックインターフェイス NAT) 宛先インターフェイスの IP アドレスを使用するには、[インターフェイス (Interface)]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。この宛先インターフェイスをブリッジグループ メンバー インターフェイスにすることはできません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT を使用することはできません。
- [アイデンティティ NAT (Identity NAT)]: 元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

[元の宛先アドレス (Original Destination Address)]

宛先アドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[インターフェイス (Interface)]を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)]は選択不可) をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

[変換済み宛先アドレス (Translated Destination Address)]

変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)]を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

[元の送信元ポート (Original Source Port)]、[変換済み送信ポート (Translated Source Port)]、[元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)]

元のパケットおよび変換済みパケットの送信元および宛先サービスを定義するポート オブジェクト。ポートを変換したり、ポートを変換せずに同じオブジェクトを選択してサービスに対するルールの感度を向上できます。サービスを設定するときは、次のルールに注意してください。

- (ダイナミック NAT または PAT) [元の送信元ポート (Original Source Port)] および [変換済み送信元ポート (Translated Source Port)] では変換できません。宛先ポートでのみ変換できます。
- NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じオブジェクトを使用できます。

詳細 NAT プロパティ

NAT を設定するとき、[詳細 (Advanced)] オプションで特別なサービスを提供するプロパティを設定できます。これらのプロパティはすべてオプションであり、該当サービスが必要な場合だけに設定します。

このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(377 ページ\)](#) を参照してください。このオプションは、スタティック NAT ルールでポート変換を行っているときは利用できません。

[インターフェイス PAT (宛先インターフェイス) へのフォールスルー (Fallthrough to Interface PAT (Destination Interface))] (ダイナミック NAT のみ)

その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。変換されたアドレスとしてすでにインターフェイス PAT を設定している場合、このオプションを選択できません。このオプションは、IPv6 ネットワークでは使用できません。

宛先インターフェイスでプロキシ ARP なし (スタティック NAT のみ)

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

宛先インターフェイスでルートルックアップを実行します（スタティック ID NAT のみ。ルーテッドモードのみ）

元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

IPv6 ネットワークの変換

IPv6 専用ネットワークと IPv4 専用ネットワークの間でトラフィックを通過させる必要がある場合、NAT を使用してアドレス タイプを変換する必要があります。2 つの IPv6 ネットワークの場合でも、外部ネットワークから内部アドレスを隠す必要がある場合があります。

IPv6 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46 : IPv6 パケットを IPv4（およびその反対）に変換します。2 つのポリシーを定義する必要があります。1 つは IPv6 から IPv4 への変換用、もう 1 つは IPv4 から IPv6 への変換用です。これは 1 つの手動 NAT ルールで実現できますが、DNS サーバが外部ネットワークにある場合は、おそらく DNS 応答をリライトする必要があります。宛先を指定するときに手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの自動 NAT ルールを作成することがより適切なソリューションです。



（注） NAT46 がサポートするのは、スタティック マッピングのみです。

- NAT66 : IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。



（注） NAT64 および NAT 46 は、標準的なルーテッドインターフェイスでのみ使用できます。NAT66 は、ルーテッドインターフェイスとブリッジグループメンバーインターフェイスの両方で使用できます。

NAT64/46 : IPv6 アドレスの IPv4 への変換

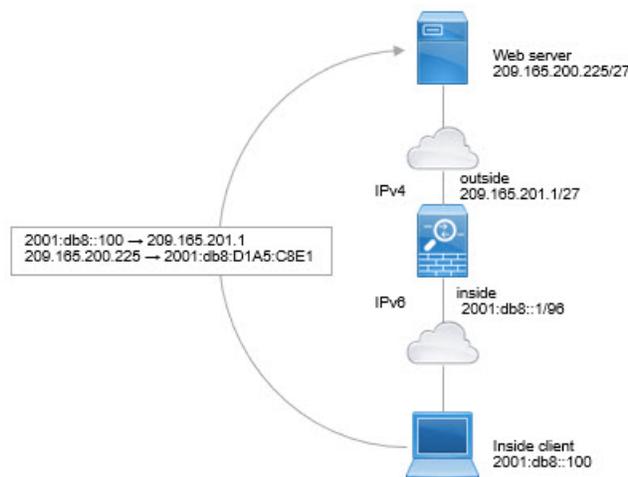
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。2 つのアドレスプール（IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレスプールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレスプール）を定義する必要があります。

- NAT64 ルール用の IPv4 アドレス プールは通常は小さく、一般的に IPv6 クライアントアドレスを使用して 1 対 1 のマッピングを設定するにはアドレスが足りない場合があります。ダイナミック PAT は、ダイナミック NAT やスタティック NAT と比べると、多数の IPv6 クライアントアドレスがある場合でも、比較的簡単に対応できます。
- NAT 46 ルールの IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数と等しいか、それより多くなります。これによって、各 IPv4 アドレスを別の IPv6 アドレスにマッピングできます。NAT 46 はスタティック マッピングのみをサポートするため、ダイナミック PAT を使用することはできません。

送信元 IPv6 ネットワークと宛先 IPv4 ネットワークの 2 つのポリシーを定義する必要があります。これは 1 つの手動 NAT ルールで実現できますが、DNS サーバが外部ネットワークにある場合は、おそらく DNS 応答をリライトする必要があります。宛先を指定するときに手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの自動 NAT ルールを作成することがより適切なソリューションです。

NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット

次に示すのは単純な例で、IPv6 のみの内部ネットワークがあり、インターネットに送信するトラフィックについて IPv4 に変換する必要があります。この例では DNS 変換の必要がないことを前提としています。そのため、単一の手動 NAT ルールで NAT64 と NAT46 の両方の変換を実行できます。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。

手順

ステップ 1 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

- a) [オブジェクト (Objects)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[+] をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前 (inside_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (2001:db8::/96) を入力します。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:DB8::/96

- d) [追加 (Add)] [OK] をクリックします。

ステップ 2 IPv6 ネットワークを IPv4 に変換して再び戻すための手動 NAT ルールを作成します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。
 - [タイトル (Title)] = PAT64Rule (またはユーザが選択する別の名前)
 - [ルールの作成対象 (Create Rule For)] = [手動 NAT (Manual NAT)]。
 - [配置 (Placement)] : [自動 NAT ルールの前 (Before Auto NAT Rules)]。
 - [タイプ (Type)] = [ダイナミック (Dynamic)]
 - [送信元インターフェイス (Source Interface)] = [内部 (inside)]
 - [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
 - [元の packets 発信元アドレス (Original Packet Source Address)] : inside_v6 ネットワーク オブジェクト。
 - [変換済み packets 発信元アドレス (Translated Packet Source Address)] : [インターフェイス (Interface)]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。

NAT64/46 の例 : 外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク

- [元の packets宛先アドレス (Original Packet Destination Address)] : inside_v6 ネットワーク オブジェクト。
- [変換済み packets宛先アドレス (Translated Packet Destination Address)] : any-ipv4 ネットワーク オブジェクト。

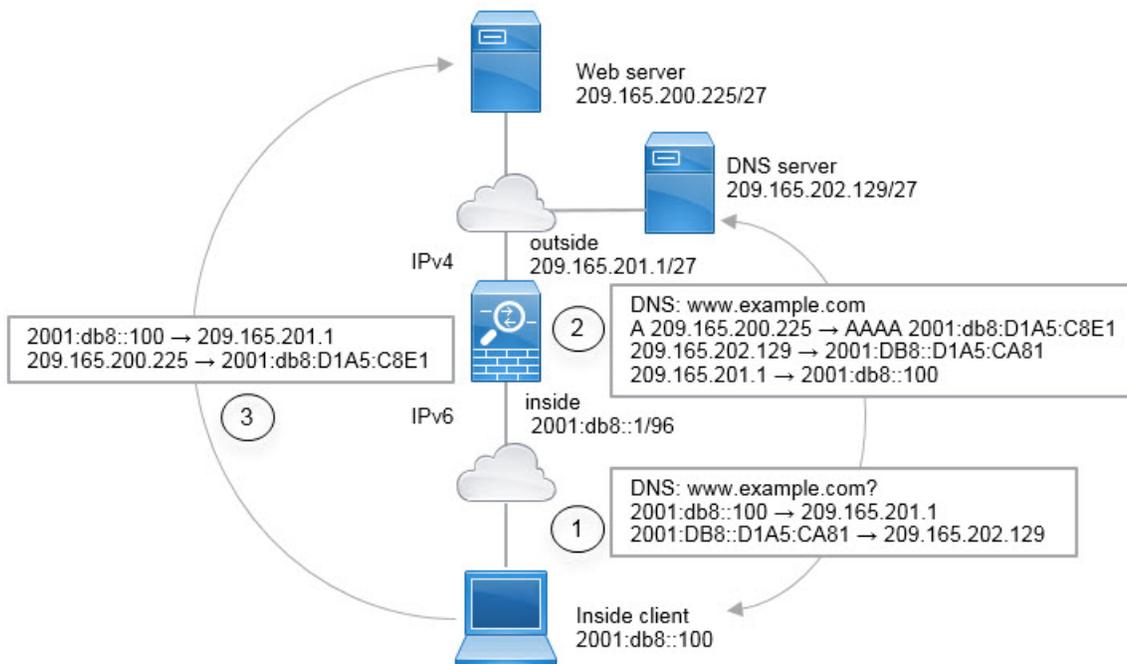
Title	Create Rule for	Status	
PAT64Rule	Manual NAT	<input checked="" type="checkbox"/>	
Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.			
Placement	Type		
Before Auto NAT Rules	Dynamic		
<div style="display: flex; justify-content: space-between;"> Packet Translation Advanced Options </div>			
ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface		Destination Interface	
inside		outside	
Source Address	Source Port	Source Address	Source Port
inside_v6	Any	Interface	Any
Destination Address	Destination Port	Destination Address	Destination Port
inside_v6	Any	any-ipv4	Any

d) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。逆に、内部インターフェイスに入る外部ネットワークの IPv4 アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。

NAT64/46 の例 : 外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク

次の図は、内部の IPv6 専用ネットワークが存在し、内部ユーザが必要とするいくつかの IPv4 専用サービスが外部のインターネット上に存在する一般的な例です。



この例では、外部インターフェイスの IP アドレスを持つ動的インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。NAT46 ルールで DNS の書き換えを有効にすると、外部 DNS サーバからの応答を A (IPv4) レコードから AAAA (IPv6) レコードに変換でき、アドレスが IPv4 から IPv6 に変換されます。

次は、内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとしている場合の Web 要求の一般的なシーケンスです。

1. クライアントのコンピュータが 2001:DB8::D1A5:CA81 にある DNS サーバに DNS 要求を送信します。NAT ルールにより、DNS 要求の送信元と宛先が次のように変換されます。
 - 2001:DB8::100 を 209.165.201.1 上の一意のポートに変換 (NAT64 インターフェイス PAT ルール)。
 - 2001:DB8::D1A5:CA81 を 209.165.202.129 に変換 (NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 に相当します)。
2. DNS サーバが、www.example.com が 209.165.200.225 であることを示す A レコードに応答します。DNS の書き換えが有効になっている NAT46 ルールにより、A レコードが IPv6 の同等の AAAA レコードに変換されて、AAAA レコードの 209.165.200.225 が 2001:db8:D1A5:C8E1 に変換されます。なお、DNS 応答の送信元アドレスと宛先アドレスは変換されません。
 - 209.165.202.129 を 2001:DB8::D1A5:CA81 に変換
 - 209.165.201.1 を 2001:db8::100 に変換

3. これで、IPv6 クライアントが Web サーバの IP アドレスを取得し、www.example.com (2001:db8:D1A5:C8E1) に HTTP 要求を送信できます。(D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します)。HTTP 要求の送信元と宛先が変換されます。
 - 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換 (NAT64 インターフェイス PAT ルール)。
 - 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換 (NAT46 ルール)。

次の手順では、この例の設定方法について説明します。

手順

ステップ 1 内部 IPv6 ネットワークと外部 IPv4 ネットワークを定義するネットワーク オブジェクトを作成します。

- a) [オブジェクト (Objects)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[+] をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

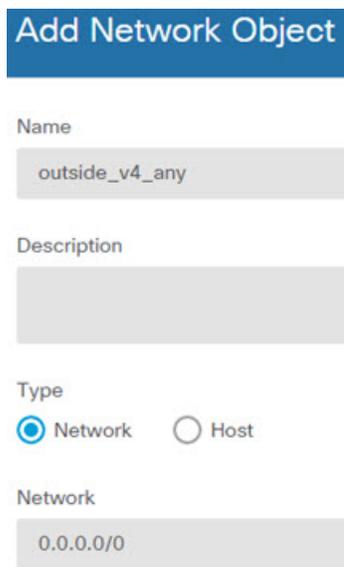
ネットワーク オブジェクトに名前 (inside_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (2001:db8::/96) を入力します。

The screenshot shows a configuration form titled "Add Network Object". It includes the following fields and options:

- Name:** A text input field containing "inside_v6".
- Description:** A larger text input field that is currently empty.
- Type:** Two radio button options: "Network" (which is selected) and "Host".
- Network:** A text input field containing "2001:DB8::/96".

- d) [追加 (Add)], [OK] をクリックします。
- e) [+] をクリックして、外部 IPv4 ネットワークを定義します。

ネットワーク オブジェクトに名前 (outside_v4_any など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (0.0.0.0/0) を入力します。



Add Network Object

Name
outside_v4_any

Description

Type
 Network Host

Network
0.0.0.0/0

ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。
 - [タイトル (Title)] = PAT64Rule (またはユーザが選択する別の名前)
 - [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
 - [タイプ (Type)] = [ダイナミック (Dynamic)]
 - [送信元インターフェイス (Source Interface)] = [内部 (inside)]
 - [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
 - [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
 - [変換済みアドレス (Translated Address)] = [インターフェイス (Interface)]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。

Add NAT Rule

Title: PAT64Rule Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Dynamic

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	inside_v6	Translated Address	Interface
Original Port	Any	Translated Port	Any

d) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。

ステップ 3 外部 IPv4 ネットワークのスタティック NAT46 ルールを設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル (Title)] = NAT46Rule (またはユーザが選択する別の名前)。
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- 送信元インターフェイス (Source Interface) = [外部 (outside)]
- 宛先インターフェイス (Destination Interface) = [内部 (inside)]
- [元のアドレス (Original Address)] = outside_v4_any ネットワーク オブジェクト (outside_v4_any network object)。
- [変換済みアドレス (Translated Address)] = inside_v6 ネットワーク オブジェクト (inside_v6 network object)

- [詳細オプション (Advanced Options)] タブで、[このルールと一致するDNS応答を変換 (Translate DNS replies that match this rule)] を選択します。

- c) [OK] をクリックします。

このルールを使用すると、内部インターフェイスに届く外部ネットワークのすべてのIPv4アドレスが、組み込みのIPv4アドレス方式を使用して2001:db8::/96ネットワークのアドレスに変換されます。また、DNS応答がA (IPv4) レコードからAAAA (IPv6) レコードに変換され、アドレスがIPv4からIPv6に変換されます。

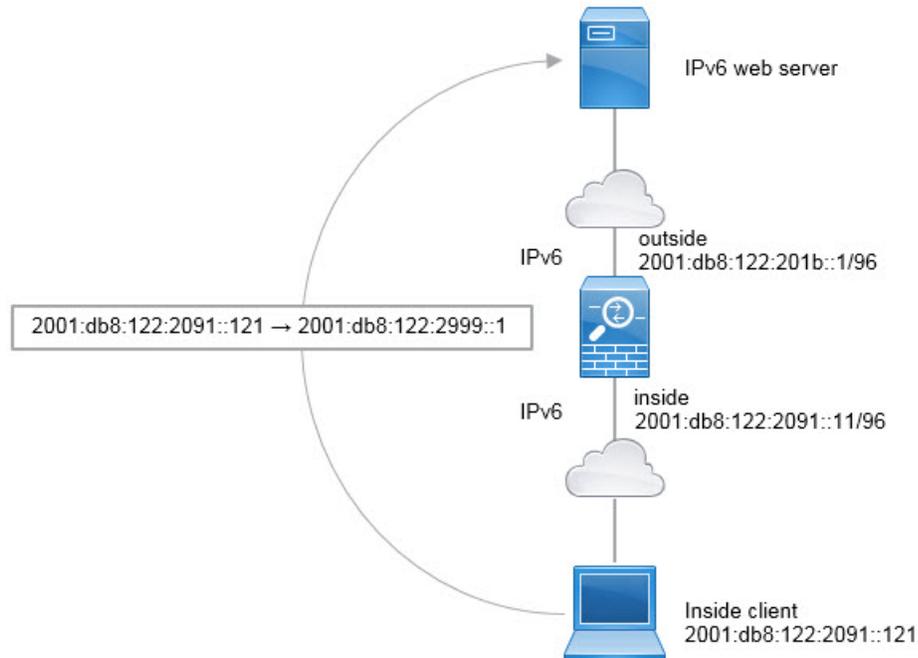
NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換

IPv6 ネットワークから別のIPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別のIPv6アドレスに変換できます。スタティック NATの使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

異なるアドレスタイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。これらのルールは、自動 NAT を使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、手動 NAT のみを使用してスタティック NAT ルールを単方向にできます。

NAT66 の例 : ネットワーク間のスタティック変換

自動 NAT を使用して、IPv6 アドレスプール間のスタティック変換を設定できます。次の例では、2001:db8:122:2091::/96 ネットワークの内部アドレスを 2001:db8:122:2999::/96 ネットワークの外部アドレスに変換する方法について説明します。



(注) この例は、内部インターフェイスがブリッジグループインターフェイス (BVI) ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

ステップ 1 内部 IPv6 ネットワークと外部 IPv6 NAT ネットワークを定義するネットワーク オブジェクトを作成します。

- a) [オブジェクト (Objects)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[+] をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前 (inside_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (2001:db8:122:2091::/96) を入力します。

Add Network Object

Name

inside_v6

Description

Type



Network



Host

Network

2001:db8:122:2091::/96

d) [追加 (Add)], [OK] をクリックします。

e) [+] をクリックして、外部 IPv6 PAT ネットワークを定義します。

ネットワークオブジェクトに名前 (outside_nat_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワークアドレス (2001:db8:122:2999::/96) を入力します。

Add Network Object

Name

outside_nat_v6

Description

Type



Network



Host

Network

2001:db8:122:2999::/96

ステップ 2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

a) [ポリシー (Policies)] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル (Title)] = NAT66Rule (またはユーザが選択する別の名前)

- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
- [変換済みアドレス (Translated Address)] = outside_nat_v6 ネットワーク オブジェクト (outside_nat_v6 network object) 。

Add NAT Rule ?

Title	Create Rule for	Status
NAT66Rule	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static ▼

Packet Translation

Advanced Options

ORIGINAL PACKET				TRANSLATED PACKET			
Source Interface				Destination Interface			
inside ▼				outside			
Original Address		Original Port		Translated Address		Translated Port	
inside_v6 ▼		Any ▼		outside_nat_v6 ▼		Any	

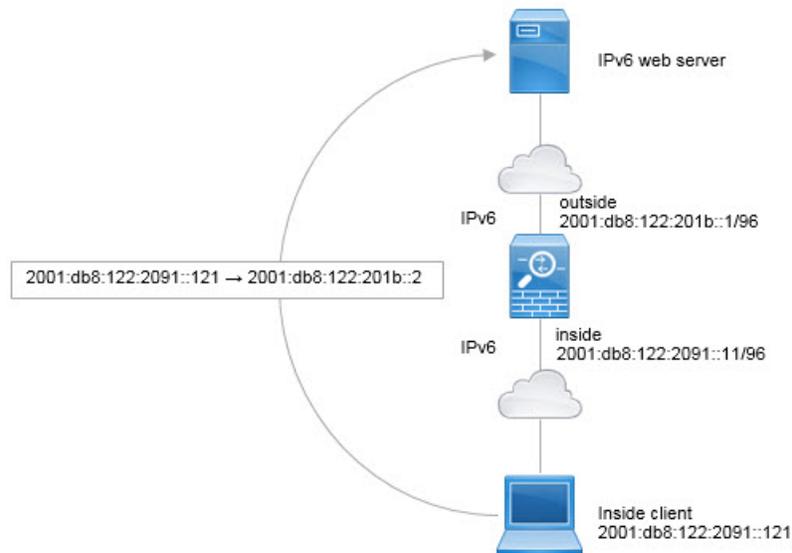
d) [OK] をクリックします。

このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスにスタティック NAT66 変換されます。

NAT66 の例 : シンプルな IPv6 インターフェイス PAT

NAT66 を実装するための簡単なアプローチは、外部インターフェイスの IPv6 アドレス上の異なるポートに内部アドレスを動的に割り当てる方法です。

ただし、Firepower Device Manager を使用して、インターフェイスの IPv6 アドレスを使用するインターフェイス PAT は設定できません。代わりに、同じネットワーク上の 1 つの空きアドレスをダイナミック PAT プールとして使用します。



(注) この例は、内部インターフェイスがブリッジグループインターフェイス (BVI) ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバーインターフェイスのルールを複製する必要があります。

手順

ステップ 1 内部 IPv6 ネットワークと IPv6 PAT アドレスを定義するネットワーク オブジェクトを作成します。

- a) [オブジェクト (Objects)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[+] をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前 (inside_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (2001:db8:122:2091::/96) を入力します。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:db8:122:2091::/96

d) [追加 (Add)], [OK] をクリックします。

e) [+] をクリックして、外部 IPv6 PAT アドレスを定義します。

ネットワーク オブジェクトに名前 (inside_v6 など) を付け、[ホスト (Host)] を選択して、ホストアドレス (2001:db8:122:201b::2) を入力します。

Add Network Object

Name
ipv6_pat

Description

Type
 Network Host

Host
2001:db8:122:201b::2

ステップ 2 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

a) [ポリシー (Policies)] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル (Title)] = PAT66Rule (またはユーザが選択する別の名前) 。

- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
- [変換済みアドレス (Translated Address)] = ipv6_pat ネットワーク オブジェクト (ipv6_pat network object).

Add NAT Rule

Title: PAT66Rule Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Dynamic

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	inside_v6	Translated Address	ipv6_pat
Original Port	Any	Translated Port	Any

d) [OK] をクリックします。

このルールを使用すると、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスに届くすべてのトラフィックが 2001:db8:122:201b::2 のポートにダイナミック PAT66 変換されます。

NAT のモニタリング

NAT 接続をモニタしてトラブルシューティングを実行するには、CLI コンソールを開くかデバイス CLI にログインして次のコマンドを使用します。

- **show nat** は NAT ルールとルールごとのヒット数を表示します。NAT の他の側面を表示するための追加キーワードがあります。
- **show xlate** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換を消去することで、クライアントの次の接続時に、システムは新しいルールに基づいてクライアントの新しい変換を作成します。（このコマンドは CLI コンソールでは使用できません。）

NAT の例

以下の各トピックでは、Threat Defense デバイスでの NAT の設定例を紹介します。

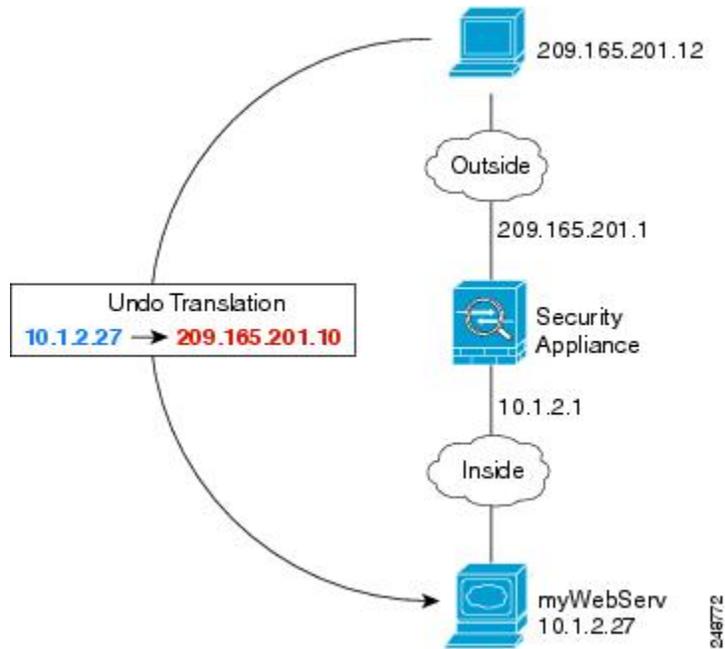
内部 Web サーバへのアクセスの提供（スタティック自動 NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるため、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です。



- (注) この例は、内部インターフェイスがブリッジグループインターフェイス (BVI) ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI の場合、Web サーバが接続されている特定のブリッジ グループ メンバー インターフェイス (inside1_3 など) を選択します。

図 16: 内部 Web サーバのスタティック NAT



手順

ステップ 1 サーバのプライベートホストアドレスとパブリックホストアドレスを定義するネットワークオブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択して、[+] をクリックします。
- Web サーバのプライベートアドレスを定義します。

ネットワークオブジェクトに名前 (WebServerPrivate など) を付け、[ホスト (Host)] を選択して、実際のホスト IP アドレス (10.1.2.27) を入力します。

New Network Object

Name
WebServerPrivate

Description

Type
 Network Host

Host
10.1.2.27

- d) [追加 (Add)], [OK] をクリックします。
- e) [+] をクリックして、パブリック アドレスを定義します。

ネットワーク オブジェクトに名前 (WebServerPublic など) を付け、[ホスト (Host)] を選択して、ホスト アドレス (209.165.201.10) を入力します。

New Network Object

Name
WebServerPublic

Description

Type
 Network Host

Host
209.165.201.10

- f) [追加 (Add)], [OK] をクリックします。

ステップ 2 オブジェクトのスタティック NAT を設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。

- [タイトル (Title)] = WebServer (またはユーザが選択する別の名前)
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] = WebServerPrivate ネットワーク オブジェクト (WebServerPrivate network object)
- [変換済みアドレス (Translated Address)] = WebServerPublic ネットワーク オブジェクト (WebServerPublic network object)

Add NAT Rule

Title: WebServer Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	outside
Original Address	WebServerPrivat	Translated Address	WebServerPublic
Original Port	Any	Translated Port	Any

d) [OK] をクリックします。

FTP、HTTP、およびSMTPの単一アドレス（ポート変換を設定したスタティック自動NAT）

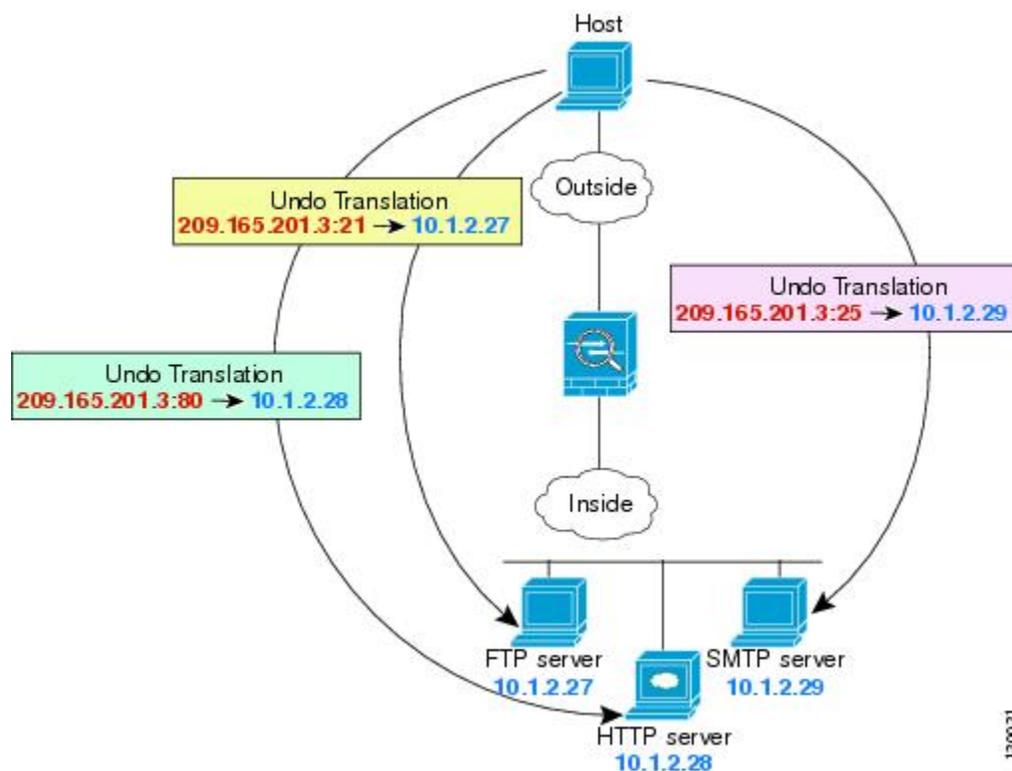
次のポート変換を設定したスタティック NAT の例では、リモートユーザがFTP、HTTP、およびSMTPにアクセスするための単一のアドレスを提供します。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定した

スタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用できます。



- (注) この例では、内部インターフェイスはスイッチに接続された標準ルーテッドインターフェイスで、スイッチにサーバが接続されていると仮定します。内部インターフェイスがブリッジグループインターフェイス (BVI) であり、サーバが別のブリッジグループメンバーインターフェイスに接続されている場合、各サーバが対応するルールで接続する特定のメンバーインターフェイスを選択します。たとえば、ルールは「inside」ではなく、送信元インターフェイスの「inside1_2」、「inside1_3」、および「inside1_4」の可能性がります。

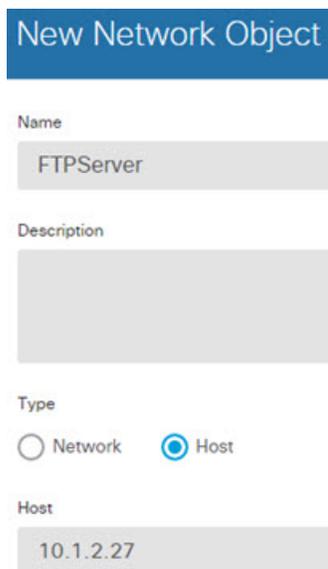
図 17: ポート変換を設定したスタティック NAT



手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- ネットワーク オブジェクトに名前を付け (たとえば FTPserver)、[ホスト (Host)] を選択し、FTP サーバの実際の IP アドレス (10.1.2.27) を入力します。



New Network Object

Name
FTPServer

Description

Type
 Network Host

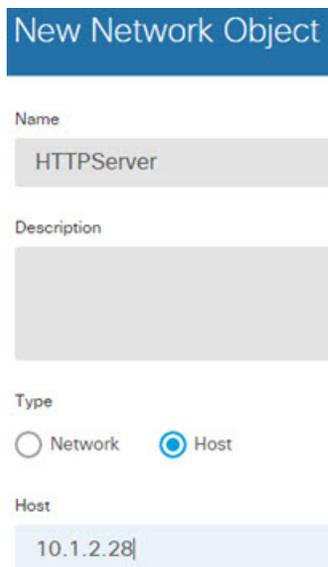
Host
10.1.2.27

d) [追加 (Add)] [OK] をクリックします。

ステップ 2 HTTP サーバのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば HTTPserver）、[ホスト (Host)] を選択し、ホストアドレス（10.1.2.28）を入力します。



New Network Object

Name
HTTPServer

Description

Type
 Network Host

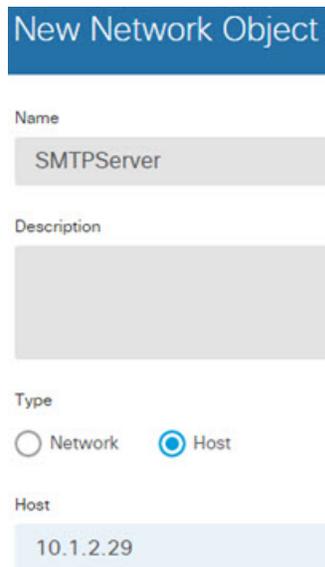
Host
10.1.2.28

c) [追加 (Add)] [OK] をクリックします。

ステップ 3 SMTP サーバのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば SMTPserver）、[ホスト (Host)] を選択し、ホストアドレス（10.1.2.29）を入力します。



New Network Object

Name
SMTPServer

Description

Type
 Network Host

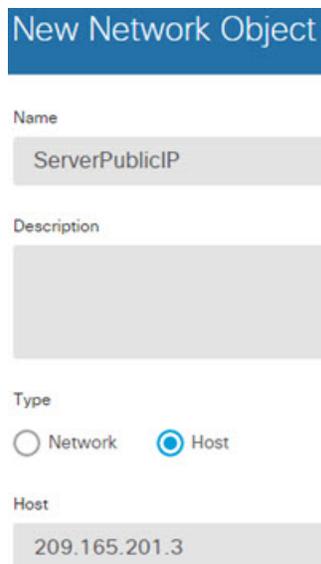
Host
10.1.2.29

c) [追加 (Add)] [OK] をクリックします。

ステップ 4 3つのサーバに使用されるパブリック IP アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば ServerPublicIP）、[ホスト (Host)] を選択し、ホストアドレス（209.165.201.3）を入力します。



New Network Object

Name
ServerPublicIP

Description

Type
 Network Host

Host
209.165.201.3

c) [追加 (Add)] [OK] をクリックします。

ステップ 5 FTP サーバのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

a) [ポリシー (Policies)] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル (Title)] = FTPServer (または任意の別の名前)
- [ルールを作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] = FTPServer ネットワーク オブジェクト (FTPserver network object)
- [変換済みアドレス (Translated Address)] = ServerPublicIP ネットワーク オブジェクト (ServerPublicIP network object) 。
- [元のポート (Original Port)] = FTP ポート オブジェクト (FTP port object) 。
- [変換済みポート (Translated Port)] = FTP ポート オブジェクト (FTP port object) 。

Add NAT Rule

Title: FTPServer Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

Original Packet

Source Interface: inside

Original Address: FTPServer Original Port: FTP

Translated Packet

Destination Interface: outside

Translated Address: ServerPublicIP Translated Port: FTP

d) [OK] をクリックします。

ステップ 6 HTTP サーバのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

- a) [+] ボタンをクリックします。
- b) 次のプロパティを設定します。

- [タイトル (Title)] = HTTPServer（または任意の別の名前）。
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] = HTTPserver ネットワーク オブジェクト (HTTPserver network object) 。
- [変換済みアドレス (Translated Address)] = ServerPublicIP ネットワーク オブジェクト (ServerPublicIP network object) 。
- [元のポート (Original Port)] = HTTP ポート オブジェクト (FTP port object) 。
- [変換済みポート (Translated Port)] = HTTP ポート オブジェクト (HTTP port object) 。

The screenshot shows the 'Add NAT Rule' configuration page. The 'Title' field is set to 'HTTPServer'. The 'Create Rule for' dropdown is set to 'Auto NAT'. The 'Placement' dropdown is set to 'Automatically placed in Auto NAT rules'. The 'Type' dropdown is set to 'Static'. The 'Packet Translation' tab is active, showing 'Source Interface' as 'inside' and 'Destination Interface' as 'outside'. Under 'Original Packet', 'Original Address' is 'HTTPServer' and 'Original Port' is 'HTTP'. Under 'Translated Packet', 'Translated Address' is 'ServerPublicIP' and 'Translated Port' is 'HTTP'.

c) [OK] をクリックします。

ステップ 7 SMTP サーバのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

- [+] ボタンをクリックします。
- 次のプロパティを設定します。

- [タイトル (Title)] = SMTPServer（または任意の別の名前）。

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = [内部（inside）]
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）] = SMTPserver ネットワーク オブジェクト（SMTPserver network object）。
- [変換済みアドレス（Translated Address）] = ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）。
- [元のポート（Original Port）] = SMTP ポート オブジェクト（SMTP port object）。
- [変換済みポート（Translated Port）] = SMTP ポート オブジェクト（SMTP port object）。

Add NAT Rule

Title: SMTPServer Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	outside
Original Address	SMTPServer	Translated Address	ServerPublicIP
Original Port	SMTP	Translated Port	SMTP

c) [OK] をクリックします。

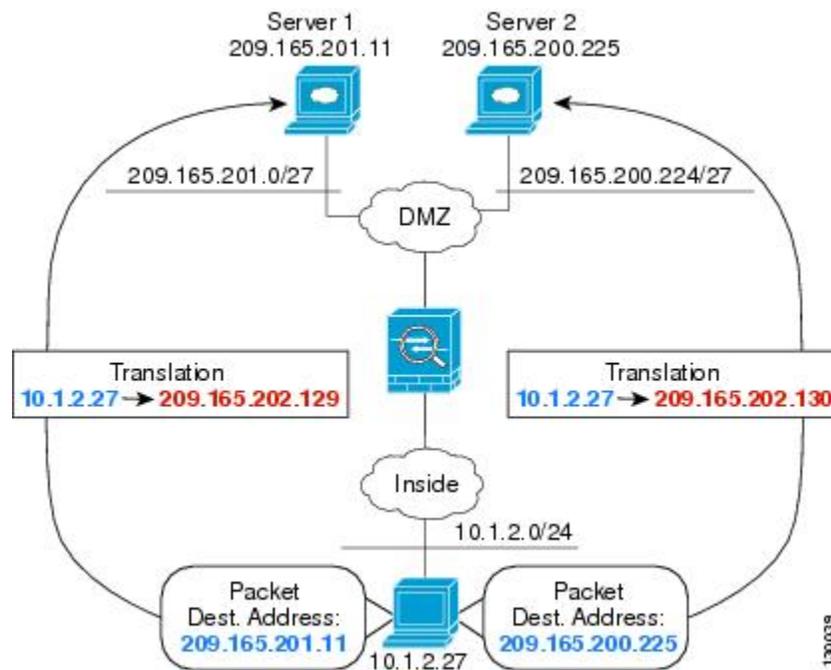
宛先に応じて異なる変換（ダイナミック手動PAT）

次の図に、2台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。



- (注) この例では、内部インターフェイスがスイッチに接続され、サーバがスイッチに接続されている標準ルーテッドインターフェイスであると仮定します。内部インターフェイスがブリッジグループインターフェイス（BVI）であり、サーバが別のブリッジグループメンバーインターフェイスに接続されている場合、対応するルールに対してサーバが接続されている特定のメンバーインターフェイスを選択します。たとえば、ルールは、内部インターフェイスではなく、送信元インターフェイスの `inside1_2` および `inside1_3` を持つ場合があります。

図 18:異なる宛先アドレスを使用する手動 NAT



手順

- ステップ 1** 内部ネットワークのネットワーク オブジェクトを作成します。
- [オブジェクト (Objects)] を選択します。
 - 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
 - ネットワーク オブジェクトに名前を付け (`myInsideNetwork` など)、[ネットワーク (Network)] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Object

Name
myInsideNetwork

Description

Type
 Network Host

Network
10.1.2.0/24

d) [追加 (Add)] [OK] をクリックします。

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを作成します。

- a) [+] をクリックします。
- b) ネットワークオブジェクトに名前を付け（DMZnetwork1 など）、[ネットワーク (Network)] を選択し、ネットワーク アドレス 209.165.201.0/27 を入力します（255.255.255.224 のサブネットマスク）。

New Network Object

Name
DMZnetwork1

Description

Type
 Network Host

Network
209.165.201.0/27

c) [追加 (Add)] [OK] をクリックします。

ステップ 3 DMZ ネットワーク 1 の PAT アドレスのネットワーク オブジェクトを作成します。

- a) [+] をクリックします。

- b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、[ホスト（Host）] を選択して、ホストアドレス 209.165.202.129 を入力します。

New Network Object

Name
PATaddress1

Description

Type
 Network Host

Host
209.165.202.129

- c) [追加（Add）][OK] をクリックします。

ステップ 4 DMZ ネットワーク 2 のネットワーク オブジェクトを作成します。

- a) [+] をクリックします。
- b) ネットワーク オブジェクトに名前を付け（DMZnetwork2 など）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 209.165.200.224/27 を入力します（255.255.255.224 のサブネットマスク）。

New Network Object

Name
DMZnetwork2

Description

Type
 Network Host

Network
209.165.200.224/27

- c) [追加 (Add)] [OK] をクリックします。

ステップ 5 DMZ ネットワーク 2 の PAT アドレスのネットワーク オブジェクトを作成します。

- a) [+] をクリックします。
b) ネットワーク オブジェクトに名前を付け (PATaddress2 など)、[ホスト (Host)] を選択して、ホストアドレス 209.165.202.130 を入力します。

New Network Object

Name
PATaddress2

Description

Type
 Network Host

Host
209.165.202.130

- c) [追加 (Add)] [OK] をクリックします。

ステップ 6 DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
b) [+] ボタンをクリックします。
c) 次のプロパティを設定します。
- [タイトル (Title)] = DMZNetwork1 (または任意の別の名前)。
 - [ルールの作成対象 (Create Rule For)] = 手動 NAT (Manual NAT)。
 - [タイプ (Type)] = [ダイナミック (Dynamic)]
 - [送信元インターフェイス (Source Interface)] = [内部 (inside)]
 - 宛先インターフェイス (Destination Interface) = dmz。
 - [元の発信元アドレス (Original Source Address)] = myInsideNetwork のネットワーク オブジェクト (myInsideNetwork network object)。
 - [変換済みの発信元アドレス (Translated Source Address)] = PATaddress1 のネットワーク オブジェクト (PATaddress1 network object)。
 - [元の宛先アドレス (Original Destination Address)] = DMZnetwork1 のネットワーク オブジェクト (DMZnetwork1 network object)。

- [変換済みの宛先アドレス (Translated Destination Address)] = DMZnetwork1 のネットワーク オブジェクト (DMZnetwork1 network object)。

(注) 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート (Port)] フィールドはすべて空白のままにします。

Add NAT Rule

Title: DMZNetwork1 Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules Type: Dynamic

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATaddress1
Source Port	Any	Source Port	Any
Destination Address	DMZnetwork1	Destination Address	DMZnetwork1
Destination Port	Any	Destination Port	Any

d) [OK] をクリックします。

ステップ 7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- タイトル (Title) = DMZNetwork2 (または任意の別の名前)。
- [ルール of 作成対象 (Create Rule For)] = 手動 NAT (Manual NAT)。
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- 宛先インターフェイス (Destination Interface) = dmz。

- [元の発信元アドレス（Original Source Address）] = myInsideNetwork のネットワーク オブジェクト（myInsideNetwork network object）。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress2 のネットワーク オブジェクト（PATaddress2 network object）。
- [元の宛先アドレス（Original Destination Address）] = DMZnetwork2 のネットワーク オブジェクト（DMZnetwork2 network object）。
- [変換済みの宛先アドレス（Translated Destination Address）] = DMZnetwork2 のネットワーク オブジェクト（DMZnetwork2 network object）。

Add NAT Rule

Title: DMZNetwork2 Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules Type: Dynamic

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATaddress2
Source Port	Any	Source Port	Any
Destination Address	DMZnetwork2	Destination Address	DMZnetwork2
Destination Port	Any	Destination Port	Any

- c) [OK] をクリックします。

宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

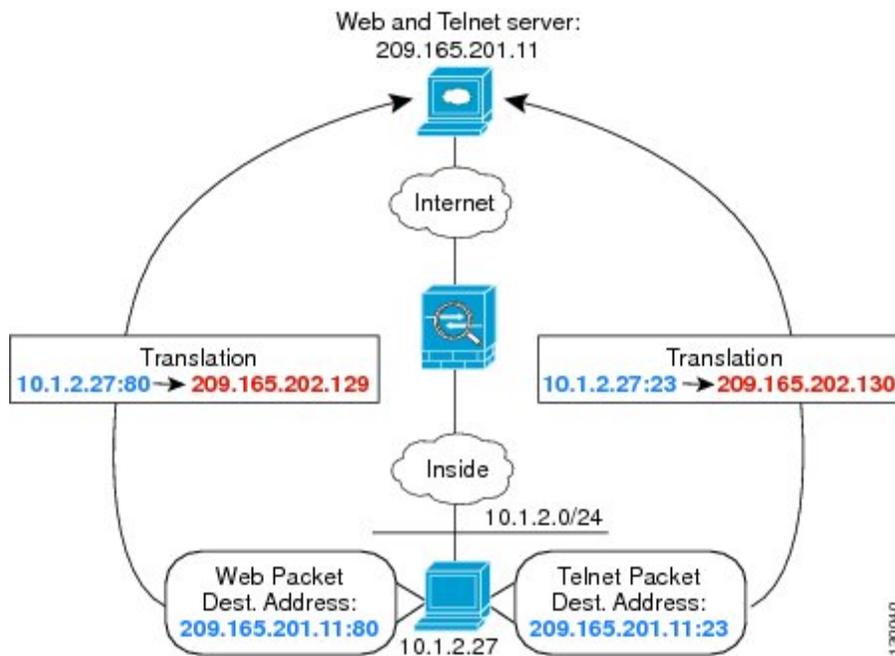
次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:

ポートに変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。



- (注) この例では、内部インターフェイスがスイッチに接続され、サーバがスイッチに接続されている標準ルーテッドインターフェイスであると仮定します。内部インターフェイスがブリッジグループインターフェイス（BVI）であり、サーバがブリッジグループメンバーインターフェイスに接続されている場合、サーバが接続されている特定のメンバーインターフェイスを選択します。たとえば、ルールは、内部インターフェイスではなく、送信元インターフェイスの `inside1_2` を持つ場合があります。

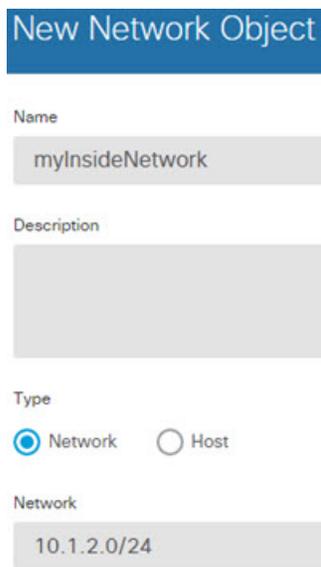
図 19:異なる宛先ポートを使用する手動 NAT



手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- ネットワーク オブジェクトに名前を付け (myInsideNetwork など)、[ネットワーク (Network)] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。



New Network Object

Name
myInsideNetwork

Description

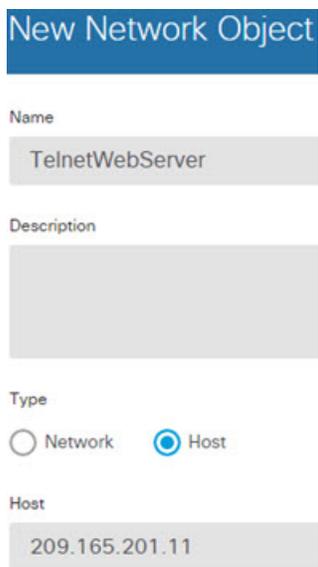
Type
 Network Host

Network
10.1.2.0/24

d) [追加 (Add)] [OK] をクリックします。

ステップ 2 Telnet/Web サーバのネットワーク オブジェクトを作成します。

- a) [+] をクリックします。
- b) ネットワーク オブジェクトに名前を付け（TelnetWebServer など）、[ホスト (Host)] を選択して、ホストアドレス 209.165.201.11 を入力します。



New Network Object

Name
TelnetWebServer

Description

Type
 Network Host

Host
209.165.201.11

c) [追加 (Add)] [OK] をクリックします。

ステップ 3 Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

- a) [+] をクリックします。
- b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、[ホスト (Host)] を選択して、ホストアドレス 209.165.202.129 を入力します。

New Network Object

Name
PATAddress1

Description

Type
 Network Host

Host
209.165.202.129

c) [追加 (Add)] [OK] をクリックします。

ステップ 4 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

- [+] をクリックします。
- ネットワーク オブジェクトに名前を付け（PATAddress2 など）、[ホスト (Host)] を選択して、ホストアドレス 209.165.202.130 を入力します。

New Network Object

Name
PATAddress2

Description

Type
 Network Host

Host
209.165.202.130

c) [追加 (Add)] [OK] をクリックします。

ステップ 5 Telnet アクセスのダイナミック手動 PAT を設定します。

- [ポリシー (Policies)] > [NAT] を選択します。
- [+] ボタンをクリックします。
- 次のプロパティを設定します。

- [タイトル (Title)] = TelnetServer (または任意の別の名前) 。
- [ルールの作成対象 (Create Rule For)] = 手動 NAT (Manual NAT) 。
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- 宛先インターフェイス (Destination Interface) = dmz。
- [元の発信元アドレス (Original Source Address)] = myInsideNetwork のネットワーク オブジェクト (myInsideNetwork network object) 。
- [変換済みの発信元アドレス (Translated Source Address)] = PATaddress1 のネットワーク オブジェクト (PATaddress1 network object) 。
- [元の宛先アドレス (Original Destination Address)] = TelnetWebServer のネットワーク オブジェクト (TelnetWebServer network object) 。
- [変換済みの宛先アドレス (Translated Destination Address)] = TelnetWebServer のネットワーク オブジェクト (TelnetWebServer network object) 。
- [元の宛先ポート (Original Destination Port)] = TELNET ポート オブジェクト (TELNET port object) 。
- [変換済みの宛先ポート (Translated Destination Port)] = TELNET ポート オブジェクト (TELNET port object) 。

(注) 宛先アドレスまたはポートを変換しないため、元アドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポートに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。

Add NAT Rule

Title: TelnetServer

Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules

Type: Dynamic

Packet Translation | Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATAddress1
Source Port	Any	Source Port	Any
Destination Address	TelnetWebServe	Destination Address	TelnetWebServe
Destination Port	TELNET	Destination Port	TELNET

d) [OK] をクリックします。

ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル (Title)] = WebServer (またはユーザが選択する別の名前)
- [ルールの作成対象 (Create Rule For)] = 手動 NAT (Manual NAT) 。
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- 宛先インターフェイス (Destination Interface) = dmz。
- [元の発信元アドレス (Original Source Address)] = myInsideNetwork のネットワーク オブジェクト (myInsideNetwork network object) 。
- [変換済みの発信元アドレス (Translated Source Address)] = PATAddress2 のネットワーク オブジェクト (PATAddress2 network object) 。
- [元の宛先アドレス (Original Destination Address)] = TelnetWebServer のネットワーク オブジェクト (TelnetWebServer network object) 。

- [変換済みの宛先アドレス (Translated Destination Address)] = TelnetWebServer のネットワーク オブジェクト (TelnetWebServer network object)。
- [元の宛先ポート (Original Destination Port)] = HTTP ポート オブジェクト (HTTP port object)。
- [変換済みの宛先ポート (Translated Destination Port)] = HTTP ポート オブジェクト (HTTP port object)。

Add NAT Rule

Title: WebServer Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules Type: Dynamic

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATAddress2
Source Port	Any	Source Port	Any
Destination Address	TelnetWebServe	Destination Address	TelnetWebServe
Destination Port	HTTP	Destination Port	HTTP

- c) [OK] をクリックします。

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT 設定と一致するアドレスに置き換えて、DNS 応答を修正するように Firepower Threat Defense デバイスを設定することが必要になる場合があります。DNS 修正は、各トランスレーションルールを設定するときに設定できます。DNS 修正は DNS 改ざんとも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスを書き換えます (たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコード)。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A

レコードはマップされた値から実際の値へ書き換えられます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。

以下に、NAT ルールで DNS の書き換えを設定する必要が生じる主な状況を示します。

- ルールは NAT64 または NAT46 であり、DNS サーバは外部ネットワークにあります。DNS A レコード (IPv4 用) と AAAA レコード (IPv6 用) を変換するために DNS の書き換えが必要です。
- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

DNS の書き換えの制限事項

次に DNS の書き換えの制限事項を示します。

- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS の書き換えは PAT には適用されません。
- 手動 NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、Firepower Threat Defense デバイスは、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- 実際には、DNS の書き換えは NAT ルールではなく `xlate` エントリで実行されます。したがって、ダイナミック ルールに `xlate` がない場合、書き換えが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS の書き換えによって、DNS ダイナミック アップデートのメッセージ (オペレーションコード 5) は書き換えられません。

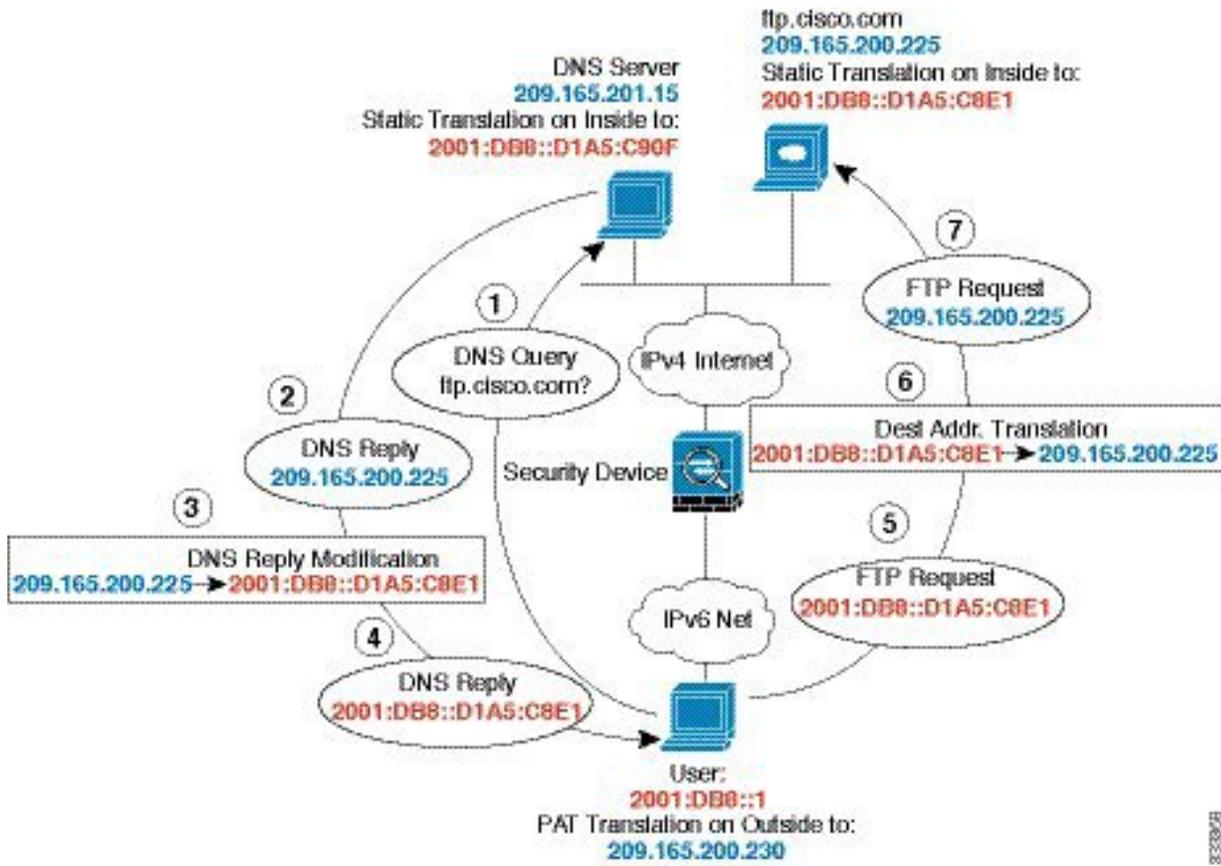
次のトピックで、NAT ルールでの DNS の書き換えの例を示します。

DNS 64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザが `ftp.cisco.com` のアドレスを DNS サーバに要求すると、DNS サーバは実際のアドレス (209.165.200.225) を応答します。

内部ユーザに `ftp.cisco.com` のマッピングアドレス (2001:DB8::D1A5:C8E1 : D1A5:C8E1 は IPv6 の 209.165.200.225 に相当) を使用させるには、スタティック変換用の DNS 応答修正を設定す

する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



(注) この例は、内部インターフェイスがブリッジグループインターフェイス (BVI) ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI である場合、各メンバーインターフェイスのルールを複製する必要があります。

手順

ステップ 1 FTP サーバ、DNS サーバ、内部ネットワーク、および PAT プールのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server など)、[ホスト (Host)] を選択して、実際のホストの IP アドレス 209.165.200.225 を入力します。

Add Network Object

Name

ftp_server

Description

Type

Network Host

Host

209.165.200.225

- d) [追加 (Add)] [OK] をクリックします。
- e) [+] をクリックして DNS サーバの実際のアドレスを定義します。
ネットワーク オブジェクトに名前を付け (dns_server など)、[ホスト (Host)] を選択して、ホスト アドレス 209.165.201.15 を入力します。

Add Network Object

Name

dns_server

Description

Type

Network Host

Host

209.165.201.15

- f) [追加 (Add)] [OK] をクリックします。
- g) [+] をクリックして内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前を付け (inside_v6 など)、[ネットワーク (Network)] を選択して、ネットワーク アドレス 2001:DB8::/96 を入力します。

Add Network Object

Name

inside_v6

Description

Type

Network Host

Network

2001:DB8::/96

- h) [追加 (Add)] [OK] をクリックします。
- i) [+] をクリックして内部 IPv6 ネットワークの IPv4 PAT アドレスを定義します。
ネットワーク オブジェクトに名前を付け (ipv4_pat など)、[ホスト (Host)] を選択して、ホストアドレス 209.165.200.230 を入力します。

Add Network Object

Name

ipv4_pat

Description

Type

Network Host

Host

209.165.200.230

- j) [追加 (Add)] [OK] をクリックします。

ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。
- [タイトル (Title)] = FTPServer (または任意の別の名前)

- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- 送信元インターフェイス (Source Interface) = [外部 (outside)]
- 宛先インターフェイス (Destination Interface) = [内部 (inside)]
- [元のアドレス (Original Address)] = ftp_server のネットワーク オブジェクト (ftp_server network object)。
- [変換済みアドレス (Translated Address)] = inside_v6 ネットワーク オブジェクト (inside_v6 network object) IPv4 アドレスを IPv6 アドレスに変換する場合、IPv4 組み込みアドレス方式が使用されているため、209.165.200.225 は IPv6 で対応する D1A5:C8E1 に変換され、ネットワーク プレフィックスが追加されて完全なアドレス 2001:DB8::D1A5:C8E1 となります。
- [詳細オプション (Advanced Options)] タブで、[このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule)] を選択します。

Add NAT Rule

Title: FTPServer Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	outside	Destination Interface	inside
Original Address	ftp_server	Translated Address	inside_v6
Original Port	Any	Translated Port	Any

d) [OK] をクリックします。

ステップ 3 DNS サーバのためのスタティック NAT ルールを設定します。

- [ポリシー (Policies)] > [NAT] を選択します。
- [+] ボタンをクリックします。
- 次のプロパティを設定します。

- [タイトル (Title)] = DNSServer (または任意の別の名前)。
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- 送信元インターフェイス (Source Interface) = [外部 (outside)]
- 宛先インターフェイス (Destination Interface) = [内部 (inside)]
- [元のアドレス (Original Address)] = dns_server のネットワーク オブジェクト (dns_server network object.)。
- [変換済みアドレス (Translated Address)] = inside_v6 ネットワーク オブジェクト (inside_v6 network object) IPv4 アドレスを IPv6 アドレスに変換する場合、IPv4 組み込みアドレス方式が使用されているため、209.165.201.15 は IPv6 で対応する D1A5:C90F に変換され、ネットワーク プレフィックスが追加されて完全なアドレス 2001:DB8::D1A5:C90F となります。

Add NAT Rule

Title: DNSServer Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	outside	Destination Interface	inside
Original Address	dns_server	Translated Address	inside_v6
Original Port	Any	Translated Port	Any

d) [OK] をクリックします。

ステップ 4 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

- [ポリシー (Policies)] > [NAT] を選択します。
- [+] ボタンをクリックします。
- 次のプロパティを設定します。

- [タイトル (Title)] = PAT64Rule (またはユーザが選択する別の名前)
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = [内部 (inside)]
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
- [変換済みのアドレス (Translated Address)] = ipv4_pat のネットワーク オブジェクト (ipv4_pat network object) 。

Add NAT Rule ?

Title PAT64Rule	Create Rule for Auto NAT	Status <input checked="" type="checkbox"/>
--------------------	-----------------------------	---

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement Automatically placed in Auto NAT rules	Type Dynamic
---	-----------------

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface inside	Destination Interface outside	Translated Address ipv4_pat	Translated Port Any
Original Address inside_v6	Original Port Any		

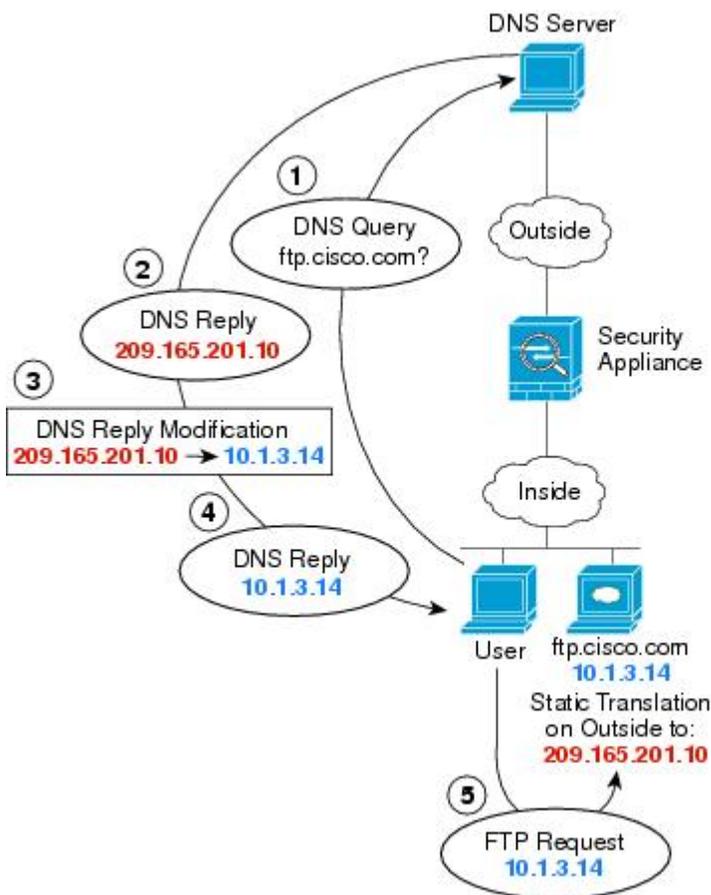
d) [OK] をクリックします。

DNS 応答修正 : 外部の DNS サーバ

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス (10.1.3.14) を、外部ネットワーク上で確認できるマッピングアドレス (209.165.201.10) にスタティックに変換するように NAT を設定します。

この場合、このスタティックルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して ftp.cisco.com にアクセスできる内部ユーザは、マッピングアドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバはマッピングアドレス (209.165.201.10) を応答します。システムは、内部サーバのスタティックルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



(注) この例は、内部インターフェイスがブリッジグループインターフェイス (BVI) ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI である場合、各メンバーインターフェイスのルールを複製する必要があります。

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

- a) [オブジェクト (Objects)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- c) 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server など)、[ホスト (Host)] を選択して、実際のホストの IP アドレス 10.1.3.14 を入力します。

Add Network Object

Name
ftp_server

Description

Type
 Network Host

Host
10.1.3.14

- d) [追加 (Add)] [[OK]] をクリックします。
- e) [+] をクリックして FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server_outside など)、[ホスト (Host)] を選択して、ホストアドレス 209.165.201.10 を入力します。

Add Network Object

Name
ftp_server_outside

Description

Type
 Network Host

Host
209.165.201.10

ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。
 - [タイトル (Title)] = FTPServer (または任意の別の名前)
 - [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
 - [タイプ (Type)] = [スタティック (Static)]
 - [送信元インターフェイス (Source Interface)] = [内部 (inside)]
 - [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
 - [元のアドレス (Original Address)] = ftp_server のネットワーク オブジェクト (ftp_server network object)。
 - [変換済みのアドレス (Translated Address)] = ftp_server_outside のネットワーク オブジェクト (ftp_server_outside network object)。
 - [詳細オプション (Advanced Options)] タブで、[このルールに一致する DNS 応答を交換する (Translate DNS replies that match this rule)] を選択します。

Add NAT Rule

Title: FTPServer Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

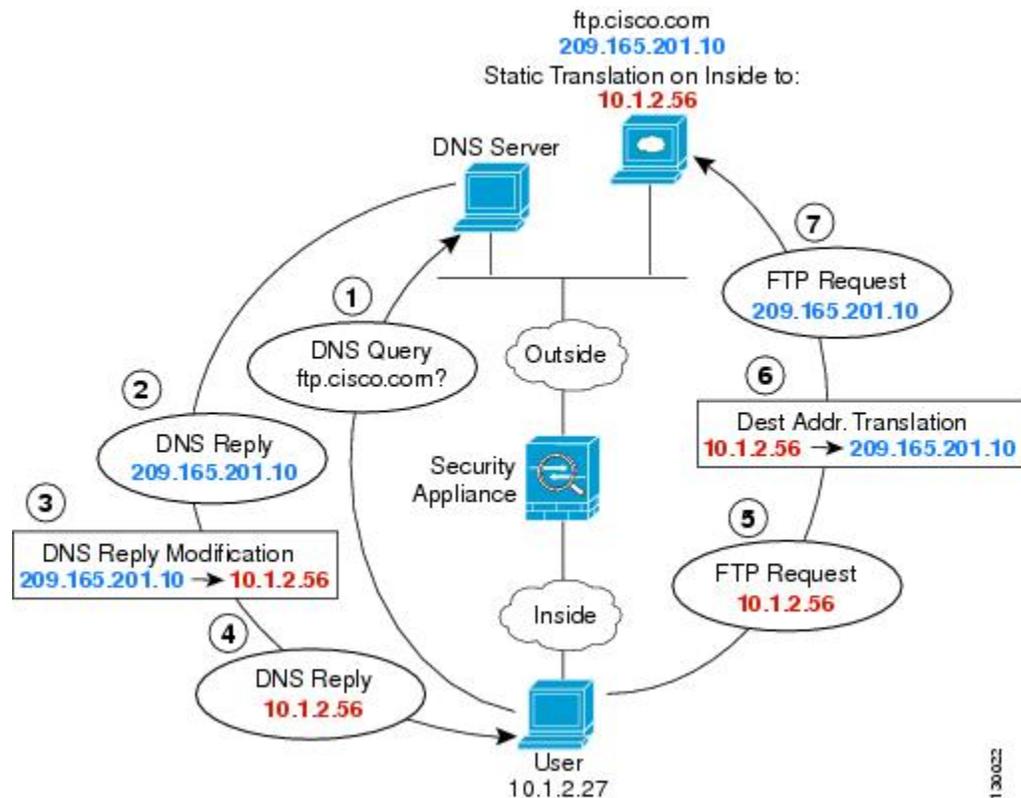
Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	ftp_server	Translated Address	ftp_server_outside
Original Port	Any	Translated Port	Any

- d) [OK] をクリックします。

DNS 応答修正：ホスト ネットワーク上の DNS サーバ

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは実際のアドレス（209.165.201.10）を応答します。内部ユーザに ftp.cisco.com のマッピングアドレス（10.1.2.56）を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。



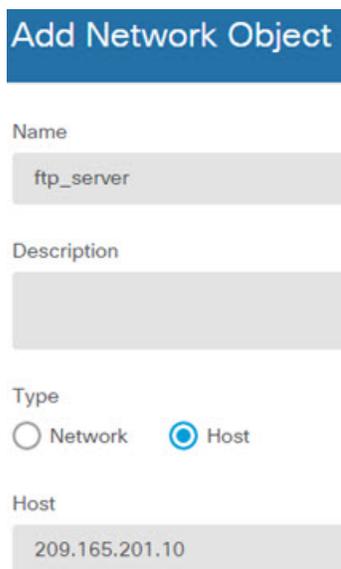
(注) この例は、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI である場合、各メンバーインターフェイスのルールを複製する必要があります。

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server など)、[ホスト (Host)] を選択して、実際のホストの IP アドレス 209.165.201.10 を入力します。



Add Network Object

Name
ftp_server

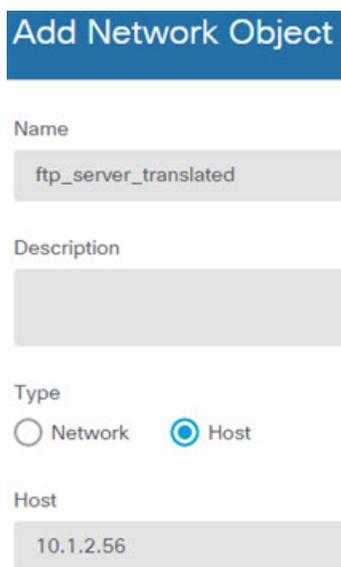
Description

Type
 Network Host

Host
209.165.201.10

- d) [追加 (Add)] [OK] をクリックします。
- e) [+] をクリックして FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server_translated など)、[ホスト (Host)] を選択して、ホストアドレス 10.1.2.56 を入力します。



Add Network Object

Name
ftp_server_translated

Description

Type
 Network Host

Host
10.1.2.56

ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル (Title)] = FTPServer (または任意の別の名前)
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- 送信元インターフェイス (Source Interface) = [外部 (outside)]
- 宛先インターフェイス (Destination Interface) = [内部 (inside)]
- 元のアドレス (Original Address) = ftp_server のネットワーク オブジェクト。
- 変換済みのアドレス (Translated Address) = ftp_server_translated のネットワーク オブジェクト。
- [詳細オプション (Advanced Options)] タブで、[このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule)] を選択します。

Add NAT Rule ?

Title	Create Rule for	Status
FTPServer	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static ▼

Packet Translation

Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	Destination Interface		
outside ▼	inside		
Original Address	Original Port	Translated Address	Translated Port
ftp_server ▼	Any ▼	ftp_server_transla ▼	Any

d) [OK] をクリックします。



第 **III** 部

バーチャル プライベート ネットワーク (VPN)

- [サイト間 VPN \(393 ページ\)](#)
- [リモート アクセス VPN \(429 ページ\)](#)



第 15 章

サイト間 VPN

バーチャルプライベートネットワーク（VPN）は、パブリック ソース（インターネットやその他のネットワークなど）を使用して、リモートピア間でセキュアなトンネルを確立するネットワーク接続です。VPN ではトンネルを使用して通常の IP パケット内のデータ パケットがカプセル化され、IP ベースのネットワークを介して転送されます。VPN ではプライバシーの確保と認証のために暗号化が使用され、データの整合性が確保されます。

- [VPN の基本](#)（393 ページ）
- [サイト間 VPN の管理](#)（398 ページ）
- [サイト間 VPN のモニタリング](#)（414 ページ）
- [サイト間 VPN の例](#)（415 ページ）

VPN の基本

トンネリングによって、インターネットなどのパブリック TCP/IP ネットワークの使用が可能となり、リモートユーザとプライベート企業ネットワークとの間でセキュアな接続を作成できます。各セキュアな接続がトンネルと呼ばれます。

IPsec ベースの VPN テクノロジーでは、Internet Security Association and Key Management Protocol（ISAKMP または IKE）と IPsec トンネリングを使用して、トンネルを構築し管理します。ISAKMP と IPsec は、次を実現します。

- トンネル パラメータのネゴシエート。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネルを経由するデータ転送の管理。
- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネル エンドポイントとして機能します。プライベート ネットワークからプレーンパケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネルの他端に送信できます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリックネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

サイト間 VPN 接続が確立された後、ローカル ゲートウェイの背後にあるホストは、セキュアな VPN トンネルを介してリモート ゲートウェイの背後にあるホストと接続できます。接続は、2つのゲートウェイの IP アドレスとホスト名、それらの背後にあるサブネット、および2つのゲートウェイが互いを認証するために使用する方式で構成されます。

インターネットキー エクスチェンジ (IKE)

インターネットキー エクスチェンジ (IKE) は、IPsec ピアを認証し、IPsec 暗号化キーをネゴシエートして配信し、IPsec セキュリティ アソシエーション (SA) を自動的に確立するために使用されるキー管理プロトコルです。

IKE ネゴシエーションは2つのフェーズで構成されています。フェーズ1では、2つのIKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ2で安全に通信できるようになります。フェーズ2のネゴシエーションでは、IKEによってIPsecなどの他のアプリケーション用のSAが確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE ポリシーは、2つのピアが、ピア間のIKE ネゴシエーションの安全性を確保するために使用する一連のアルゴリズムです。IKE ネゴシエーションは、共通 (共有) IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、どのセキュリティパラメータが後続のIKE ネゴシエーションを保護するかを規定します。IKEバージョン1 (IKEv1) の場合、IKE ポリシーには単一セットのアルゴリズムとモジュラスグループが含まれます。IKEv1とは異なり、IKEv2 ポリシーでは、フェーズ1ネゴシエーション中にピアがその中から選択できるように、複数のアルゴリズムとモジュラスグループを選択できます。単一のIKEポリシーを作成できますが、最も必要なオプションにより高い優先順位をつけるために異なるポリシーが必要となる場合もあります。サイト間VPNの場合は、単一のIKEポリシーを作成できます。

IKE ポリシーを定義するには、次を指定します。

- 固有の優先順位 (1 ~ 65,543、1が最高の優先順位)。
- データを保護し、プライバシーを確保するためのIKE ネゴシエーションの暗号化方式。
- 送信者のIDを保証し、メッセージが伝送中に変更されないように確保するためのハッシュメッセージ認証コード (HMAC) 方式 (IKEv2では整合性アルゴリズムと呼ばれる)。
- IKEv2の場合、IKEv2トンネル暗号化に必要なキーの材料とハッシュ操作を派生させるためのアルゴリズムとして使用される個別の擬似乱関数 (PRF)。オプションは、ハッシュアルゴリズムで使用されているものと同じです。
- 暗号化キー判別アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号化キーとハッシュ キーを派生させます。
- ピアの ID を保証するための認証方式。

- デバイスが暗号化キーを交換するまでに使用できる時間制限。

IKE ネゴシエーションが開始すると、ネゴシエーションを開始するピアはリモートピアに有効なポリシーをすべて送信し、リモートピアは優先順位順に自身のポリシーとの一致を検索します。ピアが、暗号化、ハッシュ (IKEv2 の場合は整合性と PRF)、認証、Diffie-Hellman 値を保持し、さらに、送信されたポリシーのライフタイム以下である SA ライフタイムを保持している場合に、IKE ポリシー間に一致が存在します。ライフタイムが同じでない場合は、リモートピアから取得した短い方のライフタイムが適用されます。デフォルトでは、DES を使用するシンプルな IKE ポリシーが唯一有効なポリシーです。より高い優先順位のその他の IKE ポリシーによってより強力な暗号化標準をネゴシエートできますが、DES ポリシーでも正常なネゴシエーションが確保されます。

VPN 接続の安全性を確保する方法

VPN トンネルは通常、インターネットなどのパブリック ネットワークを経由するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーザルを使用して、暗号化とその他のセキュリティ技術を定義し、適用します。

デバイス ライセンスによって強力な暗号化を適用できる場合は、広範な暗号化とハッシュ アルゴリズム、および Diffie-Hellman グループがあり、その中から選択できます。ただし、一般に、トンネルに適用する暗号化が強力なほど、システムパフォーマンスは低下します。効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出します。

シスコでは、どのオプションを選択するかについての特定のガイダンスは提供できません。比較的大規模な企業またはその他の組織内で運用している場合は、すでに、満たす必要がある標準が定義されている可能性があります。定義されていない場合は、時間を割いてオプションを調べてください。

以降のトピックでは、使用可能なオプションについて説明します。

使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルに使用する暗号化アルゴリズムを決定する際、選択肢は VPN のデバイスでサポートされるアルゴリズムに限られます。

IKEv2 では、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

IPsec プロポーザルでは、認証、暗号化、およびアンチリプレイ サービスを提供するカプセル化セキュリティプロトコル (ESP) によってアルゴリズムが使用されます。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の前に ESP というプレフィックスが付けられます。

デバイス ライセンスが強力な暗号化を適用できる場合、次の暗号化アルゴリズムを選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

- AES-GCM— (IKEv2 のみ) Galois/カウンタ モードの Advanced Encryption Standard は、機密性、データの発信元の認証を提供する操作のブロック暗号モードであり、AES よりも優れたセキュリティを提供します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCM は NSA Suite B をサポートするために必要となる AES モードです。NSA Suite B は、暗号化強度に関する連邦標準規格を満たすためにデバイスがサポートすべき一連の暗号化アルゴリズムです。
- AES-GMAC— (IKEv2 IPsec プロポーザルのみ)。Advanced Encryption Standard のガロアメッセージ認証コード (GMAC) は、データ発信元認証だけを行う操作のブロック暗号モードです。これは AES-GCM の一種であり、データを暗号化せずにデータ認証が行えます。AES-GMAC には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。
- AES (Advanced Encryption Standard) は DES よりも高度なセキュリティを提供する対称暗号化アルゴリズムであり、計算的には 3DES よりも効率的です。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。
- 3DES (トリプル DES) : 56 ビット キーを使用して暗号化を 3 回行います。異なるキーを使用してデータの各ブロックを 3 回処理するため、DES よりも安全です。ただし、使用するシステムリソースが多くなり、DES よりも速度が遅くなります。
- DES (データ暗号化標準) : 56 ビット キーを使用して暗号化する対称秘密鍵ブロックアルゴリズムです。ライセンスアカウントが輸出規制の要件を満たしていない場合、これは唯一のオプションです。3DES よりも高速であり、使用するシステムリソースも少ないですが、安全性も劣ります。堅牢なデータ機密保持が必要ない場合、およびシステムリソースや速度が重要である場合には、DES を選択します。
- Null : ヌル暗号化アルゴリズムは暗号化なしで認証します。通常はテスト目的にのみ使用されます。

使用するハッシュアルゴリズムの決定

IKE ポリシーでは、ハッシュアルゴリズムがメッセージダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュアルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数 (PRF) に使用されます。

IPsec プロポーザルでは、ハッシュアルゴリズムはカプセル化セキュリティプロトコル (ESP) による認証のために使用されます。IKEv2 IPsec プロポーザルでは、これは整合性のハッシュと呼ばれます。IKEv1 IPsec プロポーザルでは、アルゴリズム名に ESP というプレフィックスだけでなく HMAC というサフィックスも付けられます (ハッシュ方式認証コードを意味する)。

IKEv2 では、複数のハッシュアルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

選択可能なハッシュ アルゴリズムは、次のとおりです。

- [SHA (Secure Hash Algorithm)] : 標準 SHA (SHAI) が 160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。ただし、SHA は MD5 よりもリソース消費量が大きくなります。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。

IKEv2 の設定では、以下の SHA-2 オプションを指定して、より高度なセキュリティを実現できます。NSA Suite B 暗号化仕様を実装するには、次のいずれかを選択します。

- SHA256 : 256 ビットのダイジェストを生成するセキュアハッシュ アルゴリズム SHA 2 を指定します。
- SHA384 : 384 ビットのダイジェストを生成するセキュアハッシュ アルゴリズム SHA 2 を指定します。
- SHA512 : 512 ビットのダイジェストを生成するセキュアハッシュ アルゴリズム SHA 2 を指定します。
- MD5 (Message Digest 5) : 128 ビットのダイジェストを生成します。MD5 は処理時間が短いため、全体的なパフォーマンスが SHA より高速ですが、SHA より強度は低いと考えられています。
- NULL またはなし (NULL、ESP-NONE) : (IPsec プロポーザルのみ) NULL ハッシュ アルゴリズム。通常はテスト目的のみに使用されます。ただし、暗号化アルゴリズムとして AES-GCM/GMAC オプションのいずれかを選択した場合は、ヌル整合性アルゴリズムを選択する必要があります。NULL 以外のオプションを選択した場合、これらの暗号化標準に対しては、整合性ハッシュは無視されます。

使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec Security Association (SA : セキュリティアソシエーション) キーを生成することができます。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。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択する場合は、AES で必要な大きいキー サイズをサポートするために、Diffie-Hellman (DH : デフィーヘルマン) グループ 5 以降を使用する必要があります。IKEv1 ポリシーは、以下にリストされているすべてのグループをサポートしていません。

NSA Suite-B の暗号化の仕様を実装するには、IKEv2 を使用して楕円曲線 Diffie-Hellman (ECDH) オプション : 19、20、21 のいずれか 1 つを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

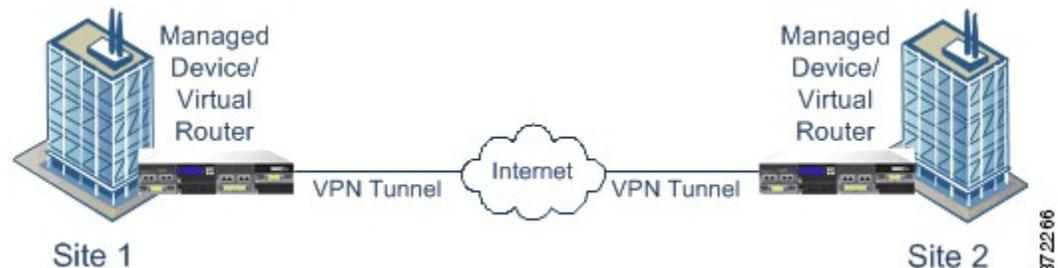
- 1 : Diffie-Hellman グループ 1 (768 ビット係数) 。DH グループ 1 はセキュアではないとみなされるため使用しないでください。

- 2 : Diffie-Hellman グループ 2 (1024 ビット Modular Exponential (MODP) グループ) 。このオプションは優れた保護とは見なされなくなりました。
- 5 : Diffie-Hellman グループ 5 (1536 ビット MODP グループ) 。以前は 128 ビット キーに対する優れた保護と見なされていましたが、このオプションは優れた保護と見なされなくなりました。
- 14 : Diffie-Hellman グループ 14 (2048 ビット Modular Exponential (MODP) グループ) 。192 ビットのキーでは十分な保護レベルです。
- 19 : Diffie-Hellman グループ 19 (国立標準技術研究所 (NIST) 256 ビット楕円曲線モジュロプライム (ECP) グループ) 。
- 20 : Diffie-Hellman グループ 20 (NIST 384 ビット ECP グループ) 。
- 21 : Diffie-Hellman グループ 21 (NIST 521 ビット ECP グループ) 。
- 24 : Diffie-Hellman グループ 24 (2048 ビット MODP グループおよび 256 素数位数サブグループ) 。このオプションは推奨されなくなりました。

VPN トポロジ

Firepower Device Manager を使用して設定できるのは、ポイントツーポイント VPN 接続のみです。すべての接続はポイントツーポイントですが、デバイスが参加する各トンネルを定義することで、より大規模なハブアンドスポーク VPN、またはメッシュ VPN にリンクできます。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。ポイントツーポイントの VPN トポロジでは、2つのエンドポイントが相互に直接通信します。2つのエンドポイントをピアデバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。



サイト間 VPN の管理

バーチャルプライベートネットワーク (VPN) は、パブリック ソース (インターネットやその他のネットワークなど) を使用して、リモートピア間でセキュアなトンネルを確立するネットワーク接続です。VPN ではトンネルを使用して通常の IP パケット内のデータ パケットがカプセル化され、IP ベースのネットワークを介して転送されます。VPN ではプライバシーの確保と認証のために暗号化が使用され、データの整合性が確保されます。

ピア デバイスへの VPN 接続を作成できます。接続はすべてポイントツーポイントですが、関連する接続をすべて設定することで、大規模なハブアンドスポークやメッシュ VPN にデバイスを接続できます。



- (注) VPN接続では、暗号化を使用してネットワークのプライバシーが保護されます。使用できる暗号化アルゴリズムは、基本ライセンスで強力な暗号化が許可されているかどうかによって異なります。これは、Cisco Smart License Manager に登録するときにデバイス上で輸出管理機能を許可するオプションを選択しているかどうかによって制御されます。評価ライセンスを使用している場合、または輸出管理機能を有効にしていない場合は、強力な暗号化を使用できません。

手順

ステップ 1 [デバイス (Device)] をクリックし、次に [サイト間VPN (Site-to-Site VPN)] グループの [設定の表示 (View Configuration)] をクリックします。

これで、[サイト間VPN (Site-to-Site VPN)] ページが開き、設定済みのすべての接続が表示されます。

ステップ 2 次のいずれかを実行します。

- 新しいサイト間 VPN 接続を作成するには、[+] ボタンをクリックします。 [サイト間 VPN 接続の設定 \(399 ページ\)](#) を参照してください。
まだ接続が存在しない場合でも、[サイト間接続の作成 (Create Site-to-Site Connection)] ボタンはクリックできます。
- 既存の接続を編集するには、その接続の編集 (🔍) アイコンをクリックします。 [サイト間 VPN 接続の設定 \(399 ページ\)](#) を参照してください。
- 接続設定のサマリーをクリップボードにコピーするには、その接続の [コピー (copy)] アイコン (📄) をクリックします。その情報をドキュメントに貼り付け、リモートデバイスの管理者に送信して、接続の一端の設定をサポートできます。
- 不要になった接続を削除するには、その接続の [削除 (delete)] アイコン (🗑️) をクリックします。

サイト間 VPN 接続の設定

リモートデバイス オーナーの協力と許可を得ている場合、ポイントツーポイント VPN 接続を作成し、デバイスを別のデバイスにリンクできます。すべての接続はポイントツーポイントですが、デバイスが参加する各トンネルを定義することで、より大きなハブアンドスポークまたはメッシュ VPN にリンクできます。



(注) ローカルネットワーク/リモートネットワークの組み合わせごとに、1つのVPN接続を作成できます。ただし、リモートネットワークが各接続プロファイルで一意である場合は、ローカルネットワークに対して複数の接続を作成できます。

手順

ステップ1 [デバイス (Device)] をクリックし、次に [サイト間VPN (Site-to-Site VPN)] グループの [設定の表示 (View Configuration)] をクリックします。

ステップ2 次のいずれかを実行します。

- 新しいサイト間VPN接続を作成するには、[+] ボタンをクリックします。
まだ接続が存在しない場合、[サイト間接続の作成 (Create Site-to-Site Connection)] ボタンをクリックします。
- 既存の接続を編集するには、接続の [編集 (edit)] アイコン (🔍) をクリックします。

不要になった接続を削除するには、接続の [削除 (delete)] アイコン (🗑️) をクリックします。

ステップ3 ポイントツーポイントVPN接続のエンドポイントを定義します。

- [接続プロファイル名 (Connection Profile Name)]: この接続の名前で、スペースなしで最大 64 文字までです。たとえば、「MainOffice」など。名前として IP アドレスは使用できません。
- [ローカルサイト (Local Site)]: これらのオプションではローカルエンドポイントを定義します。
 - [ローカルVPNのアクセスインターフェイス (Local VPN Access Interface)]: リモートピアが接続できるインターフェイスを選択します。これは通常、外部インターフェイスです。インターフェイスをブリッジグループのメンバーにはできません。
 - [ローカルネットワーク (Local Network)]: [+] をクリックし、VPN 接続に参加する必要があるローカルネットワークを識別するネットワーク オブジェクトを選択します。これらのネットワーク上のユーザは、この接続を介してリモートネットワークに到達できます。

(注) これらのネットワークに IPv4 アドレスまたは IPv6 アドレスを使用できますが、接続の各側に一致するアドレスタイプがなければなりません。たとえば、ローカル IPv4 ネットワークの VPN 接続には、少なくとも1つのリモート IPv4 ネットワークが必要です。1つの接続の両側で、IPv4 と IPv6 を組み合わせることができます。エンドポイントの保護されたネットワークは重複することはできません。

- [リモートサイト (Remote Site)] : これらのオプションでリモートエンドポイントを定義します。
 - [リモートIPアドレス (Remote IP Address)] (スタティックアドレス指定のみ) : VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレスを入力します。
 - [リモートネットワーク (Remote Network)] : [+] をクリックして、VPN 接続に参加する必要があるリモート ネットワークを特定するネットワーク オブジェクトを選択します。これらのネットワーク上のユーザは、この接続を介してローカルネットワークに到達できます。

ステップ4 [次へ (Next)] をクリックします。

ステップ5 VPN のプライバシー設定を定義します。

(注) ライセンスにより、どの暗号化プロトコルを選択できるかが決まります。最も基本的なオプション以外のものを選択するには、輸出規制を満たすなど、強力な暗号化が必要です。

- [IKEバージョン2 (IKE Version 2)]、[IKEバージョン1 (IKE Version 1)] : インターネットキーエクスチェンジ (IKE) ネゴシエーション時に使用する IKE バージョンを選択します。必要に応じて、いずれかまたは両方のオプションを選択します。デバイスがもう1つのピアとの接続のネゴシエーションを試行する場合は、ユーザが許可したバージョン、およびもう1つのピアが受け入れるバージョンのどちらでも使用されます。両方のバージョンを許可すると、最初に選択したバージョンとのネゴシエーションが正常に行われなかった場合、デバイスはもう1つのバージョンに自動的にフォールバックします。IKEv2 が設定されている場合、常に最初に試行されます。ネゴシエーションで使用するには、両方のピアが IKEv2 をサポートする必要があります。
- [IKEポリシー (IKE Policy)] : インターネットキーエクスチェンジ (IKE) は、IPsec ピアの認証、IPsec 暗号化キーのネゴシエーションと配布、および IPsec セキュリティアソシエーション (SA) の自動的な確立に使用されるキー管理プロトコルです。これはグローバルポリシーで、有効にしたオブジェクトはすべてのVPNに適用されます。[編集 (Edit)] をクリックし、IKEバージョンごとに現在グローバルに有効なポリシーを確認し、新しいポリシーを有効化し、作成します。詳細については、[グローバル IKE ポリシーの設定 \(403 ページ\)](#) を参照してください。
- [Ipsecプロポーザル (IPsec Proposal)] : IPsec プロポーザルは、IPsec トンネルのトラフィックを保護するセキュリティプロトコルとアルゴリズムの組み合わせを定義します。[編集 (Edit)] をクリックし、IKEバージョンごとのプロポーザルを選択します。ユーザに許可するすべてのプロポーザルを選択します。[デフォルトの設定 (Set Default)] をクリックし、システムデフォルトを選択します。これはエクスポートコンプライアンスに応じて異なります。一致が合意されるまで、最も強いプロポーザルから最も弱いプロポーザルまで、ピアとのネゴシエートが行われます。詳細については、「[IPsec プロポーザルの設定 \(408 ページ\)](#)」を参照してください。

- (IKEv2) [ローカル事前共有キー (Local Preshared Key)]、[リモートピア事前共有キー (Remote Peer Preshared Key)]: VPN 接続のためにこのデバイスとリモートデバイスで定義されたキー。これらのキーは IKEv2 では異なる場合があります。このキーには 1 ~ 127 の英数字を指定できます。
- (IKEv1) [事前共有キー (Preshared Key)]: ローカルデバイスとリモートデバイスの両方で定義されたキー。このキーには 1 ~ 127 の英数字を指定できます。
- [NAT免除 (NAT Exempt)]: VPN トラフィックをローカル VPN アクセス インターフェイス上の NAT ポリシーから除外するかどうか。NAT ルールをローカルネットワークに適用しない場合、ローカルネットワークをホストするインターフェイスを選択します。このオプションは、ローカルネットワークが 1 つのルーテッドインターフェイス (ブリッジグループ メンバーではない) の背後にある場合にのみ機能します。ローカルネットワークが複数のルーテッドインターフェイスまたは 1 つ以上のブリッジグループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、[NAT からのサイト間 VPN トラフィックの除外 \(415 ページ\)](#) を参照してください。
- [Perfect Forward Secrecy用Diffie-Helmanグループ (Diffie-Helman Group for Perfect Forward Secrecy)]: 暗号化されたやり取りごとに一意のセッション キーを生成および使用するため、Perfect Forward Secrecy (PFS) を使用するかどうかを指定します。一意のセッション キーを使用することによって、やり取りを以降の復号から保護します。このことは、やり取り全体が記録され、攻撃者がエンドポイントデバイスで使用される事前共有キーまたは秘密キーを入手している場合であっても該当します。Perfect Forward Secrecy を有効にする場合、[モジュラスグループ (Modulus Group)] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムを選択します。IKEv1 と IKEv2 の両方を有効にすると、オプションは IKEv1 でサポートされているものに制限されます。オプションの説明については、[使用する Diffie-Hellman 係数グループの決定 \(397 ページ\)](#) を参照してください。

ステップ 6 [次へ (Next)] をクリックします。

ステップ 7 サマリーを確認し、[終了 (Finish)] をクリックします。

サマリー情報がクリップボードにコピーされます。この情報はドキュメントに貼り付けて、リモートピアの設定、またはピアの設定責任者に送信するために使用できます。

構成を配置した後、デバイス CLI にログインし、**show ipsec sa** コマンドを使用してエンドポイントがセキュリティアソシエーションを確立することを確認します。「[サイト間 VPN 接続の確認 \(411 ページ\)](#)」を参照してください。

次のタスク

デフォルトで、VPN 終端トラフィックは、URL フィルタリング、侵入防御、ファイルポリシーなど、そのポリシーで定義されている任意の高度なインスペクションを含むアクセスコントロールポリシーをバイパスします。VPN トラフィックを評価してアクセスコントロールポリシーで検査する場合は、FlexConfig を使用して **no sysopt connection permit-vpn** コマンドを設定

します。その後アクセス制御ルールを設定して、アドレスプールと内部ネットワーク間の外部から内部インターフェイスへのトラフィックを許可することができます。システムはアクセス制御ポリシーで評価を行う前に VPN トラフィックを復号化するので、侵入防止、URL フィルタリングなどを適用できます。

グローバル IKE ポリシーの設定

Internet Key Exchange (IKE、インターネット キー エクスチェンジ) は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association (SA、セキュリティ アソシエーション) の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは2つのフェーズで構成されています。フェーズ1では、2つのIKEピア間のセキュリティアソシエーションをネゴシエートします。これにより、ピアはフェーズ2で安全に通信できるようになります。フェーズ2のネゴシエーションでは、IKEによってIPsecなどの他のアプリケーション用のSAが確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKEプロポーザルは、2つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKEネゴシエーションは、共通（共有）IKEポリシーに合意している各ピアによって開始されます。このポリシーは、後続のIKEネゴシエーションを保護するために使用されるセキュリティパラメータを示します。

IKEポリシーオブジェクトはこれらのネゴシエーションに対してIKEプロポーザルを定義します。有効にするオブジェクトは、ピアがVPN接続をネゴシエートするときに使用するものであり、接続ごとに異なるIKEポリシーを指定することはできません。各オブジェクトの相対的な優先順位は、これらの中でどのポリシーを最初に試すかを決定します。数が小さいほど、優先順位が高くなります。ネゴシエーションで両方のピアがサポートできるポリシーを見つけられなければ、接続は確立されません。

IKEグローバルポリシーを定義するには、各IKEバージョンを有効にするオブジェクトを選択します。事前定義されたオブジェクトが要件を満たさない場合、セキュリティポリシーを適用する新しいポリシーを作成します。

次に、オブジェクト ページでグローバルポリシーを設定する方法について説明します。VPN接続を編集しているときにIKEポリシー設定の[編集 (Edit)]をクリックすることで、ポリシーの有効化、無効化および作成が行えます。

手順

ステップ1 [オブジェクト (Objects)] を選択し、次に目次から [IKEポリシー (IKE Policies)] を選択します。

IKEv1 と IKEv2 のポリシーが別のリストに表示されます。

ステップ2 各IKEバージョンで許可するIKEポリシーを有効にします。

a) オブジェクト テーブル上部の [IKEv1] または [IKEv2] を選択すると、そのバージョンのポリシーが表示されます。

- b) 適切なオブジェクトを有効にし、要件を満たしていないオブジェクトを無効にするには、[状態 (State)] トグルをクリックします。

セキュリティ要件の一部が既存のオブジェクトに反映されていない場合、要件に合う新しい要件を定義します。詳細については、次のトピックを参照してください。

- [IKEv1 ポリシーの設定 \(404 ページ\)](#)
- [IKEv2 ポリシーの設定 \(406 ページ\)](#)

- c) 相対的な優先順位が要件を満たすことを確認します。

ポリシーの優先順位を変更する必要がある場合は編集します。ポリシーが事前定義されたシステムポリシーである場合、優先順位を変更するための独自のバージョンのポリシーを作成する必要があります。

優先順位は相対的であり、絶対的ではありません。たとえば、優先順位 80 は 160 より優先されます。80 が最も優先順位の高い有効なオブジェクトである場合、これが最初を選択されるポリシーとなります。その後、優先順位が 25 のポリシーを有効にすると、それが最初を選択されるポリシーとなります。

- d) 両方の IKE バージョンを使用する場合、このプロセスを他のバージョンでも繰り返します。

IKEv1 ポリシーの設定

インターネット キー エクスチェンジ (IKE) バージョン 1 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv1 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション (SA) の自動確立に使用されます。

複数の事前定義された IKEv1 ポリシーが存在します。必要に適したポリシーがあれば、[状態 (State)] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。IKEv1 設定の編集時に、オブジェクトリストに表示される [新しいIKEポリシーの作成 (Create New IKE Policy)] リンクをクリックして、IKEv1 ポリシーを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [IKEポリシー (IKE Policies)] を選択します。

ステップ 2 IKEv1 ポリシーを表示するには、オブジェクトテーブル上部の [IKEv1] を選択します。

ステップ3 システム定義ポリシーのいずれかが要件を満たす場合には、[状態 (State)] トグルをクリックして有効にします。

不要なポリシーを無効にする場合にも、[状態 (State)] トグルを使用します。番号が小さい方が高い優先順位を持つ相対的な優先順位により、どのポリシーが最初に試行されるかが決定されます。

ステップ4 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ5 IKEv1 プロパティを設定します。

- [優先順位 (Priority)] : IKE ポリシーの相対的優先度 (1 ~ 65,535)。このプライオリティによって、共通のセキュリティアソシエーション (SA) の検出試行時に、ネゴシエーションする2つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [名前 (Name)] : オブジェクトの名前 (最大 128 文字)。
- [状態 (State)] : IKE ポリシーが有効か無効かを示します。トグルをクリックして状態を変更します。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [認証 (Authentication)] : 2つのピア間で使用される認証方式。
 - [事前共有キー (Preshared Key)] : 各デバイスで定義されている事前共有キーを使用します。これらのキーを使用すると、秘密鍵を2つのピア間で共有し、認証フェーズ中に IKE で使用できます。ピアに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
- [暗号化 (Encryption)] : フェーズ2ネゴシエーションを保護するためのフェーズ1セキュリティアソシエーション (SA) の確立に使用される暗号化アルゴリズム。オプションの説明については、[使用する暗号化アルゴリズムの決定 \(395 ページ\)](#) を参照してください。
- [Diffie-Hellmanグループ (Diffie-Hellman Group)] : 2つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。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。2つのピアに、一致する係数グループが設定されている必要があります。オプションの説明については、[使用する Diffie-Hellman 係数グループの決定 \(397 ページ\)](#) を参照してください。
- [ハッシュ (Hash)] : メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュアルゴリズム。オプションの説明については、[使用するハッシュアルゴリズムの決定 \(396 ページ\)](#) を参照してください。

- [有効期間 (Lifetime)] : セキュリティアソシエーション (SA) のライフタイム (120～2147483647 までの秒数、または空白)。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティアソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません (フィールドを空白のままにします)。

ステップ 6 [OK] をクリックして変更を保存します。

IKEv2 ポリシーの設定

インターネットキーエクスチェンジ (IKE) バージョン 2 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv2 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティアソシエーション (SA) の自動確立に使用されます。

複数の事前定義された IKEv2 ポリシーがあります。必要に適したポリシーがあれば、[状態 (State)] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。IKEv2 設定の編集時に、オブジェクトリストに表示される [新しいIKEポリシー] の作成 (Create New IKE Policy) リンクをクリックして、IKEv2 ポリシーを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [IKEポリシー (IKE Policies)] を選択します。

ステップ 2 IKEv2 ポリシーを表示するには、オブジェクトテーブル上部の [IKEv2] を選択します。

ステップ 3 システム定義ポリシーのいずれかが要件を満たす場合には、[状態 (State)] トグルをクリックして有効にします。

不要なポリシーを無効にする場合にも、[状態 (State)] トグルを使用します。番号が小さい方が高い優先順位を持つ相対的な優先順位により、どのポリシーが最初に試行されるかが決定されます。

ステップ 4 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 5 IKEv2 プロパティを設定します。

- [優先順位 (Priority)] : IKE ポリシーの相対的優先度 (1 ~ 65,535)。このプライオリティによって、共通のセキュリティアソシエーション (SA) の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [名前 (Name)] : オブジェクトの名前 (最大 128 文字)。
- [状態 (State)] : IKE ポリシーが有効か無効かを示します。トグルをクリックして状態を変更します。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [暗号化 (Encryption)] : フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティアソシエーション (SA) の確立に使用される暗号化アルゴリズム。有効にするすべてのアルゴリズムを選択します。ただし、同じポリシーに混合モード (AES-GCM) と通常モードのオプションを含めることはできません (通常モードには整合性ハッシュの選択が必要ですが、混合モードは個別の整合性ハッシュの選択を無効化します)。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、[使用する暗号化アルゴリズムの決定 \(395 ページ\)](#) を参照してください。
- [Diffie-Hellman グループ (Diffie-Hellman Group)] : 2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。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。2 つのピアに、一致する係数グループが設定されている必要があります。許可するすべてのアルゴリズムを選択します。システムは、最も強いグループから始めて最も弱いグループに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、[使用する Diffie-Hellman 係数グループの決定 \(397 ページ\)](#) を参照してください。
- [整合性ハッシュ (Integrity Hash)] : メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュアルゴリズムの整合性部分。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。整合性ハッシュは、AES-GCM 暗号化オプションでは使用されません。オプションの説明については、[使用するハッシュアルゴリズムの決定 \(396 ページ\)](#) を参照してください。
- [擬似ランダム関数 (PRF) ハッシュ (Pseudo Random Function (PRF) Hash)] : IKEv2 トンネル暗号化に必要なキー材料とハッシュ操作を得るためのアルゴリズムとして使用されるハッシュアルゴリズムの擬似ランダム関数 (PRF) 部分。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエ

エートします。オプションの説明については、[使用するハッシュアルゴリズムの決定 \(396 ページ\)](#) を参照してください。

- [有効期間 (Lifetime)] : セキュリティアソシエーション (SA) のライフタイム (120～2147483647 までの秒数、または空白)。このライフタイムを超えると、SA の期限が切れ、2つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKEネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後のIPsecセキュリティアソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは86400です。無期限のライフタイムを指定するには、値を入力しません (フィールドを空白のままにします)。

ステップ 6 [OK] をクリックして変更を保存します。

IPsec プロポーザルの設定

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケットレベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、トランスフォームセットと呼ばれるセキュリティプロトコルとアルゴリズムの組み合わせによって保護されます。IPsec Security Association (SA : セキュリティアソシエーション) のネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォームセットが検索されます。

IKE バージョン (IKEv1 または IKEv2) に基づいて、別個の IPsec プロポーザルオブジェクトがあります。

- IKEv1 IPsec プロポーザルを作成する場合、IPsec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザルオブジェクトを作成して選択します。
- IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュアルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

カプセル化セキュリティプロトコル (ESP) は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。これは認証、暗号化、およびアンチリプレイサービスを提供します。ESP は、IP プロトコル タイプ 50 です。



(注) IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

次に、各 IKE バージョンの IPsec プロポーザルの設定方法を説明します。

IKEv1 の IPsec プロポーザルの設定

IKEv1 IPsec プロポーザル オブジェクトを使用して、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル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組み合わせを定義します。

定義済みの複数の IKEv1 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト (Objects)] ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv1 IPsec 設定を編集している間に、オブジェクトリストに表示される [新規 IPsec プロポーザルの作成 (Create New IPsec Proposal)] リンクをクリックして、IKEv1 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト (Objects)] を選択し、目次から [IPsec プロポーザル (IPsec Proposals)] を選択します。

ステップ 2 オブジェクト テーブルの上にある [IKEv1] を選択して、IKEv1 IPsec プロポーザルを表示します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 4 IKEv1 IPsec プロポーザルのプロパティを設定します。

- [名前 (Name)] : オブジェクトの名前 (最大 128 文字)。
- [モード (Mode)] : IPsec トンネルが動作するモード。
 - [トンネル (Tunnel)] モード : IP パケット全体がカプセル化されます。IPsec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイ

アウォール（またはその他のセキュリティゲートウェイ）間で通常の IPsec が実装される標準の方法です。

- [トランスポート (Transport)]モード：IP パケットの上位層プロトコルだけがカプセル化されます。IPsec ヘッダーは、IP ヘッダーと上位層プロトコルヘッダー（TCP など）との間に挿入されます。トランスポートモードでは、送信元ホストと宛先ホストの両方が IPsec をサポートしている必要があります。また、トランスポートモードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポートモードは、レイヤ2 またはレイヤ3 のトンネリングプロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。
- [ESP暗号化 (ESP Encryption)]：この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。オプションの説明については、[使用する暗号化アルゴリズムの決定 \(395 ページ\)](#) を参照してください。
- [ESPハッシュ (ESP Hash)]：認証に使用するハッシュまたは整合性アルゴリズム。オプションの説明については、[使用するハッシュアルゴリズムの決定 \(396 ページ\)](#) を参照してください。

ステップ 5 [OK] をクリックして変更を保存します。

IKEv2 の IPsec プロポーザルの設定

IKEv2 IPsec プロポーザル オブジェクトを使用して、IKE フェーズ2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル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組み合わせを定義します。

定義済みの複数の IKEv2 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトの編集や削除はできません。

次の手順では、[オブジェクト (Objects)]ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv2 IPsec 設定を編集している間に、オブジェクトリストに表示される [新規IPsecプロポーザルの作成 (Create New IPsec Proposal)]リンクをクリックして、IKEv2 IPsec プロポーザル オブジェクトを作成することもできます。

手順

- ステップ 1** [オブジェクト (Objects)] を選択し、目次から [IPsecプロポーザル (IPsec Proposals)] を選択します。
- ステップ 2** オブジェクトテーブルの上にある [IKEv2] を選択して、IKEv2 IPsec プロポーザルを表示します。
- ステップ 3** 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 4 IKEv2 IPsec プロポーザルのプロパティを設定します。

- [名前 (Name)] : オブジェクトの名前 (最大 128 文字) 。
- [暗号化 (Encryption)] : この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。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、[使用する暗号化アルゴリズムの決定 \(395 ページ\)](#) を参照してください。
- [整合性ハッシュ (Integrity Hash)] : 認証に使用するハッシュまたは整合性アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、[使用するハッシュアルゴリズムの決定 \(396 ページ\)](#) を参照してください。

(注) 暗号化アルゴリズムとしていずれかの AES-GCM/GMAC オプションを選択する場合は、ヌル整合性アルゴリズムを選択する必要があります。これらの暗号化基準では、ヌル以外のオプションを選択している場合でも、整合性ハッシュは使用されません。

ステップ 5 [OK] をクリックして変更を保存します。

サイト間 VPN 接続の確認

サイト間 VPN 接続を設定し、設定をデバイスに展開した後で、システムがリモートデバイスとのセキュリティ アソシエーションを確立することを確認します。

接続を確立できない場合は、デバイス CLI から `ping interface interface_name remote_ip_address` コマンドを使用して、VPN インターフェイスを介したリモートデバイスへのパスが存在することを確認します。設定したインターフェイスを介した接続が存在しない場合は、`interface interface_name` キーワードをオフにしたまま、接続が別のインターフェイスを介していないかどうかを判別します。接続に対して間違ったインターフェイスが選択されている可能性があります。保護されたネットワークに面したインターフェイスではなく、リモートデバイスに面したインターフェイスを選択する必要があります。

ネットワークパスが存在する場合は、両方のエンドポイントで設定およびサポートされている IKE バージョンとキーを確認し、必要に応じて VPN 接続を調整します。アクセス制御または NAT ルールが接続をブロックしていないことを確認します。

手順

ステップ1 デバイス CLI にログインします (CLI (コマンドラインインターフェイス) へのログイン (15 ページ) を参照)。

ステップ2 `show ipsec sa` コマンドを使用して、IPsec セキュリティ アソシエーションが確立されていることを確認します。

ご使用のデバイス (`local addr`) とリモートピア (`current_peer`) の間に VPN 接続が確立されているはずです。その接続を介してトラフィックを送信すると、パケット (`pkts`) 数が増加します。アクセスリストには、接続のローカルネットワークおよびリモートネットワークが表示されます。

たとえば、次の出力は、IKEv2 接続を示しています。

```
> show ipsec sa
interface: site-a-outside
  Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

  access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer: 192.168.4.6

  #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
  #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
  path mtu 1500, ipsec overhead 55(36), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: CD22739C
  current inbound spi : 52D2F1E4

inbound esp sas:
  spi: 0x52D2F1E4 (1389556196)
    SA State: active
    transform: esp-aes-gcm-256 esp-null-hmac no compression
    in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
    slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
    sa timing: remaining key lifetime (kB/sec): (4285434/28730)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xCD22739C (3441587100)
    SA State: active
    transform: esp-aes-gcm-256 esp-null-hmac no compression
    in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
```

```

slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
sa timing: remaining key lifetime (kB/sec): (4055034/28730)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

次の出力は、IKEv1 接続を示しています。

```

> show ipsec sa
interface: site-a-outside
Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 192.168.4.6

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 077D72C9
current inbound spi : AC146DEC

inbound esp sas:
spi: 0xAC146DEC (2887020012)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
sa timing: remaining key lifetime (kB/sec): (3914999/28567)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000007FF
outbound esp sas:
spi: 0x077D72C9 (125661897)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
sa timing: remaining key lifetime (kB/sec): (3914999/28567)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

ステップ 3 `show isakmp sa` コマンドを使用して、IKE セキュリティ アソシエーションを確認します。

sa キーワードを使用せずに（または代わりに **stats** キーワードを使用して）このコマンドを使用すると、IKE 統計情報が表示されます。

たとえば、次の出力は、IKEv2 セキュリティアソシエーションを示しています。

```
> show isakmp sa
```

```
There are no IKEv1 SAs
```

```
IKEv2 SAs:
```

```
Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote Status Role
592216161 192.168.2.15/500 192.168.4.6/500 READY INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify:
      PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector 192.168.1.0/0 - 192.168.1.255/65535
      remote selector 192.168.3.0/0 - 192.168.3.255/65535
      ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

次の出力は、IKEv1 セキュリティアソシエーションを示しています。

```
> show isakmp sa
```

```
IKEv1 SAs:
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 192.168.4.6
  Type : L2L Role : initiator
  Rekey : no State : MM_ACTIVE
```

```
There are no IKEv2 SAs
```

サイト間 VPN のモニタリング

サイト間 VPN 接続をモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。

- **show ipsec sa** は VPN セッション（セキュリティアソシエーション）を表示します。これらの統計情報は **clear ipsec sa counters** コマンドを使用してリセットできます。
- **show ipsec keyword** は IPsec 運用データおよび統計情報を表示します。**show ipsec ?** と入力し、使用可能なキーワードを確認します。
- **show isakmp** は ISAKMP 運用データおよび統計情報を表示します。

サイト間 VPN の例

以下に、サイト間 VPN を設定する例を示します。

NAT からのサイト間 VPN トラフィックの除外

インターフェイスでサイト間 VPN 接続が定義されていて、かつそのインターフェイス向けの NAT ルールを指定している場合、NAT ルールから VPN 上のトラフィックを任意で除外できます。この操作は、VPN 接続のリモート エンドが内部アドレスを処理できる場合に行うと便利です。

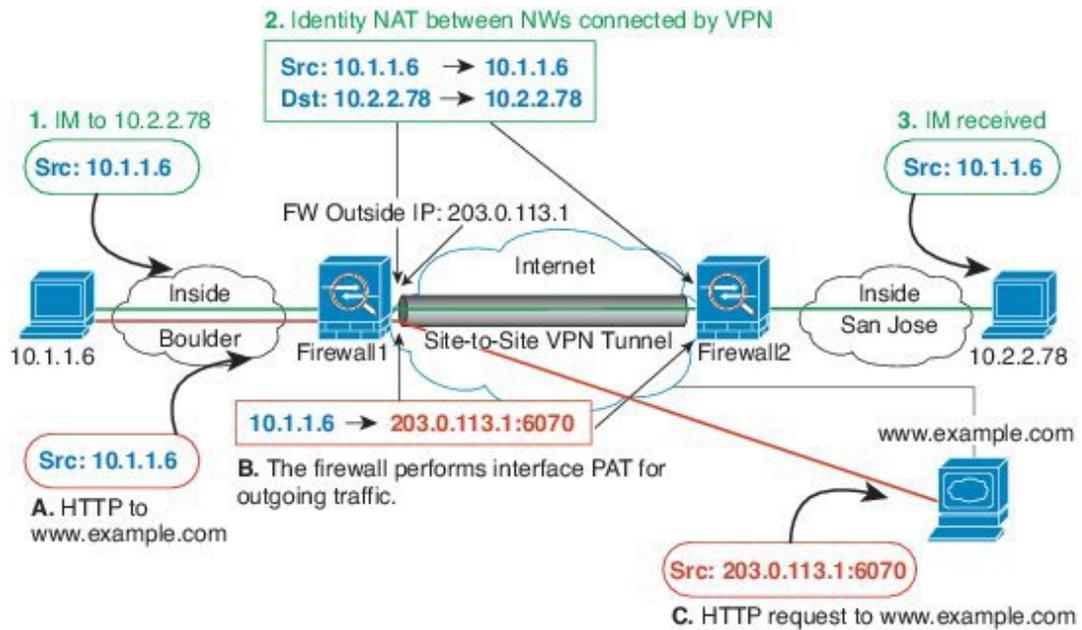
VPN 接続を作成するときに、[NATを除外 (NAT Exempt)] オプションを選択すると、ルールが自動的に作成されます。ただし、これはローカルで保護されたネットワークが単一のルーテッドインターフェイス (ブリッジグループメンバーではない) を介して接続されている場合のみ動作します。その代わりに、接続内のローカル ネットワークが複数のルーテッドインターフェイス、または 1 つ以上のブリッジグループメンバーの背後に存在する場合、NAT 免除ルールを手動で設定する必要があります。

NAT ルールから VPN トラフィックを除外するには、宛先がリモート ネットワークのときにローカルトラフィックの手動アイデンティティ NAT ルールを作成します。次に、任意の宛先 (インターネットなど) のトラフィックに NAT を適用します。ローカル ネットワークに複数のインターフェイスがある場合、各インターフェイスにルールを作成します。次の点も考慮してください。

- 接続内に複数のローカルネットワークがある場合、ネットワークを定義するオブジェクトを保持するネットワーク オブジェクト グループを作成します。
- VPN に IPv4 ネットワークと IPv6 ネットワークの両方を含める場合、それぞれに個別のアイデンティティ NAT ルールを作成します。

次の例では、ボールダーとサンノゼのオフィスを接続するサイトツーサイトトンネルを示します。インターネットに渡すトラフィックについて (たとえばボールダーの 10.1.1.6 から www.example.com へ)、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては (たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ)、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 20: サイトツーサイト VPNのためのインターフェイス PAT およびアイデンティティ NAT



次の例は、Firewall1（ボールドー）の設定を示します。例では、内部インターフェイスがブリッジグループであると仮定するため、各メンバーインターフェイスにルールを記述する必要があります。ルーティングされた内部インターフェイスが1つある場合も複数ある場合も、プロセスは同じです。

(注) この例では、IPv4のみと仮定します。VPNにIPv6ネットワークも含まれる場合、IPv6にはパラレルルールを作成します。IPv6インターフェイスPATは実装できないため、PATを使用するには固有のIPv6アドレスを持つホストオブジェクトを作成する必要があることに注意してください。

手順

ステップ 1 さまざまなネットワークを定義するには、オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- ネットワーク内でボールドーを特定します。

ネットワーク オブジェクトに名前を付け (boulder-network など)、[ネットワーク (Network)] を選択して、ネットワーク アドレス 10.1.1.0/24 を入力します。

Add Network Object

Name
boulder-network

Description

Type
 Network Host

Network
10.1.1.0/24

- d) [OK] をクリックします。
- e) [+] をクリックしてサンノゼの内部ネットワークを定義します。

ネットワーク オブジェクトに名前を付け (sanjose-network など)、[ネットワーク (Network)] を選択して、ネットワーク アドレス 10.2.2.0/24 を入力します。

Add Network Object

Name
sanjose-network

Description

Type
 Network Host

Network
10.2.2.0/24

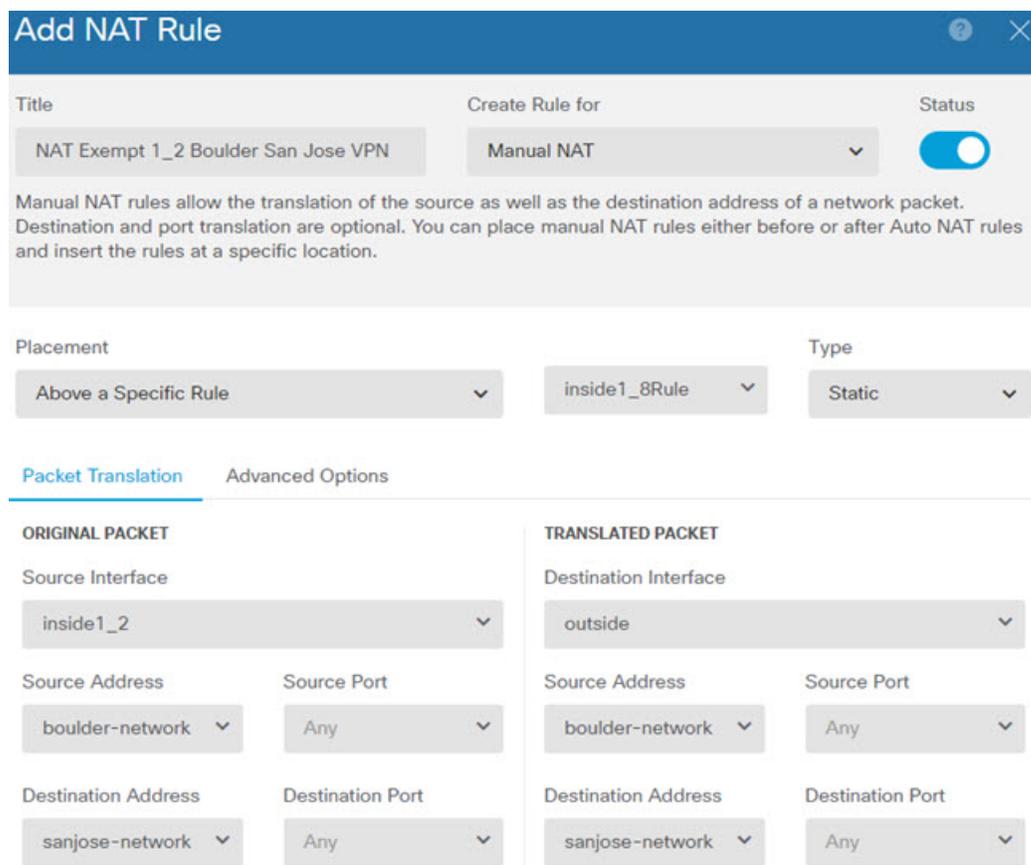
- f) [OK] をクリックします。

ステップ 2 Firewall1 (ボールダー) 上で VPN 経由でサンノゼに向かう場合、ボールダー ネットワークの手動アイデンティティ NAT を設定します。

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。

- [タイトル (Title)] = NAT Exempt 1_2 Boulder San Jose VPN (または別の名前)。
- [ルールの作成対象 (Create Rule For)] = 手動 NAT (Manual NAT)。
- [配置 (Placement)] = [特定のルールの上 (Above a Specific Rule)]。 [自動NATの前に手動NAT (Manual NAT Before Auto NAT)] セクションの最初のルールを選択します。このルールが、宛先インターフェイスの一般的なインターフェイス PAT ルールの前に来ていることを確認してください。そうでないと、ルールが正しいトラフィックに適用されない場合があります。
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = inside1_2。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元の発信元アドレス (Original Source Address)] = boulder-network のネットワーク オブジェクト (boulder-network network object)。
- [変換済みの発信元アドレス (Translated Source Address)] = boulder-network のネットワーク オブジェクト (boulder-network network object)。
- [元の宛先アドレス (Original Destination Address)] = sanjose-network のネットワーク オブジェクト (sanjose-network network object)。
- [変換済みの宛先アドレス (Translated Destination Address)] = sanjose-network のネットワーク オブジェクト (sanjose-network network object)。

(注) 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート (Port)] フィールドはすべて空白のままにします。このルールは、送信元と宛先の両方のアイデンティティ NAT を設定します。



- d) [詳細 (Advanced)] タブで [宛先インターフェイスでプロキシARPなし (Do not proxy ARP on Destination interface)] を選択します。
- e) [OK] をクリックします。
- f) 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 3 Firewall1 (ボールダー) 上でボールダーの内部ネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。

(注) これらは初期設定時にデフォルトで作成されるため、内部インターフェイスにはすでに IPv4 トラフィックをカバーするダイナミック インターフェイス PAT ルールがある可能性があります。ただし、この設定は説明を完結させるために示しています。この手順を完了する前に、内部インターフェイスとネットワークをカバーするルールがすでに存在していることを確認して、存在している場合はこの手順をスキップしてください。

- a) [+] ボタンをクリックします。
- b) 次のプロパティを設定します。
 - [タイトル (Title)] = inside1_2 インターフェイス PAT (または任意の別の名前) 。
 - [ルールの作成対象 (Create Rule For)] = 手動 NAT (Manual NAT) 。

- [配置 (Placement)] = [特定のルールの下 (Below a Specific Rule)]。 [自動NATの前に手動NAT (Manual NAT Before Auto NAT)] セクションで、このインターフェイスのために先に作成したルールを選択します。このルールは任意の宛先アドレスに適用されるため、 sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、 sanjose-network ルールは永遠に一致することがありません。デフォルトでは、新しい手動 NAT ルールは [自動NATの前にNATルール (NAT Rules Before Auto NAT)] セクションの最後に配置されますが、これでも問題ありません。
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = inside1_2。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元の発信元アドレス (Original Source Address)] = boulder-network のネットワーク オブジェクト (boulder-network network object) 。
- [変換済み発信元アドレス (Translated Source Address)] = [インターフェイス (Interface)]。このオプションは、宛先インターフェイスを使用するインターフェイス PAT を設定します。
- [元の宛先アドレス (Original Destination Address)] = 任意 (any) 。
- [変換済みの宛先アドレス (Original Destination Address)] = 任意 (any) 。

- c) [OK] をクリックします。
- d) 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 4 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

ステップ 5 Firewall2 (サンノゼ) の管理を行っている場合、そのデバイスに同様のルールを設定できます。

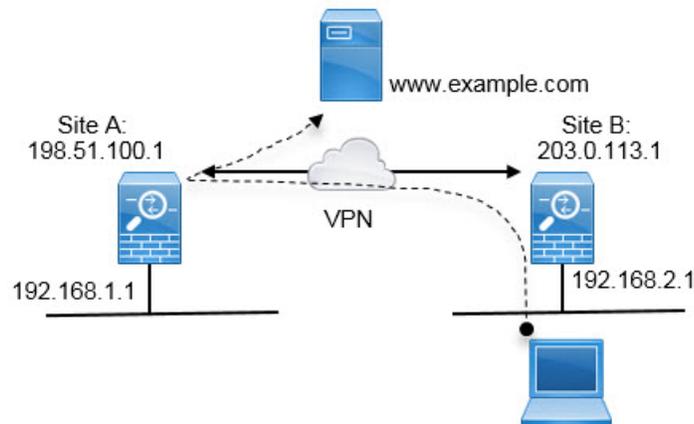
- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイスオブジェクトを作成します。

- 手動ダイナミックインターフェイスPATルールは、宛先が「任意」の場合は sanjose-network 向けになります。

外部インターフェイスで外部のサイト間VPNユーザにインターネットアクセスを提供する方法 (ヘア ピニング)

サイト間VPNでは、リモートネットワーク上のユーザに自分のデバイスを介してインターネットにアクセスさせたい場合があります。ただし、インターネットに接続している同一インターフェイス (外部インターフェイス) 上のデバイスにリモートユーザがアクセスしているため、インターネットトラフィックが外部インターフェイスの外側からそのまま返される必要があります。この手法はヘア ピニングと呼ばれる場合もあります。

次の図は例を示しています。198.51.100.1 (メインサイトのサイト A) と 203.0.113.1 (リモートサイトのサイト B) 間にサイト間VPNトンネルが設定されています。リモートサイトの内部ネットワーク (192.168.2.0/24) からのユーザトラフィックはすべてVPNを通過します。そのため、内部ネットワークのユーザがインターネット上のサーバ (www.example.com など) にアクセスする場合、接続は最初にVPNを通過し、その後198.51.100.1インターフェイスからインターネットにルートバックされます。



次の手順では、このサービスの設定方法について説明します。VPNトンネルの両方のエンドポイントを設定する必要があります。

手順

ステップ 1 (サイト A、メイン サイト) リモートサイト B へのサイト間 VPN 接続を設定します。

- [デバイス (Device)] をクリックし、[サイト間VPN (Site-to-Site VPN)] グループで [設定の表示 (View Configuration)] をクリックします。
- [+] をクリックして新しい接続を追加します。
- 次のようにエンドポイントを定義し、[次へ (Next)] をクリックします。

- [接続プロファイル名 (Connection Profile Name)] : わかりやすい接続の名前を付けます。例、Connection Profile Name。
- [ローカルVPNアクセスインターフェイス (Local VPN Access Interface)] : 外部インターフェイスを選択します。
- [ローカルネットワーク (Local Network)] : デフォルトの [任意 (Any)] のままにします。
- [リモートIPアドレス (Remote IP Address)] : リモートピアの外部インターフェイスの IP アドレスを入力します。この例では、203.0.113.1 です。
- [リモートネットワーク (Remote Network)] : [+] をクリックして、リモートピアの保護ネットワークを定義するネットワーク オブジェクトを選択します。この例では 192.168.2.0/24 です。[ネットワークの新規作成 (Create New Network)] をクリックしてすぐにオブジェクトを作成できます。

次に、最初の手順の状況を図で示します。

Connection Profile Name

Site-A-to-Site-B

LOCAL SITE	REMOTE SITE
Local VPN Access Interface	Remote IP Address
outside	203.0.113.1
Local Network	Remote Network
+	+
ANY	Site-B-Network

d) プライバシー ポリシーを定義し、[次へ (Next)] をクリックします。

- [IKEポリシー (IKE Policy)] : IKE の設定はヘア ピニングに影響を与えません。セキュリティのニーズに合わせて IKE バージョン、ポリシー、およびプロポーザルを選択します。入力するローカルとリモートの事前共有キーはメモしてください。リモートピアの設定時に必要になります。
- [NAT免除 (NAT Exempt)] : [内部 (inside)] インターフェイスを選択します。

Additional Options

NAT Exempt

inside

- [Perfect Forward SecrecyのDiffie Helmanグループ (Diffie Helman Group for Perfect Forward Secrecy)]: この設定はヘア ピニングに影響しません。必要に応じて設定します。

e) [終了 (Finish)] をクリックします。

接続の概要がクリップボードにコピーされます。接続の概要は、テキストファイルやその他のドキュメントに貼り付けて、リモートピアの設定に役立てることができます。

ステップ 2 (サイト A、メイン サイト) 外部インターフェイスから送信されたすべての接続を外部 IP アドレス (インターフェイス PAT) のポートに変換するよう NAT ルールを設定します。

デバイスの初期設定を完了すると、`InsideOutsideNatRule` という名前の NAT ルールが作成されます。このルールは、外部インターフェイス経由でデバイスを抜ける任意のインターフェイスから、インターフェイス PAT を IPv4 トラフィックに充当します。外部インターフェイスは「任意の」送信元インターフェイスに含まれるため、必要なルールは、編集または削除していない限り、すでに存在しています。

次の手順で、必要なルールを作成する方法を説明します。

a) [ポリシー (Policies)] > [NAT] をクリックします。

b) 次のいずれかを実行します。

- `InsideOutsideNatRule` を編集するには、[アクション (Action)] 列にマウス オーバーし、[編集 (edit)] アイコン () をクリックします。
- ルールを新規作成するには、[+] ボタンをクリックします。

c) 次のプロパティを使用してルールを設定します。

- [タイトル (Title)]: 新しいルールのわかりやすい名前をスペースを含めず入力します。たとえば、`OutsideInterfacePAT` と入力します。
- [ルールの作成先 (Create Rule For)]: [手動NAT (Manual NAT)]。
- [配置 (Placement)]: [自動NATルールの前 (Before Auto NAT Rules)] (デフォルト)。
- [タイプ (Type)]: [ダイナミック (Dynamic)]。
- [元の packets (Original Packet)]: [送信元アドレス (Source Address)] で [任意 (Any)] または [any-ipv4] を選択します。[送信元インターフェイス (Source Interface)] で、[任意 (Any)] (デフォルト) を選択していることを確認します。[元の packets (Original Packet)] の他のすべてのオプションは、デフォルトの [任意 (Any)] のままにします。
- [変換後の packets (Translated Packet)]: [宛先インターフェイス (Destination Interface)] で、[外部 (outside)] を選択します。[変換後のアドレス (Translated Address)] で、[インターフェイス (Interface)] を選択します。[変換後の packets (Translated Packet)] の他のすべてのオプションは、デフォルトの [任意 (Any)] のままにします。

次の図は、発信元アドレスに [任意 (Any)] を選択したシンプルな例を示しています。

The screenshot shows the configuration for a NAT rule. Key elements circled in red include:

- Create Rule for:** Manual NAT
- Placement:** Before Auto NAT Rules
- Type:** Dynamic
- ORIGINAL PACKET Source Interface:** Any
- ORIGINAL PACKET Source Address:** Any
- TRANSLATED PACKET Destination Interface:** outside
- TRANSLATED PACKET Source Address:** Interface

d) [OK] をクリックします。

ステップ 3 (サイト A、メインサイト) 変更を保存します。

a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

ステップ 4 (サイト B、リモートサイト) リモートサイトのデバイスにログインし、サイト A へのサイト間 VPN 接続を設定します。

サイト A のデバイス設定から取得した接続の概要を使用して、サイト B 側の接続を設定します。

- a) [デバイス (Device)] をクリックし、[サイト間VPN (Site-to-Site VPN)] グループで [設定の表示 (View Configuration)] をクリックします。
- b) [+] をクリックして新しい接続を追加します。
- c) 次のようにエンドポイントを定義し、[次へ (Next)] をクリックします。

- [接続プロファイル名 (Connection Profile Name)] : わかりやすい接続の名前を付けます。例、Site-B-to-Site-A。
- [ローカルVPNアクセスインターフェイス (Local VPN Access Interface)] : 外部インターフェイスを選択します。
- [ローカルネットワーク (Local Network)] : [+] をクリックして、ローカルの保護ネットワークを定義するネットワークオブジェクトを選択します。この例では192.168.2.0/24です。[ネットワークの新規作成 (Create New Network)] をクリックしてすぐにオブジェクトを作成できます。
- [リモートIPアドレス (Remote IP Address)] : メインサイトの外部インターフェイスの IP アドレスを入力します。この例では、198.51.100.1 です。
- [リモートネットワーク (Remote Network)] : デフォルトの[任意 (Any)] のままにします。警告は無視します。この使用例には関係ありません。

次に、最初の手順の状況を図で示します。

Connection Profile Name

Site-B-to-Site-A

LOCAL SITE	REMOTE SITE
Local VPN Access Interface	Remote IP Address
outside	198.51.100.1
Local Network	Remote Network
ProtectedNetwork	<p>i We don't recommend to use "ANY" for this option.</p>
	ANY

d) プライバシー ポリシーを定義し、[次へ (Next)] をクリックします。

- [IKEポリシー (IKE Policy)] : IKE の設定はヘア ピニングに影響を与えません。サイト A の VPN 接続の終端と同じオプションまたは互換性のあるオプションを設定します。事前共有キーは正しく設定する必要があります。サイト A デバイスに設定されている (IKEv2 の) ローカルキーとリモートキーを切り替えます。IKEv1 の場合、キーは1つだけで、両方のピアで同一である必要があります。
- [NAT免除 (NAT Exempt)] : [内部 (inside)] インターフェイスを選択します。

Additional Options

NAT Exempt

inside

- [Perfect Forward SecrecyのDiffie Helmanグループ (Diffie Helman Group for Perfect Forward Secrecy)]: この設定はヘア ピニングに影響しません。サイト A の VPN 接続の終端で使用されている設定と照合します。

e) [終了 (Finish)] をクリックします。

ステップ 5 (サイト B、リモートサイト) 保護ネットワークのすべての NAT ルールを削除し、そのサイトからのトラフィックがすべて VPN トンネルを通過するようにします。

サイト A のデバイスではアドレス変換が行われるため、このデバイスで NAT を実行する必要はありません。ただし、個別の状況を確認してください。複数の内部ネットワークがあり、そのすべてがこの VPN 接続に参加しているわけではない場合は、それらのネットワークに必要な NAT ルールを削除しないでください。

a) [ポリシー (Policies)] > [NAT] をクリックします。

b) 次のいずれかを実行します。

- ルールを削除するには、[アクション (Action)] 列にマウス オーバーして、[削除 (delete)] アイコン () をクリックします。
- ルールを編集して、保護ネットワークに適用されないようにするには、[アクション (Action)] 列にマウス オーバーして、[編集 (edit)] アイコン () をクリックします。

ステップ 6 (サイト B、リモートサイト) 変更を保存します。

a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



b) [今すぐ展開 (Deploy Now)] ボタンをクリックして、展開が完了するまで待ちます。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。



第 16 章

リモート アクセス VPN

リモートアクセス 仮想プライベート ネットワーク (VPN) では、各ユーザがインターネットに接続されたコンピュータまたはその他のサポート対象の iOS または Android デバイスを使用して、離れた場所からネットワークに接続できます。これにより、モバイルワーカーが各自のホーム ネットワークや公共の Wi-Fi ネットワークなどから接続できるようになります。

ここでは、ネットワークのリモート アクセス VPN を設定する方法について説明します。

- [リモート アクセス VPN の概要 \(429 ページ\)](#)
- [リモート アクセス VPN のライセンス要件 \(432 ページ\)](#)
- [リモート アクセス VPN に関する注意事項と制限事項 \(432 ページ\)](#)
- [リモート アクセス VPN の設定 \(432 ページ\)](#)
- [リモート アクセス VPN のモニタリング \(443 ページ\)](#)
- [リモート アクセス VPN のトラブルシューティング \(443 ページ\)](#)
- [リモート アクセス VPN の例 \(446 ページ\)](#)

リモート アクセス VPN の概要

Firepower Device Manager では、AnyConnect クライアント ソフトウェアを使用して SSL 経由でリモート アクセス VPN を設定できます。

AnyConnect クライアントが Firepower Threat Defense デバイスと SSL VPN 接続をネゴシエートする際、Transport Layer Security (TLS) または Datagram Transport Layer Security (DTLS) を使用して接続します。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。クライアントおよび Firepower Threat Defense デバイスは、使用する TLS/DTLS パーティションをネゴシエートします。DTLS はクライアントがサポートする場合に使用されます。

デバイス モデル別の同時 VPN セッションの最大数

デバイス モデルに基づいて、1 台のデバイスで許可される同時リモート アクセス VPN セッション数に上限が設けられます。この制限は、システムパフォーマンスが許容できないレベルに低

下しないように設計されています。これらの制限は、キャパシティプランニングに使用します。

デバイス モデル	最大同時リモート アクセス VPN セッション数
ASA 5506-X、5506H-X、5506W-X	50
ASA 5508-X	100
ASA 5512-X、ASA 5515-X	250
ASA 5516-X	300
ASA 5525-X	750
ASA 5545-X	2500
ASA 5555-X	5000
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Firepower Threat Defense Virtual	250
ISA 3000	25

AnyConnect クライアントソフトウェアのダウンロード

リモートアクセスVPNを設定するには、AnyConnectソフトウェアをワークステーションにダウンロードする必要があります。VPNを定義するときに、これらのパッケージをアップロードする必要があります。

最新の機能、バグ修正、セキュリティパッチを確保するには、最新のAnyConnectバージョンをダウンロードする必要があります。Firepower Threat Defense デバイスのパッケージは定期的に更新してください。



(注) Windows、Mac、Linux の各オペレーティングシステムごとに1つのAnyConnectをアップロードできます。1つのOSタイプに対して複数のバージョンをアップロードすることはできません。

AnyConnectソフトウェアパッケージは、software.cisco.com のAnyConnectセキュアモビリティクライアントカテゴリから取得します。クライアントの「フルインストールパッケージ」バージョンをダウンロードしてください。

AnyConnect ソフトウェアのインストール方法

VPN 接続を完了するには、ユーザは AnyConnect クライアント ソフトウェアをインストールする必要があります。既存のソフトウェア配布方式を使用して、ソフトウェアを直接インストールできます。または、ユーザに Firepower Threat Defense デバイスから AnyConnect クライアントを直接インストールしてもらうこともできます。

ソフトウェアをインストールするには、ユーザにワークステーションでの管理者権限が必要です。

AnyConnect クライアントがすでにインストールされている場合、新しい AnyConnect バージョンがアップロードされると、ユーザが次に VPN 接続を行った際、新しいバージョンが AnyConnect によって検出され、更新されたクライアント ソフトウェアのダウンロードとインストールを指示するメッセージが自動的に表示されます。この自動化により、ソフトウェアの配布が容易になります。

ソフトウェアの最初のインストールを Firepower Threat Defense デバイスからユーザに行ってもらう場合、以下の手順を実行するようにユーザに指示します。



(注) Android および iOS のユーザは、適切な App Store から AnyConnect をダウンロードする必要があります。

手順

ステップ 1 Web ブラウザを使用して、<https://ravpn-address> を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。

このインターフェイスは、リモートアクセス VPN を設定する際に指定します。ログインを指示するメッセージがユーザに示されます。

ステップ 2 サイトにログインします。

ユーザは、リモートアクセス VPN 用に設定されたディレクトリ サーバを使用して認証されます。続行するには、ログインが正常に行われる必要があります。

ログインが成功すると、システムは、必要となる AnyConnect クライアントのバージョンがインストールされているかを確認します。AnyConnect クライアントがユーザのコンピュータにないか、下位のバージョンである場合、システムは自動的に AnyConnect ソフトウェアのインストールを開始します。

インストールが終了すると、AnyConnect がリモートアクセス VPN 接続を完了します。

リモート アクセス VPN のライセンス要件

リモートアクセス VPN を設定する前に、基本デバイスライセンスがエクスポート要件を満たす必要があります。デバイスを登録するとき、エクスポート制御機能が有効になっている Smart Software Manager のアカウントを使用して登録する必要があります。また、評価ライセンスを使用して機能を設定することはできません。

さらに、次のいずれかのリモートアクセス VPN ライセンスを購入し、有効にする必要があります：AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only。これらのライセンスは、ASA ソフトウェア ベースのヘッドエンドで使用されるときにさまざまな機能セットを有効にするように設計されていますが、Firepower Threat Defense デバイスでは同じように扱われます。

ライセンスを有効にするには、[デバイス (Device)] > [スマートライセンス (Smart License)] > [設定の表示 (View Configuration)] を選択し、[RA VPN ライセンス (RA VPN License)] グループで適切なライセンスを選択します。Smart Software Manager Account で使用可能なライセンスが必要です。ライセンスの有効化の詳細については、[オプションライセンスの有効化と無効化 \(101 ページ\)](#) を参照してください。

詳細については、『Cisco AnyConnect Ordering Guide』 (<http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf>) を参照してください。<http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html> には、使用できるその他のデータシートもあります。

リモート アクセス VPN に関する注意事項と制限事項

RA VPN を設定する際は、次の注意事項と制限事項に注意してください。

- 同じ TCP ポートの同じインターフェイスで Firepower Device Manager アクセス (管理アクセスリストの HTTPS アクセス) と AnyConnect リモートアクセス SSL VPN の両方を設定することはできません。たとえば、外部インターフェイスにリモートアクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。Firepower Device Manager ではこれらの機能に使用されるポートを設定できないため、同じインターフェイスで両方の機能は設定できません。
- NAT ルールの送信元アドレスとリモートアクセス VPN アドレス プールの重複アドレスは使用できません。

リモート アクセス VPN の設定

クライアントのリモートアクセス VPN を有効化するには、いくつかの項目を設定する必要があります。次の手順を実行します。

手順

ステップ1 ライセンスを設定します。

次の2つのライセンスを有効にする必要があります。

- デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager アカウントによってエクスポートを制御する必要があります。リモートアクセス VPN を設定するには、その前に基本ライセンスが輸出規制要件を満たす必要があります。また、評価ライセンスを使用して機能を設定することはできません。デバイスを登録する手順については、[デバイスの登録 \(100 ページ\)](#) を参照してください。
- リモートアクセス VPN ライセンス。詳細は、[リモートアクセス VPN のライセンス要件 \(432 ページ\)](#) を参照してください。ライセンスを有効にするには、[オプションライセンスの有効化と無効化 \(101 ページ\)](#) を参照してください。

ステップ2 証明書を設定します。

証明書は、クライアントとデバイス間の SSL 接続を認証するために必要です。事前定義された VPN 用の DefaultInternalCertificate を使用することも、独自に作成することもできます。

認証に使われるディレクトリレルムに暗号化接続を使用する場合は、信頼される CA 証明書をアップロードする必要があります。

証明書とそれらのアップロード方法の詳細については、[証明書の設定 \(154 ページ\)](#) を参照してください。

ステップ3 (任意) クライアントプロファイルの設定およびアップロード (434 ページ)。

ステップ4 リモートユーザを認証する目的で使用されるアイデンティティレルムを設定します。AD アイデンティティレルムの設定 (143 ページ) を参照してください。

アイデンティティレルムは、ネットワークのユーザアカウントを格納するディレクトリサーバを定義します。

ステップ5 リモートアクセス VPN 接続の設定 (435 ページ)。

ステップ6 (オプション) リモートアクセス VPN グループによるリソースへのアクセスを制御する (439 ページ)。

すべてのリモートアクセスユーザにすべての内部リソースへの同じアクセスをさせない場合は、アクセス制御ルールを適用し、ユーザグループのメンバーシップに基づいてアクセスを許可または禁止できます。

ステップ7 リモートアクセス VPN 設定の確認 (441 ページ)。

接続の完了に関する問題が発生した場合は、[リモートアクセス VPN のトラブルシューティング \(443 ページ\)](#) を参照してください。

クライアントプロファイルの設定およびアップロード

AnyConnect クライアントプロファイルは AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルは、起動時の自動接続と自動再接続、エンドユーザが AnyConnect クライアント環境設定および詳細設定でオプションを変更することが許可されるかどうかといった、多数のクライアント関連オプションを定義します。

リモートアクセスVPN接続を設定する際に外部インターフェイスの完全修飾ホスト名 (FQDN) を設定すると、システムが自動的にクライアントプロファイルを作成します。このプロファイルでは、デフォルトの設定が有効にされます。クライアントプロファイルを作成してアップロードする必要があるのは、デフォルト以外の動作が必要な場合のみです。クライアントプロファイルはオプションであることに注意してください。クライアントプロファイルをアップロードしなければ、AnyConnect クライアントはプロファイルで制御されるすべてのオプションにデフォルトの設定を使用します。



- (注) 初回の接続時に、ユーザが制御できる設定のすべてを AnyConnect クライアントに表示させるには、VPNプロファイルのサーバリストに、Firepower Threat Defense デバイスの外部インターフェイスを含める必要があります。アドレスまたは FQDN をホストエントリとしてプロファイルに追加していない場合、セッションにフィルタは適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、プロファイルにデバイスをホストエントリとして追加しなければ、この証明書照合は無視されます。

次に、[オブジェクト (Objects)] ページで直接オブジェクトを作成および編集する方法について説明します。オブジェクトリストに表示される [新規 AnyConnect クライアントプロファイルの作成 (Create New AnyConnect Client Profile)] リンクをクリックして、AnyConnect クライアントプロファイルオブジェクトをプロファイルプロパティの編集集中に作成することもできます。

始める前に

クライアントプロファイルをアップロードするには、その前に、以下の作業を行う必要があります。

- AnyConnect の「Profile Editor - Windows / Standalone installer インストーラ (MSI)」をダウンロードしてインストールします。このインストールファイルは Windows 専用で、ファイル名は anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> は AnyConnect のバージョンです。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイルエディタをインストールする前に、Java JRE (1.6 以降) もインストールする必要があります。software.cisco.com から、[AnyConnect セキュアモビリティクライアント (AnyConnect Secure Mobility Client)] カテゴリに分類されている AnyConnect プロファイルエディタを入手します。
- プロファイルエディタを使用して、必要なプロファイルを作成します。プロファイルには、外部インターフェイスのホスト名または IP アドレスを指定する必要があります。詳細については、エディタのオンラインヘルプを参照してください。

手順

ステップ 1 [オブジェクト (Objects)] を選択してから、目次で [AnyConnectクライアントプロファイル (AnyConnect Client Profile)] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの[編集 (edit)] アイコン (🔗) をクリックします。
- オブジェクトに関連付けられているプロファイルをダウンロードする場合は、対象のオブジェクトの[ダウンロード (download)] アイコン (📄) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの[ごみ箱 (trash can)] アイコン (🗑️) をクリックします。

ステップ 3 名前を入力し、オプションでオブジェクトの説明を入力します。

ステップ 4 [アップロード (Upload)] をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 5 [開く (Open)] をクリックしてプロファイルをアップロードします。

ステップ 6 [OK] をクリックしてオブジェクトを追加します。

リモート アクセス VPN 接続の設定

リモートアクセスVPN接続を作成すると、ユーザがホームネットワークなどの外部ネットワークに接続しているときに、内部ネットワークに接続できるようになります。

始める前に

リモートアクセス (RA) VPN 接続を設定する前に、以下のことを行います。

- 必要な AnyConnect ソフトウェア パッケージを software.cisco.com からワークステーションにダウンロードします。
- 任意で、AnyConnect プロファイルエディタを使用してクライアント プロファイルを作成します。外部インターフェイスに完全修飾ドメイン名を指定すると、システムはデフォルトのプロファイルを作成します。クライアント プロファイルは任意で、プロファイルによって制御される機能をカスタマイズする場合にのみ作成します。
- リモートアクセス VPN 接続を終了する外部インターフェイスは、HTTPS 接続を許可する管理アクセス リストを持つこともできません。RA VPN を設定する前に、外部インターフェイスから HTTPS ルールを削除します。[管理アクセス リストの設定 \(475 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Device)] をクリックし、リモートアクセス VPN グループの [接続プロファイルの設定 (Setup Connection Profile)] をクリックします。

1 つのリモートアクセス VPN を設定できます。すでにこれを設定済みの場合は、[設定の表示 (View Configuration)] をクリックすると既存の VPN が開き、[編集 (Edit)] ボタンをクリックすると変更できます。

設定を削除するには、[設定の削除 (Clear Configuration)] をクリックします。

ステップ 2 AnyConnect クライアント設定を定義します。

- [接続プロファイル名 (Connection Profile Name)]: スペースを含めずに最大 50 文字で、この接続の名前を指定します。例、MainOffice。IP アドレスは名前として使用できません。
(注) ここで入力する名前が、AnyConnect クライアントの接続リストに表示されます。ユーザが理解しやすい名前を選択します。
- [ユーザ認証用ADレルム/ディレクトリサーバ (AD Realm/Directory Server for User Authentication)]: クライアント認証に使用するディレクトリサーバを定義するディレクトリレルム。VPN 接続を完了するには、このディレクトリサーバにエンドユーザを定義する必要があります。
- [フォールバックローカルアイデンティティソース (Fallback Local Identity Source)]: プライマリソースが外部サーバの場合、プライマリサーバが使用できない場合のフォールバックとして LocalIdentitySource を選択できます。フォールバックソースとしてローカルデータベースを使用する場合は、必ず外部サーバで定義したものと同一ローカルユーザ名/パスワードを定義します。
- [AnyConnectパッケージ (AnyConnect Packages)]: このVPN接続でサポートする AnyConnect の完全なインストールソフトウェアイメージ。パッケージごとに、ファイル名 (拡張子を含む) を 60 文字以下で指定します。Windows、Mac、Linux エンドポイント用に別々のパッケージをアップロードできます。

Software.cisco.com からパッケージをダウンロードします。エンドポイントに適切なパッケージがインストールされていない場合、ユーザは、ユーザ認証後にパッケージをダウンロードしてインストールするよう求められます。

ステップ 3 [次へ (Next)] をクリックします。

ステップ 4 デバイスのアイデンティティとクライアントアドレッシング設定を定義します。

- [デバイスアイデンティティ証明書 (Certificate of Device Identity)]: デバイスのアイデンティティを確立するために使用する内部証明書を選択します。安全なVPN接続を完了するには、クライアントがこの証明書を承認する必要があります。まだ証明書がない場合、ドロップダウンリストの [新規内部証明書の作成 (Create New Internal Certificate)] をクリックします。証明書を設定する必要があります。

- [外部インターフェイス (Outside Interface)] : リモートアクセス VPN 接続を確立するときにユーザが接続するインターフェイス。これは通常外部 (インターネットに接続された) インターフェイスですが、デバイスとこの接続プロファイルがサポートしているエンドユーザ間のインターフェイスのいずれかを選択します。
- [外部インターフェイス用完全修飾ドメイン名 (Fully-qualified Domain Name for the Outside Interface)] : インターフェイス名 (例 : ravpn.example.com) 。名前を指定すると、クライアントプロファイルが作成されます。

(注) ユーザは、クライアントによって VPN で使用される DNS サーバが、この名前から外部インターフェイスの IP アドレスを解決でききるようにする責任があります。関連する DNS サーバに FQDN を追加します。
- [IPv4、IPv6アドレスプール (IPv4, IPv6 Address Pools)] : これらのオプションはリモートエンドポイントのアドレス プールを定義します。クライアントには、VPN 接続のために使用する IP バージョンに基づき、これらのプールからアドレスが割り当てられます。サポートする IP タイプごとにサブネットを定義するネットワーク オブジェクトを選択します。その IP バージョンをサポートしない場合、[なし (None)] を選択 (または空白のままに) します。たとえば、IPv4 プールを「10.100.10.0/24」と定義できます。アドレスプールは、外部インターフェイスの IP アドレスと同じサブネット上に存在することはできません。
- [プライマリ、セカンダリDNSサーバ (Primary, Secondary DNS Servers)] : クライアントが VPN サーバに接続するときにドメイン名の解決に使用する DNS サーバ。[OpenDNS] ボタンをクリックし、これらのフィールドを OpenDNS パブリック DNS サーバにロードします。それ以外の場合、DNS サーバの IP アドレスを入力します。
- [ドメイン検索名 (Domain Search Name)] : ネットワークのドメイン名 (例 : example.com) を入力します。このドメインは、完全修飾されていないホスト名、たとえば serverA.example.com ではなく serverA に追加されます。

ステップ 5 [次へ (Next)] をクリックします。

ステップ 6 AnyConnect クライアントの動作をカスタマイズするため、接続設定を定義します。

- [認証されるクライアントのバナーテキスト (Banner Text for Authenticated Clients)] : (オプション) VPN セッションの始めにユーザに表示するメッセージを入力します。たとえば、適切な使用に関する法的免責事項や警告などです。バナーは最大 500 文字までですが、セミコロン (;) または HTML タグは使用できません。
- [最大接続時間 (Maximum Connection Time)] : ユーザがログアウト、再接続せずに VPN に接続したままにできる最大時間 (分) で、1 ~ 4473924 または空白で指定します。デフォルトは無制限 (空白) ですが、その場合でもアイドルタイムアウトは適用されます。
- [アイドルタイムアウト (Idle Timeout)] : VPN 接続が自動的に閉じられる前にアイドル状態になる時間 (分) で、1 ~ 35791394 で指定します。デフォルトは 30 分です。
- [VPNセッション中のブラウザプロキシ (Browser Proxy During VPN Sessions)] : Windows クライアントデバイス上の Internet Explorer Webブラウザで VPN セッション中にプロキシを使用するかどうか。次のオプションから選択します。

- [エンドポイント設定の変更なし (No change in endpoint settings)]: ユーザがブラウザプロキシを設定し (または設定しない) 、設定されている場合はそのプロキシを使用できるようにします。
- [ブラウザプロキシの無効化 (Disable browser proxy)]: ブラウザに定義されているプロキシ (ある場合) を使用しません。どのブラウザ接続もプロキシを経由しません。
- [自動検出設定 (Auto detect settings)]: ブラウザでの自動プロキシサーバ検出の使用を有効にします。
- [カスタム設定の使用 (Use custom settings)]: クライアントブラウザのプロキシを設定します。IP アドレスと、任意で HTTP プロキシサーバのポートを入力します (ホストとポートの合計は 100 文字を超えることはできません)。特定の Web サーバへの要求がプロキシを通ることを免除する場合、[プロキシ例外の追加 (Add Proxy Exception)] をクリックします (例外リストでのポートの指定は任意です)。すべてのアドレスとポートを合わせたプロキシ例外リスト全体で、255 文字を超えることはできません。
- [スプリットトンネリング (Split Tunneling)]: ユーザが安全な VPN トンネルを使用しているときに、ローカルネットワークまたはインターネットに直接アクセスできるようにするには、スプリット トンネリングを有効にします。VPN 接続をより安全にするには、スプリット トンネリングを無効のままにします。スプリット トンネリングを有効にする場合、[内部ネットワーク (Inside Networks)] リストで、リモートユーザがアクセスする内部ネットワークを表すネットワークオブジェクトも選択する必要があります。ネットワークリストには、サポートしているアドレスプールと同じ IP タイプを含める必要があります。指定されたネットワーク以外のネットワークでは、トラフィックを送信するためにユーザの ISP ゲートウェイが使用されます。
- [NAT免除 (NAT Exempt)]: リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を有効にします。VPN トラフィックを NAT 免除にしない場合は、外部および内部インターフェイスに対する既存の NAT ルールが RA VPN アドレスプールに適用されないことを確認してください。NAT 免除ルールは特定の送信元/宛先インターフェイスとネットワークの組み合わせに対する手動スタティックアイデンティティ NAT ルールですが、NAT ポリシーには反映されず、非表示になります。NAT 免除を有効にした場合、以下も設定する必要があります。
 - [内部インターフェイス (Inside Interfaces)]: リモートユーザがアクセスする内部ネットワークのインターフェイスを選択します。これらのインターフェイスに対して NAT ルールが作成されます。
 - [内部ネットワーク (Inside Networks)]: リモートユーザがアクセスする内部ネットワークを表すネットワークオブジェクトを選択します。ネットワークリストには、サポートしているアドレスプールと同じ IP タイプを含める必要があります。
- [AnyConnectクライアントプロファイル (AnyConnect Client Profiles)]: (オプション) 外部インターフェイスの完全修飾ドメイン名を設定すると、デフォルトプロファイルが自動的に作成されます。代わりに、自分用のクライアントプロファイルをアップロードすることもできます。スタンドアロン AnyConnect プロファイルエディタを使用してこれらのプ

ロファイルを作成します。スタンドアロン AnyConnect プロファイルエディタは、software.cisco.com からダウンロード、インストールできます。クライアントプロファイルを選択しない場合、AnyConnect クライアントはすべてのオプションにデフォルト値を使用します。このリストの項目は、プロファイル自体ではなく AnyConnect クライアントプロファイルオブジェクトです。新しいプロファイルを作成（およびアップロード）するには、ドロップダウンリストで [新規 AnyConnect クライアントプロファイルの作成 (Create New AnyConnect Client Profile)] をクリックします。

ステップ 7 [次へ (Next)] をクリックします。

ステップ 8 サマリーを確認します。

最初に、サマリーが正しいことを確認します。

次に、[手順 (Instructions)] をクリックし、AnyConnect ソフトウェアを最初にインストールし、VPN 接続が完了できることをテストするため、エンドユーザが何をやる必要があるかを確認します。[コピー (Copy)] をクリックしてこれらの手順をクリップボードにコピーし、ユーザに配布します。

ステップ 9 [終了 (Finish)] をクリックします。

リモート アクセス VPN グループによるリソースへのアクセスを制御する

ASA、または Firepower Management Center を使用する FTD デバイスでのリモートアクセス VPN の構成に精通している場合は、リモートアクセス VPN グループに基づいたネットワークのさまざまなリソースへのアクセス制御に慣れているかもしれません。

Firepower Device Manager を使用すると、単一のグループポリシーで単一の接続プロファイルを構成できます。ただし、アイデンティティポリシーとユーザグループベースのアクセス制御を実装することによってユーザグループに基づくアクセス制御もできます。

次の手順では、この構成について説明します。

始める前に

この手順では、リモートアクセス VPN および必要なアイデンティティレルムがすでに構成されていることを前提としています。ただし、アイデンティティとアクセス制御ポリシーを最初に構成してから、RA VPN を構成します。

この設定では、VPN トラフィックがアクセス制御ポリシーの対象となる必要があります。CLI で **show running-config** コマンドを使用して、**no sysopt connection permit-vpn** コマンドが表示されることを確認します。実行中のコンフィギュレーションにない場合、FlexConfig を使用してコマンドを設定します。

手順

ステップ 1 ディレクトリ サーバに必要なユーザ グループを構成します。

ディレクトリ サーバはユーザ グループを持つ必要があります。それらのグループには、展開するポリシーに基づいて適切なユーザを含める必要があります。たとえば、エンジニアリングとマーケティングのユーザを区別し、異なるリソースへのグループのメンバーのアクセスを許可する場合、それらのユーザのためのグループがディレクトリ サーバで定義されている必要があります。

FTD デバイス上で直接ユーザ グループを作成することはできません。

ユーザ グループを作成する方法については、ディレクトリ サーバのマニュアルを参照してください。

ステップ 2 [ポリシー (Policies)] > [アイデンティティ (Identity)] を選択し、アイデンティティ ポリシーを有効にして、RA VPN ユーザに対してアクティブ認証を適用するルールを作成します。

アイデンティティ ポリシーは、RA VPN 接続と同じレルムを使用します。少なくとも、RA VPN 外部インターフェイスが含まれているゾーンの RA VPN アドレスプールの IP アドレスのアクティブ認証を要求するアイデンティティ ポリシーが必要です。

すべてのアドレスとすべてのゾーンのアクティブ認証を要求する包括的なアイデンティティ ポリシーがあれば、その他のルールは必要ありません。

ポリシーの有効化とルールの作成については、[アイデンティティ ポリシーの設定 \(232 ページ\)](#) を参照してください。

アイデンティティ ポリシー認証を通じて収集された名前のみユーザベースのアクセス制御ポリシーに利用可能なため、アイデンティティルールを構成する必要があります。RA VPN 接続のみから取得したユーザ名は、アクセス制御ポリシーでは使用できません。

ステップ 3 メニューで[展開 (Deploy)] をクリックし、[今すぐ展開 (Deploy Now)] をクリックして変更を展開します。



システムはディレクトリ サーバへの接続を確立し、ユーザおよびユーザグループをダウンロードする必要があります。構成を展開すると、このユーザ/グループのダウンロードを開始します。展開を行わない場合、アクセス制御ルールでユーザとグループを選択できなくなります。

ステップ 4 [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択し、グループベースのアクセス制御ルールを作成します。

このとき RA VPN ユーザのディレクトリ レルム グループを区別するためのアクセス制御ルールを作成できます。非常に一般的なルール、または具体的なターゲットのあるルールを作成できます。アクセス制御ルールの作成の詳細については、[アクセスコントロールルールの設定 \(264 ページ\)](#) を参照してください。

たとえば、特定の RA VPN ユーザ グループを対象とするルールは、[アクセスルールの追加/編集 (Add/Edit Access Rule)] ダイアログ ボックスのタブに基づいて、次の条件を使用する可能性があります。

- [送信元/宛先 (Source/Destination)]、[ゾーン (Zones)] : [ソース (Source)] ゾーンに RA VPN 外部インターフェイスを含める必要があります。[宛先 (Destination)] ゾーンには関連する内部インターフェイスをすべて含めることができます。
- [送信元/宛先 (Source/Destination)]、[ネットワーク (Networks)] および [ポート (Ports)] : [送信元 (Source)] として RA VPN アドレスプールネットワーク オブジェクトを選択し、[宛先 (Destination)] として被制御リソースを定義するネットワーク (および必要に応じてポート) オブジェクトを選択します。宛先ネットワーク/ポートを選択する代わりに、要件により適切である場合は [アプリケーション (Application)] または [URL] タブを使用して宛先リソースを定義できます。
- [ユーザ (Users)] : このタブの特定のディレクトリ グループを選択します。これは、グループベースのアクセス制御を提供する条件です。
- [アプリケーション (Application)]、[URLs] : [送信元/宛先 (Source/Destination)] タブの宛先ネットワーク/ポート条件に加えて、またはそれらの代わりに、これらの条件を使用できます。たとえば、特定のサブネットへのルールを制限するネットワーク オブジェクトを選択してから、対象となるネットワーク上のこれらのアプリケーションへのアクセスを制御するアプリケーションを選択できます。
- [侵入ポリシー (Intrusion Policy)]、[ファイルポリシー (File Policy)] : 要件に適合するオプションを選択します。これらのオプションは脅威を制御し、特定のリソースへのアクセスは制御しません。
- [ロギング (Logging)] : 要件に適合するオプションを選択します。監視ダッシュボードまたはイベントビューアの接続イベントに結果を表示するにはロギングを有効にする必要があります。

リモート アクセス VPN 設定の確認

リモートアクセス VPN を設定し、設定をデバイスに展開した後で、リモート接続を行えることを確認します。

問題が発生した場合は、トラブルシューティングトピックに目を通し、問題の分離と修正に役立てます。[リモート アクセス VPN のトラブルシューティング \(443 ページ\)](#) を参照してください。

手順

ステップ 1 外部ネットワークから、AnyConnect クライアントを使用して VPN 接続を確立します。

Web ブラウザを使用して、<https://ravpn-address> を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。必要に応じて、クライアントソフトウェアをインストールし、接続を完了します。「[AnyConnect ソフトウェアのインストール方法 \(431 ページ\)](#)」を参照してください。

ステップ 2 デバイス CLI にログインします (CLI (コマンドラインインターフェイス) へのログイン (15 ページ) を参照)。または、CLI コンソールを開きます。

ステップ 3 `show vpn-sessiondb` コマンドを使用して、現在の VPN セッションに関する概要情報を表示します。

統計情報では、アクティブな AnyConnect クライアントセッション、および累積セッション数、ピーク同時セッション数、非アクティブセッション数の情報が示されます。次は、コマンドからの出力例です。

```
> show vpn-sessiondb
-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
-----
AnyConnect Client      :      1 :      49 :      3 :      0
  SSL/TLS/DTLS         :      1 :      49 :      3 :      0
Clientless VPN        :      0 :       1 :      1 :
  Browser              :      0 :       1 :      1 :
-----
Total Active and Inactive :      1                Total Cumulative :      50
Device Total VPN Capacity :    10000
Device Load               :       0%
-----

Tunnels Summary
-----
Active : Cumulative : Peak Concurrent
-----
Clientless              :      0 :       1 :      1
AnyConnect-Parent      :      1 :      49 :      3
SSL-Tunnel              :      1 :      46 :      3
DTLS-Tunnel            :      1 :      46 :      3
-----
Totals                  :      3 :     142 :
-----

IPv6 Usage Summary
-----
Active : Cumulative : Peak Concurrent
-----
AnyConnect SSL/TLS/DTLS :      :      :
  Tunneled IPv6         :      1 :     20 :      2
-----
```

ステップ 4 `show vpn-sessiondb anyconnect` コマンドを使用して、現在の AnyConnect VPN セッションに関する詳細情報を表示します。

詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含まれます。VPN接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

```
> show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : priya                Index      : 4820
Assigned IP   : 172.18.0.1           Public IP   : 192.168.2.20
Assigned IPv6 : 2009::1
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel:
(1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 27731                Bytes Rx    : 14427
Group Policy  : MyRaVpn|Policy        Tunnel Group : MyRaVpn
Login Time    : 21:58:10 UTC Mon Apr 10 2017
Duration      : 0h:51m:13s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN        : none
Audt Sess ID  : c0a800fd012d400058ebfff2
Security Grp  : none                  Tunnel Zone  : 0
```

リモート アクセス VPN のモニタリング

リモートアクセス VPN 接続をモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。

- **show vpn-sessiondb** は VPN セッションに関する情報を表示します。これらの統計情報は **clear vpn-sessiondb** コマンドを使用してリセットできます。
- **show webvpn keyword** はリモートアクセス VPN 設定に関する情報を表示します。統計情報とインストールされている AnyConnect イメージが含まれます。 **show webvpn ?** と入力し、使用可能なキーワードを確認します。
- **show aaa-server** はリモートアクセス VPN とともに使用されるディレクトリ サーバに関する統計情報を表示します。

リモート アクセス VPN のトラブルシューティング

リモートアクセス VPN 接続の問題の原因は、クライアントまたは Firepower Threat Defense のデバイス設定の可能性があります。次の各項で、発生する可能性のある主な問題のトラブルシューティングについて説明します。

SSL 接続問題のトラブルシューティング

ユーザが AnyConnect クライアントをダウンロードするため、外部 IP アドレスに対し AnyConnect を使用せずに初めて SSL 接続しようとしたが接続できない場合には、次の手順を実行します。

1. クライアントワークステーションから、外部インターフェイスの IP アドレスに ping を実行できるかどうかを確認します。実行できない場合は、ユーザのワークステーションからそのアドレスまでのルートが存在しない原因を特定します。
2. クライアントワークステーションから、外部インターフェイスの完全修飾ドメイン名 (FQDN) に ping を実行できるかどうかを確認します。この FQDN は、リモートアクセス (RA) VPN 接続プロファイルで定義されているものです。IP アドレスを ping できても、FQDN を ping できない場合は、クライアントおよび RA VPN 接続プロファイルで使用されている DNS サーバを更新し、FQDN と IP アドレスのマッピングを追加する必要があります。
3. 外部インターフェイスで提示される証明書をユーザが承認していることを確認します。ユーザはこの証明書を永久に受け入れる必要があります。
4. RA VPN 接続設定を調べ、正しい外部インターフェイスを選択していることを確認します。よくある誤りとして、RA VPN ユーザに面している外部インターフェイスではなく、内部ネットワークに面している内部インターフェイスを選択していることがあります。
5. SSL 暗号化が適切に設定されている場合は、外部スニファを使用して、TCP スリーウェイハンドシェイクが正常に実行されるかどうかを確認します。

AnyConnect のダウンロードおよびインストールの問題のトラブルシューティング

ユーザが外部インターフェイスに SSL 接続可能で、AnyConnect パッケージをダウンロードおよびインストールできない場合、次の点を考慮してください。

- クライアントのオペレーティングシステムに対応する AnyConnect パッケージをアップロードしていることを確認してください。たとえば、ユーザのワークステーションに Linux が搭載されているのに、Linux AnyConnect イメージをアップロードしなかった場合、インストールできるパッケージはありません。
- Windows クライアントの場合、ソフトウェアのインストールには管理者権限が必要です。
- Windows クライアントの場合、ワークステーションで ActiveX を有効にするか、または JRE 1.5 以降 (JRE 7 を推奨) をインストールする必要があります。
- Safari ブラウザの場合、Java が有効であることが必要です。
- 別のブラウザを試してみてください。あるブラウザでは失敗しても、別のブラウザでは成功することがあります。

AnyConnect 接続問題のトラブルシューティング

外部インターフェイスに接続し、AnyConnect クライアントをダウンロードしてインストールできても、AnyConnect を使用して接続を完了できなかった場合、次のことを確認してください。

- 認証が失敗した場合、ユーザが正しいユーザ名とパスワードを入力しており、ユーザ名が認証サーバで正しく定義されていることを確認してください。認証サーバもデータインターフェイスのいずれかを使用してアクセス可能である必要があります。



(注) 認証サーバが外部ネットワークにある場合は、外部ネットワークへのサイト間 VPN 接続を設定し、リモートアクセス VPN インターフェイスアドレスを VPN 内に含める必要があります。詳細は、[リモートアクセス VPN を使用して外部ネットワークのディレクトリサーバを使用する方法 \(453 ページ\)](#) を参照してください。

- リモートアクセス (RA) VPN 接続プロファイルで外部インターフェイスの完全修飾ドメイン名 (FQDN) を設定した場合、クライアントデバイスから FQDN を ping できることを確認します。IP アドレスを ping できても、FQDN を ping できない場合は、クライアントおよび RA VPN 接続プロファイルで使用されている DNS サーバを更新し、FQDN と IP アドレスのマッピングを追加する必要があります。外部インターフェイスの FQDN を指定した時に生成されたデフォルトの AnyConnect クライアントプロファイルを使用している場合、DNS が更新されるまでは IP アドレスを使用するようにサーバアドレスを編集する必要があります。
- 外部インターフェイスで提示される証明書をユーザが承認していることを確認します。ユーザはこの証明書を永久に受け入れる必要があります。
- ユーザの AnyConnect クライアントに複数の接続プロファイルが含まれている場合、正しいプロファイルを選択していることを確認します。
- クライアント側の設定がすべて正しいと考えられる場合は、Firepower Threat Defense デバイスに SSH 接続し、`debug webvpn` コマンドを入力します。接続試行中に表示されたメッセージを確認します。

RA VPN トラフィック フローの問題のトラブルシューティング

ユーザが安全なリモートアクセス (RA) VPN 接続を確立できても、トラフィックの送受信ができない場合は、次の操作を実行してください。

1. クライアントを切断して再接続します。これで、問題が解決することがあります。
2. AnyConnect クライアントで、トラフィック統計を確認して、送信カウンタと受信カウンタの両方が増えているかどうかを確認します。受信パケットカウンタがゼロのままの場合、

Firepower Threat Defense デバイスはトラフィックを返していません。Firepower Threat Defense の設定に問題がある可能性があります。一般的な問題を次に示します。

- アクセスルールでトラフィックをブロックしている。アクセス制御ポリシーのルールで、ネットワーク内と RA VPN アドレスプール間のトラフィックを妨害しているルールがないかを確認します。デフォルトのアクションでトラフィックがブロックされている場合は、明示的な [許可 (Allow)] ルールを作成する必要があります。
- NAT ルールが、RA VPN トラフィックでバイパスされていない。すべての内部インターフェイスの RA VPN 接続で NAT がオフに設定されていることを確認してください。または、NAT ルールが内部ネットワークとインターフェイス、および RA VPN アドレスプールと外部インターフェイス間の通信を妨害していないことを確認してください。
- ルートが誤って設定されている。すべての定義されたルートが有効で正しく機能していることを確認します。たとえば、外部インターフェイス用に定義したスタティック IP アドレスがある場合、ルーティングテーブルにデフォルトルート (0.0.0.0/0 および ::/0) が含まれていることを確認します。
- RA VPN の DNS サーバとドメイン名が正しく設定されており、クライアントシステムで正しく使用されていることを確認します。DNS サーバに到達可能であることを確認します。
- RA VPN でスプリットトンネリングが有効になっている場合、指定した内部ネットワークへのトラフィックがトンネルを通っており、他のすべてのトラフィックがトンネルをバイパスしている (Firepower Threat Defense デバイスが認識しない) ことを確認します。

3. Firepower Threat Defense デバイスに SSH 接続し、リモートアクセス VPN との間でトラフィックが送受信されていることを確認します。次のコマンドを使用します。

- `show webvpn anyconnect`
- `show vpn-sessiondb`

リモート アクセス VPN の例

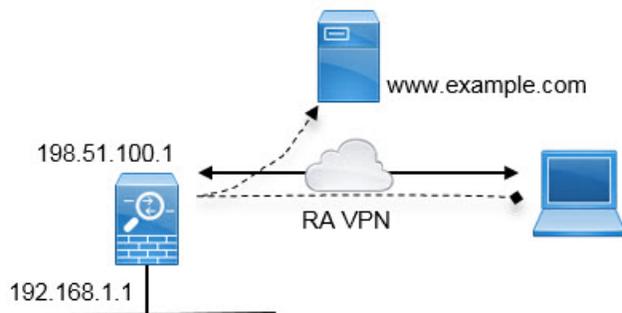
以下に、リモートアクセス VPN を設定する例を示します。

外部インターフェイスでリモートアクセス VPN ユーザにインターネットアクセスを提供する方法 (ヘア ピニング)

リモートアクセス VPN では、リモートネットワーク上のユーザに自分のデバイスを介してインターネットにアクセスさせたい場合があります。ただし、インターネットに接続している同一インターフェイス (外部インターフェイス) 上のデバイスにリモートユーザがアクセスして

いるため、インターネットトラフィックが外部インターフェイスの外側からそのまま返される必要があります。この手法はヘア ピニングと呼ばれる場合もあります。

次の図は例を示しています。外部インターフェイス、198.51.100.1 に設定されているリモートアクセス VPN があります。リモートユーザの VPN トンネルを分割し、インターネットに向かうトラフィックを外部インターフェイスから戻し、内部ネットワークに向かうトラフィックはデバイスを通し続けるようにできます。そのため、リモートユーザがインターネット上のサーバ (www.example.com など) にアクセスする場合、接続は最初に VPN を通過し、その後 198.51.100.1 インターフェイスからインターネットにルートバックされます。



次の手順では、このサービスの設定方法について説明します。

始める前に

この例は、デバイスが登録済み、リモートアクセス VPN ライセンスが適用済み、AnyConnect クライアントイメージがアップロード済みであることを前提としています。アイデンティティポリシーでも使用されるアイデンティティレルムも設定済みであると想定しています。

手順

ステップ 1 リモートアクセス VPN 接続プロファイルを設定します。

- a) [デバイス (Device)] をクリックし、[リモートアクセス VPN (Remote Access VPN)] グループで [接続プロファイルの設定 (Setup Connection Profile)] をクリックします。(プロファイルを設定済みの場合は、[設定の表示 (View Configuration)] をクリックします。)

既存の接続の場合は、[編集 (Edit)] をクリックしてプロファイルを変更します。
- b) 接続プロファイルの設定を行います。
 - [接続プロファイル名 (Connection Profile Name)] : 名前、Corporate-RAVPN などを入力します。
 - [ユーザ認証用 ADレルム/ディレクトリサーバ (AD Realm/Directory Server for User Authentication)] [ユーザ認証用アイデンティティソース (Identity Source for User Authentication)] : リモートユーザの認証に使用されるアイデンティティレルムを選択します。まだアイデンティティレルムを設定していない場合は、ドロップダウンリストの下部にある [新しいアイデンティティレルムの作成 (Create New Identity Realm)] をクリックして作成します。

- [AnyConnectパッケージ (AnyConnect Packages)] : サポートするオペレーティング システムごとに AnyConnect クライアントをアップロードします。アップロードが完了するまで待機してから、続行してください。

接続プロファイルの設定は次のようになります。

Connection Profile Name

Corporate-RAVPN

AD Realm/Directory Server for User Authentication

AD

AnyConnect Packages

Windows

 anyconnect-win-4.4.00243-webdeploy-k9.pkg

[Upload New](#)

Choose another package to upload

- c) [次へ (Next)] をクリックして、デバイスアイデンティティのプロパティを設定します。
- [デバイスアイデンティティ証明書 (Certificate of Device Identity)] : デバイスのアイデンティティを確立するために使用する内部証明書を選択します。クライアントはこの証明書を承認して、セキュアな VPN 接続を完了させる必要があります。独自の証明書がない場合は、DefaultInternalCertificate を使用できます。
 - [外部インターフェイス (Outside Interface)] : リモートユーザが接続する外部インターフェイスを選択します。このインターフェイスには通常「外部」という名前が付けられます。
 - [外部インターフェイス用完全修飾ドメイン名 (Fully-qualified Domain Name for the Outside Interface)] : 外部インターフェイスの DNS 名がわかっている場合はここで入力します。例、corporate-vpn.example.com。

ページのデバイス アイデンティティ セクションは、次のようになります。

Certificate of Device Identity

DefaultInternalCertificate

Outside Interface

AnyConnect clients connect to this interface

outside

Fully-qualified Domain Name for the Outside Interface

corporate-vpn.example.com

e.g. ad.example.com

- d) ページの下に進み、[IPv4アドレスプール (IPv4 Address Pool)] を設定し、必要に応じて [IPv6アドレスプール (IPv6 Address Pool)] を設定します。

ネットワークを識別するオブジェクトを選択します。リモートアクセス VPN ユーザには、このプールからアドレスが割り当てられます。たとえば、10.1.10.0/24 を指定するネットワークオブジェクト。オブジェクトが存在しない場合は、リストの下部にある [新しいネットワークの作成 (Create New Network)] をクリックします。IPv6 アドレスをサポートする場合は、IPv6 のプールも設定します。

IPv4 Address Pool

Endpoints are provided an address from this pool

ravpn-pool

IPv6 Address Pool

Endpoints are provided an address from this pool

Please select

- e) ページの下にスクロールし、リモート接続の DNS 設定を構成します。
- 使用する DNS サーバの IP アドレス、およびローカルドメイン名を入力します。例、example.com。[OpenDNS] をクリックして、OpenDNS サーバを使用できます。

Primary DNS IP Address

208.67.222.222

Secondary DNS IP Address

208.67.220.220

Domain Search Name

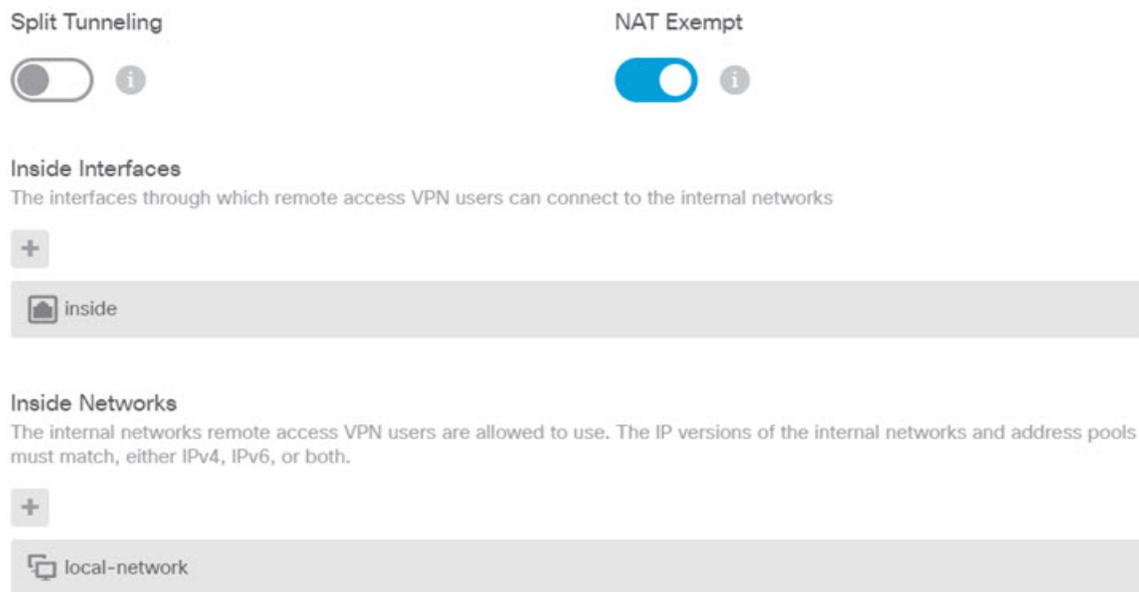
example.com

- f) [次へ (Next)] をクリックして下にスクロールし、[社内リソース (Corporate Resource)] オプションを設定します

(バナー、接続時間とタイムアウト、およびプロキシ設定も設定できますが、ヘア ピニングとは直接関係がありません)。

次の設定は、リモートアクセス VPN でヘア ピニングを可能にするために重要です。

- [スプリットトンネリング (Split Tunneling)] : この機能を無効にします。すべてのトラフィックを VPN ゲートウェイに向かわせる場合、スプリットトンネリングは、リモートクライアントが VPN の外部にあるローカルサイトやインターネットサイトに直接アクセスできるようにするための方法です。
- [NAT免除 (NAT Exempt)] : この機能を有効にします。内部インターフェイスを選択し、内部ネットワークを定義するネットワークオブジェクトを選択します。この例では、オブジェクトは 192.168.1.0/24 を指定します。内部ネットワークに向かう RA VPN トラフィックは、アドレス変換されません。ただし、ヘア ピニングされたトラフィックは外部インターフェイスの外に出るため、引き続き NAT が行われます。これは、NAT 免除は内部インターフェイスにのみ適用されるためです。



- g) 必要に応じて、[AnyConnectクライアントプロファイル (AnyConnect Client Profile)] を選択し、[次へ (Next)] をクリックします。
- h) RA VPN の設定を確認してから [完了 (Finish)] をクリックします。

ステップ 2 外部インターフェイスから送信されたすべての接続を外部 IP アドレス (インターフェイス PAT) のポートに変換するよう NAT ルールを設定します。

デバイスの初期設定を完了すると、**InsideOutsideNatRule** という名前の NAT ルールが作成されます。このルールは、外部インターフェイス経由でデバイスを抜ける任意のインターフェイスから、インターフェイス PAT を IPv4 トラフィックに充当します。外部インターフェイスは「任意の」送信元インターフェイスに含まれるため、必要なルールは、編集または削除していない限り、すでに存在しています。

次の手順で、必要なルールを作成する方法を説明します。

- a) [ポリシー (Policies)] > [NAT] をクリックします。
- b) 次のいずれかを実行します。
 - **InsideOutsideNatRule** を編集するには、[アクション (Action)] 列にマウスオーバーし、[編集 (edit)] アイコン (🔍) をクリックします。
 - ルールを新規作成するには、[+] ボタンをクリックします。
- c) 次のプロパティを使用してルールを設定します。
 - [タイトル (Title)] : 新しいルールのわかりやすい名前をスペースを含めず入力します。たとえば、**OutsideInterfacePAT** と入力します。
 - [ルールの作成先 (Create Rule For)] : [手動 NAT (Manual NAT)]。
 - [配置 (Placement)] : [自動 NAT ルールの前 (Before Auto NAT Rules)] (デフォルト)。

- [タイプ (Type)] : [ダイナミック (Dynamic)]。
- [元の packets (Original Packet)] : [送信元アドレス (Source Address)]で[任意 (Any)] または[any-ipv4]を選択します。[送信元インターフェイス (Source Interface)]で、[任意 (Any)] (デフォルト) を選択していることを確認します。[元の packets (Original Packet)]の他のすべてのオプションは、デフォルトの[任意 (Any)]のままにします。
- [変換後の packets (Translated Packet)] : [宛先インターフェイス (Destination Interface)]で、[外部 (outside)]を選択します。[変換後のアドレス (Translated Address)]で、[インターフェイス (Interface)]を選択します。[変換後の packets (Translated Packet)]の他のすべてのオプションは、デフォルトの[任意 (Any)]のままにします。

次の図は、発信元アドレスに [任意 (Any)] を選択したシンプルな例を示しています。

The screenshot shows the configuration for a NAT rule named "OutsiderInterfacePAT". The rule type is "Manual NAT" and its status is "On". The placement is "Before Auto NAT Rules" and the type is "Dynamic". Under the "Packet Translation" tab, the "ORIGINAL PACKET" section has "Source Interface" set to "Any" and "Source Address" set to "Any". The "TRANSLATED PACKET" section has "Destination Interface" set to "outside" and "Source Address" set to "Interface". Other fields like "Source Port", "Destination Address", and "Destination Port" are set to "Any".

d) [OK] をクリックします。

ステップ 3 変更を保存します。

a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

リモート アクセス VPN を使用して外部ネットワークのディレクトリサーバを使用する方法

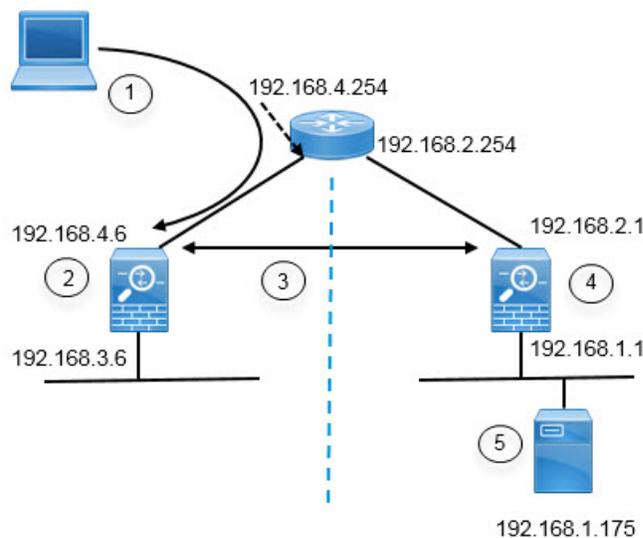
モバイルワーカーと在宅勤務者が内部ネットワークに安全に接続できるリモートアクセス VPN を設定できます。接続のセキュリティは、ユーザ接続を認証して、認可されたユーザだけがエントリを取得できるようにするディレクトリ サーバによって異なります。

ディレクトリ サーバが内部ネットワークではなく外部ネットワーク上にある場合、外部インターフェイスからディレクトリ サーバを含むネットワークへのサイト間 VPN 接続を設定する必要があります。**サイト間 VPN の設定の 1 つのテクニック**：サイト間 VPN 接続の「内部」ネットワーク内、および背後にディレクトリ サーバが存在するデバイスのリモートネットワークに、リモートアクセス VPN デバイスの外部インターフェイスアドレスを含める必要があります。詳細については、次の手順を参照してください。



(注) データインターフェイスを仮想管理インターフェイスのゲートウェイとして使用する場合、この設定により、アイデンティティポリシー用のディレクトリの使用も可能になります。データインターフェイスを管理ゲートウェイとして使用しない場合は、管理ネットワークから、サイト間 VPN 接続に参加する内部ネットワークへのルートがあることを確認します。

この使用例では、次のネットワーク シナリオを実装します。



図のコールアウト	説明
1	192.168.4.6 に VPN 接続を行うリモートアクセスホスト。クライアントは 172.18.1.0/24 アドレスプールにあるアドレスを取得します。
2	リモートアクセス VPN をホストするサイト A。
3	サイト A とサイト B の FTD デバイスの外部インターフェイス間のサイト間 VPN トンネル。
4	ディレクトリ サーバをホストするサイト B。
5	サイト B の内部ネットワークにあるディレクトリ サーバ。

始める前に

この使用例は、デバイスのセットアップウィザードを使用して、通常のベースラインの構成を構築していることを前提としています。具体的には次のとおりです。

- `inside_zone` から `outside_zone` に移動するトラフィックを許可（または信頼）する `Inside_Outside_Rule` アクセスコントロールルールがある。
- `inside_zone` と `outside_zone` のセキュリティゾーン（それぞれ）に、内部インターフェイスと外部インターフェイスが含まれている。
- 内部インターフェイスから外部インターフェイスに移動するすべてのトラフィックに対してインターフェイス PAT を実行する `InsideOutsideNATRule` がある。デフォルトで内部ブリッジグループを使用するデバイスに、インターフェイス PAT 用のルールが複数存在する場合があります。
- 外部インターフェイスを指す、`0.0.0.0/0` のスタティック IPv4 ルートがある。この例は、外部インターフェイスにスタティック IP アドレスを使用しているが、DHCP を使用してスタティックルートの動的取得も可能であることを前提としています。この例の場合、次のスタティックルートを想定しています。
 - サイト A : 外部インターフェイス、ゲートウェイは 192.168.4.254 です。
 - サイト B : 外部インターフェイス、ゲートウェイは 192.168.2.254 です。

手順

ステップ 1 ディレクトリ サーバをホストする [サイト B (Site B)] にサイト間 VPN 接続を設定します。

- [デバイス (Device)] をクリックし、[サイト間VPN (Site-to-Site VPN)] グループで [設定の表示 (View Configuration)] をクリックします。
- [+] ボタンをクリックします。
- [エンドポイントの設定 (Endpoint Settings)] に次のオプションを設定します。

- [接続プロファイル名 (Connection Profile Name)] : 名前を入力します (たとえば、サイト A への接続を示す、SiteA) 。
- [ローカルサイト (Local Site)] : これらのオプションでローカルエンドポイントを定義します。
 - [ローカルVPNアクセスインターフェイス (Local VPN Access Interface)] : [外部 (outside)] インターフェイス (図の 192.168.2.1 アドレスが付いているインターフェイス) を選択します。
 - [ローカルネットワーク (Local Network)] : [+] をクリックして、VPN 接続に参加する必要があるローカルネットワークを特定するネットワーク オブジェクトを選択します。ディレクトリサーバはこのネットワーク上にあるため、サイト間 VPN に参加できます。オブジェクトがまだ存在していない場合、[新規ネットワークの作成 (Create New Network)] をクリックして、192.168.1.0/24 ネットワークのオブジェクトを設定します。オブジェクトを保存したら、ドロップダウンリストでそのオブジェクトを選択し、[OK] をクリックします。

Add Network Object

Name

Network192.168.1.0

Description

Type

Network Host

Network

192.168.1.0/24

- [リモートサイト (Remote Site)] : これらのオプションでリモートエンドポイントを定義します。
 - [リモートIPアドレス (Remote IP Address)] : VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレスである 192.168.4.6 を入力します。
 - [リモートネットワーク (Remote Network)] : [+] をクリックして、VPN 接続に参加する必要があるリモートネットワークを特定するネットワーク オブジェクトを選択します。[新規ネットワークの作成 (Create New Network)] をクリックして、次のオブジェクトを設定し、リストでそれらのオブジェクトを選択します。

1. SiteAInside、ネットワーク、192.168.3.0/24。

Add Network Object

Name

SiteAInside

Description

Type

Network Host

Network

192.168.3.0/24

2. SiteAInterface、ホスト、192.168.4.6。重要ポイント：リモートアクセス VPN 接続ポイントのアドレスをサイト間 VPN 接続用のリモートネットワークの一部として含めて、当該インターフェイスでホストされている RA VPN でディレクトリ サーバを使用可能にする必要があります。

Add Network Object

Name

SiteAInterface

Description

Type

Network Host

Host

192.168.4.6

終了すると、エンドポイントの設定は次のようになります。

Connection Profile Name

SiteA

LOCAL SITE

Local VPN Access Interface

outside

REMOTE SITE

Remote IP Address

192.168.4.6

Local Network

+

Network192.168.1.0

Remote Network

+

SiteAInside

SiteAInterface

- d) [Next] をクリックします。
- e) VPN のプライバシー設定を定義します。

この使用例は、強力な暗号化の使用を許可する輸出管理機能を承認していることを前提としています。これらの例の設定は、お客様のニーズとライセンスコンプライアンスに合わせて調整してください。

- [IKEバージョン2 (IKE Version 2)]、[IKEバージョン1 (IKE Version 1)] : デフォルト ([IKEバージョン2 (IKE Version 2)] は有効で、[IKEバージョン1 (IKE Version 1)] は無効) のままにします。
- [IKEポリシー (IKE Policy)] : [編集 (Edit)] をクリックして、[AES-GCM-NUL-LSHA] および [AES-SHA-SHA] を有効にし、[DES-SHA-SHA] を無効にします。
- [IPsecプロポーザル (IPsec Proposal)] : [編集 (Edit)] をクリックします。[IPsecプロポーザルの選択 (Select IPsec Proposals)] ダイアログボックスで [+] をクリックし、[デフォルトに設定 (Set Default)] をクリックしてデフォルトの AES-GCM プロポーザルを選択します。
- [ローカルの事前共有キー (Local Preshared Key)]、[リモートピアの事前共有キー (Remote Peer Preshared Key)] : このデバイスおよび VPN 接続用のリモートデバイスに定義されているキーを入力します。これらのキーは IKEv2 では異なることがあります。キーは 1 ~ 127 文字の英数字で指定できます。サイト A のデバイスでサイト間 VPN 接続を作成するときと同じ文字列を設定する必要があるため、これらのキーは覚えておいてください。

IKE ポリシーは次のようになります。

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE connections.

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

Default set selected

Local Pre-shared Key

.....

Remote Peer Pre-shared Key

.....

- f) [追加オプション (Additional Options)] を設定します。
- [NAT免除 (NAT Exempt)] : 内部ネットワークをホストするインターフェイスを選択します。この例では [内部 (inside)] インターフェイス。通常、サイト間 VPN トンネル内のトラフィックの IP アドレスは変換しません。このオプションは、ローカルネットワークが (ブリッジグループのメンバーではなく) 単一のルーテッドインターフェイスの背後に存在している場合にのみ機能します。ローカルネットワークが複数のルーテッドインターフェイスまたは1つ以上のブリッジグループのメンバーの背後にある場合、NAT免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、[NAT からのサイト間 VPN トラフィックの除外 \(415 ページ\)](#) を参照してください。
 - [Perfect Forward Secrecy用のDiffie-Helmanグループ (Diffie-Helman Group for Perfect Forward Secrecy)] : [グループ19 (Group 19)] を選択します。このオプションは、暗号化された交換ごとに固有のセッションキーを生成および使用するために、Perfect Forward Secrecy (PFS) を使用するかどうかを決定します。固有のセッションキーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイントデバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。オプションの説明については、[使用する Diffie-Hellman 係数グループの決定 \(397 ページ\)](#) を参照してください。

このオプションは次のようになります。

Additional Options

NAT Exempt

inside

Diffie-Hellman Group for Perfect Forward Secrecy

19

- g) [次へ (Next)] をクリックします。
- h) サマリーを確認し、[終了 (Finish)] をクリックします。
サマリー情報がクリップボードにコピーされます。この情報はドキュメントに貼り付けて、リモートピアの設定、またはピアの設定責任者に送信するために使用できます。
- i) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。

- j) [今すぐ展開 (Deploy Now)] ボタンをクリックして、導入が正常に完了するまで待ちます。
これで、サイト B のデバイスがサイト間 VPN 接続の一端をホストできるようになりました。

ステップ 2 [サイト B (Site B)] デバイスからログアウトして、[サイト A (Site A)] デバイスにログインします。

ステップ 3 リモートアクセスVPNをホストする[サイト A (Site A)] にサイト間VPN接続を設定します。

- a) [デバイス (Device)] をクリックし、[サイト間VPN (Site-to-Site VPN)] グループで [設定の表示 (View Configuration)] をクリックします。
- b) [+] ボタンをクリックします。
- c) [エンドポイントの設定 (Endpoint Settings)] に次のオプションを設定します。
 - [接続プロファイル名 (Connection Profile Name)] : 名前を入力します (たとえば、サイト B への接続を示す、SiteB) 。
 - [ローカルサイト (Local Site)] : これらのオプションでローカル エンドポイントを定義します。
 - [ローカルVPNアクセスインターフェイス (Local VPN Access Interface)] : [外部 (outside)] インターフェイス (図内 192.168.4.6 アドレスが付いているインターフェイス) を選択します。
 - [ローカルネットワーク (Local Network)] : [+] をクリックして、VPN 接続に参加する必要があるローカルネットワークを特定するネットワーク オブジェクトを選択します。[新規ネットワークの作成 (Create New Network)] をクリックして、次のオブジェクトを設定し、リストでそれらのオブジェクトを選択します。サイト B のデバイスに同じオブジェクトを作成しましたが、サイト A のデバイスでも再度同じオブジェクトを作成する必要があります。

1. SiteAInside、ネットワーク、192.168.3.0/24。

Add Network Object

Name

SiteAInside

Description

Type

Network Host

Network

192.168.3.0/24

2. SiteAInterface、ホスト、192.168.4.6。重要ポイント：リモートアクセスVPN接続ポイントのアドレスをサイト間VPN接続用の内部ネットワークの一部として含めて、当該インターフェイスでホストされているRAVPNでリモートネットワーク上のディレクトリサーバを使用可能にする必要があります。

Add Network Object

Name

SiteAInterface

Description

Type

Network Host

Host

192.168.4.6

- [リモートサイト (Remote Site)] : これらのオプションでリモート エンドポイントを定義します。
 - [リモートIPアドレス (Remote IP Address)] : VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレスである 192.168.2.1 を入力します。
 - [リモートネットワーク (Remote Network)] : [+] をクリックして、VPN 接続に参加する必要があるリモートネットワークを特定する (ディレクトリサーバを含んでいる) ネットワークオブジェクトを選択します。[新規ネットワークの作成 (Create New Network)] をクリックし、192.168.1.0/24 ネットワークのオブジェクトを設定します。オブジェクトを保存したら、ドロップダウンリストでそのオブジェクトを選択し、[OK] をクリックします。サイト B のデバイスに同じオブジェクトを作成しましたが、サイト A のデバイスでも再度同じオブジェクトを作成する必要があります。

Add Network Object

Name

Network192.168.1.0

Description

Type

Network Host

Network

192.168.1.0/24

終了すると、エンドポイントの設定は次のようになります。ローカルおよびリモートネットワークは、サイト B の設定と比べると反転している点に注意してください。これは、ポイントツーポイント接続の両端の通常の外観を示しています。

Connection Profile Name

SiteB

LOCAL SITE

Local VPN Access Interface

outside

REMOTE SITE

Remote IP Address

192.168.2.1

Local Network

+

SiteAInside

SiteAInterface

Remote Network

+

Network192.168.1.0

- d) [次へ (Next)] をクリックします。
- e) VPN のプライバシー設定を定義します。

サイト B 接続の場合と同じ IKE バージョン、ポリシー、および IPsec プロポーザルと、同じ事前共有キーを設定します。ただし、必ず、ローカル事前共有キーとリモート事前共有キーを逆にしてください。

IKE ポリシーは次のようになります。

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE connections.

IKE VERSION 2



IKE VERSION 1



IKE Policy

Globally applied

EDIT...

IPSec Proposal

Default set selected

EDIT...

Local Pre-shared Key

●●●●●●●●

Remote Peer Pre-shared Key

●●●●●●●●

- f) [追加オプション (Additional Options)] を設定します。
- [NAT免除 (NAT Exempt)] : 内部ネットワークをホストするインターフェイスを選択します。この例では [内部 (inside)] インターフェイス。通常、サイト間 VPN トンネル内のトラフィックの IP アドレスは変換しません。このオプションは、ローカルネットワークが (ブリッジグループのメンバーではなく) 単一のルーテッドインターフェイスの背後に存在している場合にのみ機能します。ローカルネットワークが複数のルーテッドインターフェイスまたは1つ以上のブリッジグループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、[NAT からのサイト間 VPN トラフィックの除外 \(415 ページ\)](#) を参照してください。
 - [Perfect Forward Secrecy用のDiffie-Helmanグループ (Diffie-Helman Group for Perfect Forward Secrecy)] : [グループ19 (Group 19)] を選択します。

このオプションは次のようになります。

Additional Options

NAT Exempt

Diffie-Hellman Group for Perfect Forward Secrecy

inside

19

- g) [次へ (Next)] をクリックします。
- h) サマリーを確認し、[終了 (Finish)] をクリックします。
- i) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- j) [今すぐ展開 (Deploy Now)] ボタンをクリックして、導入が正常に完了するまで待ちます。

これで、サイト A のデバイスがサイト間 VPN 接続のもう一端をホストできるようになりました。サイト B は互換性のある設定ですでに設定されているため、2 台のデバイスは VPN 接続をネゴシエートする必要があります。

デバイスの CLI にログインし、ディレクトリ サーバに ping することで、接続を確認できます。 **show ipsec sa** コマンドを使用して、このセッション情報を表示することもできます。

ステップ 4 [サイト A (Site A)] のディレクトリ サーバを設定します。[テスト (Test)] をクリックして、接続があることを確認します。

- a) [オブジェクト (Objects)] を選択し、目次から [アイデンティティレルム (Identity Realm)] [アイデンティティソース (Identity Sources)] を選択します。
- b) [+] ボタンをクリックします。
- c) 基本レルムのプロパティを設定します。

- [名前 (Name)] : ディレクトリ レルムの名前。例、AD。
- [タイプ (Type)] : ディレクトリ サーバのタイプ。サポートされるタイプは Active Directory のみで、このフィールドを変更することはできません。
- [ディレクトリユーザ名 (Directory Username)]、[ディレクトリパスワード (Directory Password)] : 取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com (Administrator だけでなく) などの完全修飾名である必要があります。

(注) この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=adminisntrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN (Base DN)] : ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリ ツリー。例、

cn=users,dc=example,dc=com。ベース DN の検索の詳細については、[ディレクトリ ベースの DN の決定 \(148 ページ\)](#) を参照してください。

- [ADプライマリドメイン (AD Primary Domain)] : デバイスが参加する必要がある完全修飾 Active Directory ドメイン名。例、example.com。

<p>Name</p> <p>AD</p>	<p>Type</p> <p>Active Directory (AD)</p>
<p>Directory Username</p> <p>Administrator@example.com</p> <p><i>e.g. user@example.com</i></p>	<p>Directory Password</p> <p>.....</p>
<p>Base DN</p> <p>cn=users,dc=example,dc=com</p> <p><i>e.g. ou=user, dc=example, dc=com</i></p>	<p>AD Primary Domain</p> <p>example.com</p> <p><i>e.g. example.com</i></p>

d) ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス (Hostname/IP Address)] : ディレクトリ サーバのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。この例では、「192.168.1.175」と入力します。
- [ポート (Port)] : サーバとの通信に使用するポート番号。デフォルトは389です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。この例では、389 のままにします。
- [暗号化 (Encryption)] : ユーザおよびグループ情報のダウンロードに暗号化された接続を使用します。デフォルトは[なし (None)]で、ユーザおよびグループ情報はクリアテキストでダウンロードされます。RA VPN の場合は、LDAP over SSL である [LDAPS] を使用できます。このオプションを選択する場合は、ポート 636 を使用します。RA VPN は STARTTLS をサポートしていません。この例では、[なし (None)] を選択します。
- [信頼できるCA証明書 (Trusted CA Certificate)] : 暗号化方式を選択する場合、認証局 (CA) の証明書をアップロードして、システムとディレクトリ サーバ間の信頼できる接続を有効にします。認証に証明書を使用する場合、証明書内のサーバの名前は、サーバの [ホスト名またはIPアドレス (Hostname/IP Address)] と一致している必要があります。たとえば、IP アドレスとして 192.168.1.175 を使用し、証明書では ad.example.com を使用している場合、接続は失敗します。

Directory Server Configuration

Hostname / IP Address	Port
<input type="text" value="192.168.1.175"/>	<input type="text" value="389"/>
<i>e.g. ad.example.com</i>	
Encryption	Trusted CA certificate
<input type="text" value="NONE"/>	<input type="text" value="Please select a certificate"/>

- e) [テスト (Test)] ボタンをクリックして、システムがサーバに接続できることを確認します。

サーバアクセスには異なるプロセスが使用されるため、アイデンティティ ポリシーには使用できるが、リモートアクセス VPN には使用できないなど、あるタイプの使用においては接続が機能するが別のタイプでは機能しないことを示すエラーが表示されることがあります。サーバに到達できない場合は、正しい IP アドレスとホスト名を指定していること、DNS サーバに当該ホスト名のエントリなどが設定されていることを確認します。また、サイト間 VPN 接続が機能していること、サイト A の外部インターフェイスアドレスを VPN に含めていること、および NAT がディレクトリ サーバのトラフィックを変換していないことを確認します。サーバのスタティックルートを設定する必要がある場合もあります。

- f) [OK] をクリックします。

ステップ 5 [デバイス (Device)] > [スマートライセンス (Smart License)] > [設定の表示 (View Configuration)] をクリックし、RA VPN ライセンスを有効にします。

RA VPN ライセンスを有効にする場合は、購入したライセンスのタイプ (Plus、Apex (または両方)、VPN Only) を選択します。詳細については、[リモートアクセス VPN のライセンス要件 \(432 ページ\)](#) を参照してください。

RA VPN License Type

Enabled

Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

ステップ 6 サイト A のリモートアクセス VPN を設定します。

- a) [デバイス (Device)] をクリックし、[リモートアクセス VPN (Remote Access VPN)] グループで [接続プロファイルの設定 (Setup Connection Profile)] をクリックします。
- b) AnyConnect クライアントの設定を定義します。

- [接続プロファイル名 (Connection Profile Name)] : スペースを含めずに最大 50 文字で、この接続の名前を指定します。例、MainOffice。IP アドレスは名前として使用できません。

(注) ここで入力する名前が、AnyConnect クライアントの接続リストに表示されません。ユーザにとって意味のある名前を選択します。

- [ユーザ認証用ADレルム/ディレクトリサーバ (AD Realm/Directory Server for User Authentication)][ユーザ認証用アイデンティティソース (Identity Source for User Authentication)] : ディレクトリレルムを選択します。
- [AnyConnectパッケージ (AnyConnect Packages)] : この VPN 接続でサポートする AnyConnect の完全なインストール ソフトウェア イメージ。パッケージごとに、ファイル名 (拡張子を含む) を 60 文字以下で指定します。Windows、Mac、Linux のエンドポイントに対して別々のパッケージをアップロードできます。

パッケージは software.cisco.com からダウンロードします (ページの最後に適切な場所へのリンクがあります)。エンドポイントにまだ適切なパッケージがインストールされていない場合、ユーザ認証後に、パッケージをダウンロードしてインストールするように求められます。

Connection Profile Name

MainOffice

AD Realm/Directory Server for User Authentication

AD

AnyConnect Packages

Windows

 anyconnect-win-4.4.00243-webdeploy-k9.pkg

Upload New

Choose another package to upload

- c) [次へ (Next)] をクリックします。
- d) デバイス ID とクライアントアドレッシングの設定を定義します。
 - [デバイスIDの証明書 (Certificate of Device Identity)] : DefaultInternalCertificate を選択します。これは、デバイスの ID の確立に使用される内部証明書です。クライアントはこの証明書を承認して、セキュアな VPN 接続を完了させる必要があります。他に使用したい証明書がある場合は、ドロップダウンリストで [新しい内部証明書の作成

(Create New Internal Certificate)] をクリックして、その証明書をアップロードします。

- [外部インターフェイス (Outside Interface)] : [外部 (outside)] (192.168.4.6 の IP アドレスが設定されているインターフェイス) を選択します。これは、リモートアクセス VPN 接続を行うときにユーザが接続するインターフェイスです。

Certificate of Device Identity

DefaultInternalCertificate

Outside Interface

AnyConnect clients connect to this interface

outside

- [外部インターフェイスの完全修飾ドメイン名 (Fully-qualified Domain Name for the Outside Interface)] : インターフェイスの名前。例、ravpn.example.com。名前を指定すると、クライアントプロファイルが作成されます。この例では、空白のままにします。

(注) VPN およびクライアントで使用される DNS サーバが、外部インターフェイスの IP アドレスに対してこの名前を解決できることを保証する必要があります。関連する DNS サーバに FQDN を追加します。

- [IPv4、IPv6 アドレスプール (IPv4, IPv6 Address Pools)] : これらのオプションでリモートエンドポイントのアドレスプールを定義します。この例では、IPv4 アドレスプールで [新規ネットワークの作成 (Create New Network)] を選択し、172.18.1.0/24 ネットワークのオブジェクトを作成して、そのオブジェクトを選択します。クライアントには、このプールからアドレスが割り当てられます。IPv6 プールは空白のままにします。アドレスプールを外部インターフェイスの IP アドレスと同じサブネット上に設定することはできません。

オブジェクトは次のようになります。

Name

ra-vpn-pool

Description

Type

 Network

Network

172.18.1.0/24

プールの仕様は次のようになります。

IPv4 Address Pool

Endpoints are provided an address from this pool

ra-vpn-pool

IPv6 Address Pool

Endpoints are provided an address from this pool

Please select

- [プライマリ、セカンダリDNSサーバ (Primary, Secondary DNS Servers)]: この例では、[OpenDNS] ボタンをクリックして、OpenDNS パブリック DNS サーバとともにこれらのフィールドをロードします。RA VPN クライアントは、VPN に接続するときに、これらの DNS サーバのクライアントを使用してドメイン名を解決します。必要に応じて、DNS サーバの IP アドレスを入力します。
- [ドメイン検索名 (Domain Search Name)]: ネットワークのドメイン名 (example.com など) を入力します。このドメインは、完全修飾されていないホスト名 (たとえば、serverA.example.com ではなく serverA) に追加されます。

Primary DNS IP Address

208.67.222.222

Secondary DNS IP Address

208.67.220.220

Domain Search Name

example.com

- e) [次へ (Next)] をクリックします。
- f) AnyConnect クライアントの動作をカスタマイズするための接続の設定を定義します。

デフォルトの設定はほとんどのネットワークに適しているため、すべてのオプションをデフォルトのままにします。

[NAT免除 (NAT Exempt)] を選択しているため、次のオプションを設定する必要がありません。

- [内部インターフェイス (Inside Interfaces)] : [内部 (inside)] インターフェイスを選択します。これらは、内部ネットワークのリモート ユーザがアクセスするインターフェイスです。これらのインターフェイスには NAT ルールが作成されます。
- [内部ネットワーク (Inside Networks)] : SiteAInside ネットワーク オブジェクトを選択します。これらは、内部ネットワークのリモートユーザがアクセスするオブジェクトを表すネットワーク オブジェクトです。

Split Tunneling



NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal


 inside

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions must match, either IPv4, IPv6, or both.


 SiteAInside

- g) [次へ (Next)] をクリックします。
- h) サマリーを確認します。

最初に、サマリーが正しいことを確認します。

次に、[手順 (Instructions)] をクリックして、AnyConnect ソフトウェアをインストールし、VPN 接続を完了できることをテストするためにエンドユーザが最初に行う必要がある内容を確認します。[コピー (Copy)] をクリックして、それらの手順をクリップボードにコピーし、テキストファイルまたは電子メールに貼り付けます。

- i) [終了 (Finish)] をクリックします。

ステップ 7 Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



ステップ 8 [今すぐ展開 (Deploy Now)] ボタンをクリックして、導入が正常に完了するまで待ちます。

これで、サイト A のデバイスが RA VPN の接続を承認できるようになりました。外部ユーザに AnyConnect クライアントをインストールさせて、VPN 接続を完了させます。

接続を確認するには、デバイス CLI にログインし、**show vpn-sessiondb anyconnect** コマンドを使用してセッション情報を表示します。



第 **IV** 部

システム管理

- システム設定 (475 ページ)
- システム管理 (489 ページ)



第 17 章

システム設定

ここでは、[システム設定 (System Settings)] ページでグループ化されているさまざまなシステム設定の設定方法について説明します。設定は、システムの機能全体を網羅しています。

- [管理アクセス リストの設定 \(475 ページ\)](#)
- [診断ロギングの設定 \(477 ページ\)](#)
- [DHCP サーバの設定 \(479 ページ\)](#)
- [DNS の設定 \(481 ページ\)](#)
- [管理インターフェイスの設定 \(482 ページ\)](#)
- [デバイスのホスト名の設定 \(484 ページ\)](#)
- [Network Time Protocol \(NTP\) の設定 \(484 ページ\)](#)
- [URL フィルタリングの設定 \(485 ページ\)](#)
- [クラウドサービスの設定 \(486 ページ\)](#)

管理アクセス リストの設定

デフォルトでは、任意の IP アドレスから、デバイスの Firepower Device Manager ウェブまたは管理アドレスの CLI インターフェイスにアクセスできます。システム アクセスは、ユーザ名/パスワードのみで保護されています。ただし、特定の IP アドレスまたはサブネットのみからの接続を許可するようアクセス リストを設定し、さらにレベルの高い保護を提供できます。

また、データインターフェイスを開いて、Firepower Device Manager または SSH による CLI 接続を許可することもできます。これにより、管理アドレスを使用せずにデバイスを管理できます。たとえば、外部インターフェイスへの管理アクセスを許可し、デバイスをリモートで設定できます。ユーザ名/パスワードにより、不要な接続から保護します。デフォルトでは、データインターフェイスへの HTTPS 管理アクセスは内部インターフェイスで有効になっていますが、外部インターフェイスでは無効になっています。デフォルトの「内部」ブリッジグループを持つデバイス モデルの場合、ブリッジグループ内の任意のデータインターフェイスを介して、ブリッジグループ IP アドレス (デフォルトは 192.168.1.1) への Firepower Device Manager 接続が可能になります。管理接続は、デバイスに入るインターフェイス上でのみ開くことができます。



注意 特定のアドレスへのアクセスを制限すると、システムから簡単にロックアウトできます。現在使用している IP アドレスへのアクセスを削除し、「任意」のアドレスへのエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。アクセスリストを設定する場合は、特に注意してください。

始める前に

同じ TCP ポートの同じインターフェイスで Firepower Device Manager アクセス (HTTPS アクセス)、AnyConnect リモート アクセス SSL VPN の両方を構成することはできません。たとえば、外部インターフェイスにリモートアクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。Firepower Device Manager ではこれらの機能に使用されるポートを設定できないため、同じインターフェイスで両方の機能は設定できません。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[System Settings] > [Management Access] の順にリンクをクリックします。

[システム設定 (System Settings)] ページがすでに表示されている場合は、目次で [管理アクセスリスト (Management Access List)] [管理アクセス (Management Access)] をクリックします。

ステップ 2 管理アドレスのルールを作成するには、以下の手順に従います。

a) [管理インターフェイス (Management Interface)] タブを選択します。

ルールのリストは、指定したポートへのアクセスが許可されるアドレスを定義します。Firepower Device Manager (HTTPS Web インターフェイス) の場合は 443、SSH CLI の場合は 22 です。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

(注) ルールを削除するには、ルールの [ごみ箱 (trash can)] アイコン (🗑️) をクリックします。すべてのプロトコルのルールを削除した場合は、誰もプロトコルを使用してそのインターフェイスのデバイスにアクセスすることはできません。

b) [+] をクリックし、次のオプションを入力します。

- [プロトコル (Protocol)] : ルールが HTTPS (ポート 443) または SSH (ポート 22) 用かを選択します。
- [IP アドレス (IP Address)] : システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワーク オブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

c) [OK] をクリックします。

ステップ3 データインターフェイスへのルールを作成するには、以下の手順に従います。

a) [データインターフェイス (Data Interfaces)] タブを選択します。

ルールのリストには、インターフェイス上の指定されたポート (Firepower Device Manager (HTTPS Web インターフェイス) の場合は 443、SSH CLI の場合は 22) へのアクセスが許可されるアドレスが定義されています。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

(注) ルールを削除するには、ルールの [ごみ箱 (trash can)] アイコン (🗑️) をクリックします。すべてのプロトコルのルールを削除した場合は、誰もプロトコルを使用してそのインターフェイスのデバイスにアクセスすることはできません。

b) [+] をクリックし、次のオプションを入力します。

- [インターフェイス (Interface)] : 管理アクセスを許可するインターフェイスを選択します。
- [プロトコル (Protocols)] : ルールが HTTPS (ポート 443) または SSH (ポート 22) 、またはその両方用かを選択します。外部インターフェイスがリモート アクセス VPN 接続プロファイルで使用されている場合、その外部インターフェイスに HTTPS ルールを設定することはできません。
- [許可されたネットワーク (Allowed Networks)] : システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワークオブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4](0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

c) [OK] をクリックします。

診断ロギングの設定

診断ロギングは、接続に関係していないイベントの syslog メッセージを提供します。個々のアクセスコントロールルール内に接続ロギングを設定します。次の手順では、診断メッセージのロギングの設定方法について説明します。

手順

ステップ1 [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [ログ設定 (Logging Settings)] リンクの順にクリックします。

[システム設定 (System Settings)] ページをすでに開いている場合、目次の [ロギングの設定 (Logging Settings)] をクリックします。

ステップ 2 [診断ログの設定 (Diagnostic Log Settings)] > [オン (On)] をクリックします。

このページの残りのフィールドを設定しても、この設定を有効にしなければ診断ログメッセージは生成されません。

ステップ 3 診断ログメッセージを確認したい各場所のスライダを [オン (On)] に切り替えて、最低の重大度レベルを選択します。

メッセージは次の場所に記録できます。

- [コンソール (Console)] : メッセージは、コンソールポートの CLI にログインすると表示されます。さらに、**show console-output** コマンドを使用することで、他のインターフェイス (管理アドレスを含む) に対する SSH セッションでもこれらのログが表示されます。さらに、メイン CLI から **system support diagnostic-cli** と入力すると診断 CLI でリアルタイムでこれらのメッセージを表示できます。
- [Syslog] : メッセージは、指定する外部の syslog サーバに送信されます。[+] をクリックして syslog サーバオブジェクトを選択し、ポップアップダイアログボックスで [OK] をクリックします。サーバのオブジェクトがまだ存在していない場合は、[Syslogサーバの追加 (Add Syslog Server)] をクリックして作成します。

ステップ 4 [保存 (Save)] をクリックします。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。

表 9: Syslog メッセージの重大度

レベル番号	重大度	説明
0	緊急	システムが使用不可能な状態です。
1	アラート	すぐに措置する必要があります。
2	重大	深刻な状況です。
3	エラー	エラー状態です。
4	警告	警告状態です。
5	通知	正常ですが、注意を必要とする状況です。
6	情報	情報メッセージです。
7	デバッグ	デバッグメッセージです。



(注) Firepower Threat Defense は、重大度 0（緊急）の syslog メッセージを生成しません。

DHCP サーバの設定

DHCP サーバは、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。接続されたネットワークで DHCP クライアントに構成パラメータを提供するように、インターフェイスで DHCP サーバを設定できます。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。DHCP サーバは、BOOTP 要求をサポートしていません。

DHCP クライアントは、サーバが有効になっているインターフェイスと同じネットワークに属している必要があります。つまり、スイッチがあるとしても、サーバとクライアントの間にルータを介在させることはできません。



(注) すでに DHCP サーバが動作しているネットワークで DHCP サーバを設定しないでください。2 つのサーバが競合するため、結果は予測不可能になります。

手順

- ステップ 1** [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [DHCP サーバ (DHCP Server)] リンクをクリックします。
- [システム設定 (System Settings)] ページをすでに開いている場合、目次の [DHCP サーバ (DHCP Server)] をクリックします。
- ページには 2 つのタブがあります。当初、[設定 (Configuration)] タブには、グローバルパラメータが表示されます。
- [DHCP サーバ (DHCP Servers)] タブには、DHCP サーバを設定したインターフェイスと、サーバが有効にされているかどうか、そしてサーバのアドレスプールが表示されます。
- ステップ 2** [設定 (Configuration)] タブで、自動設定およびグローバル設定を設定します。
- DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。通常、外部インターフェイスで DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

- a) 自動設定を利用する場合、**[自動設定を有効にする (Enable Auto Configuration)]** > **[オン (On)]** をクリックしてから (スライダは右側に移動)、DHCP を介してアドレスを取得するインターフェイスを **[次のインターフェイスから取得 (From Interface)]** で選択します。
- b) 自動設定を有効にしない場合、または自動設定された設定を上書きするには、次のグローバルオプションを設定します。これらの設定は、DHCPサーバをホストするすべてのインターフェイスで DHCP クライアントに送信されます。
 - **[プライマリ WINS IP アドレス (Primary WINS IP Address)]**、**[セカンダリ WINS IP アドレス (Secondary WINS IP Address)]** : Windows インターネット ネーム サービス (WINS) サーバクライアントのアドレスは、NetBIOS の名前解決に使用されます。
 - **[プライマリ DNS IP アドレス (Primary DNS IP Address)]**、**[セカンダリ DNS IP アドレス (Secondary DNS IP Address)]** : クライアントがドメイン名の解決に使用するドメインネーム システム (DNS) サーバのアドレス。OpenDNS パブリック DNS サーバを設定するには、**[OpenDNS を使用する (Use OpenDNS)]** をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。
- c) **[保存 (Save)]** をクリックします。

ステップ 3 [DHCPサーバ (DHCP Servers)] タブをクリックし、サーバを設定します。

- a) 次のいずれかを実行します。
 - まだリストされていないインターフェイスの DHCP サーバを設定するには、**[+]** をクリックします。
 - 既存の DHCP サーバを編集するには、そのサーバの編集アイコン (🔍) をクリックします。

サーバを削除するには、サーバのごみ箱アイコン (🗑️) をクリックします。

- b) サーバプロパティを設定します。
 - **[DHCPサーバを有効にする (Enable DHCP Server)]** : サーバを有効にするかどうかを決定します。サーバを設定できますが、使用する準備が整うまでサーバは無効にしておきます。
 - **[インターフェイス (Interface)]** : クライアントに DHCP アドレスを提供するインターフェイスを選択します。インターフェイスは静的 IP アドレスを持っている必要があります。インターフェイスで DHCP サーバを実行する場合、インターフェイスアドレスの取得に DHCP を使用することはできません。ブリッジグループの場合、メンバーインターフェイスではなく、ブリッジ仮想インターフェイス (BVI) で DHCP サーバを設定します。そうすると、サーバはすべてのメンバーインターフェイスで有効になります。

診断インターフェイスで DHCP サーバを設定することはできません。**[デバイス (Device)]** > **[システム設定 (System Settings)]** > **[管理インターフェイス (Management Interface)]** ページの管理インターフェイスで設定します。

- [アドレスプール (Address Pool)] : アドレスを要求するクライアントにサーバが提供できる IP アドレスの最小から最大までの範囲。プールの開始アドレスと終了アドレスをハイフンで区切って指定します。たとえば、10.100.10.12-10.100.10.250 のように指定します。

IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。

アドレスプールのサイズは、FTD デバイス上のプールあたり 256 アドレスに制限されています。アドレスプールの範囲が 253 アドレスよりも大きい場合、FTD インターフェイスのネットマスクは、クラス C アドレス (たとえば、255.255.255.0) にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

- c) [OK] をクリックします。

DNS の設定

ドメイン ネーム システム (DNS) サーバは、IP アドレスのホスト名の解決に使用されます。これらのサーバは管理インターフェイスによって使用されます。DNS サーバは初期システム設定の際に設定しますが、次のプロシージャを使用して設定を変更できます。

configure network dns servers および **configure network dns searchdomains** コマンドを使用して、CLI で DNS の設定を変更することもできます。

DNS 解決に関する問題が発生した場合は、[管理インターフェイスの DNS のトラブルシューティング \(508 ページ\)](#) を参照してください。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[システム設定 (System Settings)] > [DNSサーバ (DNS Server)] リンクの順にクリックします。

[システム設定 (System Settings)] ページをすでに開いている場合、目次の [DNSサーバ (DNS Server)] をクリックします。

- ステップ 2** [プライマリ、セカンダリ、ターシャリ DNS IP アドレス (Primary, Secondary, Tertiary DNS IP address)] に、DNS サーバの IP アドレスを優先順位に従って 3 つまで入力します。

使用していたプライマリ DNS サーバからの応答がなくなると、セカンダリが使用され、最後にターシャリが使用されます。

OpenDNS パブリック DNS サーバを設定するには、[OpenDNSを使用する (Use OpenDNS)] をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

ステップ 3 [ドメイン検索名 (Domain Search Name)] に、`example.com` などのネットワークのドメイン名を入力します。

このドメインは、完全修飾されていないホスト名に追加されます (たとえば `serverA.example.com` ではなく `serverA` のようなホスト名)。

ステップ 4 [保存 (Save)] をクリックします。

管理インターフェイスの設定

管理インターフェイスは物理的な管理ポートに接続されている仮想インターフェイスです。物理ポートは診断インターフェイスと呼ばれ、他の物理ポートとともにインターフェイスページで設定できます。Firepower Threat Defense Virtual では、両方のインターフェイスが仮想であってもこの二重性が維持されます。

管理インターフェイスには 2 つの使い方があります。

- IP アドレスへの Web および SSH 接続を開き、インターフェイスからデバイスを設定できます。
- システムはこの IP アドレスを使用してスマート ライセンスおよびデータベースの更新情報を取得します。

CLI セットアップウィザードを使用すると、システムの初期設定時にデバイスの管理アドレスとゲートウェイを設定します。Firepower Device Manager のセットアップウィザードを使用すると、管理アドレスとゲートウェイ アドレスはデフォルトのまま変更されません。

必要に応じて、Firepower Device Manager を通じてこれらのアドレスを変更できます。**configure network ipv4 manual** および **configure network ipv6 manual** コマンドを使用して、CLI で管理アドレスおよびゲートウェイを変更することもできます。

管理ネットワーク上の他のデバイスが DHCP サーバとして機能している場合、スタティックアドレスを定義するか、または DHCP を介してアドレスを取得できます。デフォルトでは、管理アドレスは静的であり、DHCP サーバはポートで実行されます (DHCP サーバのない Firepower Threat Defense Virtual は除く)。そのため、デバイスを管理ポートに直接接続し、ワークステーションの DHCP アドレスを取得できます。これにより、デバイスの接続と設定が容易になります。



注意 現在接続されているアドレスを変更した場合は、その変更がすぐに適用されるため、変更の保存と同時に、Firepower Device Manager (または CLI) にアクセスできなくなります。デバイスに接続し直す必要があります。新しいアドレスが管理ネットワークで使用できることを確認します。

手順

ステップ 1 [デバイス (Device)] をクリックし、次に [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] リンクをクリックします。

すでにシステム設定ページを開いている場合、目次の [管理インターフェイス (Management Interface)] をクリックします。

ステップ 2 管理ゲートウェイの定義方法を選択します。

ゲートウェイは、システムがインターネット経由でスマートライセンスとデータベース更新 (VDB、ルール、地理位置情報、URL など) を取得し、管理 DNS サーバと NTP サーバに到達する方法を決定します。次のオプションから選択します。

- [データインターフェイスをゲートウェイとして使用 (Use the Data Interfaces as the Gateway)] : 物理管理インターフェイスに接続されている別の管理ネットワークがない場合、このオプションを選択します。トラフィックは、ルーティングテーブルに基づいてインターネットにルーティングされ、通常は、外部インターフェイスを通過します。これがデフォルトのオプションです。ただし、このオプションは Firepower Threat Defense Virtual デバイスではサポートされません。
- [IP アドレスに固有のゲートウェイを使用 (Use Unique Gateways for the Management Interface)] : 管理インターフェイスに接続されている別の管理ネットワークがある場合、IPv4 および IPv6 に固有のゲートウェイ (以下) を指定します。

ステップ 3 管理アドレス、サブネット マスクまたは IPv6 プレフィックス、および IPv4、IPv6、またはその両方のゲートウェイ (必要に応じて) を設定します。

少なくとも 1 組のプロパティを設定する必要があります。1 組は空白にし、そのアドレッシング方式を無効にします。

[タイプ (Type)] > {DHCP} を選択し、DHCP または IPv6 自動設定によってアドレスおよびゲートウェイを取得します。ただし、ゲートウェイとしてデータインターフェイスを使用している場合、DHCP を使用することはできません。この場合はスタティックアドレスを使用する必要があります。

ステップ 4 (オプション) スタティック IPv4 アドレスを設定する場合、ポート上で DHCP サーバを設定します。

管理ポート上で DHCP サーバを設定する場合、直接接続されているクライアント、または管理ネットワーク上のクライアントは、DHCP プールからそれぞれのアドレスを取得できます。このオプションは Firepower Threat Defense Virtual デバイスではサポートされません。

- a) [DHCP サーバを有効化 (Enable DHCP Server)] > [オン (On)] をクリックします。
- b) サーバの [アドレスプール (Address Pool)] を入力します。

アドレスプールとは、アドレスを要求するクライアントに対してサーバが提供できる、最小から最大までの IP アドレスの範囲です。IP アドレスの範囲は管理アドレスと同じサブネット上にある必要があり、次のものを含めることはできません: インターフェイス自体の IP アドレス、ブロードキャストアドレス、またはサブネットのネットワークアドレス。

プールに開始/終了アドレスをハイフンで区切って指定します。たとえば、192.168.45.46-192.168.45.254 などです。

ステップ 5 [保存 (Save)] をクリックして警告を読み、[OK] をクリックします。

デバイスのホスト名の設定

デバイス ホスト名を変更できます。

また、CLI で **configure network hostname** コマンドを使用してホスト名を変更することもできます。



注意 ホスト名を使用してシステムに接続しているときにホスト名を変更すると、変更はただちに適用されるため、変更を保存するときに Firepower Device Manager へのアクセスが失われます。デバイスに接続し直す必要があります。

手順

ステップ 1 [デバイス (Device)] をクリックし、[システム設定 (System Settings)] > [ホスト名 (Hostname)] リンクの順にクリックします。

すでにシステム設定ページを開いている場合、目次の[ホスト名 (Hostname)] をクリックします。

ステップ 2 新しいホスト名を入力します。

ステップ 3 [保存 (Save)] をクリックします。

Network Time Protocol (NTP) の設定

システムの時刻を定義するには、Network Time Protocol (NTP) サーバを設定する必要があります。NTP サーバはシステムの初期設定時に設定しますが、次の手順を使用して変更できます。NTP 通信に関する問題が発生した場合は、[NTP のトラブルシューティング \(507 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Device)] をクリックし、[システム設定 (System Settings)] > [NTP] リンクの順にクリックします。

すでに [システム設定 (System Settings)] ページが表示されている場合は、目次の [NTP] をクリックします。

ステップ 2 [NTPタイムサーバ (NTP Time Server)] で、独自のタイムサーバとシスコのタイムサーバのどちらを使用するか選択します。

- [Cisco NTPタイムサーバ (Cisco NTP Time Server)] [[デフォルトNTPタイムサーバ (Default NTP Time Server)] [[デフォルトNTPサーバ (Default NTP Servers)]: このオプションを選択すると、NTP に使用するサーバ名がサーバリストに表示されます。
- [手動入力 (Manually Input)] [[ユーザ定義NTPサーバ (User-Defined NTP Servers)]: このオプションを選択する場合は、使用する NTP サーバの完全修飾ドメイン名または IP アドレスを入力します。例、ntp1.example.com または 10.100.10.10。複数の NTP サーバがある場合は、[別のNTPタイムサーバを追加 (Add Another NTP Time Server)] をクリックしてアドレスを入力します。

ステップ 3 [保存 (Save)] をクリックします。

URL フィルタリングの設定

URL カテゴリおよびレピュテーションデータベースは Cisco Collective Security Intelligence (CSI) から取得されます。これらの設定により、データベースの更新とシステムが不明なカテゴリまたはレピュテーションの URL を処理する方法が制御されます。これらの設定を行うには、URL フィルタリング ライセンスを有効にする必要があります。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [URL フィルタリングの設定 (URL Filtering Preferences)] リンクの順にクリックします。

[システム設定 (System Settings)] ページをすでに開いている場合、目次の [クラウドの基本設定 (Cloud Preferences)] と [URL フィルタリングの基本設定 (Filtering Preferences)] をクリックします。

ステップ 2 次のオプションを設定します。

- [自動更新の有効化 (Enable Automatic Updates)]: カテゴリとレピュテーションを含む更新された URL データをチェックしてダウンロードすることをシステムに許可します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。デフォルトでは、更新が有効になっています。このオプションを選択解除した状態でカテゴリとレピュテーションのフィルタリングを使用している場合、このオプションを周期的に有効にして新しい URL データを取得してください。
- [不明なURLに対するCisco CSIのクエリ (Query Cisco CSI for Unknown URLs)]: ローカル URL フィルタリングデータベースのカテゴリおよびレピュテーションのデータを含ま

ない URL の更新情報を Cisco CSI でチェックするかどうかを切り替えます。ルックアップが適度な制限時間内に更新情報を返した場合、その情報は、URL の状況に基づいてアクセスルールを選択する際に使用されます。それ以外の場合、URL は分類されていないカテゴリと照合されます。メモリ制限によりインストールされる URL データベースが小さいローエンドのシステムでは、このオプションを選択することが重要です。

ステップ 3 [保存 (Save)] をクリックします。

クラウドサービスの設定

[クラウドサービス (Cloud Services)] ページを使用すると、デバイスによって使用されるクラウドベースのサービスをデバイス側から管理できます。特定のサービスを登録した後は、クラウドから管理する必要があります。

ページの上部にある [クラウドサービスポータル (Cloud Services Portal)] リンクをクリックして、[シスコクラウドサービス (Cisco Cloud Services)] に移動し、クラウドベースのサービスを管理できます。

ここでは、クラウドサービスのオプションについて説明します。

クラウド管理の設定 (Cisco Defense Orchestrator)

Cisco Defense Orchestrator のクラウドベースのポータルを使用してデバイスを管理できます。Cisco Defense Orchestrator を使用すると、次のテクニックによりデバイス管理にアプローチできます。

- 初期設定のダウンロード：このアプローチでは、Cisco Defense Orchestrator からデバイスの初期設定をダウンロードしますが、その後 Firepower Device Manager を使用してデバイスをローカルで設定します。



(注) Firepower Device Manager を使用してデバイスを設定した後、代わりにクラウド経由でデバイスを管理することにした場合、クラウドベースの設定でローカルの変更を重複させるようにします。

- クラウドによるリモート設定管理：このアプローチでは、Cisco Defense Orchestrator を使用してデバイス設定を作成および更新します。このアプローチを使用する場合、ローカルで設定を変更しないでください。各クラウドの導入では、クラウドで定義した設定によりデバイスのローカル設定が置き換えられるためです。ローカルで変更した場合、変更を維持するには、クラウドベースの設定でも同じ設定を繰り返してください。

クラウド管理の仕組みの詳細については、Cisco Defense Orchestrator ポータル (<http://www.cisco.com/go/cdo>) を参照するか、共に作業している再販業者またはパートナーにお問い合わせください。

始める前に

Cisco Defense Orchestrator の登録キーを取得します。

デバイスを Cisco Smart Software Manager (CSSM) にすでに登録している場合は、最初に [スマートライセンス (Smart Licensing)] ページからデバイスを登録解除することを強く推奨します。トークンを使用して Cisco Defense Orchestrator を有効にした後で再登録できます。

また、デバイスにインターネットへのルートがあることを確認します。

手順

ステップ 1 [デバイス (Device)] をクリックし、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] リンクの順にクリックします。

すでに [システム設定 (System Settings)] ページを表示している場合は、目次の [クラウドサービス (Cloud Services)] をクリックします。

ステップ 2 [Cisco Defense Orchestrator] グループで、[始める (Get Started)] をクリックします。

ステップ 3 [登録キー (Registration Key)] にキーを貼り付け、[接続 (Connect)] をクリックします。

登録要求がクラウドポータルに送信されます。キーが有効で、インターネットへのルートがある場合、デバイスはポータルに正常に登録されるはずですが、その後、ポータルを使用してデバイスを管理できます。

クラウド管理を使用しない場合は、[無効化 (Disable)] をクリックします。

Cisco Success Network への接続

デバイスを登録するときに、Cisco Success Network への接続を有効にするかどうかを決めます。[デバイスの登録 \(100 ページ\)](#) を参照してください。

Cisco Success Network を有効にすると、テクニカルサポートを提供するために不可欠な使用状況の情報と統計情報がシスコに提供されます。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。

接続を有効にすると、シスコから提供されているテクニカルサポートサービス、クラウド管理および監視サービスなどの追加サービスに参加できるように、デバイスで Cisco Cloud へのセキュアな接続が確立されます。お使いのデバイスは、いつでもこのセキュアな接続を確立して維持できます。

この接続は、Cisco Success Network および Cisco Defense Orchestrator の両方を無効にすることで、いつでもオフにできます。両方を無効にすると、デバイスがクラウドから切断されます。切断しても更新の受信やスマートライセンス機能の操作には影響せず、正常に動作を継続します。

デバイスを登録した後で Cisco Success Network の設定を変更できます。



(注) システムがシスコにデータを送信する際に、タスク リストにテレメトリ ジョブが表示されません。

始める前に

Cisco Success Network を有効にするには、デバイスをクラウドに登録する必要があります。デバイスを登録するには、([スマートライセンス (Smart Licensing)] ページで) Cisco Smart Software Manager にデバイスを登録するか、または登録キーを入力して Cisco Defense Orchestrator に登録します。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] リンクの順にクリックします。

[システム設定 (System Settings)] ページがすでに表示されている場合は、目次で [クラウドサービス (Cloud Services)] をクリックします。

ステップ 2 必要に応じて Cisco Success Network 機能の [有効化 (Enable)]/[無効化 (Disable)] コントロールをクリックして設定を変更します。

[サンプルデータ (sample data)] リンクをクリックするとシスコに送信される情報の種類を確認できます。

接続を有効にする場合、情報開示を読み、[同意 (Accept)] をクリックします。



第 18 章

システム管理

ここでは、システムデータベースの更新やシステムのバックアップおよび復元などの、システム管理タスクの実行方法について説明します。

- [ソフトウェアアップデートのインストール \(489 ページ\)](#)
- [システムのバックアップと復元 \(496 ページ\)](#)
- [システムの再起動 \(501 ページ\)](#)
- [システムのトラブルシューティング \(501 ページ\)](#)
- [一般的でない管理タスク \(515 ページ\)](#)

ソフトウェアアップデートのインストール

システムデータベースとシステムソフトウェアの更新プログラムをインストールできます。ここでは、これらの更新プログラムのインストール方法について説明します。

システムデータベースおよびフィードの更新

システムは、複数のデータベースおよびセキュリティインテリジェンスフィードを使用して高度なサービスを提供します。シスコでは、セキュリティポリシーで最新の情報が使用されるよう、これらのデータベースおよびフィードに対する更新を提供しています。

システムデータベースおよびフィードの更新の概要

Firepower Threat Defense は次のデータベースおよびフィードを使用して高度なサービスを提供します。

侵入ルール

新たな脆弱性が発見されると、Cisco Talos Intelligence Group (Talos) から侵入ルールのアップデートがリリースされ、インポートできます。それらの更新は、侵入ルール、プリプロセッサルール、およびルールを使用するポリシーに影響を及ぼします。

侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれて

います。ルールを更新では、ルールが削除されたり、新しいルールカテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。

侵入ルールの更新によって行われた変更を有効にするには、設定を再展開する必要があります。

侵入ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに実行してください。低速ネットワークでは更新試行が失敗する可能性があります。再試行する必要があります。

位置情報データベース (GeoDB)

シスコの地理位置情報データベース (GeoDB) は、ルート可能な IP アドレスに関連する位置情報データ (国、都市、緯度と経度の座標など)、および接続関係のデータ (インターネットサービスプロバイダー、ドメイン名、接続タイプなど) のデータベースです。

GeoDB の更新には、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する更新情報が含まれています。位置情報データは、アクセス コントロールルールとして使用できます。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30～40 分かかります。GeoDB の更新は他のシステムの機能 (実行中の地理情報の収集など) を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。更新を計画する場合には、この点について考慮してください。

脆弱性データベース (VDB)

シスコの脆弱性データベース (VDB) は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。Firepower システムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。Cisco Talos Intelligence Group (Talos) では、VDB の定期的な更新を配布しています。

脆弱性のマッピングを更新するのにかかる時間は、ネットワークマップ内のホストの数によって異なります。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間帯に更新をスケジュールすることをお勧めします。一般的に、更新の実行にかかるおおよその時間 (分) を判断するには、ネットワーク上のホストの数を 1000 で割ります。

VDB を更新した後、更新されたアプリケーションディテクタとオペレーティング システムフィンガープリントを有効にするために、設定を再展開する必要があります。

Cisco Talos Intelligence Group (Talos) セキュリティ インテリジェンスのフィード

Talos は、セキュリティ インテリジェンス ポリシーで使用するため定期的に更新されるインテリジェンス フィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。これらのフィードには、既知の脅威のアドレスや URL が含まれています。システムによってフィードが更新される場合、再展開する必要はありません。後続の接続の評価には新しい一覧が使用されます。

URL カテゴリ/レピュテーション データベース

システムは、Cisco Collective Security Intelligence (CSI) から URL カテゴリとレピュテーションデータベースを取得します。カテゴリとレピュテーションに関してフィルタリングする URL フィルタリング アクセス制御ルールを設定すると、要求された URL がデータベースと照合されます。[システム設定 (System Settings)] > [URL フィルタリングの設定 (URL Filtering Preferences)] でデータベースの更新といくつかのその他の URL フィルタリング設定を設定できます。URL カテゴリ/レピュテーションデータベースの更新は、他のシステム データベースの更新を管理する方法では管理できません。

システム データベースの更新

必要に応じて、手動でシステムデータベースの更新を取得して適用できます。更新はシスコサポートサイトから取得されます。したがって、システムの管理アドレスからインターネットへのパスが存在する必要があります。

またデータベースの更新を取得して適用するよう、定期的なスケジュールを設定することもできます。これらの更新はサイズが大きい場合があるため、ネットワークアクティビティが少ない時間帯にスケジュールしてください。



(注) データベース更新が進行中の場合、ユーザインターフェイスのアクションへの応答が遅くなる場合があります。

始める前に

保留中の変更に対して潜在的な影響を与えることを避けるため、これらのデータベースを手動で更新する前に、デバイスに設定を展開します。

VDB と URL カテゴリの更新によって、アプリケーションまたはカテゴリが削除される可能性があることに注意してください。変更を展開する前に、これらの廃止された項目を使用しているアクセス制御ルールまたは SSL 復号ルールを更新する必要があります。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[更新 (Updates)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

これによって、[更新 (Updates)] ページが開きます。このページの情報には、各データベースの現在のバージョン、および各データベースの最終更新日時が表示されます。

ステップ 2 手動でデータベースを更新するには、そのデータベースのセクションで [今すぐ更新 (Update Now)] をクリックします。

ルールおよび VDB の更新では、アクティブにするための設定の展開が必要です。今すぐ展開するかどうかを尋ねられます。[はい (Yes)] をクリックします。[いいえ (No)] をクリックする場合は、都合の良いときにできるだけ早く展開ジョブを開始してください。

ステップ 3 (オプション) 定期的なデータベース更新スケジュールを設定するには、次の手順に従います。

- a) 目的のデータベースのセクションで[設定 (Configure)] リンクをクリックします。すでにスケジュールが設定されている場合、[編集 (Edit)] をクリックします。

データベースの更新スケジュールは独立しています。スケジュールは別途定義する必要があります。

- b) 更新開始時刻を設定します。

- 更新の頻度 (日次、週次、または月次) 。
- 週次または月次の場合、更新が必要な曜日または日付。
- 更新を開始する時刻。指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

- c) ルールまたは VDB の更新では、データベースが更新されるたびにシステムが設定を展開するようにする場合は、[更新の自動展開 (Automatically Deploy the Update)] チェックボックスをオンにします。

更新は、展開されるまでは有効になりません。自動展開では、まだ展開されていないその他の設定変更も展開されます。

- d) [保存 (Save)] をクリックします。

(注) 定期的なスケジュールを削除する場合、[編集 (Edit)] リンクをクリックしてスケジューリング ダイアログボックスを開き、[削除 (Remove)] ボタンをクリックします。

Cisco Security Intelligence フィードの更新

Cisco Talos Intelligence Group (Talos) は、定期的に更新されるセキュリティインテリジェンスフィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。システムによってフィードが更新される場合、再展開する必要はありません。後続の接続の評価には新しい一覧が使用されます。

システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にできます。ただし、自動更新を行えば、最新の関連するデータであることが確実にあります。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[更新 (Updates)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

これによって、[更新 (Updates)] ページが開きます。ページには、[セキュリティインテリジェンスフィード (Security Intelligence Feeds)] の現在のバージョン、およびフィードの最終更新日時が表示されます。

ステップ 2 フィードを手動で更新するには、[セキュリティインテリジェンスフィード (Security Intelligence Feeds)] グループで [今すぐ更新 (Update Now)] をクリックします。

ステップ 3 (オプション) 定期的な更新の頻度を設定するには：

a) [シスコのフィード (Cisco Feeds)] セクションにある [設定 (Configure)] リンクをクリックします。すでにスケジュールが設定されている場合、[編集 (Edit)] をクリックします。

b) 希望する頻度を選択します。

デフォルトは [毎時 (Hourly)] です。[毎日 (Daily)] 更新 (時刻を指定) または [毎週 (Weekly)] 更新 (曜日と時刻を指定) を設定することもできます。指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

[削除 (Delete)] をクリックして、自動更新されないようにします。

c) [OK] をクリックします。

Firepower Threat Defense ソフトウェアのアップグレード

Firepower Threat Defense ソフトウェア アップグレードが使用可能になると、インストールできます。次の手順は、システム上ですでに Firepower Threat Defense バージョン 6.2.0 以降が稼働していて、正常に動作していることを前提としています。

アップグレードには、ホットフィックス、マイナーアップグレード、メジャーアップグレードの 3 種類があります。ホットフィックスアップグレードは再起動を必要としない場合がありますが、マイナーバージョンおよびメジャーバージョンのアップグレードには再起動が必要です。再起動が必要な場合、インストール後に自動的に再起動します。更新のインストールによりトラフィックが中断される可能性があるため、インストールは時間外に行ってください。

この手順では、デバイスのイメージ再作成も、ASA ソフトウェアから Firepower Threat Defense ソフトウェアへの移行もできません。



(注) 更新をインストールする前に、保留中の変更がすべて展開されていることを確認します。またバックアップを実行し、バックアップ コピーをダウンロードする必要があります。

始める前に

タスクリストを確認し、実行中のタスクがないことを確認します。アップグレードをインストールする前に、データベースの更新など、すべてのタスクが完了するまで待機してください。また、スケジュール設定したタスクがないか確認してください。アップグレードタスクとスケジュールタスクが重複しないようにしてください。

更新を実行する前に、廃止されたアプリケーションがアプリケーションフィルタ、アクセスルール、またはSSL復号ルールに存在しないことを確認してください。これらのアプリケーションには、アプリケーション名の後に「(廃止) (Deprecated)」が付加されています。これらのオブジェクトに廃止されたアプリケーションを追加することはできませんが、後続のVDB更新により、以前は有効だったアプリケーションが廃止される場合があります。廃止されると、アップグレードは失敗し、デバイスは使用不能状態になります。

Cisco.com にログインし、アップグレードイメージをダウンロードします。

- 適切なアップグレードファイル（ファイルタイプが REL.tar）を入手していることを確認します。システムソフトウェアパッケージまたはブートイメージをダウンロードしないでください。
- アップグレードファイルの名前を変更しないでください。名前が変更されたファイルは無効だと見なされます。
- パッチをダウングレードまたはアンインストールすることはできません。
- アップグレードに必要なベースラインイメージを実行していることを確認します。互換性の情報については、『Cisco Firepower 互換性ガイド』、<http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html> を参照してください。
- 新しいバージョンの場合は、リリースノートをお読みください。リリースノートは <http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html> をご覧ください。

手順

ステップ 1 [デバイス (Device)] をクリックし、[更新サマリー (Updates summary)] の [設定の表示 (View Configuration)] をクリックします。

[システムアップグレード (System Upgrade)] セクションには、現在実行中のソフトウェアバージョン、およびすでにアップロードされた更新が表示されます。

ステップ 2 アップグレードファイルをアップロードします。

- アップグレードファイルをまだアップロードしていない場合、[検索 (Browse)] をクリックしてファイルを選択します。
- すでにアップロードされたファイルがあるか、別のファイルをアップロードする場合、[別のファイルをアップロード (Upload Another File)] をクリックします。1つのファイルの

みアップロードできます。新規ファイルをアップロードすると、古いファイルが置き換えられます。

- ファイルを削除するには、[削除 (Delete)]アイコン () をクリックします。

ステップ3 [インストール (Install)] をクリックして、インストールプロセスを開始します。

アイコンの隣の情報は、インストール中にデバイスが再起動するかどうかを示します。システムから自動的にログアウトされます。インストールには 30 分以上かかることがあります。

待機してからシステムに再度ログインしてください。[デバイスサマリー (Device Summary)] または [システム監視ダッシュボード (System monitoring dashboard)] には、新しいバージョンが表示されます。

- (注) 単にブラウザ ウィンドウを更新するだけではありません。代わりに、URL からパスを削除してホームページに再接続します。これにより、最新のコードではキャッシュされている情報が更新されます。

ステップ4 (オプション) システム データベースを更新します。

地理位置情報、ルール、脆弱性 (VDB) データベースに設定された自動更新ジョブがない場合、この機会に更新してください。

デバイスの再イメージ化

デバイスを再イメージ化すると、デバイス設定が消去され、新しいソフトウェアイメージがインストールされます。再イメージ化の目的は、工場出荷時のデフォルト設定でクリーンインストールすることです。

次の場合に、デバイスを再イメージ化します。

- ASA ソフトウェアから Firepower Threat Defense ソフトウェアにシステムを変換する場合。ASA イメージを実行しているデバイスを Firepower Threat Defense イメージを実行しているデバイスにアップグレードすることはできません。
- デバイスが 6.1.0 以前のイメージを実行していて、6.1 以降のイメージにアップグレードし、Firepower Device Manager を使用してデバイスを設定したい場合。Firepower Management Center を使用して、6.1 以前のデバイスをアップグレードしてからローカル管理を切り替えることはできません。
- デバイスが正しく機能せず、設定の修正ですべての試行が失敗した場合。

デバイスの再イメージ化の詳細については、ご使用のデバイス モデルの『*Reimage the Cisco ASA or Firepower Threat Defense Device*』または *Firepower Threat Defense* のクイック スタートガイドを参照してください。これらのガイドは、

<http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html> で入手できます。

システムのバックアップと復元

後の設定ミスまたは物理的な事故が原因で設定が損なわれた場合にデバイスを復元できるように、システム設定をバックアップできます。

代替のデバイスにバックアップを復元できるのは、どちらのデバイスも同じモデルで、（同時リリースだけでなく、ビルド番号を含む）同じバージョンのソフトウェアを実行している場合のみです。アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップファイルには、この方法で共有することができないようにアプライアンスを一意に特定する情報が含まれます。



(注) バックアップには管理 IP アドレス設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップコピーにより置き換えられることはありません。これにより、アドレスに行きたいかなる変更も保持され、別のネットワークセグメント上のさまざまなデバイスの設定を復元することも可能になります。

バックアップには設定だけが含まれ、システムソフトウェアは含まれません。デバイスを完全に再イメージ化する必要がある場合、ソフトウェアを再インストールしてからバックアップをアップロードして、設定を回復する必要があります。

バックアップ中は設定データベースがロックされます。バックアップの間はポリシー、ダッシュボードなどを表示できますが、設定を変更することはできません。復元を行っている間、システムは完全に使用できません。

「バックアップと復元」ページの表は、バックアップのファイル名、作成日時、ファイルサイズを含む、システムで使用できる既存のすべてのバックアップコピーを示します。バックアップのタイプ（手動、スケジュール、繰り返し）は、システムに指示したバックアップコピーの作成方法に基づいています。



ヒント バックアップコピーはシステム自体に作成されます。ディザスタリカバリのために必要なバックアップコピーを確保するため、バックアップコピーは手動でダウンロードし、安全なサーバに保存する必要があります。

次に、バックアップの管理と復元操作について説明します。

システムの即時バックアップ

希望する場合はいつでもバックアップを開始できます。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

これにより、[バックアップおよび復元 (Backup and Restore)] ページが開きます。使用可能なすべての既存のバックアップ コピーが表にリストされています。

ステップ 2 [手動バックアップ (Manual Backup)] > [今すぐバックアップ (Back Up Now)] をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

今すぐではなく、将来のある時刻にバックアップする場合は、代わりに [スケジュール (Schedule)] をクリックできます。

ステップ 4 [今すぐバックアップ (Back Up Now)] をクリックします。

システムがバックアップ プロセスを開始します。バックアップが完了すると、バックアップ ファイルが表に表示されます。必要に応じて、バックアップ コピーをシステムにダウンロードして、他の場所に保存できます。

バックアップが開始されたら、[バックアップと復元 (Backup and Restore)] ページを閉じてもかまいません。ただし、システムの動作が遅くなる可能性があるため、バックアップが完了するまで作業を一時停止することを検討する必要があります。

また、一部または全部のバックアップ中に、システムによってコンフィギュレーション データベースのロックが取得され、それが原因でバックアップ プロセス中に変更を加えることができなくなる場合があります。

スケジュールされた時間でのシステムのバックアップ

システムを将来の特定の日にバックアップするために、スケジュールバックアップを設定できます。スケジュールバックアップは、1回だけ実行されます。定期的にバックアップを作成するようにバックアップスケジュールを作成するには、スケジュールバックアップではなく、繰り返しバックアップを設定します。



(注) 将来のバックアップのスケジュールを削除するには、スケジュールを編集して、[削除 (Remove)] をクリックします。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

ステップ 2 [スケジュールバックアップ (Scheduled Backup)] > [バックアップをスケジュール (Schedule a Backup)] をクリックします。

すでにスケジュールバックアップがある場合は、[スケジュールバックアップ (Scheduled Backup)] > [編集 (Edit)] をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

ステップ 4 バックアップの日時を入力します。

ステップ 5 [スケジュール (Schedule)] をクリックします。

選択した日時に達すると、システムがバックアップされます。完了すると、バックアップ コピーがバックアップの表に一覧されます。

定期的なバックアップスケジュールの設定

定期的なバックアップを設定し、システムを定期的にバックアップできます。たとえば、毎週金曜日の真夜中にバックアップをとることもできます。定期的なバックアップスケジュールにより、常に最新のバックアップセットを保持できます。



(注) 定期的なスケジュールを削除する場合、スケジュールを編集し、[削除 (Delete)] をクリックします。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

ステップ 2 [定期バックアップ (Recurring Backup)] > [設定 (Configure)] をクリックします。

すでに定期バックアップを設定している場合は、[定期バックアップ (Recurring Backup)] > [編集 (Edit)] をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

ステップ 4 [頻度 (Frequency)] と関連スケジュールを選択します。

- [日次 (Daily)] : 時刻を選択します。バックアップは毎日、スケジュールされた時刻に取得されます。
- [週次 (Weekly)] : 曜日と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、毎週月曜日、水曜日、金曜日の 23 時 (午後 11 時) にバックアップをスケジュールすることもできます。
- [月次 (Monthly)] : 日付と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、1 日、15 日、28 日の 23 時 (午後 11 時) にバックアップをスケジュールすることもできます。

指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに1時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

ステップ 5 [保存 (Save)] をクリックします。

選択した日付と時刻になると、バックアップが取得されます。完了すると、バックアップコピーがバックアップテーブルにリストされます。

定期的なスケジュールを変更または削除するまで、バックアップを取得し続けます。

バックアップの復元

デバイスでバックアップを取得したときに実行されていたものと同じソフトウェアバージョン（ビルド番号を含む）が実行されている限り、バックアップを復元できます。代替のデバイスにバックアップを復元できるのは、どちらのデバイスも同じモデルで、同じバージョンのソフトウェア（ビルド番号を含む）を実行している場合のみです。

復元するバックアップコピーがまだデバイスに存在しない場合、復元する前にまずバックアップをアップロードする必要があります。

復元している間、システムはまったく使用できません。



(注) バックアップには管理 IP アドレスの設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップ コピーにより置き換えられることはありません。これにより、アドレスに対する変更はすべて保持され、また異なるネットワークセグメント上の別のデバイスに設定を復元することもできます。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

これにより、[バックアップおよび復元 (Backup and Restore)] ページが開きます。使用可能なすべての既存のバックアップコピーが表にリストされています。

ステップ 2 復元しようとするバックアップコピーが、使用可能なバックアップのリストにない場合、[アップロード (Upload)] > [検索 (Browse)] をクリックし、バックアップコピーをアップロードします。

ステップ 3 ファイルの [復元 (restore)] アイコン (🔄) をクリックします。

復元するかどうかの確認が求められます。デフォルトでは、復元後にバックアップコピーは削除されますが、これを保持するには、復元を続行する前に、[復元後にバックアップを削除しない (Do not remove the backup after restoring)] を選択します。

復元が完了すると、システムは再起動します。

- (注) システムが再起動後、脆弱性データベース (VDB)、地理位置情報、およびルールデータベースの更新が自動的にチェックされ、必要に応じてダウンロードされます。これらの更新は大規模な場合があるため、初回の試行が失敗する可能性があります。タスクリストを確認し、ダウンロードが失敗した場合は[システムデータベースの更新 \(491 ページ\)](#)の説明に従って手動で更新をダウンロードしてください。またポリシーも再展開されます。更新が成功しないと、それ以降の展開はすべて失敗します。

バックアップファイルの管理

新しいバックアップを作成すると、バックアップファイルがバックアップと復元ページに表示されます。バックアップコピーは無期限に保たれません。デバイスのディスク領域の利用量が最大しきい値に達すると、新しいバックアップコピー用の場所を空けるために、古いバックアップコピーが削除されます。したがって、定期的にバックアップファイルを管理し、最も保持したい特定のバックアップコピーが削除されていないことを確認してください。

バックアップコピーを管理するには、次の操作を行うことができます。

- ファイルを安全なストレージにダウンロード：バックアップファイルをワークステーションにダウンロードするには、ファイルの[ダウンロード (download)]アイコン (📄) をクリックします。その後、安全なファイルストレージにファイルを移動できます。
- システムにバックアップファイルをアップロードする：デバイスで使用できなくなったバックアップコピーを復元する場合は、[アップロード (Upload)] > [ファイルの参照 (Browse File)] をクリックして、バックアップコピーをワークステーションからアップロードします。その後、復元できます。



- (注) アップロードされたファイルは、元のファイル名と一致するように名前が変更される場合があります。また、システムに 10 以上のバックアップコピーがすでに存在する場合、アップロードされたファイル用の場所を空けるために最も古いものは削除されます。古いソフトウェアバージョンによって作成されたファイルをアップロードすることはできません。

- バックアップを復元する：バックアップコピーを復元するには、ファイルの[復元 (restore)]アイコン (🔄) をクリックします。復元の間システムは使用できなくなり、復元が完了するとリブートします。システムが稼働していて、動作中になってから設定を展開してください。
- バックアップファイルを削除する：特定のバックアップが必要でなくなったら、ファイルの削除アイコン (🗑️) をクリックします。削除の確認が求められます。削除すると、バックアップファイルを回復することはできません。

システムの再起動

システムが正常に動作していないときに、他の問題解決手段では解決しない場合は、デバイスを再起動できます。デバイスはCLIから再起動する必要があります。Firepower Device Managerからは再起動できません。

手順

ステップ 1 SSH クライアントを使用して管理 IP アドレスへの接続を開き、Configuration CLI 権限があるユーザ名でデバイスの CLI にログインします。たとえば、[管理者 (admin)] ユーザ名を使用します。

ステップ 2 `reboot` コマンドを入力します。

例：

```
> reboot
```

システムのトラブルシューティング

ここでは、いくつかのシステムレベルのトラブルシューティングのタスクおよび機能について説明します。特定の機能（アクセスコントロールなど）のトラブルシューティングの詳細については、その機能に関する章を参照してください。

接続をテストするための ping アドレス

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。これは基本接続が機能していることを意味します。ただし、デバイスで実行されている他のポリシーにより、特定のタイプのトラフィックは正常にデバイスを通過できないことがあります。ping CLI コンソールを開く、またはデバイス CLI へのログインによって、使用することができます。



(注) システムには複数のインターフェイスがあるため、アドレスの ping に使用されるインターフェイスを制御できます。接続をテストすることが重要であるため、確実に正しいコマンドを使用する必要があります。たとえば、システムは仮想管理インターフェイスを介してシスコライセンスサーバに到達できる必要があるため、`ping system` コマンドを使用して接続をテストする必要があります。ping を使用すると、複数のデータ インターフェイスを通じて到達できるかをテストするため、同じ結果が得られない可能性があります。

通常の ping は、ICMP パケットを使用して接続をテストします。ネットワークで ICMP が禁止されている場合は、代わりに TCP ping を使用できます（データ インターフェイスの ping のみ）。

次に、ネットワーク アドレスを ping するための主なオプションを示します。

仮想管理インターフェイスを介したアドレスの ping

ping system コマンドを使用します。

ping system host

ホストは IP アドレスまたは完全修飾ドメイン名 (FQDN) (www.example.com など) できます。データ インターフェイスを介した ping とは違い、システム ping のデフォルト数はありません。ping は Ctrl+c を使用して停止するまで続けられます。次に例を示します。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

ルーティング テーブルを使用するデータ インターフェイスを介したアドレスの ping

ping コマンドを使用します。インターフェイスを指定せずに、システムが一般的にホストへのルートを検索できるかどうかをテストします。システムは通常このようにしてトラフィックをルーティングするため、一般的に実行する必要があるのはこのテストです。

ping host

ホストの IP アドレスを指定します。FQDN のみ判明している場合は、**nslookup fqdn-name** コマンドを使用して、IP アドレスを判別します。次に例を示します。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```



(注) タイムアウト、繰り返し回数、パケット サイズ、さらには送信するデータ パターンを指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

特定のデータ インターフェイスを介したアドレスの ping

特定のデータインターフェイスを経由した接続をテストする場合、**ping interface *if_name*** コマンドを使用します。このコマンドを使用して診断インターフェイスを指定することもできますが、仮想管理インターフェイスは指定できません。

ping interface *if_name* host

ホストの IP アドレスを指定します。FQDN のみ判明している場合は、**nslookup *fqdn-name*** コマンドを使用して、IP アドレスを判別します。次に例を示します。

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

TCP ping を使用するデータ インターフェイスを介したアドレスの ping

ping tcp コマンドを使用します。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。

ping tcp [interface *if_name*] host port

ホストと TCP ポートを指定する必要があります。FQDN のみ判明している場合は、**nslookup *fqdn-name*** コマンドを使用して、IP アドレスを判別します。

オプションで、**ping** を送信するインターフェイスではなく、**ping** の送信元インターフェイスであるインターフェイスを指定できます。このタイプの **ping** では、必ずルーティング テーブルを使用します。

TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。次に例を示します。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



(注) タイムアウト、繰り返し回数、および TCP ping の送信元アドレスも指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワークパスに問題がないかどうかを確認できます。トレースルートでは、宛先に対して、無効なポートで UDP パケットを送信したり、ICMPv6 エコーを送信したり

します。宛先までの途中にあるルータから ICMP Time Exceeded メッセージが返され、トレースルートにそのエラーが報告されます。各ノードは3つのパケットを受信するため、有益な結果を得る機会が1台のノードにつき3回あります。**traceroute CLI** コンソールを開く、またはデバイス CLI へのログインによって、使用することができます。



- (注) データインターフェイス (**traceroute**) または仮想管理インターフェイス (**traceroute system**) を経由するルートをトレースするための個別のコマンドがあります。適切なコマンドを使用するようにしてください。

次の表に、パケットによって出力に表示される可能性のある結果を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
<i>nn msec</i>	各ノードに対する、指定した数のプローブのラウンドトリップ時間 (ミリ秒)。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。
!A	ICMP が管理者によって禁止されています。
?	原因不明の ICMP エラーが発生しました。

仮想管理インターフェイスを介したルートの追跡

traceroute system コマンドを使用します。

traceroute system 接続先 (*Destination*)

ホストには、IPv4/IPv6 アドレスまたは完全修飾ドメイン名 (FQDN) (`www.example.com` など) を使用できます。次に例を示します。

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
```

```
14 www1.example.com (172.16.4.161) 11.645 ms 7.958 ms 7.936 ms
```

データ インターフェイスを介したルートの追跡

traceroute コマンドを使用します。

traceroute 接続先 (*Destination*)

ホストの IP アドレスを指定します。FQDN のみ判明している場合は、**nslookup fqdn-name** コマンドを使用して、IP アドレスを判別します。次に例を示します。

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 0 10.83.194.1 0 msec 10 msec 0 msec
 1 10.83.193.65 0 msec 0 msec 0 msec
 2 10.88.193.101 0 msec 10 msec 0 msec
 3 10.88.193.97 0 msec 0 msec 10 msec
 4 10.88.239.9 0 msec 10 msec 0 msec
 5 10.88.238.65 10 msec 10 msec 0 msec
 6 172.16.7.221 70 msec 70 msec 80 msec
 7 209.165.200.225 70 msec 70 msec 70 msec
```



- (注) タイムアウト、パケット存続時間、1 ノードあたりのパケット数、およびトレースルートの送信元として使用する IP アドレスまたはインターフェイスを指定できます。使用可能なオプションを表示するには、CLI でヘルプインジケータの「?」を使用します。

Firepower Threat Defense デバイスのトレースルートへの表示

デフォルトでは、Firepower Threat Defense デバイスは、トレースルートにホップとして表示されません。表示されるようにするには、デバイスを通過するパケットの存続可能時間を減らし、ICMP 到達不能メッセージのレート制限を増やす必要があります。そのためには、必要なサービス ポリシー ルールとその他のオプションを設定する FlexConfig オブジェクトを作成する必要があります。

サービス ポリシー とトラフィック クラスの詳細については、<https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html> で入手可能な『Cisco ASA Series Firewall Configuration Guide』を参照してください。



- (注) パケット存続時間 (TTL) をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、パケット存続時間 (TTL) をデクリメントすると、予期しない結果が発生する可能性があります。トラフィック クラスを定義する際には、これらの考慮事項に注意してください。

手順

ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。

ステップ 2 詳細設定の目次で [FlexConfig] > [FlexConfigオブジェクト (FlexConfig Objects)] をクリックします。

ステップ 3 TTL を減らすためのオブジェクトを作成します。

- 新しいオブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトの名前を入力します。例、**Decrement_TTL**。
- [テンプレート (Template)] エディタで、インデントを含む次の行を入力します。

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
  class class-default
    set connection decrement-ttl
```

- [ネゲートテンプレート (Negate Template)] エディタで、この設定を元に戻すために必要な行を入力します。

適切なサブモードでコマンドを有効にするために、ネゲートテンプレートに、親コマンドと同様にこれらのコマンドも含める必要があります。

FlexConfig ポリシーからこのオブジェクトを削除した場合（正常に導入された後）、および導入が失敗した場合でも（設定を前の状態にリセットするため）、ネゲートテンプレートが適用されます。

したがって、この例では、ネゲートテンプレートは次のようになります。

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
  class class-default
    no set connection decrement-ttl
```

- [OK] をクリックしてオブジェクトを保存します。

ステップ 4 オブジェクトを FlexConfig ポリシーに追加します。

FlexConfig ポリシー内の選択したオブジェクトのみ展開されます。

- 目次で [FlexConfigポリシー (FlexConfig Policy)] をクリックします。
- [グループリスト (Group List)] で [+] をクリックします。
- Decrement_TTL オブジェクトを選択し、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

- [保存 (Save)] をクリックします。

これでポリシーを展開できます。

NTP のトラブルシューティング

システムは、正確で一貫性のある時間に基づいて正しく動作し、イベントやその他のデータポイントを正確に処理します。少なくとも1つ、理想的には3つの Network Time Protocol (NTP) サーバで、システムが常に信頼できる時間情報を取得できるようにする必要があります。

デバイスの接続概要図 (メインメニューで [デバイス (Device)] をクリック) に、NTP サーバへの接続ステータスが示されます。ステータスが黄色またはオレンジ色の場合、設定したサーバへの接続に問題があります。接続の問題が解消されない (一時的な問題ではない) 場合は、次の操作を試します。

- まず、[デバイス (Device)] > [システム設定 (System Settings)] > [NTP (NTP)] で3つ以上のNTPサーバが設定されていることを確認します。これは要件になっていませんが、NTPサーバが3つ以上あると信頼性が大幅に向上します。
- 管理インターフェイス IP アドレス ([デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で定義される) と NTP サーバの間にネットワークパスがあることを確認します。
 - 管理インターフェイス ゲートウェイがデータインターフェイスであり、デフォルトルートが不適切な場合、[デバイス (Device)] > [ルーティング (Routing)] で NTP サーバに対するスタティックルートを設定できます。
 - 明示的な管理インターフェイス ゲートウェイを設定する場合は、デバイス CLI にログインし、**ping system** コマンドを使用して各 NTP サーバへのネットワークパスがあるかどうかテストします。
- デバイス CLI にログインし、次のコマンドを使用して NTP サーバのステータスを確認します。
 - **show ntp** : このコマンドは、NTP サーバとその可用性に関する基本的な情報を示します。ただし、Firepower Device Manager の接続ステータスではその他の情報を使用してステータスを示すため、このコマンドが示す内容や接続ステータス図が示す内容と一致しないことがあります。このコマンドは CLI コンソールから発行することもできます。
 - **system support ntp** : このコマンドには、**show ntp** の出力と、NTP プロトコルで記載される標準 NTP コマンド **ntpq** の出力が含まれています。NTP 同期を確認する必要がある場合は、このコマンドを使用します。

「Results of 'ntpq -pn」の部分を探します。たとえば、次のように表示されます。

```
Results of 'ntpq -pn'
remote                : +216.229.0.50
refid                  : 129.7.1.66
st                     : 2
```

```

t                : u
when             : 704
poll             : 1024
reach            : 377
delay            : 90.455
offset           : 2.954
jitter           : 2.473

```

この例では、NTP サーバのアドレスの前の「+」は、潜在的な候補であることを示します。アスタリスク * は、現在の時刻源のピアを示します。

NTP デーモン (NTPD) は、各ピアの 8 つのスライディングウィンドウサンプルを使用して 1 つのサンプルを選択します。その後、クロックの選択によって正しいチャイマーと不正なチッカーが特定されます。次に、NTPD がラウンドトリップ距離を特定します (候補のオフセットをラウンドトリップ遅延の半分以上にすることはできません)。接続の遅延、パケットの損失、またはサーバの問題が発生して 1 つまたはすべての候補が拒否されると、同期中に長い遅延が生じます。また、調整にも非常に長い時間がかかります。クロック規律アルゴリズムによって、クロックオフセットおよびオシレータエラーを解決する必要がありますが、これには数時間かかる可能性があります。



(注) refid が .LOCL. の場合は、ピアが無規律のローカルクロックであることを示します。つまり、時間設定にそのローカルクロックのみを使用します。選択したピアが .LOCL. の場合、Firepower Device Manager は NTP 接続を常に黄色 (非同期) にマークします。通常 NTP は、より適切な候補を利用できる場合、.LOCL. 候補を選択しません。そのため、サーバを 3 つ以上設定する必要があります。

管理インターフェイスの DNS のトラブルシューティング

管理インターフェイスで使用する少なくとも 1 つの DNS サーバを設定する必要があります。DNS サーバは、スマートライセンス、データベースの更新 (GeoDB、ルール、VDB など)、およびドメイン名を解決する必要があるその他すべてのアクティビティなどのサービスへのクラウド接続のために必要です。

DNS サーバの設定は簡単な作業です。デバイスの初回設定時に、使用する DNS サーバの IP アドレスを入力するだけです。この設定は、**[デバイス (Device)] > [システム設定 (System Settings)] > [DNSサーバ (DNS Server)]** ページで後で変更できます。

ただし、ネットワークの接続性の問題や DNS サーバ自体の問題のために、システムが完全修飾ドメイン名 (FQDN) を解決できないことがあります。システムが DNS サーバを使用できない場合は、問題を特定して解決するために、以下の操作を検討してください。

手順

ステップ1 問題の有無を確認します。

- a) SSH を使用してデバイスの CLI にログインします。
- b) **ping system www.cisco.com** を入力します。次のような「unknown host」メッセージが表示される場合、システムはドメイン名を解決できていません。ping が成功する場合は、これで終了です。DNS は機能しています (ping を停止するには、Ctrl+C キーを押します)。

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

(注) **system** キーワードを **ping** コマンドに含めることが極めて重要です。**system** キーワードを指定すると、管理 IP アドレスから ping が送信されます。このインターフェイスは、管理 DNS サーバを使用する唯一のインターフェイスです。スマートライセンスや更新のためにサーバへのルートが必要なため、**www.cisco.com** の ping 実行も適切なオプションです。

ステップ2 管理インターフェイスの設定を確認します。

- a) [デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] をクリックして、次の点を確認します。変更を加える場合、それらの変更は [保存 (Save)] をクリックするとすぐに適用されます。管理アドレスを変更する場合は、再度接続してログインし直す必要があります。
 - 管理ネットワークのゲートウェイ IP アドレスが正しいこと。データ インターフェイスをゲートウェイとして使用している場合は、後続の手順でその設定を確認します。
 - データ インターフェイスをゲートウェイとして使用していない場合は、管理 IP アドレスとサブネットマスク、およびゲートウェイ IP アドレスが同じサブネット上にあることを確認します。
- b) [デバイス (Device)] > [システム設定 (System Settings)] > [DNSサーバ (DNS Server)] をクリックして、正しい DNS サーバが設定されていることを確認します。

ネットワーク エッジにデバイスを展開している場合は、使用できる DNS サーバに関するサービス プロバイダー固有の要件が存在する場合があります。
- c) データ インターフェイスをゲートウェイとして使用している場合は、必要なルートがあることを確認します。

0.0.0.0 のデフォルト ルートが必要です。デフォルト ルートのゲートウェイを介して DNS サーバを使用できない場合は、追加のルートが必要になります。次に、2 つの基本的な状況を示します。

 - 外部インターフェイスのアドレスを取得するために DHCP を使用していて、[DHCP を使用してデフォルトルートを取得 (Obtain Default Route using DHCP)] オプションを選択した場合、デフォルト ルートは Firepower Device Manager には表示されません。SSH から **show route** を入力して、0.0.0.0 のルートがあることを確認します。これは外

部インターフェイスのデフォルト設定であるため、発生する可能性が高い状況です。
 ([**デバイス (Device)**] > [**インターフェイス (Interfaces)**]) に移動して、外部インターフェイスの設定を確認します)。

- 外部インターフェイスで静的 IP アドレスを使用している場合、または DHCP からデフォルトルートを取得していない場合は、[**デバイス (Device)**] > [**ルーティング (Routing)**] を開きます。デフォルトルートに正しいゲートウェイが使用されていることを確認します。

デフォルトルートから DNS サーバに到達できない場合は、[**ルーティング (Routing)**] ページで DNS サーバへのスタティックルートを定義する必要があります。直接接続ネットワーク (つまり、システムのいずれかのデータインターフェイスに直接接続されているネットワーク) のルートは追加しないでください。システムは、それらのネットワークに自動的にルーティングできるためです。

また、誤ったインターフェイスからサーバにトラフィックをミス誘導するスタティックルートが存在しないことを確認します。

- d) 展開ボタンに未展開の変更の存在が示されている場合は、ここで展開して、展開が完了するまで待ちます。



- e) **ping system www.cisco.com** を再テストします。問題が解消しない場合は、次の手順に進みます。

ステップ 3 SSH セッションで **nslookup www.cisco.com** と入力します。

- **nslookup** に、DNS サーバから応答を得たことが示されているのに、サーバが名前を検出できない場合、DNS は正しく設定されているものの、使用している DNS サーバに FQDN のアドレスが設定されていないことを意味しています。応答は次のようになります。

```
> nslookup www.cisco.com
Server:      10.163.47.11
Address:    10.163.47.11#53

** server can't find www.cisco.com: NXDOMAIN
```

解決策: この場合、別の DNS サーバを設定するか、更新した DNS サーバを使用して、解決する必要がある FQDN を解決できるようにします。ネットワーク管理者や ISP と協力して、ネットワークで動作する DNS サーバの IP アドレスを取得します。

- 「connection timed out」メッセージが表示される場合、システムが DNS サーバに到達できないか、または現在すべての DNS サーバがダウンしていて応答していません (この可能性は低いです)。次の手順に進みます。

```
> nslookup www.cisco.com
; ; connection timed out; no servers could be reached
```

ステップ 4 `traceroute system DNS_server_ip_address` コマンドを使用して、DNS サーバへのルートをトレースします。

たとえば、DNS サーバが 10.100.10.1 の場合は、次のように入力します。

```
> traceroute system 10.100.10.1
```

可能性がある結果を以下に示します。

- トレースルートが完了し、DNS サーバに到達している。この場合、DNS サーバへのルートが実際にあり、システムが到達できます。したがって、ルーティングの問題はありません。ただし、何らかの理由でこのサーバに対する DNS 要求の応答を得られていません。

解決策：パス沿いのルータやファイアウォールで、DNS に使用されるポートである UDP/53 のトラフィックがドロップされている可能性があります。異なるネットワークパスに沿って DNS サーバへのアクセスを試すことができます。これは解決が難しい問題です。トラフィックをブロックしているノードを確認し、システム管理者と協力してアクセスルールを変更する必要があります。

- トレースルートから 1 つのノードにさえ到達できない。これは、次のように表示されません。

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 * * *
 (and so forth)
```

解決策：この場合、システム内にルーティングの問題があります。ゲートウェイ IP アドレスに対して `ping system` を試行してください。前述の手順に従い、管理インターフェイスの設定を再度確認し、必要なゲートウェイとルートを設定していることを確認します。

- トレースルートは、ルートを解決できなくなる前にいくつかのノードを通過します。これは、次のように表示されます。

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1 192.168.0.254 (192.168.0.254) 0.475 ms 0.532 ms 0.542 ms
 2 10.88.127.1 (10.88.127.1) 0.803 ms 1.434 ms 1.443 ms
 3 site04-lab-gw1.example.com (10.89.128.25) 1.390 ms 1.399 ms 1.435 ms
 4 * * *
 5 * * *
 6 * * *
```

解決策：この場合、最後のノードでルーティングが中断されています。システム管理者と協力して、そのノードに設定されているルートを修正する必要があります。ただし、意図的にそのノードから DNS サーバへのルートを設定していない場合は、ゲートウェイを変

更するか、または独自のスタティック ルートを作成して、トラフィックを DNS サーバにルーティングできるルータを指すようにする必要があります。

CPU およびメモリ使用率の分析

CPU とメモリ使用率についてのシステムレベルの情報を表示するには、**[モニタリング (Monitoring)]** > **[システム (System)]** を選択して、CPU およびメモリ使用率を表す棒グラフを確認します。これらのグラフは **show cpu system** および **show memory system** コマンドを使用して CLI で収集した情報を表示します。

CLI コンソールを開くか CLI にログインして、これらのコマンドの別バージョンを使用すると、他の情報を表示できます。通常、この情報を確認するのは使用状況に関する永続的な問題がある場合や、Cisco Technical Assistance Center (TAC) の指示があった場合に限られます。詳細情報の多くは複雑で、TAC の解釈が必要です。

以下に、調べることができるいくつかのポイントを示します。これらのコマンドの詳細については、『[Cisco Firepower Threat Defense コマンドリファレンス](http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html)』 (http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) を参照してください。

- **show cpu** はデータ プレーンの CPU 使用率を表示します。
- **show cpu core** は、各 CPU コアの使用率を別々に表示します。
- **show cpu detailed** は、追加のコアごと、およびデータ プレーン全体の CPU の使用率を表示します。
- **show memory** はデータ プレーンのメモリ使用量を表示します。



(注) 一部のキーワード (上記に説明されていない) は、最初に **cpu** または **memory** コマンドを使用して、プロファイリングまたは他の機能を設定する必要があります。これらの機能は、TAC の指示があった場合のみ使用します。

ログの表示

システムはさまざまなアクションに関する情報をログに記録します。システムログを開くには **system support view-files** コマンドを使用します。Cisco Technical Assistance Center (TAC) への問い合わせ時にこのコマンドを使用すると、出力を解釈して、適切なログを表示できるようになります。

コマンドは、ログを選択するためのメニューを表示します。ウィザードに移動するには、次のコマンドを使用します。

- サブディレクトリに変更するには、ディレクトリの名前を入力して、Enter を押します。

- 表示するファイルを選択するには、プロンプトで **s** と入力します。その後、ファイル名の入力が求められます。完全な名前を入力する必要があります。大文字と小文字は区別されます。ファイルリストにはログのサイズが示されます。非常に大きいログを開く前には検討が必要な場合があります。
- 「--More--」が表示されたら **Space** キーを押してログエントリの次のページを表示します。次のログエントリのみを表示するには **Enter** を押します。ログの最後に到達すると、メインメニューに戻ります。「--More--」の行には、ログのサイズと表示した量が示されます。**ログのすべてのページを表示する必要がなく、ログを閉じて、コマンドを終了するには、Ctrl+C を使用します。**
- メニュー構造のレベルを 1 つ上がるには、**b** を入力します。

ログを開いたままにして、新しいメッセージが追加されたときにそのメッセージを確認できるようにするには、**system support view-files** コマンドの代わりに **tail-logs** コマンドを使用します。

次の例は、システムへのログイン試行を追跡する `cisco/audit.log` ファイルがどのように表示されるかを示しています。ファイルリストは、最上位のディレクトリで始まり、その後、現在のディレクトリ内のファイルリストが続きます。

```
> system support view-files

===View Logs===

=====
Directory: /ngfw/var/log
-----sub-dirs-----
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----files-----
2016-10-14 18:12:04.514783 | 5371      | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353      | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517   | action_queue.log
2016-10-06 16:00:56.620019 | 1018     | brl.down.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

=====
Directory: /ngfw/var/log/cisco
-----files-----
2017-02-13 22:44:42.394907 | 472      | audit.log
2017-02-13 23:40:30.858198 | 903615   | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0        | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338  | ev_stats.log.1
```

```

2017-02-12 08:41:00.478103 | 1024338 | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218 | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848 | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160 | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login
successful,
2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login
successful,
2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login
successful,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked
account.,

<remaining log truncated>

```

トラブルシューティング ファイルの作成

問題レポートを提出した際に、Cisco Technical Assistance Center (TAC) の担当者により、システムログ情報の提出を求められることがあります。この情報は、問題の診断に役立ちます。診断ファイルの提出は、求められた場合だけでかまいません。

次の手順では、ログレベルを設定して診断ファイルを作成する方法について説明します。

手順

-
- ステップ 1** [the name of the device in the menu] をクリックします。[デバイス (Device)]
- ステップ 2** [トラブルシューティング (Troubleshooting)] の下で、[ファイルの作成を要求 (Request File to be Created)] または [ファイルの作成を再要求 (Re-Request File to be Created)] (事前に作成していた場合) をクリックします。
- システムが診断ファイルの生成を開始します。他のページに移動して、後で戻ってきてステータスを確認できます。ファイルの準備が整うと、ファイル作成日時が [ダウンロード (Download)] ボタンとともに表示されます。
- ステップ 3** ファイルの準備が整ったら、[ダウンロード (Download)] ボタンをクリックします。
- ファイルは、ブラウザの標準のダウンロード方式を使用してワークステーションにダウンロードされます。
-

一般的でない管理タスク

次に、ごくまれにしか行われたいアクションについて説明します。これらすべてのアクションは、デバイス設定の消去を引き起こします。これらの変更を加える前に、デバイスが現在、実稼働ネットワークに対して重要なサービスを提供していないことを確認します。

ローカル管理とリモート管理の切り替え

デバイスに直接ホストされているローカルの Firepower Device Manager を使用し、またはリモートで Firepower Management Center の複数のデバイス マネージャを使用して、デバイスを設定および管理できます。Firepower Device Manager でサポートされていない機能を設定する場合、または Firepower Management Center で使用可能な電力と分析機能が必要な場合、リモート マネージャを使用できます。

トランスペアレントファイアウォールモードでデバイスを実行する場合、Firepower Management Center も使用する必要があります。

ソフトウェアを再インストールすることなく、ローカル管理とリモートの管理を切り替えることができます。リモート管理からローカル管理に切り替える前に、Firepower Device Manager がすべての設定要件を満たしていることを確認します。



注意

マネージャを切り替えると、デバイス設定は削除され、デフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は保持されます。

始める前に

デバイスを登録した場合、特に機能ライセンスを有効にした場合、リモート管理に切り替える前に、Firepower Device Manager を介してデバイスを登録解除する必要があります。デバイスを登録解除すると、基本ライセンスとすべての機能ライセンスが解放されます。デバイスを登録解除しない場合、これらのライセンスは Cisco Smart Software Manager のデバイスに割り当てられたままになります。「[デバイスの登録解除 \(103 ページ\)](#)」を参照してください。

手順

- ステップ 1** SSH クライアントを使用して [管理IPアドレス (management IP address)] への接続を開き、設定 CLI アクセスを持つユーザ名でデバイス CLI にログインします。たとえば、[管理者 (admin)] ユーザ名など。

管理 IP アドレスに接続している間は、この手順に従うことが重要です。Firepower Device Manager を使用する場合、データインターフェイスの IP アドレスを介してデバイスを管理することもできます。ただしデバイスをリモートで管理するには、管理物理ポートと管理 IP アドレスを使用する必要があります。

管理 IP アドレスに接続できない場合、次のように対処します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理 IP アドレスとゲートウェイが設定されていることを確認します。FirePOWER Device Manager から、[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択して、アドレスおよびゲートウェイを設定します (CLI では、**configure network ipv4/ipv6 manual** コマンドを使用します)。

(注) 管理 IP アドレスに外部ゲートウェイを使用していることを確認します。リモート マネージャを使用する場合、データ インターフェイスをゲートウェイとして使用することはできません。

ステップ 2 ローカル管理からリモート管理へ切り替えるには、次の手順に従います。

- a) 現在ローカル管理モードになっていることを確認します。

```
> show managers
Managed locally.
```

- b) リモート マネージャを設定します。

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

ここで、

- **{hostname | IPv4_address | IPv6_address | DONTRESOLVE}** で、このデバイスを管理する Firepower Management Center の DNS ホスト名または IP アドレス (IPv4 あるいは IPv6) を指定します。Firepower Management Center が直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、**nat_id** が必要です。
- **Regkey** はデバイスを Firepower Management Center へ登録するのに必要な、英数字の一意の登録キーです。
- **nat_id** は、Firepower Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。**hostname** が **DONTRESOLVE** に設定されている場合に必要です。

たとえば、登録キー **secret** で 192.168.0.123 のマネージャを使用するには、以下のコマンドを入力します。

```
> configure manager add 192.168.0.123 secret
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before switching to remote management.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue [yes/no] yes
Manager successfully configured.
Please make note of reg_key as this will be required while adding
```

Device in FMC.

```
> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status         :
```

(注) 登録が保留中の場合は、**configure manager delete** を使用して登録を取り消してから、**configure manager local** を使用してローカル管理に戻ることができます。

- c) Firepower Management Center にログインし、デバイスを追加します。

詳細については、Firepower Management Center オンライン ヘルプを参照してください。

ステップ 3 リモート管理からローカル管理へ切り替えるには、次の手順に従います。

- a) 現在リモート管理モードになっていることを確認します。

```
> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status         :
```

- b) リモート マネージャを削除すると、マネージャなしのモードになります。

リモート管理からローカル管理に直接移行することはできません。マネージャを削除するには、**configure manager delete** コマンドを使用します。

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

```
>
> show managers
No managers configured.
```

- c) ローカル マネージャを設定します。

configure manager local

次に例を示します。

```
> configure manager local
Deleting task list
```

```
> show managers
Managed locally.
```

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

ファイアウォールモードの変更

Firepower Threat Defense ファイアウォールは、ルーテッドモードまたはトランスペアレントモードで実行できます。ルーテッドモードのファイアウォールはルーテッドホップであり、スクリーンサブネットのいずれかに接続するホストのデフォルトゲートウェイとして機能します。一方、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。

ローカルの Firepower Device Manager はルーテッドモードのみをサポートします。ただし、デバイスをトランスペアレントモードで実行する必要がある場合は、ファイアウォールモードを変更して、Firepower Management Center でデバイスの管理を始めることができます。逆に、トランスペアレントモードのデバイスをルーテッドモードに変換すると、ローカルマネージャでそのデバイスを設定することができ、Firepower Management Center を使用してルーテッドモードのデバイスを管理することもできます。

ローカル管理であるか、リモート管理であるかに関係なく、モードを変更するためにはデバイスの CLI を使用する必要があります。

次の手順では、ローカルマネージャを使用している場合、またはローカルマネージャを使用予定の場合のモードの変更方法について説明します。



注意 ファイアウォールモードを変更すると、デバイス設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は保持されます。

始める前に

トランスペアレントモードに変換する場合は、ファイアウォールモードを変更する前に Firepower Management Center をインストールします。

いずれかの機能ライセンスを有効にしている場合、ローカルマネージャを削除してリモート管理に切り替える前に、Firepower Device Manager でそれらのライセンスを無効にする必要があります。無効にしないと、それらのライセンスは Cisco Smart Software Manager でデバイスに割り当てられたままになります。「[オプションライセンスの有効化と無効化 \(101 ページ\)](#)」を参照してください。

手順

ステップ 1 SSH クライアントを使用して [管理 IP アドレス (management IP address)] への接続を開き、設定 CLI アクセスを持つユーザ名でデバイス CLI にログインします。たとえば、[管理者 (admin)] ユーザ名など。

管理 IP アドレスに接続している間は、この手順に従うことが重要です。Firepower Device Manager を使用する場合は、データインターフェイスの IP アドレスを介してデバイスを管理することもできます。ただしデバイスをリモートで管理するには、管理物理ポートと管理 IP アドレスを使用する必要があります。

管理 IP アドレスに接続できない場合、次のように対処します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理 IP アドレスとゲートウェイが設定されていることを確認します。FirePOWER Device Manager から、[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択して、アドレスおよびゲートウェイを設定します (CLI では、**configure network ipv4/ipv6 manual** コマンドを使用します)。

(注) 管理 IP アドレスに外部ゲートウェイを使用していることを確認します。リモート マネージャを使用している場合、データ インターフェイスをゲートウェイとして使用することはできません。

ステップ 2 モードをルーテッドからトランスペアレントに変更して、リモート管理を使用するには、次の手順を実行します。

- a) ローカル管理を無効にし、ノー マネージャ モードを開始します。

アクティブなマネージャが存在する間は、ファイアウォールモードを変更できません。マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

- b) ファイアウォール モードをトランスペアレントに変更します。

configure firewall transparent

例 :

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

- c) リモート マネージャを設定します。

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

ここで、

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} で、このデバイスを管理する Firepower Management Center の DNS ホスト名または IP アドレス (IPv4 あるいは

IPv6) を指定します。Firepower Management Center が直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、*nat_id* が必要です。

- *Regkey* はデバイスを Firepower Management Center へ登録するのに必要な、英数字の一意の登録キーです。
- *nat_id* は、Firepower Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が **DONTRESOLVE** に設定されている場合に必要です。

たとえば、登録キー **secret** で 192.168.0.123 のマネージャを使用するには、以下のコマンドを入力します。

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                : 192.168.0.123
Registration Key     : ****
Registration         : pending
RPC Status          :
```

- d) Firepower Management Center にログインし、デバイスを追加します。

詳細については、Firepower Management Center のオンライン ヘルプを参照してください。

ステップ 3 モードをトランスペアレントからルーテッドに変更して、ローカル管理に変換するには、次の手順を実行します。

- FMC からデバイスを登録解除します。
- FTD デバイスの CLI にアクセスします。可能ならばコンソール ポートからアクセスします。

これは、モードを変更すると設定が削除され、管理 IP アドレスはデフォルトに戻ってしまうため、モード変更後に管理 IP アドレスへの SSH 接続が失われることがあるためです。

- c) ファイアウォールモードをルーテッドに変更します。

configure firewall routed

例 :

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

- d) ローカル マネージャを有効にします。

configure manager local

次に例を示します。

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

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

設定のリセット

最初からやり直す場合は、システム設定を工場出荷時のデフォルトにリセットできます。設定を直接リセットすることはできませんが、マネージャを削除して追加すると設定がクリアされます。

設定を消去してバックアップを復元する場合は、復元するバックアップコピーを既にダウンロードしていることを確認してください。システムを復元するには、システムのリセット後にバックアップコピーをアップロードする必要があります。

始める前に

いずれかの機能ライセンスを有効にした場合は、ローカルマネージャを削除する前に Firepower Device Manager でそれらを無効にする必要があります。無効にしないと、それらのライセンスが Cisco Smart Software Manager のデバイスに割り当てられたままになります。「[オプションライセンスの有効化と無効化（101 ページ）](#)」を参照してください。

手順

- ステップ 1** SSH クライアントを使用して、管理 IP アドレスへの接続を開き、設定 CLI アクセス権を持つユーザ名でデバイスの CLI にログインします。たとえば、[管理者 (admin)] ユーザ名を使用します。
- ステップ 2** マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ3 ローカル マネージャを設定します。

configure manager local

次に例を示します。

```
> configure manager local  
Deleting task list  
  
> show managers  
Managed locally.
```

これで、Web ブラウザで **https://management-IP-address** にアクセスしてローカル マネージャを開くことができるようになりました。設定をクリアすると、デバイスセットアップ ウィザードの完了を求めるメッセージが表示されます。



付録 **A**

詳細設定

いくつかのデバイスの機能は、ASA 設定コマンドを使用して設定されます。Firepower Device Manager はコマンドベースの多くの機能を設定できますが、それらのすべてはサポートしません。Firepower Device Manager でサポートされていないこれらの ASA 機能の一部を使用する必要がある場合は、Smart CLI または FlexConfig を使用して手動で機能を設定できます。

次のトピックでは、このタイプの高度な設定について、より詳細に説明します。

- [Smart CLI と FlexConfig について \(523 ページ\)](#)
- [Smart CLI および FlexConfig に関する注意事項と制限事項 \(532 ページ\)](#)
- [Smart CLI オブジェクトの設定 \(532 ページ\)](#)
- [FlexConfig ポリシーの設定 \(534 ページ\)](#)
- [FlexConfig ポリシーのトラブルシューティング \(546 ページ\)](#)
- [FlexConfig の例 \(547 ページ\)](#)

Smart CLI と FlexConfig について

Firepower Threat Defense では、ASA 設定コマンドを使用して、すべての機能ではなく一部の機能を実装します。Firepower Threat Defense 設定コマンドの一意のセットはありません。

次の方法により CLI を使用して機能を設定できます。

- **Smart CLI** : (推奨の方法です。) Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。
- **FlexConfig** : FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI 変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。

Smart CLI と FlexConfig のポイントは、Firepower Device Manager のポリシーと設定によって直接サポートされていない機能を設定できることです。



注意 Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。ブラックリストに登録されていない任意のコマンドも設定できます。Smart CLI と FlexConfig を使用して機能を有効にすると、その他の設定済みの機能で予期しない結果が生じる可能性があります。

設定した Smart CLI と FlexConfig のオブジェクトに関するサポートについては、Cisco Technical Assistance Center にお問い合わせください。Cisco Technical Assistance Center は、顧客に代わってカスタム設定を設計したり、作成したりしません。正常な動作や他の Firepower Threat Defense 機能の相互運用性について、シスコは一切保証しません。Smart CLI と FlexConfig の機能は、いつでも廃止になる可能性があります。完全に保証された機能のサポートについては、Firepower Device Manager のサポートを待つ必要があります。疑問がある場合、Smart CLI または FlexConfig は使用しないでください。

ここでは、これらの機能についてさらに詳しく説明します。

Smart CLI と FlexConfig の推奨される使用法

FlexConfig ポリシーには、推奨される使用法が主に 2 つあります。

- ASA から FTD に移行中で、互換性はあるが、Firepower Device Manager が直接サポートしていない機能を使用しています（および使用を継続する必要があります）。この場合、ASA で **show running-config** コマンドを使用してその互換機能の設定を確認し、その機能を実装する FlexConfig オブジェクトを作成します。2 台のデバイスでの **show running-config** の出力を比較して確認します。
- FTD を使用しているものの、構成が必要な設定または機能がある場合（たとえば、Cisco Technical Assistance Center から、発生している特定の問題を解決するための具体的な設定を指示された場合）。複雑な機能については、ラボ デバイスを使用して FlexConfig をテストし、期待する動作を得られることを確認します。

ASA 設定を再作成する前に、まず標準的なポリシーで同等の機能を設定できるかどうかを判断します。たとえば、アクセスコントロールポリシーには侵入検知および防御、HTTP およびその他のタイプのプロトコルインスペクション、URL フィルタリング、アプリケーション フィルタリング、アクセス制御が含まれており、ASA はこれらの要素を別個の機能を使用して実装します。多くの機能は CLI コマンドを使用して設定されていないため、**show running-config** の出力内にすべてのポリシーが表示されるわけではありません。



(注) 常に、ASA と FTD との間の重複は 1 対 1 であるわけではないことに注意してください。FTD デバイスで ASA 設定を完全に作成し直そうとしないでください。設定する機能は、FlexConfig を使用して慎重にテストする必要があります。

Smart CLI および FlexConfig オブジェクトの CLI コマンド

FTD では一部の機能の設定に ASA コンフィギュレーション コマンドを使用します。すべての ASA 機能が FTD と互換性があるわけではありませんが、FTD で動作できても Firepower Device Manager ポリシーで設定できない機能があります。Smart CLI および FlexConfig オブジェクトを使用すると、これらの機能を設定するために必要な CLI を指定できます。

Smart CLI または FlexConfig を使用して機能を手動で設定することに決めた場合、適切な構文を認識し、これに従ってコマンドを実装する必要があります。FlexConfig は CLI コマンド構文を検証しません。正しいシンタックスと CLI コマンドの設定に関する詳細については、ASA ドキュメンテーションを参照してください。

- 『ASA CLI configuration guides』では機能を設定する方法について説明しています。ガイドはこちらからご覧ください。 <http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>
- 『ASA コマンドリファレンス』ではコマンド名ごとにその他の情報が記載されています。リファレンスはこちらからご覧ください。 <http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html>

ここでは、コンフィギュレーション コマンドについて詳しく説明します。

ASA ソフトウェアのバージョンおよび現在の CLI 設定の特定

システムが ASA ソフトウェア コマンドを使用して一部の機能を設定するため、FTD デバイスで実行するソフトウェアで使用されている現在の ASA バージョンを特定する必要があります。このバージョン番号に従って、機能設定時の手順に使用する ASA CLI 設定ガイドを選択します。また、現在の CLI ベースの設定を確認し、実装する ASA 設定と比較する必要があります。

FTD 設定とどの ASA 設定も大きく異なることに注意してください。FTD ポリシーの多くは CLI の外部で設定されるため、コマンドを調べても設定を確認することができません。ASA と FTD 設定が 1 対 1 で対応するように作成しようとししないでください。

この情報を表示するには、Firepower Device Manager の CLI コンソールを開くか、デバイスの管理インターフェイスに SSH 接続し、次のコマンドを発行します。

- **show version system** また、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号を検索します。
- **show running-config** 現在の CLI 設定を表示します。
- **show running-config all** 現在の CLI 設定にすべてのデフォルト コマンドを含めます。

禁止された CLI コマンド

Smart CLI と FlexConfig の目的は、Firepower Device Manager を使用して FTD デバイスで設定できない ASA デバイスで利用可能な機能を設定することです。

したがって、Firepower Device Manager と同等の ASA 機能は設定できません。次の表に、これらの禁止されたコマンド領域のいくつかを示します。このリストには、設定モードを開始する

多数の親コマンドが含まれています。親コマンドの禁止には子コマンドの禁止が含まれていません。また、コマンドの **no** バージョンと、関連する **clear** コマンドも含まれます。

FlexConfig オブジェクトエディタでは、これらのコマンドをオブジェクトに含めることはできません。SmartCLI テンプレートについては、有効に設定できるコマンドのみが含まれるため、このリストは適用されません。

禁止された CLI コマンド	説明
aaa	[オブジェクト (Objects)] > [アイデンティティレルム (Identity Realm)] を使用します。
aaa-server	[オブジェクト (Objects)] > [アイデンティティレルム (Identity Realm)] を使用します。
access-group	[ポリシー (Policies)] > [アクセスコントロール (Access Control)] を使用してアクセス ルールを設定します。
access-list	部分的にブロックされます。 <ul style="list-style-type: none"> • extended および standard のアクセスリストを作成し、access-group 以外のコマンドで一致基準として使用できます。たとえば、サービス ポリシー ルールの一致基準に extended アクセス リストを使用できます。 • ethertype アクセス リストを作成できます。 • advanced アクセス リスト (システムが access-group コマンドで使用する) は作成できません。代わりに、[ポリシー (Policies)] > [アクセスコントロール (Access Control)] を使用してアクセス ルールを設定します。 • webtype アクセス リストは作成できません。
anyconnect-custom-data	[デバイス (Device)] > [リモートアクセスVPN (Remote Access VPN)] を使用して AnyConnect を設定します。
asdm	この機能は FTD システムには適用されません。
attribute	—
auth-prompt	この機能は FTD システムには適用されません。
boot	—
call-home	—
captive-portal	[ポリシー (Policies)] > [アイデンティティ (Identity)] を使用して、アクティブな認証に使用するキャプティブ ポータルを設定します。
clear	—

禁止された CLI コマンド	説明
client-update	—
clock	[デバイス (Device)] > [システム設定 (System Settings)] > [NTP] を使用してシステム時間を設定します。
cluster	—
command-alias	—
compression	—
configure	—
crypto	[オブジェクト (Objects)] ページで、[証明書 (Certificates)]、[IKEポリシー (IKE Policies)]、および [IPsec プロポーザル (IPsec Proposals)] を使用します。
dhcp-client	—
dhcpd	[デバイス (Device)] > [システム設定 (System Settings)] > [DHCPサーバ (DHCP Server)] を使用します。
dns	—
domain-name	—
dynamic-access-policy-config	—
dynamic-access-policy-record	—
enable	—
event	—
failover	—
fips	—
firewall	Firepower Device Manager はルーテッドファイアウォールモードのみをサポートします。
hostname	[デバイス (Device)] > [システム設定 (System Settings)] > [ホスト名 (Hostname)] を使用します。
hpm	この機能は FTD システムには適用されません。
http	[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス (Management Access)] で [データインターフェイス (Data Interfaces)] タブを使用します。
inline-set	—

禁止された CLI コマンド	説明
interface (BVI、管理、イーサネット、GigabitEthernet、およびサブインターフェイス用)	<p>部分的にブロックされます。</p> <p>[デバイス (Device)]>[インターフェイス (Interfaces)] ページで物理インターフェイス、サブインターフェイス、およびブリッジ仮想インターフェイスを設定します。FlexConfig を使用して追加のオプションを設定できます。</p> <p>ただし、次の interface モードコマンドは、これらのタイプのインターフェイスでは禁止されます。</p> <p>cts ip address ip address dhcp ipv6 address ipv6 enable ipv6 nd dad ipv6 nd suppress-ra mode nameif security-level shutdown zone-member</p>
vni 、 redundant 、 tunnel 、 portchannel の interface	[デバイス (Device)]>[インターフェイス (Interfaces)] ページでインターフェイスを設定します。Firepower Device Manager では、これらのタイプのインターフェイスはサポートされません。
ip audit	この機能は FTD システムには適用されません。代わりに、アクセス制御ルールを使用して侵入ポリシーを適用します。
ip-client	管理ゲートウェイとしてデータ インターフェイスを使用するようシステムを設定するには、[デバイス (Device)]>[システム設定 (System Settings)]>[管理インターフェイス (Management Interface)] を使用します。
ip local pool	[デバイス (Device)]>[リモートアクセスVPN (Remote Access VPN)] を使用してアドレス プールを設定します。
ipsec	—
ipv6	—
ipv6-vpn-addr-assign	[デバイス (Device)]>[リモートアクセスVPN (Remote Access VPN)] を使用してアドレス プールを設定します。
isakmp	[デバイス (Device)]>[サイト間VPN (Site-to-Site VPN)] を使用します。

禁止された CLI コマンド	説明
jumbo-frame	デフォルトの 1500 以上のインターフェイスの MTU を増やす場合、システムは自動的にジャンボ フレームのサポートを有効にします。
ldap	—
license-server	[デバイス (Device)]>[スマートライセンス (Smart License)] を使用します。
logging	[オブジェクト (Objects)]>[Syslogサーバ (Syslog Servers)] および [デバイス (Device)]>[システム設定 (System Settings)]>[ロギング設定 (Logging Settings)]を使用しま す。
management-access	—
migrate	[デバイス (Device)]>[リモートアクセスVPN (Remote Access VPN)]および [デバイス (Device)]>[サイト間VPN (Site-to-Site VPN)]を使用して IKEv2 サポートを有効にし ます。
mode	Firepower Device Manager は単一コンテキスト モードのみをサ ポートします。
mount	—
mtu	[デバイス (Device)]>[インターフェイス (Interfaces)]で インターフェイスごとに MTU を設定します。
nat	[ポリシー (Policies)]>[NAT] を使用します。
ngips	—
ntp	[デバイス (Device)]>[システム設定 (System Settings)]> [NTP] を使用します。
object-group network object network	[オブジェクト (Objects)]>[ネットワーク (Network)]を使 用します。 FlexConfig でネットワーク オブジェクトまたはグループを作 成することはできませんが、テンプレート内で変数としてオ ブジェクト マネージャで定義されているネットワーク オブ ジェクトおよびグループは使用できます。
object service natorigsvc object service natmappedsvc	object service コマンドは一般に使用できますが、 natorigsvc または natmappedsvc という内部オブジェクトは編集できませ ん。これらの名前の垂直バーは意図的であり、制限されてい るオブジェクト名の最初の文字です。

禁止された CLI コマンド	説明
passwd password	—
password-policy	—
policy-map サブコマンド	ポリシー マップでは次のコマンドを設定できません。 priority police match tunnel-group
priority-queue	—
privilege	—
reload	リロードはスケジュールできません。システムは、システムを再起動するために reload コマンドを使用せず、 reboot コマンドを使用します。
rest-api	この機能は FTD システムには適用されません。REST API は常にインストールされ、有効になります。
route	[デバイス (Device)] > [ルーティング (Routing)] を使用してスタティック ルートを設定します。
router ospf	OSPF には Smart CLI テンプレートを使用します。
scansafe	この機能は FTD システムには適用されません。代わりに、アクセス制御ルールで URL フィルタリングを設定します。
setup	この機能は FTD システムには適用されません。
sla	—
ssh	[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス (Management Access)] で [データインターフェイス (Data Interfaces)] タブを使用します。
ssl	—
telnet	FTD は Telnet 接続をサポートしません。デバイス CLI にアクセスするには、Telnet の代わりに SSH を使用します。
time-range	—
tunnel-group	[デバイス (Device)] > [リモートアクセスVPN (Remote Access VPN)] および [デバイス (Device)] > [サイト間VPN (Site-to-Site VPN)] を使用します。

禁止された CLI コマンド	説明
tunnel-group-map	[デバイス (Device)]>[リモートアクセスVPN (Remote Access VPN)]および [デバイス (Device)]>[サイト間VPN (Site-to-Site VPN)]を使用します。
user-identity	[ポリシー (Policies)]>[アイデンティティ (Identity)]を使用します。
username	CLI ユーザを作成するには、デバイスに対して SSH またはコンソールセッションを開き、 configure user コマンドを使用します。
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	この機能は FTD システムには適用されません。

Smart CLI テンプレート

次の表では、機能に基づく Smart CLI テンプレートについて説明します。

機能	テンプレート	説明
ルーティング : OSPFv2	OSPF インターフェイス	OSPF テンプレートを使用してルーティングプロセスを設定し、インターフェイス テンプレートを使用してインターフェイスごとの OSPF の動作を設定します。 ヒント : <ul style="list-style-type: none"> 他のルーティング プロセスからのルートを再配布する場合は、まずそれらのプロセスを設定する必要があります。たとえば、EIGRP ルートを再配布する OSPF を構成する前に、まず EIGRP を設定する FlexConfig オブジェクトを展開します。 最大 2 つの OSPF プロセスを設定できます。

Smart CLI および FlexConfig に関する注意事項と制限事項

Smart CLI または FlexConfig を介して機能を設定するときは、次の点に注意してください。

- FlexConfig オブジェクトで定義されているコマンドは、Smart CLI を含む Firepower Device Manager で定義された機能のすべてのコマンドの後に展開されます。したがって、デバイスに対してこれらのコマンドが発行される前に設定されているオブジェクト、インターフェイスなどに依存する場合があります。Smart CLI テンプレートで FlexConfig が展開された項目を使用する必要がある場合は、Smart CLI テンプレートを作成して展開する前に FlexConfig を作成して展開します。たとえば、OSPF Smart CLI テンプレートを使用して EIGRP ルートを再配布する場合は、最初に FlexConfig を使用して EIGRP を設定し、それから OSPF Smart CLI テンプレートを作成します。
- FlexConfig から設定した機能または機能の一部を削除するが、Smart CLI テンプレートがその機能を参照している場合は、最初に機能を使用する Smart CLI テンプレートでコマンドを削除する必要があります。その後、Smart CLI で設定された機能が参照しないように設定を展開します。FlexConfig から機能を削除して設定を再展開すると、最終的に完全削除できます。

Smart CLI オブジェクトの設定

Smart CLI オブジェクトは、Firepower Device Manager の他では構成することができない機能を定義します。Smart CLI オブジェクトは、機能の構成において一定レベルのガイダンスを提供します。指定された機能（テンプレート）について、すべての可能なコマンドが事前に読み込まれ、入力した変数が検証されます。したがって、機能を構成するために CLI コマンドを使用しても、Smart CLI オブジェクトは FlexConfig オブジェクトほど自由な形式ではありません。

Smart CLI テンプレートは一定レベルのガイダンスを提供しますが、ネットワークで正しく動作するように値を選択するために ASA 構成ガイドとコマンドリファレンスを読み、コマンドの使用方法を理解する必要があります。理想的には、動作する ASA 構成はすでにあり、必要とされるのは Smart CLI オブジェクトでコマンドの同じシーケンスを構築することだけです。

Smart CLI オブジェクトは、ルーティングなどの機能分野によってグループ化されます。



- (注) 定義したすべての Smart CLI オブジェクトが展開されます。FlexConfig とは異なり、いくつかの Smart CLI オブジェクトを作成し、その中から選択して展開することはできません。構成する機能に対してのみ Smart CLI オブジェクトを作成します。

手順

ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。

ステップ 2 詳細設定の目次で [スマートCLI (Smart CLI)] の下の該当する機能のエリアをクリックします。たとえば、[スマートCLI (Smart CLI)] > [ルーティング (Routing)] です。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

オブジェクトを削除するには、そのオブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 4 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 5 構成する機能の [CLIテンプレート (CLI Template)] を選択します。

システムはコマンドテンプレートを [テンプレート (Template)] ウィンドウに読み込みます。最初に必要なコマンドのみが表示されます。これらはテンプレートに必要な最小構成を表します。

- (注) いくつかの機能では、複数のテンプレートを必要とします。たとえば、OSPFv2 を構成するには、[OSPF] と [インターフェイス (Interface)] テンプレートを使用して、2 つの SmartCLI オブジェクトを作成する必要があります。OSPF テンプレートは OSPFv3 を構成するために使用できないことに注意してください。

ステップ 6 変数を入力し、必要に応じてテンプレートにコマンドを追加します。

理想的には、ASA または Firepower Threat Defense デバイス (Firepower Management Center によって管理されているもの) から既存の構成を使用して作業します。所有している構成では、単にネットワーク内のこの特定のデバイスの場所に応じて IP アドレス、インターフェイス名などの変数を変更して、テンプレートをそれに適合させる必要があります。

テンプレートへの入力に関するいくつかのヒントを次に示します。

- 変数の値を選択するには、変数のいずれかをクリックして適切な値を入力するか、リストから選択します (値が列挙されている場合)。入力を必要とする変数をマウスオーバーすると、数値の範囲など、オプションの有効な値が表示されます。一部のケースでは推奨値が記載されています。

たとえば、OSPF のテンプレートでは、必要なコマンドの **router ospf process-id** をマウスオーバーすると「Process ID (1-65535)」と表示され、*process-id* をクリックするとフィールドが強調表示されます。単に希望の数値を入力します。

- 変数のオプションを選択するときに、オプションを構成するために使用できる追加のコマンドがある場合、それらが自動的に公開され必要に応じて有効または無効になります。これらの追加のコマンドを確認します。

- テンプレート上の [表示 (Show)]/[無効を非表示 (Hide Disabled)] リンクを使用してビューを制御します。無効なコマンドは構成されませんが、それらを表示して構成する必要があります。完全なテンプレートを表示するには、テンプレート上の [無効を表示 (Show Disabled)] リンクをクリックします。構成されるコマンドのみを表示するには、テーブル上の [無効を非表示 (Hide Disabled)] リンクをクリックします。
- オブジェクトを最後に保存して以降のすべての編集をクリアするには、テンプレートの上の [リセット (Reset)] リンクをクリックします。
- オプションのコマンドを有効にするには、行番号の左側にある [+] のボタンをクリックします。
- オプションのコマンドを無効にするには、行番号の左側にある [-] のボタンをクリックします。行を編集した場合、編集内容は削除されません。
- コマンドを複製するには、[オプション... (Options...)] ボタンをクリックして [複製 (Duplicate)] を選択します。コマンドを複数回入力することが有効な場合にのみ、コマンドを複製できます。
- 複製したコマンドを削除するには、[オプション... (Options...)] ボタンをクリックして [削除 (Delete)] を選択します。ベース テンプレートの一部であるコマンドは削除できません。

ステップ7 [OK] をクリックします。

FlexConfig ポリシーの設定

FlexConfig ポリシーは単にデバイスの構成に展開する FlexConfig オブジェクトのリストです。ポリシーに含まれるこれらのオブジェクトのみが展開され、他はすべてが単に定義されるだけで使用されません。

FlexConfig オブジェクトで定義されているコマンドは、Smart CLI を含む Firepower Device Manager で定義された機能のすべてのコマンドの後に展開されます。したがって、デバイスに対してこれらのコマンドが発行される前に設定されているオブジェクト、インターフェイスなどに依存する場合があります。Smart CLI テンプレートで FlexConfig が展開された項目を使用する必要がある場合は、Smart CLI テンプレートを作成して展開する前に FlexConfig を作成して展開します。たとえば、OSPF Smart CLI テンプレートを使用して EIGRP ルートを再配布する場合は、最初に FlexConfig を使用して EIGRP を設定し、それから OSPF Smart CLI テンプレートを作成します。



(注) 機能の Smart CLI テンプレートがある場合、FlexConfig を使用してそれを構成できません。Smart CLI オブジェクトを使用する必要があります。

始める前に

FlexConfig オブジェクトを作成します。次のトピックを参照してください。

- [FlexConfig オブジェクトの設定 \(536 ページ\)](#)
- [FlexConfig オブジェクトの変数の作成 \(538 ページ\)](#)
- [秘密キー オブジェクトの設定 \(545 ページ\)](#)

手順

ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。

ステップ 2 詳細設定の目次で [FlexConfig] > [FlexConfigポリシー (FlexConfig Policy)] をクリックします。

ステップ 3 [グループリスト (Group List)] 内のオブジェクトのリストを管理します。

- オブジェクトを追加するには、[+] ボタンをクリックします。オブジェクトがまだ存在しない場合は、[新規FlexConfigオブジェクトを作成 (Create New FlexConfig Object)] をクリックして定義します。
- オブジェクトを削除するには、オブジェクトエントリの右側にある [X] ボタンをクリックします。

(注) 各オブジェクトは完全に自己完結型で、他の FlexConfig オブジェクトで定義されている構成に依存しないことをお勧めします。これにより、他のオブジェクトに影響を与えずにオブジェクトを追加または削除できます。リスト内のオブジェクトの位置は変更できますが、順序は保存されず、オブジェクトが展開された順序は変更されません。

ステップ 4 [プレビュー (Preview)] ペインで提案されたコマンドを評価します。

[展開 (Expand)] ボタン (その後 [折りたたむ (Collapse)]) をクリックすると画面を拡大できます。これにより長いコマンドがより見やすくなります。

プレビューは、変数を評価し、発行される正確なコマンドを生成します。これらのコマンドが正しく有効なことを確認します。コマンドがエラーを生じたり、デバイスが使用できなくなる不適切な構成でないことを確保する責任があります。

注意 システムはコマンドを検証しません。無効なコマンドや、破壊の可能性があるコマンドも展開が可能です。変更を展開する前に慎重にプレビューを確認します。

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

FlexConfig ポリシーを編集した後は、次の展開の結果を慎重に調べてください。エラーがある場合は、オブジェクトの CLI を修正します。[FlexConfig ポリシーのトラブルシューティング \(546 ページ\)](#) を参照してください。

FlexConfig オブジェクトの設定

FlexConfig オブジェクトには、別の方法では Firepower Device Manager を使用して設定できない特定の機能を設定するために必要な ASA コマンドが含まれます。コマンドのシーケンスは、入力ミスなく正しく入力する必要があります。システムは、FlexConfig オブジェクトの内容を検証しません。

設定する一般的な機能ごとに別のオブジェクトを作成することをお勧めします。たとえば、バナーを定義し、RIP ルーティング プロトコルも設定する場合は、2 つの独立したオブジェクトを使用します。機能を別のオブジェクトに分離すると、展開するオブジェクトの選択が容易になり、またトラブルシューティングも容易になります。



(注) **enable** および **configure terminal** コマンドは含めないでください。システムは、自動的にコンフィギュレーション コマンドに適切なモードに入ります。

手順

ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。

ステップ 2 詳細設定の目次で [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Objects)] をクリックします。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。

ステップ 4 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 5 [変数 (Variables)] セクションで、オブジェクト本文内で使用する変数を作成します。

作成する必要がある唯一の変数は Firepower Device Manager 内で定義されているオブジェクトを指すもので、具体的にはネットワーク、ポート、および秘密キーの変数の型、または名前付きインターフェイスを指すインターフェイス変数です。他の変数の型では、単にオブジェクト本文に値を入力できます。

変数の作成と使用の詳細については、[FlexConfig オブジェクトの変数の作成 \(538 ページ\)](#) を参照してください。

ステップ 6 [テンプレート (Template)]セクションに、機能を設定するために必要な ASA コマンドを入力します。

機能を設定するために正しい順序でコマンドを入力する必要があります。ASA CLI 構成ガイドを使用して、コマンドを入力する方法を学習します。理想的には、ASA または参照として使用できる別の FTD デバイスからの事前テスト済みの構成ファイルが必要です。

変数を参照および処理するために Mustache 表記を使用することもできます。詳細については、[FlexConfig 変数の参照と値の取得 \(540 ページ\)](#) を参照してください。

オブジェクト本文を作成するためのいくつかのヒントを次に示します。

- 行を追加するには、行の末尾にカーソルを置いて、Enter キーを押します。
- 変数を使用するには、二重括弧間に変数名を入力します：`{{変数名}}`。オブジェクトを参照する変数では、取得する値の属性を含める必要があります：`{{変数名.属性}}`。使用可能な属性は、オブジェクトタイプによって異なります。詳細については、[変数参照：`{{variable}}` \(540 ページ\)](#) を参照してください。
- テンプレート本体の上の [展開する/折りたたむ (Expand/Collapse)] リンクをクリックして、本体を大きくまたは小さくします。
- [リセット (Reset)] リンクをクリックして、オブジェクトを最後に保存した後に行ったすべての変更を消去します。

ステップ 7 [ネゲートテンプレート (Negate Template)]セクションに、オブジェクト本体で設定したコマンドを削除または入れ替えるために必要なコマンドを入力します。

ネゲートセクションは非常に重要であり、2つの目的を果たします。

- 展開を簡単にします。本体でコマンドを再展開する前に、最初に設定を消去したり元に戻すためにこれらのコマンドを使用します。これにより正常に展開されます。
- FlexConfig ポリシーからオブジェクトを削除することによって機能を削除する場合、システムはデバイスからコマンドを削除するためにこれらのコマンドを使用します。

オブジェクト本体内で CLI をネゲートまたは入れ替えるために必要なコマンドを指定しない場合、展開ではデバイス全体の構成をクリアし、オブジェクト内のコマンドだけではなく、すべてのポリシーを再展開する必要があります。これにより展開にかかる時間が長くなり、またトラフィックが中断されます。オブジェクト本体で定義されている構成を元に戻すために必要なこれらのコマンドがすべてあり、これだけであることを確認します。ネゲートコマンドは通常、テンプレートで **no** 形式または **clear** 形式のコマンドになりますが、有効だった機能を実際にオフする場合、「ネゲート」コマンドは実際には機能を有効にする正形式のコマンドになります。

ASA 構成ガイドとコマンドリファレンスを使用して、適切なコマンドを判断します。場合によっては、単一のコマンドで設定を元に戻すことができます。たとえば RIP を構成するオブ

ジェクトでは、単純な **no router rip** コマンドで、サブコマンドを含めた **router rip** 構成全体を削除します。

同様に、複数行のバナーを作成するために **banner login** コマンドをいくつか入力した場合、単一の **no banner login** コマンドでログインバナー全体をネグートします。

テンプレートで複数のネストされたオブジェクトを作成する場合、ネグートテンプレートでは逆の順番でオブジェクトを削除する必要があります（つまり、オブジェクトを削除する前にオブジェクトへの参照を最初に削除します）。たとえば、まず ACL を作成して、トラフィッククラスで ACL を参照し、ポリシーマップでトラフィッククラスを参照し、最後にサービスポリシーを使用してポリシー マップを有効にする場合、ネグートテンプレートではまずサービスポリシーを削除してからポリシーマップ、トラフィッククラス、最後に ACL の順で削除して、設定を元に戻す必要があります。

ステップ 8 [OK] をクリックします。

次のタスク

単に FlexConfig オブジェクトを作成するだけでは、それを展開するには十分ではありません。オブジェクトを FlexConfig ポリシーに追加する必要があります。FlexConfig ポリシー内のこれらのオブジェクトのみ展開されます。これにより FlexConfig オブジェクトの改善が可能になり、すべてが自動的に展開されるのではなくいくつかは特別な用途のために利用可能になります。FlexConfig ポリシーの設定 (534 ページ) を参照してください。

FlexConfig オブジェクトの変数の作成

FlexConfig オブジェクト内部で使用する変数は、オブジェクト自体の内部で定義されます。変数の個別のリストはありません。したがって、変数を定義して個別の FlexConfig オブジェクト内で使用することはできません。

変数はこれらの主な利点を提供します。

- Firepower Device Manager を使用して定義されているオブジェクトを指し示すことを可能にします。これには、ネットワーク、ポート、および秘密鍵オブジェクトが含まれます。
- これらは変更する可能性がある値をオブジェクト本体から分離します。したがって、値を変更する場合は単に変数を編集します。オブジェクト本体を編集する必要はありません。これは、いくつかのコマンドライン内のオブジェクトを参照する必要がある場合に特に便利です。

この手順では、FlexConfig オブジェクトに変数を追加するプロセスについて説明します。

手順

ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] ページから FlexConfig オブジェクトを編集または作成します。

「[FlexConfig オブジェクトの設定 \(536 ページ\)](#)」を参照してください。

ステップ 2 [変数 (Variables)] セクションで次のいずれかを実行します。

- 変数を追加するには、[+] ボタンをクリックします (またはまだ定義されていない場合は [変数の追加 (Add Variable)] をクリックします)。
- 変数を編集するには、その変数の編集アイコン (🔍) をクリックします。

変数を削除するには、その変数のごみ箱アイコン (🗑️) をクリックします。その変数への参照をテンプレート本体から削除していることを確認します。

ステップ 3 変数の名前を入力し、任意で説明を入力します。

ステップ 4 変数のデータの [タイプ (Type)] を選択し、値を入力または選択します。

次のタイプの変数を作成できます。変数を使用するコマンドのデータ要件に適合するタイプを選択します。

- [文字列 (String)] : テキスト文字列です。たとえば、ホスト名、ユーザ名など。
- [数値 (Numeric)] : 整数値です。コンマ、小数、(マイナスなどの) 記号または 16 進数表記を含めないでください。非整数の場合は文字列変数を使用します。
- [ブール値 (Boolean)] : 論理的 true/false です。True または False を選択します。
- [ネットワーク (Network)] : [オブジェクト (Objects)] ページで定義されているネットワーク オブジェクトやグループです。ネットワーク オブジェクトまたはグループを選択します。
- [ポート (Port)] : [オブジェクト (Objects)] ページで定義されている TCP または UDP ポート オブジェクトです。ポート オブジェクトを選択します。グループやその他のプロトコル用のオブジェクトは選択できません。
- [インターフェイス (Interface)] : [デバイス (Device)] > [インターフェイス (Interfaces)] のページで定義されている名前付きインターフェイスです。インターフェイスを選択します。名前を持たないインターフェイスは選択できません。
- [IP] : ネットマスクまたはプレフィックス長がない単一の IPv4 または IPv6 IP アドレスです。
- [秘密 (Secret)] : FlexConfig に定義された秘密キー オブジェクトです。オブジェクトを選択します。秘密キー オブジェクトの作成の詳細については、[秘密キー オブジェクトの設定 \(545 ページ\)](#) を参照してください。

ステップ 5 [変数 (Variable)] ダイアログ ボックスで [追加 (Add)] または [保存 (Save)] をクリックします。

これで FlexConfig オブジェクトの本体内の変数を使用できます。変数を参照する方法は、変数のタイプによって異なります。これらの変数の使用方法の詳細については、次のトピックを参照してください。

- [変数参照 : {{variable}}](#) (540 ページ)

- セクション `{{#key}} {{/key}}` と逆セクション `{{^key}} {{/key}}` (543 ページ)

ステップ 6 [FlexConfigオブジェクト (FlexConfig Object)]ダイアログボックスで[OK]をクリックします。

FlexConfig 変数の参照と値の取得

FlexConfig はテンプレート言語として Mustache を使用しますが、サポートは、次のセクションで説明する機能に限定されます。これらの機能を使用して、変数を参照し、その値を取得して、処理します。

変数参照 : `{{variable}}`

FlexConfig オブジェクト内で定義した変数を参照するには、次の表記を使用します。

```
{{variable_name}}
```

次の種類の変数を含む、単一値の変数の場合はこれで十分です：[数値 (Numeric)]、[文字列 (String)]、[ブール値 (Boolean)]、[IP]。

ただし、構成データベース内のオブジェクトとしてモデル化される要素を指し示す変数の場合は、ドット表記を使用し、取得するオブジェクト属性の名前を含める必要があります。関連するオブジェクトタイプの API エクスプローラでのモデルを調べることによって、これらの属性名を確認できます。次の種類の変数を使用するには次の標記を使用する必要があります：[秘密 (Secret)]、[ネットワーク (Network)]、[ポート (Port)]、[インターフェイス (Interface)]。

```
{{variable_name.attribute}}
```

たとえば、net-object1 (ネットワーク グループではなく、ネットワーク オブジェクトを示す) という名前のネットワーク変数のアドレスを取得するには、次を使用します。

```
{{net-object1.value}}
```

オブジェクト内のオブジェクトから属性値を取得しようとする場合は、一連のドット区切りの属性を使用して、目的の値にドリルダウンする必要があります。たとえば、インターフェイスの IP アドレスは、ipv4 と ipv6 という名前のサブオブジェクトとして、インターフェイス オブジェクトにモデル化されます。したがって、int-inside という名前の (内部インターフェイスを示す) インターフェイス変数の IPv4 アドレスとサブネット マスクを取得するには、次を使用します。

```
{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}
```



(注) API エクスプローラを開くには、ブラウザで URL の最後の部分を `/#/api-explorer` に変更します。

次の表に、変数の型とそれらを参照する方法、オブジェクトの場合は、API モデルの名前と使用する可能性が高い参照を示します。

変数の型	参照モデル	説明
ブール値 (単純変数)	変数 : <pre> {{variable_name}} </pre> セクション : <pre> {{#variable_name}} commands {{/variable_name}} </pre> 反転セクション : <pre> {{^variable_name}} commands {{/variable_name}} </pre>	論理的 true/false。ブール変数の主な目的は、セクションまたは反転セクションです。たとえば、定期的にはまたは特別な事情の下でのみ機能を有効にする必要がある場合、ブール変数の値を編集してコマンドのセクションをオンまたはオフにできます。 いくつかのオブジェクトにも、セクションのオプションの処理を提供するために使用できるそれらのモデルのブール型の属性があります。
インターフェイス (オブジェクト変数 : API モデルはインターフェイスです)	変数 : <pre> {{variable_name.attribute}} </pre> セクション : <pre> {{#variable_name.attribute}} commands {{/variable_name.attribute}} </pre> 反転セクション : <pre> {{^variable_name.attribute}} commands {{/variable_name.attribute}} </pre>	[デバイス (Device)]>[インターフェイス (Interfaces)] のページで定義されている名前付きインターフェイス。無名のインターフェイスを指定することはできません。 インターフェイス モデルで使用できるさまざまな属性があります。またインターフェイス モデルには、サブオブジェクト、たとえば IP アドレスが含まれます。 次に、役に立つ主な属性をいくつか示します。 <ul style="list-style-type: none"> • variable_name.name はインターフェイスの論理名を返します。 • variable_name.hardwareName は GigabitEthernet1/8 などのインターフェイス ポート名を返します。 • variable_name.managementOnly はブール値です。TRUE は、インターフェイスが管理限定として定義されていることを意味します。FALSE は、インターフェイスが through-the-device トラフィックであることを意味します。このオプションは、セクションキーとして使用できます。 • variable_name.ipv4.ipAddress.ipAddress はインターフェイスの IPv4 アドレスを返します。 • variable_name.ipv4.ipAddress.netmask はインターフェイスの IPv4 アドレスのサブネットマスクを返します。
IP (単純変数)	変数 : <pre> {{variable_name}} </pre>	ネットマスクまたはプレフィックス長がない単一の IPv4 または IPv6 IP アドレス。

変数の型	参照モデル	説明
ネットワーク (オブジェクト変数 : API モデルは NetworkObject です)	変数 (ネットワークオブジェクト) : <pre> {{variable_name.attribute}} </pre> セクション (グループオブジェクト) : <pre> {{#variable_name.objects}} commands referring to one of {{value}} {{name}} {{/variable_name.objects}} </pre>	<p>[オブジェクト (Objects)] ページで定義されているネットワーク オブジェクトやグループです。セクションを使用してネットワーク グループを処理できます。</p> <p>次に、役に立つ主な属性を示します。</p> <ul style="list-style-type: none"> • <code>{{variable_name.name}}</code> はネットワーク オブジェクトまたはグループの名前を返します。 • <code>{{variable_name.value}}</code> はネットワーク オブジェクト (ネットワーク グループではありません) の IP アドレスの内容を返します。ネットワーク オブジェクトの持つ内容のタイプが指定されたコマンドに対して正しいことを確認します。たとえば、サブネットアドレスではなくホストアドレスです。 • <code>{{variable_name.groups}}</code> はネットワーク グループに含まれるネットワーク オブジェクトのリストを返します。これはネットワーク グループを指す変数でのみ使用します。またグループの内容を繰り返し処理するセクションタグに使用します。 <code>{{value}}</code> または <code>{{name}}</code> のいずれかを使用して、次に各ネットワークオブジェクトの内容を取得します。
数値 (単純変数)	変数 : <pre> {{variable_name}} </pre>	<p>整数値。コンマ、小数、(マイナスなどの) 記号または 16 進数表記を含めないでください。非整数の場合は文字列変数を使用します。</p>
ポート (オブジェクト変数 : API モデルは、PortObject、tcpports または udpports です)	変数 : <pre> {{variable_name.attribute}} </pre>	<p>[オブジェクト (Objects)] ページで定義されている TCP または UDP ポートオブジェクトです。これは、ポートグループではなく、ポート オブジェクトである必要があります。</p> <p>次に、役に立つ主な属性を示します。</p> <ul style="list-style-type: none"> • <code>{{variable_name.port}}</code> はポート番号を返します。プロトコルは含まれません。 • <code>{{variable_name.name}}</code> はポートオブジェクトの名前を返します。
秘密 (オブジェクト変数 : API モデルは Secret です)	変数 : <pre> {{variable_name.password}} </pre>	<p>FlexConfig に定義された秘密キー オブジェクトです。</p> <p>作成する必要がある唯一の参照は、暗号化された文字列を返す <code>password</code> 属性です。</p>

変数の型	参照モデル	説明
文字列 (単純変数)	変数： <code>{{variable_name}}</code>	テキスト文字列です。たとえば、ホスト名、ユーザ名など。

セクション `{{#key}}{/key}}` と逆セクション `{{^key}}{/key}}`

セクションまたは逆セクションは、セクションの開始タグと終了タグの間のコマンドのブロックで、処理条件としてキーを使用します。セクションの処理方法は、それが通常か逆セクションかによって異なります。

- 通常のセクション（または単にセクション）は、キーが **TRUE** であるか、または空でないコンテンツを含む場合に処理されます。キーが **FALSE** であるか、またはオブジェクトにコンテンツがない場合、セクション内のコマンドは設定されません。セクションはバイパスされます。

次に、通常のセクションの構文を示します。

```
{{#key}}
one or more commands
{/key}}
```

- 逆セクションは、セクションの反対です。キーが **FALSE** であるか、またはオブジェクトにコンテンツがない場合に処理されます。キーが **TRUE** であるか、またはオブジェクトにコンテンツがある場合、逆セクションはバイパスされます。

次に、逆セクションの構文を示します。唯一の違いは、キャレットがハッシュタグを置き換えることです。

```
{{^key}}
one or more commands
{/key}}
```

次のトピックで、セクションおよび逆セクションの主な用途について説明します。

複数値の変数を処理する方法

複数値の変数の処理の主な例は、ネットワークグループを指すネットワーク変数です。グループに複数のオブジェクトが含まれている (**objects** 属性の下) ので、ネットワークグループ内の値を繰り返し実行し、異なる値を使用して複数回同じコマンドを設定できます。

たとえば、ホスト 192.168.30.0、192.168.20.0、192.168.10.0 を含む **net-group** という名前のネットワークグループがある場合は、次の方法を使用して、RIP ルーティング用の各アドレスにネットワークコマンドを設定できます。ネットワークオブジェクトの **value** 属性を単独で使用し、**net-group.objects.value** 全体の参照を指定しないことに注意してください。セクションの開始で **net-group.objects** を使用することは、この使用を意味するからです (FlexConfig オブジェクト内の「value」属性に個別の変数を作成しないでください)。

```
router rip
{{#net-group.objects}}
  network {{value}}
{{/net-group.objects}}
```

システムはセクションの構造を次のように変換します。

```
router rip
  network 192.168.10.0
  network 192.168.20.0
  network 192.168.30.0
```

ブール値または空のオブジェクトに基づいて省略可能な処理を実行する方法

セクションの開始タグ内の変数のコンテンツがTRUEの場合、またはオブジェクトが空でない場合、セクションは処理されます。ブール値がFALSEまたは空（空のオブジェクトなど）のセクションは省略されます。

ここでの主な用途はブール値用です。たとえば、ブール変数を作成し、変数の対象であるセクション内にコマンドを置きます。その後、FlexConfig オブジェクト内のコマンドのセクションを有効または無効にする必要がある場合、ブール変数の値を変更する必要があるだけで、これらの行をコードから削除する必要はありません。これにより、簡単に、機能を有効または無効にできます。

たとえば、SNMP を有効にする FlexConfig を使用する場合、SNMP トラップをオフにできません。enable-traps という名前のブール変数を作成し、最初はTRUEに設定します。次に、トラップをオフにする場合、変数を編集してFALSEに変更し、オブジェクトを保存して、設定を再展開するだけです。コマンドシーケンスは次のようになります。

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

オブジェクト内のブール値に基づいてこのタイプの処理を行うこともできます。たとえば、ここでいくつかの特性を設定する前に、インターフェイスが管理専用かどうかをチェックできます。次の例で、int-inside はinside という名前のインターフェイスを指すインターフェイス変数です。インターフェイスが管理専用設定されていない場合にのみ、FlexConfig はそのインターフェイスでEIGRP 関連のインターフェイス オプションを設定します。ブール値がFALSEの場合にのみコマンドが設定されるように、逆セクションを使用します。

```
router eigrp 2
  network 192.168.1.0 255.255.255.0
  {{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
  hello interval eigrp 2 60
  delay 200
  {{/int-inside.managementOnly}}
```

秘密キー オブジェクトの設定

秘密キー オブジェクトのポイントは、パスワードや機密性の高い文字列を隠すことです。FlexConfig オブジェクトまたは Smart CLI テンプレートで使用される文字列を誰かに見られるリスクを避けたい場合は、文字列の秘密キー オブジェクトを作成します。

手順

-
- ステップ 1** [オブジェクト (Objects)] を選択し、コンテンツ テーブルから [秘密キー (Secret Keys)] を選択します。
- ステップ 2** 次のいずれかを実行します。
- オブジェクトを作成するには、[+] ボタンをクリックします。
 - オブジェクトを編集するには、オブジェクトの編集アイコン (🔍) をクリックします。
- 参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン (🗑️) をクリックします。
- ステップ 3** オブジェクトの名前、さらにオプションで説明を入力します。
- ステップ 4** [パスワード (Password)] と [パスワードの確認 (Confirm Password)] フィールドの両方にパスワードまたはその他秘密の文字列を入力します。
- 入力すると、システムがテキストを隠します。
- ステップ 5** [OK] をクリックします。
-

次のタスク

- 新しいオブジェクトの場合は、FlexConfig でそれを使用するために、FlexConfig オブジェクトを編集し、秘密キーの型の変数を作成してオブジェクトを選択します。その後、オブジェクト本体内で変数を参照します。詳細については、[FlexConfig オブジェクトの変数の作成 \(538 ページ\)](#) を参照してください。
- FlexConfig ポリシーの一部である FlexConfig オブジェクトで使用されている既存のオブジェクトを編集する場合は、新しい文字列でデバイスを更新するために構成を展開する必要があります。
- Smart CLI テンプレートでは、コマンドに秘密キーが必要な場合、関連するプロパティを編集するときにこれらのオブジェクトの一覧が表示されます。目的にあわせて適切なキーを選択します。

FlexConfig ポリシーのトラブルシューティング

FlexConfig ポリシーを編集した後は、次の展開の結果を慎重に調べてください。「展開は失敗しました (Deployment has failed)」というメッセージを受信した場合は、[展開サマリー (Deployment Summary)] ダイアログ ボックスの [ステータス (Status)] 列を確認してください。失敗したジョブのステータスには、[詳細の表示 (See Details)] リンクが含まれています。

展開が FlexConfig の問題のため失敗した場合、詳細には不正なコマンドを含む FlexConfig オブジェクトについて記述され、失敗したコマンドが表示されます。この情報を使用して、オブジェクトを修正し、もう一度展開を試みてください。オブジェクト名はリンクであり、クリックしてオブジェクトの編集のダイアログを開きます。

たとえば、最大 TCP セグメント サイズ (TCP MSS) を設定できます。 `sysopt connection tcpmss` コマンドを使用して、この設定を制御できます。Firepower Device Manager により設定する場合、このオプションに対する Firepower Threat Defense のデフォルトは 0 で、ASA のデフォルトは 1380 です。

MTU のデフォルトの 1500 を使用するインターフェイスで IPv4 VPN を実行している場合、ASA のデフォルトは処理を最適化するように設計されています。システムでは、VPN のヘッダーに 120 バイトが必要です。IPv6 の場合、システムでは 140 バイト必要です。Firepower Threat Defense のデフォルトの 0 では、エンドポイントによる MSS のネゴシエートが許可されるだけで、これは通常のトラフィック、特にデバイス上のインターフェイス間で、1500 以上の MTU を含む、異なる MTU を使用する場合には理想的な設定です。TCP の MSS はグローバル設定であり、インターフェイスごとに設定されないため、トラフィックのかなりの割合が VPN を介すものであり、過剰に断片化している場合のみ変更します。その場合は、TCP の MSS を MTU マイナス 120 (IPv4 用) または 140 (IPv6 用) に設定し、すべてのインターフェイスに同じ MTU を使用します。

この図では、TCP の MSS を 3 バイトに設定するとします。コマンドは最小値として 48 バイトを取るため、次のような展開エラーが発生します。

- "Template" field of `sysopt-connection-tcpmss` caused an error. ERROR: [3] is smaller than minimum allowed MSS of 48 by RFC 791 Usage: [no] `sysopt connection { permit-vpn | reclassify-vpn | preserve-vpn-flows | timewait | {tcpmss [minimum] [bytes]} [no] sysopt noproxyarp [if-name] [no] sysopt nodnsalias { inbound | outbound } [no] sysopt radius ignore-secret [no] sysopt traffic detailed-statistics [no] sysopt uauth allow-http-cache [DEPRECATED] show running-config [all] sysopt clear configure sysopt`

```
1 sysopt connection tcpmss 3
```

エラーは、これらの要素で構成されます。

1. エラーが発生した FlexConfig オブジェクトの名前が含まれている展開エラーメッセージ。オブジェクト名は編集ダイアログボックスにリンクされているので、オブジェクトを開いてすぐにエラーを修正できます。これはメッセージの最初の文です。
2. 「ERROR:」から始まるテキストがデバイスから返されるメッセージです。これは SSH クライアントの書式なしで、誤ったコマンドで入力した場合の、ASA の正確な応答内容です。この例では、エラーメッセージは「エラー: [3] は RFC 791 で許可されている MSS の最小値 48 よりも小さいです。(ERROR: [3] is smaller than the minimum allowed MSS of 48

by RFC 791.)」です。「Usage:」の後の情報は追加情報であり、実際に CLI を使用しているユーザを支援するもので、無視できます。SSH を使用する ASA を使用していた場合、インタラクションは次のようになります。

```
asa3(config)# sysopt connection tcpmss 3
ERROR: <3> is smaller than minimum allowed MSS of 48 by RFC 791
Usage:
  [no] sysopt connection { permit-vpn | reclassify-vpn | preserve-vpn-flows |
                        timewait | {tcpmss [minimum] <bytes>}
  [no] sysopt noproxyarp <if-name>
  [no] sysopt nodnsalias { inbound | outbound }
  [no] sysopt radius ignore-secret
  [no] sysopt traffic detailed-statistics
  [no] sysopt uauth allow-http-cache [DEPRECATED]
  show running-config [all] sysopt
  clear configure sysopt
```

3. 黒のテキストは、エラーを引き起こした FlexConfig オブジェクトからの実際の行です。この行を修正する必要があります。この例では、MTU 1500 インターフェイス（共通の状態）上の IPv4 VPN トラフィックに対応しようとする場合、3 を 1380 に変更します。

この例を修正する場合、CLI コンソールを開いたままにし、**show running-config all sysopt** を使用して、**sysopt** コマンドのすべての設定を確認できます。ほとんどの **sysopt** コマンドにはほとんどの用途に適したデフォルトの設定があり、実行中の設定には表示されません。**all** キーワードでは、出力にこれらのデフォルト設定が含まれます。

FlexConfig の例

ここでは、FlexConfig を使用して機能を設定するいくつかの例を示します。

グローバル デフォルト インスペクションを有効/無効にする方法

一部のプロトコルでは、IP アドレッシング情報がユーザ データ パケットに埋め込まれるか、動的に割り当てられたポートにセカンダリ チャネルが開かれます。そのようなプロトコルの場合、システムはディープ パケット インスペクションを実行し、NAT を適用して、セカンダリ チャネルを許可できるようにする必要があります。いくつかの一般的なインスペクションエンジンはデフォルトで有効になっていますが、ネットワークによっては、他のインスペクションエンジンを有効化したり、デフォルトのインスペクションを無効化したりする必要があります。

現在有効になっているインスペクションの一覧を表示するには、CLI コンソールまたは SSH セッションで **show running-config policy-map** コマンドを使用します。以下の出力は、インスペクションの設定に変更が加えられていないシステムで表示される内容です。この出力では、出力の最後にある **inspect** コマンドの一覧に有効になっているプロトコルインスペクションが表示されています。先行するコマンドにより、**inspection_default** トラフィック クラスでこれらのインスペクションが有効になります（通常のプロトコル、該当する場合はインスペクション 済みプロトコルのポート番号）。このクラスは **global_policy** ポリシー マップの一部で、

`service-policy` コマンド（出力には未表示）を使用して、すべてのインターフェイスに対するインスペクションに適用されます。たとえば、ICMP インスペクションは、デバイスを通過するすべての ICMP トラフィックに対して行われます。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
  no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
    inspect icmp error
!
```



(注) 各インスペクションの詳細については、<https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html> で入手可能な『Cisco ASA Series Firewall Configuration Guide』を参照してください。

次の手順では、このグローバルに適用されるデフォルトインスペクションクラスのインスペクションを有効化または無効化する方法を示します。説明のための例：

- PPTP (Point-to-Point Tunneling Protocol) を有効にします。このプロトコルは、エンドポイント間のポイントツーポイント接続のトンネリングに使用されます。
- SIP (Session Initiation Protocol) を無効にします。通常は、インスペクションによってネットワークに問題が発生している場合にのみ SIP を無効化します。SIP を無効化する場合は、アクセスコントロールポリシーで SIP トラフィック (UDP/TCP 5060) と動的に割り当てられるポートが許可されていること、SIP 接続に NAT のサポートが必要ないことを確認します。アクセスコントロールポリシーと NAT ポリシーを、FlexConfig ではなく、標準のページを使用して適宜調整します。

始める前に

適切な計画を立てることで FlexConfig を効率的に使用できます。この例では、同じトラフィッククラスに変更を加えていますが、2つの異なる関連性のないインスペクションを変更してい

ます。ただし、それらのポリシーを変更する必要がある場合（可能性は高い）は、個別に変更します。

そのため、この例のインスペクションごとに個別の FlexConfig オブジェクトを作成することをお勧めします。そうすることで、他のインスペクションを変更することなく、1つのインスペクションの設定を簡単に変更でき、FlexConfig オブジェクトを編集する必要もありません。

手順

- ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。
- ステップ 2 詳細設定の目次で [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Objects)] をクリックします。
- ステップ 3 PPTP インスペクションを有効にするオブジェクトを作成します。
 - a) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。
 - b) オブジェクトの名前を入力します。例、**Enable_PPTP_Global_Inspection**。
 - c) [テンプレート (Template)] エディタで、インデントを含む次の行を入力します。

```
policy-map global_policy
  class inspection_default
    inspect pptp
```

- d) [ネゲートテンプレート (Negate Template)] エディタで、この設定を元に戻すために必要な行を入力します。

適切なサブモードでコマンドを有効にするために、ネゲートテンプレートに、親コマンドと同様にこれらのコマンドも含める必要があります。

FlexConfig ポリシーからこのオブジェクトを削除した場合（正常に導入された後）、および導入が失敗した場合でも（設定を前の状態にリセットするため）、ネゲートテンプレートが適用されます。

したがって、この例では、ネゲートテンプレートは次のようになります。

```
policy-map global_policy
  class inspection_default
    no inspect pptp
```

オブジェクトは次のようになります。

Name

Enable_PPTP_Global_Inspection

Description

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

```
1 policy-map global_policy
2   class inspection_default
3     inspect pptp
```

Negate Template 

```
1 policy-map global_policy
2   class inspection_default
3     no inspect pptp
```

(注) `inspection_default` クラスには有効になっているその他のインスペクションコマンドがあるため、クラス全体を無効にはしたくありません。同様に、`global_policy` ポリシーマップにはその他のインスペクションが含まれているため、ポリシーマップも無効にはしたくありません。

- e) [OK] をクリックしてオブジェクトを保存します。

ステップ 4 SIP 検査を無効にするオブジェクトを作成します。

- 新しいオブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトの名前を入力します。例、**Disable_SIP_Global_Inspection**。
- [テンプレート (Template)] エディタで、インデントを含む次の行を入力します。

```
policy-map global_policy
  class inspection_default
    no inspect sip
```

- d) [ネゲートテンプレート (Negate Template)] エディタで、この設定を元に戻すために必要な行を入力します。

「no」コマンドを無効化するための「negate」コマンドは、機能を有効化するコマンドです。そのため、「ネゲート」テンプレートは機能を無効化するためのコマンドではな

く、「ポジティブ」テンプレートでの操作を元に戻すためのコマンドです。ネゲートテンプレートの要点は、変更を元に戻す点にあります。

したがって、この例では、ネゲートテンプレートは次のようになります。

```
policy-map global_policy
  class inspection_default
    inspect sip
```

オブジェクトは次のようになります。

Name

Disable_SIP_Global_Inspection

Description

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

```
1 policy-map global_policy
2   class inspection_default
3     no inspect sip
```

Negate Template

```
1 policy-map global_policy
2   class inspection_default
3     inspect sip
```

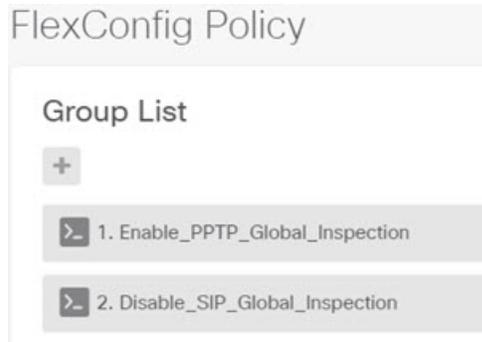
e) [OK] をクリックしてオブジェクトを保存します。

ステップ 5 オブジェクトを FlexConfig ポリシーに追加します。

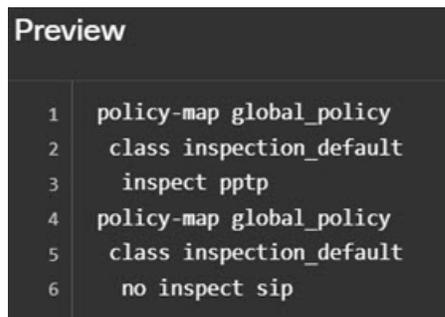
オブジェクトを作成するだけでは不十分です。オブジェクトは、FlexConfig ポリシーに追加（および変更を保存）した場合にのみ展開されます。これにより、未終了の作業で展開が失敗するリスクを犯すことなく、オブジェクトを試す（および部分的に完了した状態で残す）ことができます。その後、オブジェクトを追加および削除することで、機能を簡単にオン/オフできます。オブジェクトを毎回再作成する必要はありません。

- 目次で [FlexConfig ポリシー (FlexConfig Policy)] をクリックします。
- [グループリスト (Group List)] で [+] をクリックします。

- c) `Enable_PPTP_Global_Inspection` オブジェクトと `Disable_SIP_Global_Inspection` オブジェクトを選択して、[OK] をクリックします。
グループリストは次のようになります。



プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。



- d) [保存 (Save)] をクリックします。
これでポリシーを展開できます。

ステップ 6 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

ステップ 7 CLI コンソールまたは SSH セッションで、`show running-config policy-map` コマンドを使用し、実行コンフィギュレーションが正しく変更されているか確認します。

次の出力では、`inspect pptp` が `inspection_default` クラスの最後に追加されていて、`inspect sip` はクラスに含まれていないことに注意してください。これにより、FlexConfig オブジェクトで定義された変更が正常に導入されたことが確認されます

```
> show running-config policy-map
!  
policy-map type inspect dns preset_dns_map  
  parameters  
    message-length maximum client auto  
    message-length maximum 512  
    no tcp-inspection  
policy-map global_policy  
  class inspection_default  
    inspect dns preset_dns_map  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect rsh  
    inspect rtsp  
    inspect sqlnet  
    inspect skinny  
    inspect sunrpc  
    inspect xdmcp  
    inspect netbios  
    inspect tftp  
    inspect ip-options  
    inspect icmp  
    inspect icmp error  
    inspect pptp  
!
```

FlexConfig の変更を元に戻す方法

FlexConfig オブジェクトに正しいネゲートテンプレートをを入力すると、そのオブジェクトを使用して行った変更の削除が容易になります。FlexConfig ポリシーから単純にオブジェクトを削除すると、次の展開時に、システムがネゲートテンプレートを使用して変更を元に戻します。

変更を元に戻すために新しいオブジェクトを作成する必要はありません。

次の例は、グローバルな SIP 検査を再度有効にする方法を示しています。この例では、SIP 検査を無効化している [グローバルデフォルトインスペクションを有効/無効にする方法 \(547 ページ\)](#) で説明した変更を元に戻しています。

始める前に

FlexConfig オブジェクトにネゲートテンプレートが正しく設定されていることを確認します。正しくない場合は、オブジェクトを編集してネゲートテンプレートを修正します。

手順

- ステップ 1** [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。
- ステップ 2** 詳細設定の目次で [FlexConfig] > [FlexConfig ポリシー (FlexConfig Policy)] をクリックします。

ステップ 3 FlexConfig ポリシーの **Disable_SIP_Global_Inspection** オブジェクトのエントリの右側にある [X] をクリックして、ポリシーから削除します。



オブジェクトのコマンドは、プレビューから削除されます。negate コマンドはプレビューには追加されず、バックグラウンドで実行されます。

ステップ 4 [保存 (Save)] をクリックします。

ステップ 5 変更を保存します。

a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

ステップ 6 CLI コンソールまたは SSH セッションで、**show running-config policy-map** コマンドを使用し、実行コンフィギュレーションが正しく変更されているか確認します。

次の出力では、**inspect sip** が **inspection_default** クラスの一番下に追加されていることに注意してください。これにより、FlexConfig オブジェクトで定義された変更が正常に導入されたことが確認されます（このクラスでは順序は重要ではないため、**inspect sip** が最後にあり、元の場所になくても問題ありません）。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
    inspect icmp error
    inspect pptp
    inspect sip
```

!

一意のトラフィック クラスのインスペクションを有効にする方法

この例では、特定のインターフェイスの2つのエンドポイント間でトラフィックの PPTP インスペクションを有効にします。これは、エンドポイント間にポイントツーポイントトンネルが設定されているエンドポイントのインスペクションだけをターゲットにします。

2つのエンドポイント間で PPTP インスペクションを有効にするために必要な CLI には、以下の内容が含まれます。

1. 送信元と宛先がエンドポイントのホストの IP アドレスに設定されている ACL。
2. この ACL を参照するトラフィック クラス。
3. トラフィック クラスを含み、そのトラフィック クラスでの PPTP インスペクションを有効にするポリシー マップ。
4. 目的のインターフェイスにポリシー マップを適用するサービス ポリシー。これは、実際にポリシーをアクティブにして、インスペクションを有効にする手順です。



- (注) インスペクション関連のサービス ポリシーの詳細については、<https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html> で入手可能な『Cisco ASA Series Firewall Configuration Guide』を参照してください。

手順

- ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。
- ステップ 2 詳細設定の目次で [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Objects)] をクリックします。
- ステップ 3 新しいオブジェクトを作成するには、[+] ボタンをクリックします。
- ステップ 4 オブジェクトの名前を入力します。例、[Enable_PPTP_Inspection_on_Interface]。
- ステップ 5 内部インターフェイスの変数を追加します。
 - a) [変数 (Variables)] リストの上にある [+] をクリックします。
 - b) 変数の名前、[pptp-if] などを入力します。
 - c) [種類 (Type)] で [インターフェイス (Interface)] を選択します。
 - d) [値 (Value)] で [内部 (inside)] インターフェイスを選択します。

ダイアログボックスは次のようになります。

Add New Variable

Name

pptp-if

Description

Type

Interface

Value

inside

e) [追加 (Add)] をクリックします。

ステップ 6 [テンプレート (Template)] エディタで、インデントを含む次の行を入力します。

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
  match access-list MATCH_ACL
policy-map PPTP_POLICY
  class MATCH_CMAP
    inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

変数を使用するには、二重ブレースの間に変数名を入力する点に注意してください。また、インターフェイスを定義するオブジェクトには多数の属性が設定されているため、取得する属性を選択するにはドット表記法を使用する必要があります。インターフェイス名は「name」属性に保持されるため、`{{pptp-if.name}}`を入力すると、変数に割り当てられているインターフェイスのname属性の値が取得されます。PPTP インспекションのインターフェイスを変更する必要がある場合は、変数定義で単純に別のインターフェイスを選択する必要があります。

ステップ 7 [ネゲートテンプレート (Negate Template)] エディタで、この設定を元に戻すために必要な行を入力します。

この例では、クラス マップ、ポリシー マップ、およびサービス ポリシーは、PPTP インспекションを適用するためにのみ存在していると仮定しています。したがって、ネゲートテンプレートでこれらをすべて削除します。

ただし、インターフェイスの既存のサービス ポリシーに PPTP インспекションを実際に追加する場合は、ポリシー マップやサービス ポリシーを無効にはしません。ポリシー マップからクラスを無効にするか、またはポリシー マップ内のクラス内でインспекションを単純にオフにします。ネゲートテンプレートで予期せぬ結果が生じないようにするには、その他の FlexConfig オブジェクトに実装している内容について明確に把握する必要があります。

ネストされた項目を削除する場合は、作成順とは逆の順番で削除する必要があります。したがって、最初にサービス ポリシーを削除して、最後にアクセス リストを削除します。そうし

ないと、使用中のオブジェクトを削除しようとして、システムからエラーが返され、削除できなくなります。

```
no service-policy PPTP_POLICY interface {{pttp-if.name}}
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

オブジェクトは次のようになります。

Name

Enable_PPTP_Inspection_on_Interface

Description

Variables +

NAME	TYPE	VALUE	DESCRIPTION	ACTIONS
pptp-if	Interface	 inside		

Template ↕ Expand | ↻ Reset

```
1 access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
2 class-map MATCH_CMAP
3 match access-list MATCH_ACL
4 policy-map PPTP_POLICY
5 class MATCH_CMAP
6 inspect pptp
7 service-policy PPTP_POLICY interface {{pttp-if.name}}
```

Negate Template ⚠ ↕ Expand | ↻ Reset

```
1 no service-policy PPTP_POLICY interface {{pttp-if.name}}
2 no policy-map PPTP_POLICY
3 no class-map MATCH_CMAP
4 no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ステップ 9 オブジェクトを FlexConfig ポリシーに追加します。

- 目次で [FlexConfigポリシー (FlexConfig Policy)] をクリックします。
- [グループリスト (Group List)] で [+] をクリックします。
- [Enable_PPTP_Inspection_on_Interface] オブジェクトを選択し、[OK] をクリックします。

グループリストは次のようになります。

FlexConfig Policy

Group List

+ Drag and drop to reorder

> 1. Enable_PPTP_Inspection_on_Interface

プレビューはテンプレートのコマンドで更新されます。次の図に示されているように、予想していたコマンドが表示されていることを確認します。プレビューでは、インターフェイス変数は名前「inside」に解決されることに注意してください。変数には特に注意してください。プレビューで正しく解決されていない場合、変数は正確に展開されません。プレビューで変数が正しく変換されるまで、FlexConfig オブジェクトを編集します。

```

Preview ↔ Expand
1 access-list MATCH_ACL permit ip host 192.168.1.55 host
  198.51.100.1
2 class-map MATCH_CMAP
3   match access-list MATCH_ACL
4 policy-map PPTP_POLICY
5   class MATCH_CMAP
6     inspect pptp
7 service-policy PPTP_POLICY interface inside
8

```

d) [保存 (Save)] をクリックします。

これでポリシーを展開できます。

ステップ 10 変更を保存します。

a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

ステップ 11 CLI コンソールまたは SSH セッションで **show running-config** コマンドのバリエーションを使用して、実行コンフィギュレーションに正しい変更が含まれていることを確認します。

show running-config を入力して CLI の設定全体を検査したり、以下のコマンドを使用して、この設定の各部分を確認したりできます。

- **show running-config access-list MATCH_ACL** show running-config access-list MATCH_ACL (ACL の確認用)。
- **show running-config class** show running-config class (クラス マップの確認用)。すべてのクラス マップが表示されます。
- **show running-config policy-map PPTP_POLICY** show running-config policy-map PPTP_POLICY (クラスおよびポリシー マップ設定の確認用)。
- **show running-config service-policy** show running-config service-policy (インターフェイスに適用されているポリシーマップの確認用)。すべてのサービス ポリシーが表示されます。

次の出力には、この一連のコマンドが表示されており、設定が正しく適用されていることを確認できます。

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
  match access-list MATCH_ACL
class-map inspection_default
  match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
  class MATCH_CMAP
    inspect pptp
!

> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```
